CYBER AND PRIVACY LIABILITY EXPOSURES AND HOW TO INSURE THEM

Published by WebCE, Inc.

(877)-488-9308

www.webce.com • customerservice@webce.com

IRMI®
International Risk Management Institute, Inc.®
12222 Merit Drive, Suite 1600
Dallas, TX 75251-2266
(972) 960-7693
Fax (972) 371-5120
www.IRMI.com

Cyber and Privacy Liability Exposures and How to Insure Them
Contents

Introduction

This course has two major objectives.

The first objective of the course is to provide an overview of the kinds of situations that can give rise to both property and liability losses when a business engages in various cyber activities. More specifically, companies that use email, operate a website, take orders online (and collect customer data in the process), participate in social media activities, or engage the services of a cloud provider (just to name a few examples) are exposed to significant potential first-party property and third-party liability claims. The first half of the course—Chapters 2 through 12—examines these exposures in depth.

The second objective of this course is to offer a detailed look at the kinds of policy forms that have been designed to cover these exposures. Thus, the second half of the course—Chapters 8 through 13—begins by analyzing the policies' insuring agreements and continues by discussing other key provisions, such as insured persons, insured organizations, defense/settlement, coverage limits, and retentions. This second section of the course concludes by examining the most common exclusions found within cyber and privacy policy forms, focusing on the manner in which such wordings vary from insurer-to-insurer, and explaining how these variations exert significant impact on the scope of coverage that cyber and privacy policies provide.

A Glossary following the final chapter defines key terms and concepts used in this course.

Course Objectives

On completion of this course, you should be able to do the following.

- Recognize key areas of confusion inherent in cyber and privacy coverage, beginning with the fact that it is referred to under different names by different insurers.
- Identify the major types of third-party liability losses that result from cyber activities: (1) information security liability, (2) privacy liability, and (3) content liability.
- Recognize the major types of first-party property losses that result from cyber and online activities: (1) business interruption, (2) dependent business interruption, (3) extra expense, (4) data asset loss, (5) cyber extortion, (6) computer fraud, (7) funds transfer fraud, and (8) miscellaneous crime losses.
- Recognize how social media and cloud computing create many of the property and liability exposures noted above.
- Identify various loss control measures that can be applied to eliminate, or at least reduce, the extent to which a business can be financially impacted by these loss exposures.
- Recognize how cyber and privacy insurance is rated by insurers and identify the key factors that underwriters consider in pricing the coverage.

- Recognize the effect of the key first-party property and third-party liability insuring agreements found within the policies.
- Recognize how the following types of provisions operate within a cyber and privacy policy: (1) insured persons/organizations, (2) defense/settlement, (3) limits, and (4) retentions.
- Identify the most important exclusions found within cyber and privacy forms, recognize how different insurers' versions of these same exclusions vary, and recognize how such differences impact the scope of coverage the policies provide.

Chapter 1
Demystifying Cyber and Privacy Loss Exposures and Insurance Coverage

Overview

The purpose of this chapter is to introduce cyber and privacy insurance coverage and to clarify an often confusing coverage. In light of the fact that what we may call "traditional" insurance (e.g., general liability, property, and so on) continues to distance itself from offering coverage for cyber-related exposures, it is all the more important for purchasers and providers of cyber and privacy insurance to understand its nuances and distinctions from so-called traditional insurance.

Chapter Objectives

On completion of this chapter, you should be able to do the following.

- Recognize various names by which cyber and privacy insurance is referred to.
- Differentiate between cyber and privacy insurance and technology errors and omissions (E&O) insurance.
- Identify the basic types of property and liability exposures covered by cyber and privacy insurance policies.
- Recognize the decisions that purchasers of cyber and privacy insurance policies must make when selecting insuring agreements, limits, and retentions.
- Recognize some of the important overlaps in coverage between cyber and privacy policies and the following types of insurance: commercial general liability (CGL), property insurance, and media liability insurance.
- Identify several unusual coverage elements found within cyber and privacy insurance policies.

Confusing Aspects of Cyber and Privacy Insurance

Virtually no organizations are immune to the risks associated with the Internet and electronic commerce. Nearly all businesses—regardless of industry or size—now, at a minimum, have access to the Internet, operate an internal email system, and maintain their own websites. In addition, a vast amount of businesses are also in a position to solicit and process orders for their products using "e-commerce." Moreover, such firms are also engaging in social media and cloud computing. In combination, these diverse types of cyber activities give rise to a variety of liability and property loss exposures, along with the need for insurance policies that cover these exposures.

There are at least 10 reasons why cyber and privacy insurance is considered one of the more confusing, if not outright mystifying, lines of coverage available in today's market.

Exhibit 1.1
Confusing Aspects of Cyber and Privacy Insurance Coverage

- The coverage is referred to by various names.
- It is often confused with technology E&O coverage.
- Both cyber and privacy *and* technology E&O policies cover many of the same risks.
- Both property *and* liability exposures are covered under cyber and privacy insurance.
- The nature of the coverage varies considerably from insurer to insurer.
- The menu-driven nature of the policies creates special problems.
- The cyber and privacy exposure is rapidly evolving.
- Cyber and privacy policies are also rapidly evolving.
- Cyber and privacy coverage aspects overlap with commercial general liability (CGL), professional, and media liability policies.
- Cyber and privacy forms contain a number of idiosyncrasies.

Policies Go by Various Names

Any time a line of insurance is referred to by a wide variety of names or terms, it is an invitation to misunderstanding. More specifically, here are some examples of the titles of various cyber and privacy policies offered by a number of leading insurers. Furthermore, it is not uncommon for one insurance company to have numerous cyber and privacy policy forms, each named differently.

- Information Security and Privacy Insurance
- CyberRisk
- Security and Privacy Protection
- CyberSecurity
- Enterprise Professional Solutions

Such terminology notwithstanding, each of these policies—with some variations, of course—covers the following.

- Data breaches and attendant post-breach costs
- Costs necessary to prevent future breaches
- Fines and penalties levied by state regulators
- Public relations costs following a breach
- Liability for denial of service from or access to electronic data
- Loss of or damage to such data
- Content-related claims pertaining to this data
- Various property losses arising from cyber-related damage to or corruption of data
- Time element losses arising from these events

For the purposes of this course, we will use the term cyber and privacy insurance to discuss and analyze the various policies that cover the aforementioned types of exposures.

Confusion with Technology E&O Coverage

Cyber and privacy insurance is often confused with technology E&O insurance coverage. Although the terms "cyber and privacy insurance" and "technology errors and omissions insurance" are sometimes used interchangeably, there is indeed a clear distinction between the types of risks that each of these two types of policies seeks to address.

In a nutshell, technology E&O coverage is intended to cover *providers* of technology services and products. In contrast, cyber and privacy coverage is intended for *users* of technology services and products, encompassing a much broader range of business types.

Technology E&O: Coverage for Providers of Technology Services and Products

Two types of businesses require technology E&O insurance—providers of technology services and providers of technology products.

Providers of Technology Services

Data storage companies that store customer data on an offsite basis and businesses that offer website design, maintenance, and hosting services for a fee are examples of firms that are in the business of providing *technology services*. For example, companies like this could face (and *have* faced) errors and omissions liability for failing to properly secure a website that they design, ultimately leading to the site being compromised.

Providers of Technology Products

Computer software manufacturers (such as those that write various types of applications and programs) and computer manufacturers (that actually make computer hardware) are examples of companies that provide *technology products.* Manufacturing insecure or faulty products could lead to errors and omissions liability for these technology companies.

Cyber and Privacy Coverage: Coverage for Users of Technology Services and Products

Conversely, firms that use technology products and services in their business require cyber and privacy coverage. Although such services and products are an integral part of their businesses, they do not make money *selling* those services or products to customers. Rather, they merely *use* technology products to do so.

Examples

Banks are obvious users (although they can certainly also be providers in various ways) of technology services since the vast majority of transactions are recorded electronically. Similarly, any company that takes orders over the Internet must avail itself of technology services and products. Healthcare institutions and law firms also regularly use electronic records to track sensitive and critical patient and client

information. Lastly, publishing companies that provide online content are also users of technology services and products.

These are just a few examples of exposures applicable to cyber and privacy coverage. In reality, essentially every type of organization faces this risk now.

Both Cyber and Privacy Policies and Technology E&O Policies Cover Many of the Same Risks

Adding to the confusion between cyber and privacy insurance and technology E&O insurance is that *both* types of policies *may* cover many of the *same* exposures. Specifically, both cyber and privacy and technology E&O policies may have some degree of coverage for liability arising out of a breach of customer data (also known as personally identifiable information, or "PII").

Coverage of Property and Liability Exposures under the Same Policy Form

Adding to the enigmatic nature of cyber and privacy insurance is the fact that some policies cover *both* property *and* liability exposures. In contrast, commercial insurance policies almost always cover either property or liability exposures, but generally not both. (Businessowners policies, which cover both, are one of the few exceptions.)

Therefore, unlike nearly every other type of professional and E&O policy form, cyber and privacy policies *also* may include coverage of items such as business interruption, loss of data, and loss of money, as well as tangible property—areas addressed under property insurance forms.

Lack of Coverage Standardization—Especially as to Property Coverage

Although most cyber and privacy insurance policies provide at least some level of property insurance (business interruption, extra expense, dependent business interruption), the forms vary considerably as to the actual extent of property coverage they provide.

On one hand, some insurers philosophically view cyber and privacy coverage as essentially a type of liability insurance. Accordingly, such insurers offer only a relatively bare-bones package of property coverage—and some do so only by means of an endorsement (rather than including property coverage in their standard form).

At the other end of the spectrum, other insurers afford a more comprehensive cyber and privacy policy that includes a robust set of property coverages, like business interruption and extra expense.

Menu-Driven Nature of the Coverage

Unlike most types of professional/E&O policy forms, cyber and privacy policies contain as many as 10 separate insuring agreements—a fact that, in some instances, requires the insured to select up to 10 separate individual coverage limits, as well as 10 individual deductible amounts (i.e., one for each type of coverage selected).

Yet Another Problem: The Policy Aggregate Limit

As if choosing 10 separate coverage limits and deductibles weren't an already challenging task, the policies are also written with an *annual aggregate limit* that applies across *all* coverages the insured has selected—a fact that creates the need for the insured to make yet another limit-related decision.

Emerging Nature of the Exposure

The cyber and privacy exposure has evolved much more rapidly in more recent years than, for example, the liability exposures facing fiduciaries, insurance professionals, or real estate agents. Cloud computing, social media, evolving forms of cyber attacks, and shifting regulatory environments are just a few of the factors that impact the rapid evolution of cyber exposures.

Not only is the exposure evolving in type and frequency, but the average cost of resolving data breaches has become more costly over the years.

Emerging Nature of the Coverage

Just as the cyber and privacy exposure has advanced at breakneck pace, so too has the nature of the policy forms written to address the exposure. Consider that in years past, the vast majority of policies focused on providing coverage for liability arising out of a data breach but not on affording coverage for data breach response costs (e.g., notification, credit monitoring, public relations expenses) to the extent that the more recent policies do.

Overlap with CGL, Professional Liability, and Property Insurance Policies

Another confusing aspect of cyber and privacy policies is that *some* coverage for several of the same exposures provided by cyber and privacy forms is also made available under CGL, management liability, and property insurance policy forms.

CGL Coverage Overlaps

Occasionally, there may be coverage for advertising injury liability under *both* the CGL and the content liability coverage section offered under cyber and privacy liability policies. However, it should be recognized that CGL advertising injury liability does *not* apply to (1) media firms and (2) advertising of

any but an insured's *own* products.

Management Liability Coverage Overlaps

A number of management liability policies cover some of the exposures addressed by cyber and privacy forms, albeit on a restrictive, sublimited, and third-party-only basis. Case-in-point: most (although not all) employment practices liability insurance (EPLI) policies cover claims alleging breach of privacy, such as when an employee's personnel file is accessed by unauthorized persons within the insured company. Although these forms likely intend to cover physical, in-person "breaches," evolving methods of cyber breaches may blur the line between what is an EPLI exposure and what is strictly a cyber and privacy exposure. Furthermore, a "breach" in this case would likely need to come from an employee (rather than an outside actor) in order for coverage to apply.

Property Insurance Coverage Overlaps

Property insurance policies vary widely as to the nature of coverage they afford when an insured suffers a loss involving electronic data and the systems used to process such data. For example, the broadest property insurers' forms will cover business interruption loss due to a company's e-commerce system being rendered inoperable as the result of a cyber incident. In contrast, other property insurers' forms require actual physical damage to these systems (such as from fire, vandalism, windstorm, or flood) as a condition precedent to providing coverage.

Miscellaneous Idiosyncratic Coverage Provisions

Lastly, a number of coverage provisions found within cyber and privacy policies are unique to this particular area of insurance. Following are three notable examples.

Fines and Penalties

Cyber and privacy policies almost universally cover fines and penalties. As an example, coverage is often provided when a state or local authority levies a fine or penalty against an insured for failing to prevent a breach of customer data or for failing to notify the customer that such a breach has occurred. This approach represents a distinct departure from other lines of professional/E&O insurance, which almost universally exclude coverage for fines and penalties.

Content Liability

Another example of an idiosyncratic coverage approach (albeit more specifically related to media firms) is that some insurers will not cover a media firm's content risks under a cyber and privacy form. Their philosophy is that such businesses require more robust—and thus separate—policies to cover more significant content risks such as plagiarism, copyright infringement, defamation, and trademark violations, to which media firms like publishers, advertising agencies, and radio and television broadcasters are subject. It should be noted that as more and more companies delve deeper into online publishing (e.g., detailed social media posts and/or professional-level blog posts), this coverage nuance is becoming all the more applicable to a broader range of companies offering different products and services.

Dual Coverage Triggers

Since both liability and property exposures are often times addressed by cyber and privacy policies, the forms are often written with two *different* types of coverage triggers—claims-made triggers applying to the liability insuring agreements and occurrence triggers (possibly including time element deductibles) to the property sections. As a consequence, various foreseeable complications can result in the event that a single loss involves *both* liability and property insuring agreements and, therefore, claims-made *and* occurrence coverage triggers.

Summary

Cyber and privacy insurance coverage can be confusing for a number of reasons, including the following.

- The coverage is referred to by various names.
- It is often confused with technology E&O coverage.
- Both cyber and privacy *and* technology E&O policies cover many of the same risks.
- Both property *and* liability exposures are covered under cyber and privacy insurance.
- The nature of the coverage varies considerably from insurer to insurer.
- The menu-driven nature of the policies creates special problems.
- The cyber and privacy exposure is rapidly evolving.
- Cyber and privacy policies are also rapidly evolving.
- Cyber and privacy coverage aspects overlap with CGL, professional, and media liability policies.
- Cyber and privacy forms contain a number of idiosyncrasies.

Chapter 2
Information Security Liability Exposures

Overview

There are four broad categories of third-party liability exposures to which businesses are subject when they engage in cyber activities.

- Information security liability
- Privacy liability
- Content liability
- Bodily injury and property damage liability

This chapter addresses the nature of information security liability exposures, which refer to the liabilities that result from breaches of an electronic network.

Chapter Objectives

On completion of this chapter, you should be able to do the following.

- Identify three types of information security liability exposures.
- Recognize the loss exposures existing in a given scenario.

What Is Information Security Liability?

Information security liability refers to the liabilities that result from sensitive information being exposed after (or during) breaches of an electronic network.

A *network breach* occurs when someone

- gains access to a computer network despite not being authorized to do so,
- transmits malicious code (e.g., a virus) or otherwise attacks a computer network, or
- prevents a third party who is authorized to do so from gaining access to a computer network (i.e., a denial of service attack).

"Computer network," as used in the points above, should be understood to include not only servers and Web applications regularly accessed by desktop and mobile device users but also credit card processors, mobile apps, and other devices connected to the Internet in some capacity (commonly referred to as "The Internet of Things").

The following scenario, which involves a hospital, illustrates the various types of liability that each of these three kinds of network breaches can produce. Hospitals are an excellent example to examine from a cyber and privacy liability perspective due to the sensitive, private information they store as well as the serious harm that can be done if this information is not readily accessible during and after a breach.

Liability for Failure To Prevent Unauthorized Access to a Computer System

Assume that a hacker gains access to a hospital's database that contains the personal health records of the 200,000 patients it has treated during the past decade. As a result of this unauthorized intrusion into its computer system, the hospital has incurred what is known as *privacy liability,* a type of liability that will be discussed in more detail within the pages that follow. This liability could be especially applicable in the event that a company failed to adequately encrypt its data or take other security measures a company in its position could be reasonably expected to take.

It should not be assumed that a hacker like the one alluded to above is an individual or group that has no previous affiliation with the affected organization itself. Exposure from frustrated employees that feel like they have been wronged by the organization can also be significant. This is especially true given the fact that these employees may already possess the credentials or security clearance necessary to breach a network, which an outsider may have greater difficulty obtaining.

Liability for Transmission of Malicious Code

In the scenario above, assume that the hacker has also found a way to infect the hospital's database with a virus that renders some of its patients' health records unusable. More specifically, *malicious code* means any virus, Trojan horse, malware, worm, or any other similar software program, code, or script intentionally designed to insert itself into computer memory or onto a computer disk and spread itself from one computer or network to another. This transmission could very likely have the effect of compromising the quality of care delivered by the hospital, which could potentially give rise to liability claims against it.

Computer Virus Deletes Files: A Non-Hospital Claim Scenario

Customers and suppliers routinely communicate via email, and it is becoming more common to even allow customers access to company intranets (i.e., a company's internal Internet system). Computer viruses can be spread from the supplier to the customer, resulting in the deletion of files in the customers' systems. Such an event can cause a customer to incur substantial costs in repairing its purchasing system as well as lost revenue from its inability to purchase raw material in a timely fashion to meet delivery requirements. The customer may sue the supplier for the expenses of repairing the damage caused by the virus as well as for lost revenue. Viruses can enter computer systems through a variety of means. Nevertheless, the supplier may still be found liable to the customer for the damage caused by the virus from the supplier's system.

Liability for Preventing an Authorized Third Party from Gaining Access to a Computer System: Denial of Service Attacks

Continuing with this hospital claim scenario (above), also assume that a number of physicians working outside of the hospital are authorized to access the hospital's computer system. Such access facilitates treatment of former hospital patients who are now being treated at the individual physicians' offices. However, as a result of the hacking, these physicians are unable to access their patients' records, a situation that compromises the quality of the patients' care and ultimately generates liability for the physicians when this occurs. The physicians, in turn, could then sue the hospital, based on the hospital's negligence in not preventing the initial breach of its computer system.

Liability for Network Breaches Affects All Industries

This hospital scenario notwithstanding, it is important to recognize that the types of liability incurred above are in no sense limited to the healthcare industry. For example, as a result of a network breach, a credit card processing company would incur liability if a hacker gained access to the personal data belonging to its cardholders. A clothing retailer that operates an online order system would incur liability if that same hacker transmitted a virus to its computer network and the virus infected the computer systems or stole the personal information of all of its customers who placed orders on the clothing retailer's network. Lastly, a company operating a website offering a subscription service that provided stock market data could be held liable if the hacker also found a way to block access to the website when the company's subscribers attempted to log on.

Summary

Information security liability results from the breach of a computer network and occurs when (1) an unauthorized person *gains access* to that network, (2) an unauthorized person *injects or transmits a virus* or other kind of malicious code into the network, or (3) an unauthorized breach *prevents* an authorized third party from gaining access to the network.

Chapter 3
Privacy Liability Exposures

Overview

Privacy liability is incurred by a company when its computer system is breached by a hacker or other bad actor and, as a consequence, personally identifiable information (PII) is obtained and/or released to unauthorized persons.

Chapter Objectives

On completion of this chapter, you should be able to do the following.

- Recognize instances of privacy liability.
- Recognize the meaning of the all-important term PII.
- Recognize the special privacy exposures of healthcare companies.
- Identify various laws relating to privacy liability.
- Identify the frequency, costs, and causes of privacy breaches.

What Is Privacy Liability?

Privacy liability, defined above, is closely tied in with PII.

Exhibit 3.1
What Is Personally Identifiable Information (PII)?

PII is information that can be used to uniquely identify, contact, or locate a single person or can be used in conjunction with other sources to uniquely identify a single individual.

The following data, often used for the express purpose of distinguishing individual identity, are typically considered PII.

- Full name (if not common)
- National identification number (i.e., Social Security number)
- Internet Protocol (IP) address
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, handwriting, and biometric identifiers
- Credit card numbers
- Digital identity
- Date of birth
- Birthplace
- Genetic information

Privacy Breaches Are Not Always Electronic

It is critical to note that privacy breaches are *not* confined to breaches of computer networks or electronic systems. Small businesses are especially vulnerable to privacy breaches that occur by nonelectronic means.

Specifically, privacy breaches can occur from loss, theft, improper disposal of, or misplacement of the following.

- Laptop/notebook computers
- Paper files
- Customer lists
- Human resources records
- Mobile phones and tablets
- Flash drives

According to one security survey, about 15 percent of breaches are due to lost or stolen devices.[1] Even today, there are still a frightening number of incidents in which security personnel responsible for valuable, high-risk operations (for example, those working at nuclear power plants) have had mobile phones or identity cards compromised. Clearly, despite the electronic origins of many privacy breaches, the simple threat of lost or stolen devices is still a significant exposure, even in high-value/risk areas such as these examples.

Types of Costs Incurred in Responding to a Privacy Breach

Consider the following hospital privacy breach scenario. A hacker breaches the computer system of a major hospital and, in the process, obtains the complete health records of 50,000 patients. The hospital must expend a total of $15 million to respond to this breach.

Among the costs incurred by the hospital, which now faces a multitude of privacy liability claims from patients whose records have been exposed, are the following.

- Set up a call center following the breach.
- Notify each of the patients affected.
- Monitor the credit of the affected patients (usually for 1 year).
- Incur identity theft insurance costs for the affected patients.
- Pay the costs required to restore stolen identities resulting from the breach.
- Pay actual losses sustained from the theft of the patients' identities (e.g., the loss resulting when a thief gains access to and withdraws the proceeds of a victim's entire stock brokerage account).
- Hire a computer security/forensics company to investigate the source of the breach and recommend measures to prevent further disclosures of records from similar vulnerabilities.
- Engage the services of a public relations firm.
- Defend a class action suit brought against the hospital by patients whose records were compromised.
- Pay various fines levied by regulators.
- Hire a so-called breach coach, typically an attorney, who will walk the insured through the entire process of responding to the situation, including many of the steps above.

The Special Privacy Exposures of Healthcare-Related Companies

The healthcare and social assistance industry is routinely considered the largest single-industry employer in the country. Because they frequently handle sensitive patient financial and health information, hospitals are data-rich targets for hackers. This is especially true with the continual increase in the use of electronic medical records (EMRs), which are electronic versions of a patient's detailed medical history.

As required by the American Recovery and Reinvestment Act of 2009, also known as the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), the Office of Civil Rights' website posts a list of the covered entities that have reported breaches of unsecured protected health information affecting more than 500 individuals.

On March 12, 2012, the Office of Civil Rights reached its first settlement under the HITECH Act, settling with Blue Cross Blue Shield of Tennessee for $1.5 million due to a data breach occurring in 2009. In this case, 57 unencrypted hard drives were stolen from a closet in a Blue Cross Blue Shield facility. On these hard drives were the medical records of approximately 1 million patients. On top of the $1.5 million settlement, it was estimated that Blue Cross Blue Shield spent $17 million in additional costs responding to the breach.[2]

Other Office of Civil Rights settlements include the following.[3]

- **Premera Blue Cross: $6.85 million settlement, September 25, 2020.** Hackers used a phishing email to install malware and obtain information of 10.4 million individuals.
- **CHSPSC LLC: $2.3 million settlement and corrective action plan, September 23, 2020.** Hackers gained access using compromised administrative credentials and obtained information of over 6 million individuals.
- **Athens Orthopedic Clinic, PA: $1.5 million settlement, September 21, 2020.** Hackers used a vendor's credentials to obtain patient records for 200,000 individuals.

Privacy Loss Scenarios

Now consider the following privacy claim scenario not involving a hospital. A company sets up and operates a website for the online trading of securities. To trade using the site, customers must supply personal and financial information to the company, and they are assured the information will be secure. However, a glitch in the encryption software allows unauthorized persons to access information transmitted to and from the site. Customers may sue the Web services provider for any losses incurred as a result of the glitch that permitted others to access their confidential information. At a minimum, such losses may include the costs of changing accounts and account numbers at banks and brokerage firms and might even include lost investment income during the changeover periods.

The following real-world loss scenario illustrates a privacy claim not involving a computer network.[4] A

vehicle being used by an employee of CBR Systems, a stem cell storage company, was broken into. Included in the stolen items was a backpack containing a laptop and other portable devices. These devices contained unencrypted PII, including names, addresses, Social Security numbers, medical histories, and payment details for approximately 300,000 clients of CBR. Although no computer network was breached per se, CBR was still penalized with a 20-year consent order from the Federal Trade Commission (FTC), requiring the company to maintain information security programs, allowing an independent auditor to monitor their operations, and reporting back to the FTC on a periodic basis. Furthermore, the company was forced to settle a class action lawsuit brought by its clients, resulting in a total settlement amount of about $112 million, including identity theft-related losses, credit monitoring, and attorneys' fees.

Privacy Liability Laws

The liability incurred by the hospital in the scenario noted above results from a patchwork of privacy laws that have been enacted in various states. Such laws indicate that responsibility for a breach lies with the company or business that *collected* and *stored* the affected data. Additionally, attorneys general in the various states have broad enforcement powers (similar to the FTC). Under such laws, they have the power to investigate breaches and file lawsuits against the offending companies, levy fines/penalties, and enforce federal laws against the company responsible for the breach (such as the Health Insurance Portability and Accountability Act, known as HIPAA).

Lack of an Overriding Federal Law for Privacy Breaches

Importantly, there is no overarching US federal law that sets standards mandating either (1) specific data protection requirements or (2) definitive loss notification benchmarks to regulators or to individuals affected by a breach. Rather, as noted above, the individual state laws, as well as federal law and consumer privacy laws that are industry-based, often apply simultaneously and may contradict one another in some cases.

The Varying Nature of State Breach Notification Laws

All states in the United States of America have enacted some form of legislation requiring notification of breaches or potential breaches of PII for private, governmental, or educational entities. Unfortunately, each state varies in exactly what is required, and this hodgepodge system of regulations makes it difficult for most businesses to comply with this maze of laws, particularly for those that do business in multiple states.

Which State's Law Applies in the Event of a Breach?

The specific state law that applies to any given breach is typically based on two factors: (1) the consumer's state of residence, and (2) the state in which the business is incorporated. Compliance, especially for firms in highly regulated industries such as health care, legal, educational, and financial services, is therefore no easy task.

How, Whom, and When To Notify: The "Safe Harbor"

Owing to the inherently confusing nature of the compliance process, the data breach notification laws applicable in many states provide a "safe harbor," which requires companies to notify *only* when sensitive information was exposed in unencrypted form *or* if the information was misused, despite encryption.

States laws vary as to *how*, *whom*, and *when* to notify. Some states may require information security action plans following a breach; enforce fines in the thousands of dollars per individual violation; require regular monitoring and reviews; have overly broad definitions of "affected individuals," thereby broadening the scope of notification requirements; and/or have specific data disposal laws that go along with notification requirements.

Companies should be in consultation with cyber and privacy legal experts in order to fully understand their notification obligations from state to state in the event of a major breach. Until a federal law is

enacted to set consistent cyber-related enforcement expectations, companies will be faced with this ongoing challenge of navigating a patchwork legal environment.

Securities and Exchange Commission (SEC) Breach Notification Requirements

The Securities and Exchange Commission (SEC) has issued guidance that encourages companies to disclose privacy breaches in an effective manner.[5] The guidance was aimed at instructing businesses on what it terms a "material cyber attack," notice of which should be included within the SEC's already required annual/quarterly disclosures and filings.

Under the SEC guidance, the following information should be included within a disclosure.

- Remediation costs that were incurred, which include the costs of credit monitoring for affected individuals and the costs of providing data breach notifications to affected individuals
- Plans for and anticipated costs of the company's enhanced cyber security program, aimed at preventing future data breach incidents
- Estimates of the potential loss in sales caused by damage to the company's reputation resulting from the data breach
- Anticipated legal costs based on potential litigation that could be filed against the company

Moreover, if the company believes that there is a relatively high risk of future cyber security/data breach incidents because its systems are not effectively securing its data, the business should disclose such conditions if they make "… investment in the company speculative or risky...."

International Laws

With data breaches becoming more common, specific privacy and breach-related requirements are increasingly being enacted. For example, the European Union has enacted the General Data Protection Regulation (GDPR). As detailed on the regulation's own information website, the regulation is aimed at improving security for all companies processing personal data for subjects in the European Union, regardless of the company's location. GDPR states that organizations can be fined "up to 4 percent of annual global turnover or €20 million (whichever is greater)" for the most serious violations.

Specifically in regard to breach notification requirements, GDPR makes notification mandatory in all member states when a breach is likely to result in a substantial risk to affected individuals. This notification must take place within 72 hours of the company becoming aware of the breach.

Frequency and Costs of Electronic Privacy Breaches

The number of new malware strains is growing year-over-year by upwards of 70 percent according to some reports.[6] In other words, there are hundreds of thousands of new strains and cyber exposures to contend with each year on top of all of the existing threats.

Accompanying the rapid increase in malware strains is the fact that cyber attacks may be subject to underreporting—although this trend may improve over time as reporting obligations continue to be laid

out more concretely by state and national requirements.

The average organizational cost of a data breach has been reported around $4.24 million, trending upwards from previous years. The estimated cost of a data breach on a per-record basis is around $160 and is also trending upwards.[7]

Costs associated with breaches can be substantial and, in some cases, astronomical. For instance, in what is still cited as one of the most extreme cases on record, a 2011 breach of the marketing firm Epsilon had some analysts predicting the costs of the breach could reach $4 billion.

Effective response to breaches can significantly decrease costs. Utilizing an incident response team, in combination with extensive encryption, has been shown to decrease the cost of a data breach on a per-record basis (potentially by around 10 percent).

Smaller Companies Are Not Immune to Cyber and Privacy Breaches

Many small businesses believe that their information would not attract cyber thieves. Unfortunately, this belief is a misperception. Small businesses are targeted by cyber thieves because sensitive information kept by small businesses is often much easier to obtain due to the lack of sophisticated security measures, as compared with larger firms.

In addition, it is important to understand that the information stolen from small businesses often is the owners' personal information. Business owners that use their personal accounts information for business transactions face a higher risk of identity fraud.

In fact, some statistics have shown that:[8]

- More than 60 percent of small and midsize businesses (SMBs) may experience a data breach in any given year.
- SMBs spend an average of more than $1 million addressing theft of IT assets and other infrastructure costs.
- SMBs face an average of nearly $2 million in costs related to disruption of operations after a cyber incident.
- Most SMBs are reporting that the time required to respond to a cyber incident has either remained unchanged or increased over time.
- SMBs often feel that IT leadership is lacking at their organization, and compliance efforts are a burden.

According to one report, around 56 percent of all data breaches were at companies with less than 1,000 employees. Among this size of employers, system intrusions and basic Web application attacks made up the vast majority of incidents, with a fairly close to even split between external and internal bad actors. In many ways, small businesses were exposed to the same types of incidents that their larger counterparts have faced.[9]

Key Causes of Network and Privacy Breaches

Causes of network and privacy breaches fall under two categories: (1) human error, and (2) computer hacking/viruses. The latter category is the result of intentional acts, whereas the former results largely from (1) lost/stolen/compromised laptops, media, smartphones, and tablets—all of which were left unattended, were poorly secured, or lacked encryption/strong password protection, (2) improper disposal of computer data/devices, (3) employee misuse of data/media, or (4) vendor negligence.

Summary

Privacy liability is often incurred by a company when its computer system is breached by a hacker and, as a consequence, PII is released to unauthorized persons. However, privacy breaches are *not* confined to breaches of computer networks or electronic systems. In fact, small businesses are especially vulnerable to privacy breaches that occur by nonelectronic means.

The liability incurred by businesses results from a patchwork of privacy laws that have been enacted in various states. Such laws indicate that responsibility for a breach lies with the company or business that *collected* and *stored* the affected data. Importantly, as of the time of writing there is no overarching US federal law that sets standards mandating either (1) specific data protection requirements, or (2) definitive loss notification benchmarks to regulators or to individuals affected by a breach. However, entities like the SEC have issued guidance that encourages companies to adequately and responsibly disclose privacy breaches.

The average organizational cost of a data breach has been reported upwards of $4 million and is trending higher compared to prior years.

Firms of all types and sizes, and even governmental organizations, have reported that they have been the victim of cyber-security incidents or information breaches.

Chapter 4
First-Party Property Loss Exposures

Overview

Cyber activity exposes businesses to a number of first-party property loss exposures, which include the following.

- Business interruption
- Dependent business interruption
- Extra expense
- Data asset loss
- Cyber extortion
- Computer fraud (or “computer crime”)
- Funds transfer fraud
- Miscellaneous crime losses

These exposures will be examined in the pages that follow.

Chapter Objectives

This chapter addresses the eight types of first-party property loss exposures to which businesses are exposed as a result of cyber activities. On completion of this chapter, you should be able to do the following.

- Recognize the nature of the exposures.
- Identify the specific types of losses that can happen as a result of these exposures.

Business Interruption

Business interruption losses result when a breach of or malfunction of a business's computer systems causes a loss of income. For example, a business interruption loss occurs when an online retailer suffers a loss of revenue during the time in which its website cannot process orders because it has been compromised by a cyber attack.

Business Interruption Loss Scenarios

The following are examples of when other types of business interruption losses can arise.

- A fast food restaurant that takes online orders has its server fail. The malfunction causes the restaurant to lose sales during the time it takes to get operations up and running again.
- An electronic order system must be shut down as a result of a planned upgrade (performed during off-hours) that is required by a rapidly growing Web-based retailer. The additional capacity and an upgrade are installed incorrectly. As a consequence, the upgrade malfunctions and causes several hours of downtime, unfortunately during a peak period for receiving orders. The company suffers loss of revenue when customers are denied access to the system during the busiest part of the business day.
- Instead of developing and maintaining its own website, a company has decided to outsource all of its Web-related activities. As part of the arrangement, it allows a third party access to some of the company's internal systems to keep the website current. During routine maintenance, negligence by the third-party website operator results in downtime and consequent loss of revenue for the client. (Recognize that the third-party operator will/should ultimately be held liable for the loss. However, in the absence of the third party's ability to indemnify its client for the loss, the client's first-party business interruption coverage is likely to be the sole source of indemnification.)

Dependent Business Interruption

A dependent business interruption loss, as defined by those insurers whom offer this coverage within their cyber and privacy forms, typically results from the failure of service providers' computer systems (rather than the insured's systems). This failure, in turn, leads to an interruption in the insured's business and a subsequent loss of revenue.

More specifically, the coverage usually applies to *technology* service providers. These technology service providers typically perform the following services for insureds.

- Maintaining, managing, or controlling computer systems
- Hosting or facilitating the insured's website

- Handling, managing, storing, or destroying the company's nonpublic personal information and confidential corporate information
- Other information technology services

While these technology-related services are representative of what can be found in the "service provider" definition in many insurers' forms, some policies *also* state that "service providers" may include those that perform administrative, human resources, marketing, and other similar services for insureds.

A Dependent Business Interruption Loss Scenario

Company A, a midsize retailer, utilizes its website for the vast majority of its customers' purchase orders (rather than maintaining a large quantity of physical storefronts). Given the complexity and importance of keeping the website fully functioning, Company A hires an outside technology service provider to host and facilitate the website. However, the service provider becomes unable to maintain Company A's website for a period of several days during the holiday season due to an internal systems failure caused by a hacker compromising the provider's computer system. This causes Company A's online shopping cart to be unusable, which prevents customers from placing online orders and results in a substantial loss of revenue for Company A during the several days in which the service provider's system is rendered inoperable.

Extra Expense

An extra expense loss occurs when extraordinary costs must be incurred to minimize the time during which a business' electronic network is rendered inoperative.

An Extra Expense Loss Scenario

A major credit card processor suffers a data breach, which requires the company to shut down its processing systems. However, were the company to suspend its operations for any significant period of time, it would likely lose some of its major accounts and would sustain a loss from which it may never be able to recover. Accordingly, the credit card processor must expend substantial monies to first ascertain the source of the breach, then address and remove the vulnerability, and then take steps to secure its systems to prevent a subsequent incursion. Accomplishing all of this in a brief period of time (e.g., 24 hours or less) may necessitate that the company incurs enormous costs, such as hiring top-tier experts; paying double or triple overtime labor charges; and purchasing expensive, state-of-the-art data protection systems.

Data Asset Loss

Just as malware can shut down a company's operating system, so too can it destroy valuable data assets. For example, a virus may corrupt and make a company's customer lists unreadable and inaccessible. Similarly, it could destroy a company's proprietary software programs.

Data Asset Loss Scenarios

An online retailer suffers a cyber attack, rendering its customer lists no longer readable or usable.

A Wall Street brokerage has developed a proprietary software program for analyzing the financial statements of publicly traded businesses. The firm uses the software to make its trading decisions. Imposition of a virus by a hacker damages the software so that it is inoperable.

In both instances, the affected companies maintain backups of their customer lists and financial analysis software, respectively. However, properly recovering with these backups requires hiring consultants to assist the organizations—in both cases, at a substantial cost. Note also that both companies would sustain business interruption losses during the periods of time in which they could not operate (i.e., during the backup recovery period)

Cyber Extortion

Cyber extortion occurs when a criminal threatens to damage or shut down a company's electronic systems unless the company pays the criminal a specific ransom amount. In addition, criminals could threaten to expose electronic data or information belonging to a victim if the target does not pay the ransom demanded.

Two Cyber Extortion Loss Scenarios

A bank receives a ransom message from a hacker threatening to penetrate its customer database and disclose all of its individual account holders' PII if the bank does not pay $5 million.

An online gaming website receives a message from a hacker demanding that $1 million be transferred to a bank account in the Cayman Islands. If the money is not transferred within 12 hours, the hacker promises to shut down the website and disclose sensitive information.

In both situations, the affected businesses might choose to pay the respective ransom demands and suffer the loss of $5 million and $1 million, respectively. Or, alternatively, they could ignore the demands and potentially suffer losses resulting in privacy liability (the bank) and business interruption (the gaming site).

Ransomware

Yet another means of electronic extortion is use of what has become known as **ransomware**. In using this technique, hackers typically compromise an organization's network and make it inaccessible and/or steal sensitive data to "hold hostage." Then, a ransom demand is made, to be paid by the organization in exchange for a promise that the hacker will restore the network to functionality and/or unencrypt any stolen data (for example, an organization may pay a ransom in the hopes that a hacker will stay true to a promise to provide an unencryption key to regain access to data). These ransom demands are often made in cryptocurrencies so as to be harder for authorities to track the bad actors.

Ransomware attacks have frequently targeted the medical industry, largely due to the massive quantity of detailed patient records with sensitive and valuable information. However, this is far from the only impacted industry. As hackers have learned how potentially lucrative this attack vector is, ransomware, in general, has skyrocketed in prevalence. This rise has also been fueled by an increase in remote work in the aftermath of the COVID-19 pandemic, as workers use potentially less secure devices in their home environment. Now, companies of virtually every size, industry, location, and so on are exposed to serious threats of ransomware. In fact, some statistics show that a ransomware incident occurs every 11 seconds—and average downtime while recovering from a ransomware attack can be about 3 weeks.[10] Payouts have been made in the tens of millions of dollars to regain access to networks and data, and average ransomware demands have ballooned to around $200,000.

As incidents of this type become more sophisticated and difficult to defend, potentially resulting in more ransoms actually being paid out, it is important for businesses to ensure that any existing cyber-extortion coverage they may have in place provides sufficient levels of protection against ransomware scenarios.

Computer Fraud (or "Computer Crime")

In a computer fraud situation, after gaining access to a company's network, the criminal uses such access to obtain valuable data or information. This is frequently in contrast to a cyber-extortion scenario, in which the actual data or information is restored if the company gives in to the criminal's demands. In the extortion scenario, it would be "bad for business" if hackers were to develop a reputation of refusing to relinquish control of sensitive information even after a company paid up. Due to this, companies that have been breached and extorted have generally found that hackers follow through on their word upon receiving payment.

Computer Fraud Loss Scenarios

A maker of computer chips has its operating system hacked by a bad actor who obtains step-by-step details of its manufacturing process and then sells it to a competitor.

An Eastern European crime organization accesses a retailer's online ordering system and steals credit card numbers with the hopes of selling the information on the dark web.

A hacker gains access to an online stock brokerage account that contains $50,000 in cash. Before being blocked from making further transactions, the thief uses the account's proceeds to pay $25,000 in personal bills.

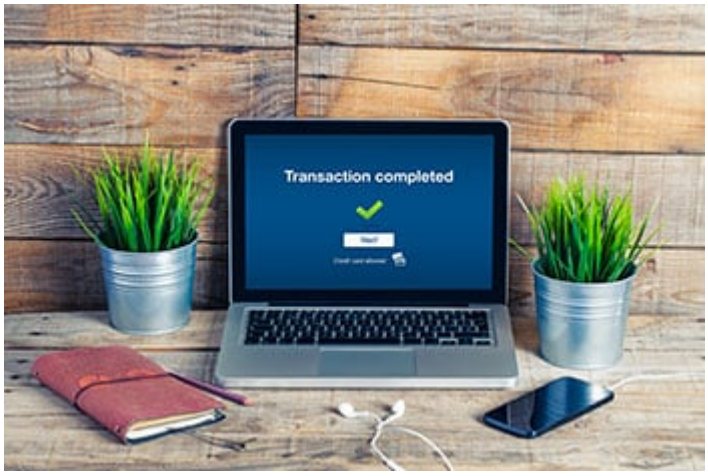
In each of the above scenarios, the criminal gains access to a business' electronic systems and then uses such access to obtain something of value (i.e., trade secrets and cash, in these respective examples).

Phishing

Phishing constitutes one of the classic computer fraud loss scenarios. Phishing begins by sending an email message falsely claiming to be from a lawful business or "legitimate" individual and then directing the recipient to visit an illegitimate website or supply sensitive information that can be used nefariously. The recipient is often asked to provide personal information, such as Social Security, credit card, and bank account numbers. Such information will later be used to commit identity theft or another kind of cyber wrongdoing.

While regular phishing uses a more "shotgun" targeting approach, "spear phishing" is aimed at specific individuals and/or companies, relying on the use of personal information to make emails appear convincing and trustworthy.

Funds Transfer Fraud



Funds transfer fraud occurs when a cyber criminal accesses a computer network and then uses such access to fraudulently transfer monies from one account to another.

Funds Transfer Fraud Loss Scenario

A credit union received an email that *appeared* to be from a stock brokerage firm but was not. The credit union's employee opened the email, which activated a computer virus that was able to read keystrokes entered from the employee's computer. The criminal used this information to access the account number and password information of one of the credit union's customers and then initiate a fraudulent wire transfer from the customer's credit union account to the criminal's account with a bank in Costa Rica.

Computer Fraud versus Funds Transfer Fraud

The key difference between *computer fraud* and *funds transfer fraud* is that the latter involves the transfer of monies from one financial institution to another, whereas the former does not involve a two-way transfer of this kind.

Miscellaneous Crime Losses

A number of crime loss types do not fit neatly into any of the aforementioned categories.

Exhibit 4.1
Miscellaneous Cyber Crime Loss Scenarios

- **Defacing Web pages.** Hackers access a firm's website and change pieces of information found within it, wreaking havoc with the company's business. However, they do so without actually stealing any information, merchandise, or funds.
- **Intercepting emails of a proprietary nature.** A competitor gains access to a company's email system and learns the date on which the company will introduce a new product. This allows the competitor to accelerate the introduction of its own competing product before its competitor's version is released.
- **Posting embarrassing material.** A hacker posts pornographic material on a newspaper's website. The newspaper incurs expenses and downtime to remove the hacked-in material.
- **Posting source codes.** A hacker penetrates the internal system of a software company and posts the details of its software product source codes on a website. The software company incurs costs to restore its system, as well as to find and bring a lawsuit against the responsible hacker.
- **Sabotage by employees.** A programmer for a publisher is terminated from employment. During the evening of the day he is terminated, the employee logs onto the employer's internal network. The former employee then deletes an entire issue of the magazine, along with any backups, and the publisher incurs substantial expenses to recreate it.
- **Spamming.** Spam is unwanted and unsolicited communications or traffic sent to another's website, computer systems, or networks. A massive spam attack on a telephone company takes up so much space on the company's server that it produces a degradation in service, causing the system to crash.

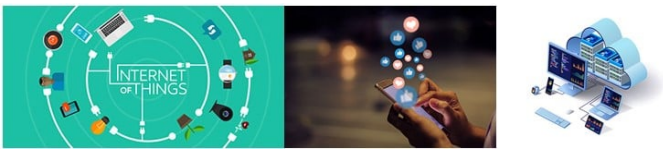
Summary

This chapter examined the eight types of first-party property loss exposures faced by businesses that operate electronically. These exposures include the following.

- Business interruption
- Dependent business interruption
- Extra expense
- Data asset loss
- Cyber extortion
- Computer fraud
- Funds transfer fraud
- Miscellaneous crime losses

Chapter 5
Emerging Cyber and Privacy Exposures

Overview



This section will discuss the *Internet of Things, social media,* and *cloud computing*, three constantly evolving cyber exposures, each of which has the potential to generate both first-party property and third-party liability losses.

Chapter Objectives

On completion of this chapter, you should be able to do the following.

- Recognize exposures associated with the IoT, social media, and cloud computing.
- Identify the types of devices that make up the IoT and the unique exposures associated with each.

The Internet of Things

The **Internet of Things (IoT)** is a term that collectively refers to the everyday devices that are connected in some way to the Internet. Many of these devices are referred to as "smart" devices: smartphones, smart homes (Internet-capable thermostats, appliances, and so on), smart televisions, and many more devices. Through Bluetooth, Wi-Fi, and other wireless communication, users of smart devices are able to control them and often times connect them functionally with *other* smart devices. Connections to the Internet allow these devices to track usage habits, provide useful recommendations, and generally offer users a more interactive and feature-rich experience.

The amount of IoT devices is expected to continue its massive growth. With this growth will come the continued expansion of cyber and privacy liability exposures due to security challenges inherent in these devices.

The range of IoT cyber attacks that have made the news covers the spectrum from absurd (hacking and speaking through baby monitors installed near cribs) to potentially serious (remotely hacking into moving automobiles). Part of the widespread nature of the exposure at the time of this writing seems to be the "hacking for sport" nature of some of these acts; often times there is no apparent end goal for hackers outside of demonstrating their ability to gain access to these devices. This is somewhat contrary to breaches of personally identifiable information (PII), for example, which possess financial value and thereby serve a clear purpose for financially driven hackers.

Unfortunately, the more troubling exposures, such as the remote override of moving vehicles alluded to above, have serious liability implications for product manufacturers. In the event of a serious accident causing damage, injury, or death that is traced back to the actions of a hacker, manufacturers of IoT devices could face liability for failing to take appropriate measures to safeguard such devices from unwanted access. In the event that a smart device contains personal, potentially embarrassing information, cyber and privacy liability exposure could also exist for the manufacturer in the event that such information is made public.

One method that makers of IoT devices have utilized more frequently over time in order to detect vulnerabilities is the usage of "white hat" hackers, or hackers tasked with finding "holes" in security and informing the company so that it may take action to resolve them. While many white hat hackers have informed companies of such vulnerabilities without any expectation of monetary reward, other companies have even taken the step of offering money or other "prizes" for those that are able to detect and report previously unknown security issues.

Social Media

Social media includes Web-based and mobile-based technologies that are used to turn communication into interactive dialogue between organizations, communities, and individuals. In the *Business Horizons* article "Users of the World, Unite! The Challenges and Opportunities of Social Media," authors Andreas Kaplan and Michael Haenlein define social media as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content."

Social media technologies take on many different forms and mediums, including feeds, forums, blogs, wikis, podcasts, photographs or pictures, video, product rating, and dedicated social media apps.

According to Kaplan and Haenlein, there are six different types of social media.

- Collaborative projects (e.g., Wikipedia)
- Blogs and microblogs (e.g., Twitter)
- Content communities (e.g., YouTube)
- Social networking sites (e.g., Facebook)
- Virtual game worlds (e.g., massively multiplayer online games)
- Virtual social worlds (e.g., metaverse projects)

Social media technologies include blogs, picture-sharing, vlogs, "wall" postings, feeds, email, instant messaging, music-sharing, crowdsourcing, and voice over IP, to name a few. Many of these social media services can be integrated via social network aggregation platforms. Social media sites include Facebook, Twitter, Instagram, LinkedIn, Reddit, TikTok, and many more.

The following are statistics regarding social media usage.[11]

- There are nearly 4.5 billion social media users worldwide.
- Average users engage with more than 6 social media platforms.
- Around 61 percent of the global population uses social media.
- 93 percent of Internet users are on some form of social media.
- The average person spends nearly 2.5 hours per day on social media.

Social Media Legal Liability Exposures

Social media websites have users numbering in the billions, including, of course, employees. Social media has exploded on the scene because it (1) is free, (2) is accessible to all, (3) is easy to use, (4) has a broad reach, and (5) allows for instant feedback.

The following types of allegations can emanate from the use of the various kinds of social media.

Privacy Violations

A company that digs too deeply into someone's personal social media activities can expose itself to privacy violation claims—almost a kind of cyber stalking! These claims may relate to the disclosure of medical information or a disability (thereby invoking the Americans with Disabilities Act, HIPAA, and a host of other laws). Such disclosures have the potential to generate claims involving discrimination on the basis of marital status, sexual orientation, and national origin, among other bases. Clearly, a company that improperly relies on information obtained from social media sites to make discriminatory decisions in the hiring process, or uses it to improperly manage its employees on a post-hire basis, can set itself up for breach of privacy and possibly discrimination claims.

Most employers feel they have the right to access any information that is publicly displayed on their employees' social media pages. Conversely, most employees felt that access to such information was none of their employer's business.

In fact, one study offered the following insights.[12]

- 92 percent of recruiters use or plan to use social media.
- For many recruiters, social recruiting ranks ahead of ads, employee referrals, and job boards.
- 2 million small businesses are using LinkedIn to hire employees.
- 86 percent of job seekers are using social media in their searches.
- 78 percent of recruiters expect the use of social media in recruiting to increase from current levels.

Sexual Harassment and Discrimination Claims

As is the case with many forms of cyber activity, social media has a never-ending shelf life. Once sexually harassing or discriminatory material is posted, it's very difficult to ever be truly and completely eradicated. In fact, companies that actually try to alter and remove unfavorable information or erase negative comments will be identified and harshly criticized by online communities, a number of which carefully monitor instances of Web and social media manipulation.

Wrongful Termination

Employees who are disciplined or even terminated for their social media-based activities can claim that the termination constituted a violation of public policy (i.e., infringement on privacy rights) or First Amendment rights, or make a claim on some other grounds. In *City of Ontario v. Quon*, 560 U.S. 746 (U.S. 2010), a police officer in Ontario, California, sued (although his wrongful termination claim was eventually rejected by the US Supreme Court) because he was fired for using the cell phone issued to him (supposedly for professional use) for excessive texting to a girlfriend. The officer argued that simply because he was given a phone for business purposes didn't mean he couldn't *also* use it for other things, nor was he warned against such personal use.

In August 2016, the National Labor Relations Board (NLRB) confirmed an earlier administrative law judge's decision that Chipotle had erred in terminating an employee that had been critical of the company on social media, as well as trying to limit his social media posts. A significant aspect of the ruling was focused on whether the wording and requirements of Chipotle's employee social media policy were lawful. As reported by Kwabena Appenteng and Philip Gordon in the August 30, 2016, article "NLRB Ruling in Social Media Case Provides Useful Guidance for Employers," appearing in *JD Supra Business Advisor*, Chipotle's restrictions on false and disparaging social media statements were "overbroad." Specifically, the article notes that the ruling "equated 'disparaging' statements with those that are derogatory and ruled that employees have a protected right to make derogatory statements about the terms and conditions of employment." As a result of the ruling, Chipotle was ordered to make corresponding changes to its social media policies and re-hire the affected employee (with back pay).

The Impact of Disgruntled Employees

Unhappy employees can cause considerable damage to former employers using social media postings. Their derogatory social media postings can cause possible new-hire applicants to think twice about joining the firm, and sour clients and competitors on the organization. Disgruntled workers can also disclose confidential or proprietary information. Just as an employee who "says too much" at a trade show can undermine a company's efforts to maintain trade secrets, so too can an employee who does likewise on their personal or company social networks.

Third-Party Lawsuits

Employees who inappropriately make comments in social media that relate to clients, customers, other employees, competitors, or other third parties can also provoke lawsuits against the organization. For example, the worker who talks about a client they hated or an employee who betrayed them, or tries to denigrate the company's products, may invite lawsuits for libel and/or interference with business relationships against the employer. Employee posts on social media may also expose a firm to fines and penalties brought by the Federal Trade Commission (FTC) and other governmental entities.

Cloud Computing*

*Based on “How Cloud Computing Works,” by Jonathan Strickland.

The term “cloud computing” means anything that involves delivering what are considered “hosted computing services” over the Internet. A cloud computing system allows workers at a company to use the resources of a Web-based, remotely located service that provides for all the computing power and remote storage requirements the individual employee would need to perform his or her job. Remote machines owned by another company (i.e., the “cloud provider”) run everything ranging from simple tasks to compute-heavy processes that a company does not have the bandwidth to run on its own. Thus, all electronic and data processing operations that would ordinarily take place on an in-house basis are handled in a “cloud” computing system. Cloud computing systems can generate claims alleging data breaches and privacy violations. In addition, such arrangements have the potential to create business interruption losses.

Key Characteristics of a “Cloud” System

The following are important aspects of cloud computing systems.

- Resources such as data storage space, computer applications, and computing are shared by all of the customers of a cloud vendor.
- A cloud system shifts the computing and data storage workload from the end user to the cloud system provider. Accordingly, the end user’s computers no longer have to do the work of running applications because the network of computers that comprise the cloud handles them instead.
- By using a cloud provider, the end user’s need for both hardware and software is reduced considerably.
- Customers do not own the cloud provider’s physical, computer network infrastructure. Instead, by availing themselves of the provider’s services, companies avoid incurring the expenses normally associated with hardware and software ownership because they rent their usage from the third-party “cloud” provider.
- The only thing the user’s computer needs to be able to do is run the cloud computing system’s application software, which can be as simple as a remote desktop application or a Web browser interface. The cloud’s network handles the rest.
- The “front end” of a cloud computing system includes the client’s computer or computer network and the application required to access the cloud computing system.
- On the “back end” of the system are the various computers, servers, and data storage systems that comprise the “cloud” of computing services.
- A central server administers the system, monitoring traffic and client demands, to ensure that everything runs smoothly.

- A cloud computing company with numerous clients will likely have a great deal of storage space and might need thousands of digital storage devices to keep all its clients' information stored. Some of the largest cloud providers have hundreds of thousands of servers.
- A cloud computing system must maintain a copy of all its clients' data and store it on other devices. The copies allow the central server to access backup machines to retrieve data that otherwise would be unreachable or permanently lost.
- A "public cloud" operates outside of the company's computer network, and it is provided by a third party.

Why a Cloud Provider Can Enhance the Security of a Company's Data

However valid a business' concerns regarding the security of its data when it is in the possession of a cloud provider, it can also be argued that a cloud provider's entire reputation is based on the ironclad security provided by its (hopefully) state-of-the-art protection systems. Compared to a company that manufactures the proverbial "widgets," a cloud provider can assert that it is surely in a better position to protect the widget manufacturer's crucial data than the widget manufacturer itself is. Since a cloud provider would be in danger of losing many of its accounts and suffering reputational damage if it were to suffer a data breach, the cloud provider's customers can be confident that it will make every possible effort to secure its customers' data.

Property and Liability Exposures Resulting from Cloud Computing

The three most significant exposures produced by cloud computing involve (1) data breach, (2) privacy breach, and (3) business interruption loss.

Data Breach

Many businesses are philosophically opposed to the idea of handing over their critical data to a third party—no matter how reliable the cloud provider or regardless of how strong the indemnification agreements that backstop such arrangements. Since companies already face a challenge in protecting their data, many firms are simply not comfortable with the fact that another organization will have custody and control of what is, in effect, the "life blood" of its entire operation.

Thus, when a company engages in a relationship with a cloud provider, the security of its entire database is dependent on the strength of the cloud provider's security systems.

The Risks of Cloud Storage

Cloud storage, similar to cloud computing, allows clients to store data on remote servers in the cloud, making it accessible from many different devices and shareable with others.

Of course, cloud storage is an appealing option for those that have (1) massive amounts of data in their control, which would not be feasible to store "in-house," and/or (2) highly sensitive, private information that they are more inclined to trust in the hands of an experienced cloud storage provider. Unfortunately, both of these aspects that make cloud storage useful also provide for tantalizing targets for malicious hackers.

In late August 2016, the popular cloud storage company Dropbox announced that a hack dating back to 2012 had exposed the user IDs and password of approximately 68 million users, as reported in *The Economic Times*. The company subsequently forced many users to reset their passwords upon their next attempted login.

While this hack immediately compromised user credentials rather than the stored data itself, it still serves to illustrate the potential risk in utilizing the services of cloud storage companies, which make for potentially appetizing cyber targets.

Privacy Breach

Since a cloud customer can log on from any location to access data and applications, the client's privacy

could be compromised if, for example, a hacker were to somehow gain access to the system and release the PII of a company's customers.

To counteract this exposure, cloud providers employ the most sophisticated and up-to-date authentication techniques, such as utilizing encryption and requiring "strong" usernames and passwords in conjunction with multifactor authentication (for example, a user signing in on their laptop may also be prompted to enter a SMS code that is texted to their cell phone). Another effective security measure is to implement a strict authorization format, whereby each user can only access the data and applications that pertain to their respective job or department within the company (the security principle of "least privilege").

Business Interruption

The possibility of physical damage to a cloud provider's premises *or* an internal system failure—not caused by physical damage—creates the chance that a client's electronic systems could be rendered inoperable and its data inaccessible for a given period of time. Both types of situations could produce a loss of income during the respective periods of outage.

Despite such possibilities, the question again arises as to whether a client is better able to ensure that such interruptions would not occur than the cloud provider is. Since the provider's *entire* business rests on its ability to prevent these types of situations, a business must realistically evaluate whether it may, in fact, be better off entrusting the operation of its electronic systems to a specialist rather than attempting to forestall such events using purely in-house resources.

Summary

The Internet of Things, social media, and cloud computing are three constantly evolving forms of electronic activity that, in their own unique way, can generate both property and liability exposures for a business.

The Internet of Things (IoT) consists of a variety of everyday devices that are connected, in some degree, to the Internet. As the growth of such devices continues, so too do the cyber and privacy liability exposures associated with them.

There are at least six different types of social media.

- Collaborative projects (e.g., Wikipedia)
- Blogs and microblogs (e.g., Twitter)
- Content communities (e.g., YouTube)
- Social networking sites (e.g., Facebook)
- Virtual game worlds (e.g., massively multiplayer online games)
- Virtual social worlds (e.g., metaverse applications)

Social media has the potential to generate claims alleging (1) privacy violations, (2) sexual harassment/discrimination, (3) wrongful termination, (4) damage caused by disgruntled employees, and (5) damage caused to other third parties.

A cloud computing system allows workers at a company to utilize a Web-based service that provides necessary computing power and bandwidth and hosts *all* the programs the individual employee would need to perform their job. Remote machines owned by another company (i.e., the "cloud provider") run everything ranging from mundane tasks to complex, compute-heavy processes. Thus, many electronic and data processing operations that would ordinarily take place on an in-house basis can be handled in a "cloud" computing system. Cloud computing systems can generate claims alleging data breaches and privacy violations. In addition, such arrangements have the potential to create business interruption losses.

Chapter 6
Cyber and Privacy Loss Control

Overview

As is the case with any loss exposure, despite the fact that insurance coverage has been arranged, no insurance policy can cover *every* possible aspect of all losses. Given the presence of limits, retentions, exclusions, and the administrative time required to work with insurers in settling claims, companies will end up self-insuring substantial portions of nearly every cyber and privacy loss, regardless of the existence of insurance coverage. Thus, businesses have a clear interest in preventing cyber and privacy claims. And in the event that losses cannot be avoided, such losses can, in many instances, be controlled once they occur.

Chapter Objectives

On completion of this chapter, you should be able to do the following.

- Recognize why centralizing responsibility for cyber and privacy is the crucial step in loss control.
- Recognize how to deal effectively with data and data servers.
- Identify means of reducing claim exposures.
- Recognize the threats posed by mobile devices.
- Identify threats that exist both inside and outside a business.
- Identify ways to control claims caused by emails and other messaging.

Steps To Reduce Cyber and Privacy Loss Exposures

There are a number of loss control steps that an organization can take to reduce its exposure to cyber and privacy losses.

Exhibit 6.1
13 Steps To Reduce Cyber and Privacy Loss Exposures

1. Centralize responsibility for data security.
2. Fill out an application for coverage.
3. Have a cyber audit by an outside firm.
4. Monitor and manage outside service providers.
5. Get a handle on laptops, mobile phones, and other portable electronic devices.
6. Develop and test an incident response plan.
7. Train employees on how to spot "phishing" attempts.
8. Encrypt data.
9. Design systems to handle higher-than-normal volumes of data.
10. Secure physical servers.
11. Limit online data collection.
12. Use liability disclaimers.
13. Employ email security techniques.

Centralize Responsibility for Data Security

The first step in preventing cyber and privacy losses is to create centralized responsibility for identifying and correcting weak points in an organization's computer security system. This may be the responsibility of the company's chief information officer, management information system manager, information technology (IT) manager, chief technology officer, or risk manager. The crucial point is that a *single individual* should be ultimately accountable (with the support of team members along the way, of course) for discovering and fixing any cyber and privacy-related vulnerabilities. Or, for example, within the IT department in large companies, an individual with the title of Information Security Director would have this responsibility.

Fill Out an Application for Insurance Coverage

Given the detailed nature of the questions it contains regarding a businesses' cyber-security/loss control program, an application for cyber-insurance coverage serves as a "self-audit." By completing an application for coverage, a company is compelled to assess its risks and vulnerabilities to cyber loss. The exercise also requires the applicant to *quantify potential losses* (given the questions regarding areas such as numbers of transactions, customer records, sales volumes, and business locations). Answers to these kinds of questions will help in selecting appropriate policy limits and understanding the full scope of risk. Lastly, by completing an application for coverage, support within the organization is likely to rise for an outside audit of the business—one that will provide a truly objective assessment of the company's cyber-risk profile.

Have a Cyber Audit by an Outside Firm

Only an outside expert can provide a truly objective assessment of a businesses' cyber-protection status. Insurers are excellent sources of qualified auditors, and most carriers will be more than happy to recommend a list of experienced providers.

As a complement to an outside audit, some businesses also engage "white hat hackers" who attempt to penetrate their computer systems. This exercise is yet another means of assessing the effectiveness of a company's cyber-protection system.

Frequently, there will be internal opposition to an outside audit, especially from a company's IT department, which may consider the company's cyber security and data protection regime to already be at a "state of the art level." Nevertheless, an outside audit should be insisted upon.

As a result of having had such an audit, an insurer is likely to provide a quotation for cyber and privacy coverage that affords a lower premium, higher limits, and broader coverage than if the insured had not undergone an independent review of its cyber exposures. In many cases, the prospective insured may not even have an option—some form of outside audit may be a required step in the application process, depending on the size and nature of the risk.

Monitor and Manage Outside Service Providers

Since a high percentage of data breaches and other cyber incidents result from the negligence of outside service providers, it is imperative that businesses manage these relationships effectively and in a manner that prevents losses and contractually shifts financial responsibility (to the contractor) in situations where losses are the result of the technology contractor's actions.

Limit Access

To the extent possible, businesses should limit access to their computer systems by third-party contractors. A number of high profile (and extremely costly) cyber incidents have resulted from the negligence of outside contractors, which permitted hackers to gain access to clients' computer systems.

Require Hold Harmless Agreements

Outside service providers should be required to sign hold harmless agreements in which they agree to indemnify the business if the contractor's negligence is the cause of a loss. Importantly, however, the value of such an agreement is negligible in the absence of funds available to honor the indemnification commitment and should be in the form of an insurance policy purchased by the technology provider.

Require Service Providers To Buy Technology E&O Insurance

Requiring contractors to purchase technology errors and omissions (E&O) coverage assures that funds will be available to fulfill the loss assumption obligations contained within hold harmless agreements. Businesses should be wary of dealing with technology providers that do not maintain and/or resist purchasing such coverage.

Get a Handle on Laptops, Mobile Phones, and Other Portable Electronic Devices

The Ponemon Institute's landmark study, *The Billion Dollar Lost Laptop Problem,* indicated that the 329 organizations surveyed lost more than 86,000 laptops over the course of a year. These findings, coupled with the survey *Business Risk of a Lost Laptop*, estimated that the average cost per lost laptop was $49,246, with a total annual cost amounting to more than $2.1 billion, or $6.4 million per organization. Following are some other key findings of the report.

- While 46 percent of the lost laptops contained confidential data, only 30 percent of those were encrypted.
- Only 10 percent of the laptops contained any antitheft technologies.
- 71 percent of the laptops lost did not have their data backed up.

Given the magnitude of these exposures, businesses need to provide employees with laptops, mobile phones, and other portable electronic devices that do the following.

- Uses strong passwords (i.e., a minimum of 12 characters, with at least one capital letter, one number, and one special character)
- Employs two-factor authentication (e.g., users are prompted to enter an SMS code that is texted to them before they can complete the sign-in process on their laptop)
- Is equipped with antivirus software
- Adequately encrypts and backs up data

- Follows the “least privilege” security principle (i.e., individual users only have access to documents and programs that they truly need access to, as opposed to broad access to all company files)

Develop and Test an Incident Response Plan

As referred to earlier in this course, the average cost per stolen electronic record is around $160. Yet, when a company that suffers a breach has an incident response plan in place, the per-record cost can often be reduced by nearly 10 percent. This difference matters considerably when millions of records are involved. The specific aspects of such a plan should include the following.

- **A written plan** noting exactly what must be done in responding to an incident and then restoring operations as quickly as possible.
- **A public relations strategy** explaining how the company will respond to/manage customer complaints in the event of a shutdown. The strategy should indicate the name of a public relations (PR) agency and with whom a contract has already been negotiated. PR agencies may also be utilized through a company's cyber-insurance policy (i.e., they can rely on the PR agencies that are partnered with their insurer).
- **A formal test of the plan.** It does no good to have a written plan that merely sits on a shelf. Therefore, the response plan should actually be tested at some point. Many cyber insurers offer services in which insureds can participate in guided "tabletop" exercises to walk through hypothetical incidents with cyber-security experts.

Train Employees on How To Spot Phishing Attempts

A high percentage of data breaches are caused by "phishing," a technique already described in Chapter 4. Phishing is used as a sort of preliminary step to implant malware and/or steal entry credentials. Phishing is also employed as a means of requesting fund transfers, a technique known as "social engineering."

Fortunately, many effective software training packages are now available that teach employees how to recognize phishing emails. After completing these training modules, employees should then be sent follow-up mock phishing emails as a test of whether they immediately recognize them as phishing attempts. Falling for the mock phishing email should result in a constructive follow-up in which the employee learns what red flags should have signaled the email's illegitimacy.

Encrypt Data

Encryption software scrambles data, making the data difficult, if not impossible, to decipher. Encryption is an excellent risk control technique because it is both inexpensive as well as relatively easy for an IT department to implement.

Design Systems To Handle Higher-than-Normal Volumes of Data

A website that can handle significantly more traffic than normally anticipated makes a company less

vulnerable to distributed denial-of-service attacks by hackers or competitors who attempt to flood a system with traffic (i.e., “spamming”) in an effort to shut it down.

Secure Physical Servers

Access to a business’ servers should be strictly limited. In addition, companies need to use locks, as well as all standard hazard protections, including halogen fire protection systems, to protect servers and the rooms in which they are housed.

Limit Online Data Collection

Web servers retain a great deal of information about website visitors’ personal information (e.g., what site they came from, browsing preferences, some demographic data, and so on). Businesses should know exactly what information is being collected and stored, and both should be minimized. This is especially true in light of the European Union’s General Data Protection Regulation (GDPR), which implemented much more strict guidelines on data protection and privacy and can extend to anyone doing business with customers in the European Union.

Credit card and payment data should also be erased when it is no longer needed. These techniques will go a long way in mitigating privacy claims down the road.

Use Liability Disclaimers

Liability disclaimers can limit a company’s liability to customers in the event that third parties illegally obtain their customers’ PII, although these disclaimers are by no means bulletproof. A business should prominently post liability disclaimers on customer-facing mediums.

Employ Email Security Techniques

Employees should be advised to use caution when communicating via email since documents traveling over the Internet are not secure unless encrypted. Security concerns are legitimate but addressable. Corporations are wise to invest in encryption software and to develop email guidelines that reduce the odds of interlopers intercepting sensitive information on the Internet.

Exhibit 6.2
Email Security Techniques

1. **Use common sense and discretion.** Do not put anything in an email that you would not want printed on the front page of your local newspaper or read aloud in a courtroom, since email messages are discoverable in litigation.
2. **Do not use for sensitive items.** Do not use email for sensitive, risk-related information, such as conveying proprietary data. This is particularly true with attachments to emails, which can often involve highly sensitive documents. Such documents should be shared in a more secure way (e.g., via file sharing services built for sending sensitive, secured information between parties).
3. **Recognize the lack of security in email communications.** Remember that, in general, emails are often no more secure than communications sent through nonelectronic means. This should temper the sending of message content that could be considered "extreme."

Summary

There is no single technique or method to reduce the threat of cyber and privacy claims. However, by adhering to the program laid out in this chapter, an organization will vastly reduce the threat of sustaining a loss. These approaches include (1) centralizing responsibility for data security, (2) filling out an application for cyber insurance coverage, (3) having a cyber audit by an outside firm, (4) monitoring and managing outside service providers, (5) getting a handle on laptops, mobile phones, and other portable electronic devices, (6) developing and testing an incident response plan, (7) training employees on how to spot phishing attempts, (8) encrypting data, (9) designing systems to handle higher-than-normal volumes of data, (10) securing physical servers, (11) limiting online data collection, (12) using liability disclaimers, and (13) employing email security techniques.

Chapter 7
Underwriting Cyber and Privacy Insurance

Overview

Underwriting cyber and privacy insurance presents a number of challenges. First, the forms cover a wide variety of both property and liability exposures, including information security, privacy, and content liability. In addition, cyber and privacy policies also cover a number of first-party property losses, including business interruption, extra expense, and various types of cyber-related crime perils, such as cyber extortion and electronic fraud (to name a few). Also, compared to other, more established lines of insurance, insurers lack a substantial database of specific types of losses on which to price certain insuring agreements. Lastly, the nature of the cyber and privacy exposure is rapidly evolving, requiring extra vigilance from the market to utilize appropriate policy wording and pricing so as to manage loss ratios.

Chapter Objectives

On completion of this chapter, you should be able to do the following.

- Recognize how cyber and privacy policies are rated and priced.
- Identify the various factors underwriters use to modify basic rates.
- Recognize other factors considered in the underwriting decision-making process, which include internal security measures, personnel policies and procedures, information security approaches, the nature of a company's website and content information, the extent to which it transfers its cyber and privacy risks to technology providers by contractual means, and loss history.

Pricing Cyber and Privacy Policies

Compared to more "traditional" lines of insurance, cyber and privacy coverage is a relatively new form of insurance, having been introduced in the early 2000s. Therefore, even the largest insurers lack a substantial amount of historical loss data. Thus, pricing such policies is at times a fairly subjective process and, in part, dependent on an underwriter's individual judgment concerning any particular risk.

Rating Base

Premiums for each of the different insuring agreements correlate with, though they are not directly based upon, the size of a business's assets and/or its number of electronic records, in combination with the business's tangible cyber-security practices, loss history, industry, and more. Like other lines of insurance, policy premiums are adjusted annually to reflect changes in actual exposure.

Pricing Is on a Per-Insuring Agreement Basis

It should be recognized that cyber and privacy coverage is priced on a per-insuring agreement basis. That is, a separate rate will be applied to *each* of the coverages selected under a policy. For example, a cyber-policy form may contain the following eight insuring agreements.

- Network Security Liability Coverage
- Privacy Liability Coverage
- Privacy Breach Expenses Coverage
- Regulatory Fines and Proceeding Coverage
- Internet Media Liability Coverage
- Digital Asset Expenses Coverage
- Business Interruption and Income Loss Coverage
- Network and Data Extortion Threat and Reward Payments Coverage

An insured could conceivably select anywhere from just one all the way up to eight different coverages, each of which carries a different rate. Moreover, the final premium for each coverage selected will be modified by the limit and retention selected, since different limits/retentions are available for each of the eight available coverages.

Annual Aggregate Limit

Lastly, in addition to pricing the policy's individual insuring agreements, cyber and privacy forms are also subject to an annual aggregate limit, which is separately rated.

Modification Factors

The pricing of cyber/privacy coverage is sometimes subject to modification, based on several factors, which include the following.

- Network security measures
- Personnel, policies, and procedures
- Information security
- Website and content information
- Extent of contractual risk transfer
- Loss history

Network Security Measures

Underwriters will look favorably on applicants that (1) have a designated chief security officer who is responsible for the firm's computer systems; (2) have a formal program to test or audit network security controls; (3) use firewall technology; (4) use both antivirus and encryption software that is installed on all of their computer systems, including (a) laptops, (b) personal computers, and (c) networks; (5) use intrusion detection software to detect unauthorized access to internal networks and computer systems; (6) have adopted a corporate policy to upgrade all security software as new releases or improvements become available; (7) provide remote access to their network using a virtual private network; (8) use a multi-factor authentication process or a layered security approach to verify the identity of a customer or authorized user when granting access to secure areas of the company's website; (9) use remote deposit capture technology when sending or accepting financial transactions intended for deposit; (10) (a) have a disaster recovery plan, (b) have a business continuity plan (c) have an incident response plan for network intrusions and virus incidents, and (d) test such plans regularly; (11) have a secondary computer system or site available if the primary system becomes inoperative and (a) are able to operationalize such secondary resources immediately and (b) have designed the secondary system so it can handle a high percentage of the company's operations; and (12) back up all valuable and sensitive data on a regular basis.

Personnel, Policies, and Procedures

Insurers seek to insure companies that (1) regularly conduct training on security issues and procedures for employees who utilize computer systems, (2) publish and distribute written computer and information systems policies and procedures to their employees, (3) terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company, and (4) have a formal documented procedure in place for creating and periodically updating passwords used by employees and

customers.

Information Security

The manner in which an applicant handles its data is another critical factor that underwriters evaluate.

Types of Data Maintained

First, an insurer is interested in learning about the actual types of data collected by a company. Such data types include (a) credit/debit card numbers, (b) Social Security numbers, (c) intellectual property belonging to others, (d) medical information, (e) employee/human resources information, (f) bank accounts and records, and (g) customer information.

Number of Individual Records

Next, underwriters seek the number of individual records containing one or more types of the preceding types of information that an applicant company stores. The smallest risks often have fewer than 1,000, whereas the largest may have in excess of 100 million. Of course, the larger the number of stored records, the more premium an underwriter may require for a given limit of liability.

Information Security Procedures

Once an underwriter has ascertained the *type(s)* and *number* of personal records that a company maintains, they are then concerned about specific procedures that apply to such data. More specifically, the insurer will favor an applicant that (1) has written procedures in place that comply with laws governing the handling and disclosure of such information, and (2) requires service providers who may have access to the applicant's company's confidential information (or personally identifiable information (PII) belonging to its customers) to demonstrate that they maintain adequate security policies and procedures.

Encryption and Storage

The manner in which data is stored has an important bearing on an underwriter's assessment of an applicant. Specifically, insurers want to know (1) whether user-specific, private, sensitive, or confidential information stored on the applicant's servers is encrypted, (2) if the applicant has a procedure for the secure handling, care, and storage of the private, sensitive, and confidential information stored on portable communications equipment, and if so, (3) what percentage of the data maintained on portable communications equipment is encrypted.

Data Sharing and Outside Access

The underwriter is also interested in (1) the extent to which and form in which an applicant company shares its sensitive, private, or personal information (that it gathers from customers) with third parties and service providers and, to the extent the company does collect such information, (2) whether the company requires service providers/third parties to demonstrate that they employ adequate security procedures.

Website and Content Information

The process of assessing the risks inherent in the content provided by an applicant's website requires an underwriter to evaluate a number of areas.

Website Type

The underwriter begins by ascertaining the type of website the company provides. The following are among the major types.

- **Information-only** (provides general information about the applicant's products/services)
- **Accessible** (has login capabilities allowing access to secure or restricted content, such as accounts, subscriptions, or profiles, and allows the user to upload or download secure data)

- **Transactional** (accepts orders or purchases using credit/debit cards, accepts bill payment, and allows customers to view account balances and statements or transfer funds between accounts)

Companies operating "information-only" websites will be charged a lower rate than those with "accessible" websites, which, in turn, pay a lower rate than do companies maintaining "transactional" websites.

Types of Material Provided

The type of material provided on a company's website influences the premium it is charged for coverage. The following types of website content are among the most popular.

- Music/sound clips
- Forums/message boards/blogs
- Executable programs
- Movies/movie clips
- Advertising of others' products
- Interactive gaming/games of chance
- Sweepstakes or coupons
- Sexually explicit material
- Content specifically targeted at minors

Each of these nine types would likely carry a different rate.

Legal Procedures

Underwriters seek applicants that have a written intellectual property clearance procedure for content disseminated on their website. Such procedures should include (1) screening content by a qualified attorney; (2) screening content for (a) disparagement issues, (b) copyright infringement, (c) trademark infringement, and (d) invasion of privacy; (3) obtaining agreements with outside content providers or consultants that include provisions granting the applicant company ownership of the intellectual property rights in any work for hire supplied by the outside consultant/provider; (4) requiring employees and independent contractors to sign a statement that they will not use previous employers' or clients' trade secrets or other intellectual property; (5) obtaining the written permission of any website to which the applicant company links or frames; (6) providing evidence of a formal procedure (a) to review all content prior to posting and (b) for editing or removing controversial, offensive, or infringing material from material distributed, broadcast, or published by or on behalf of the applicant; (7) responding to allegations that content created, displayed, or published by the applicant is libelous, infringing, or in violation of a third party's privacy rights; and (8) screening all trademarks used by the applicant for infringement with existing trademarks prior to first use.

Underwriters seek information about whether the company collects any data from children, and if so, the applicant must describe the method used to secure parental permission.

Extent of Contractual Risk Transfer

The extent to which a client company has obtained indemnity agreements from the technology providers with which it has significant relationships should be considered in pricing decisions made by an underwriter of cyber and privacy coverage. Additionally, the fact that technology providers maintain an insurance policy to cover the liabilities they have assumed is also a factor that should reduce the premium charged by the underwriter. This is indicated by the example below.

An Example

A bank enters into an agreement with a cloud computing provider in which the provider will handle all of

the bank's computer system and data processing needs. As part of the agreement, the cloud computing firm also assumes full responsibility for all loss that is the result of its sole negligence. To back this assumption of liability, the provider agrees to maintain a technology errors and omissions (E&O) policy with a $10 million limit.

Two months after the agreement goes into effect, a hacker gains access to the bank's systems and transfers $5 million from the bank to an account in the Cayman Islands. A post-loss forensic expert's investigation reveals that the breach was the result of a fully preventable vulnerability in the cloud provider's system. In other words, the loss was caused by the provider's negligence.

Accordingly, the bank will, in theory at least, be able to obtain indemnification from the cloud provider's insurance policy rather than its own cyber and privacy insurer. Alternatively, the bank's cyber and privacy insurer will be able to subrogate against the cloud provider after it pays the $5 million loss to the bank. Either way, the cloud provider's liability assumption, coupled with the existence of a technology E&O policy, vastly reduces the cyber and privacy underwriter's exposure to loss.

Loss History

Prior claim history is a key element in evaluating an applicant for cyber and privacy liability. In addition to charging a higher-than-usual premium as a result of a poor claim record, insurers also sometimes impose larger-than-normal retentions on a company that seeks coverage under these circumstances. In a hard market, insureds with a subpar cyber-loss history may even face nonrenewals and have trouble finding coverage at all (or at least not at a premium they deem to be affordable).

Frequency Matters More than Severity

However, underwriters are typically more concerned about frequency than severity. A frequency problem is more indicative of a poor risk than is a single major claim in which unusual circumstances, rather than gross negligence, produced a high-dollar loss. And *after* such a loss, underwriters are especially interested in learning the nature of the protective measures that a company has taken to prevent future occurrences of a similar nature.

Details of Prior Losses

Underwriters want to know if an applicant has had any claims, incidents, or reports of circumstances involving the following.

- **Unauthorized access** to confidential information, failing to notify appropriate individuals of any such unauthorized access, or failing to allow authorized users access to the applicant's computer systems
- **Dissemination of content** on or via the applicant's websites or company email that infringed on the intellectual property rights of another party or caused harm to the reputation of another party
- **Extortion attempts** or demands involving its computer systems, or suffering a loss of money, securities, or other property due to fraud committed by means of unauthorized access to or fraudulent entry into computer instructions or code, by someone other than an employee
- **Intrusions,** such as unauthorized access, security breach, and denial of service attacks, that impaired the functionality of its computer systems
- **Circumstances or incidents** that have not yet given, but could potentially give, rise to a claim against the applicant under the insurance policy for which the applicant is applying (Of course, any known incidents of this kind will not be covered by a policy issued to the applicant.)

Summary

Underwriting cyber and privacy coverage is a challenging endeavor since it encompasses both property and liability coverages, the need to work with limited historical loss data, and new, emerging sources of loss.

In developing rates for cyber and privacy policies, underwriters begin by grouping a risk into a broad hazard class. Then, within that class, they apply a specific rate for *each* of the individual insuring agreements selected by the insured. Finally, a separate rate is applied to the policy's annual aggregate limit.

The last step of the underwriting process involves modifying these basic rates, according to the following factors particular to the risk.

- Network security measures
- Personnel, policies, and procedures
- Information security
- Website and content information
- Extent of contractual risk transfer
- Loss history

Chapter 8
Cyber and Privacy Insurance: An Overview of the Insuring Agreements within a Cyber and Privacy Policy and the First-Party Post Breach Response Insuring Agreement

Overview

This chapter will provide an overview of the most common insuring agreements found within cyber and privacy insurance policy forms. In addition, this chapter analyzes the insuring agreement covering privacy notification and crisis management expenses.

Chapter Objectives

On completion of this chapter, you should be able to do the following.

- Identify the 13 types of insuring agreements found within cyber and privacy policy forms and classify them into one of four coverage categories.
- Recognize the major coverage components found within the insuring agreement providing privacy notification and crisis management expense coverage.
- Recognize loss scenarios in which the privacy notification and crisis management insuring agreement would apply.
- Recognize why the privacy notification and crisis management insuring agreement is often considered the single most important insuring agreement contained within cyber and privacy policies.

The 13 Types of Insuring Agreements within Cyber and Privacy Policies

There are 13 different insuring agreements typically contained within cyber and privacy policy forms, which appear in the following chart.. These insuring agreements will be analyzed in subsequent chapters of this course.

13 Key Insuring Agreements	
Coverage Type	Insuring Agreement
First-Party/Post Breach Response Coverage	1. Privacy Notification and Crisis Management Expense
Third-Party/Liability Coverages	1. Information Security and Privacy Liability 2. Regulatory Defense and Penalties 3. Payment Card Industry Fines and Assessments 4. Website Media Content Liability 5. Bodily Injury and Property Damage Liability
First-Party/Time Element Coverages	1. Business Interruption 2. Extra Expense
First-Party/Theft of Property Coverages	1. Data Assets 2. Cyber Extortion 3. Computer Fraud 4. Funds Transfer Fraud 5. Social Engineering/Fraudulent Instruction Coverage

Cyber and Privacy Policies Use a "Menu" Approach

It should also be recognized that few insurers offer all 13 of these insuring agreements within their policy forms. For example, many insurers do not offer any of the first-party time element or first-party theft of property insuring agreements. (This is because they consider cyber and privacy policies to function solely as third-party liability insurance and as coverage for response to a data breach, rather than a type of insurance to cover property.)

When purchasing cyber and privacy policies, an insured has the opportunity to buy any number of insuring agreements, depending upon which of these insuring agreements a specific insurer offers. For example, referring to Exhibit 8.1, Insurer X's policy may only include insuring agreement numbers 1, 2, 3, 7, 9, and 10. From this list, an insured could then conceivably buy any number of these insuring agreements.

Categories of Insuring Agreements

It is also important to recognize that these 13 insuring agreements can be classified within one of four categories.

- First-Party/Post Breach Response Coverage
- Third-Party/Liability Coverages
- First-Party/Time Element Coverages
- First-Party/Theft of Property Coverages

Additionally, each of the 13 insuring agreements contains the following.

- A separate per-claim limit

- A separate per-claim deductible

Lastly, cyber and privacy policies are written with an annual aggregate limit of coverage. This annual aggregate is the most that an insurer will pay in overall losses sustained during a policy period. Generally, the annual aggregate limit is the total of the per-claim limits for all of the individual insuring agreements that an insured has purchased.

The 13 Insuring Agreements: Complications and Caveats

As already explained, few, if any, of the insurers in today's market write policies that contain *all* 13 insuring agreements. Rather, the typical policy contains roughly five to eight insuring agreements.

In fact, coverage for cyber-related bodily injury and property damage is available by buying an *entirely separate* policy form.

Cyber and Privacy Policies: The Essence of Nonstandard Coverage

At this juncture, it should be apparent that there is no standard cyber and privacy policy—a fact that makes them exceedingly difficult to compare on a side-by-side basis.

Identical Coverage, Varying Terminology

To complicate matters even further, different insurers use different terminology to identify what are essentially *the same* insuring agreements. For example, one insurer uses the term "E-Threat Coverage" to identify the insuring agreement covering situations in which an insured's computer network is threatened with severe damage unless a ransom is paid. Another insurer, offering virtually identical coverage, uses the name "Cyber Extortion Coverage" to designate this kind of insurance. While this may happen to some degree across other lines of insurance, cyber-related terminology has a tendency to be more unclear about what exactly is being covered.

Combining Insuring Agreements

Even more confusing is the fact that some insurers *combine* coverage found within one or more of these 13 insuring agreements into a *single* insuring agreement. For example, a handful of insurers write policies that combine coverage for both regulatory defense and penalties (insuring agreement 3 in Exhibit 8.1) with the coverage provided by privacy notification and crisis management expense (insuring agreement 1 in Exhibit 8.1) within *one* insuring agreement.

Splitting Up Insuring Agreements

Yet again, certain insurers offer singular coverage elements that are almost always combined with other coverages elsewhere. Case-in-point, normally, crisis management expense coverage (i.e., the cost of hiring a public relations firm following a data breach) is one of the coverage elements found within the privacy notification and crisis management expense insuring agreement. Despite this, several insurers provide crisis management expense coverage as an *entirely separate* insuring agreement.

Privacy Notification and Crisis Management Expense Coverage

This insuring agreement covers the direct expenses required to respond to a data breach immediately after it occurs. Accordingly, privacy notification and crisis management expense coverage functions as the "loss containment" or "loss minimization" element of a policy. The specific items it covers include, but are not necessarily limited to, the following costs.

- **Computer Forensics.** Hire a computer forensics expert to suggest measures that will (1) secure the insured's information system immediately following a breach, (2) determine the cause of the breach, and (3) offer advice on how to prevent future breaches, items collectively referred to as "remediation."
- **Public Relations and Crisis Management Assistance.** Engage a public relations firm to guide the insured during the early days following the breach and assist in communicating with the public about the breach.
- **Call Center.** Set up and provide access to a post-breach call center, allowing customers to receive up-to-the-minute details about the breach and learn how their PII may have been affected by it.
- **Notification.** Notify affected customers that their personally identifiable information (PII) has been compromised, a need driven largely by the applicable, state-specific notification requirements, which is, in turn, a function of the state in which the customer resides rather than the location of the insured's business.
- **Credit Monitoring.** Monitor affected customers' credit (usually for 1 year).
- **Identity Theft Monitoring.** Provide identity theft monitoring, a service that is even more comprehensive than credit monitoring. The latter only detects situations where a "bad actor" attempts to open new or use existing credit lines, whereas identity theft monitoring can detect additional fraudulent uses of PII.
- **Bank Notification.** Notify banks and credit card companies whose credit card numbers have been compromised.

Privacy Notification and Crisis Management Expense Coverage: The Single Most Important Insuring Agreement

Industry observers have often asserted that the privacy notification and crisis management expense insuring agreement is the single most important insuring agreement found within a cyber and privacy policy. This is because notification and crisis management expense coverage provides an insured with access to insurer's expertise in the hours/days immediately following the discovery of a data breach, which is termed "breach coaching."

Because few insureds have the know-how to deal with the complexities of a data breach, an insurer's

assistance is especially valuable during this critical period of time. The more efficiently and effectively a company's immediate response to a data breach is, the lower its overall loss will be. Usually, if the immediate response to a data breach is handled well, such actions will minimize the company's business interruption loss, loss of critical data, and the extent of its ultimate liability to its customers for the breach of their PII. For these reasons, the notification and crisis management expense insuring agreement is often considered the single most important coverage contained within cyber and privacy policies.

Claim Scenario

To place the magnitude of the costs covered by the privacy notification and crisis management insuring agreement in perspective, a large retailer reported that it incurred $28 million in breach response costs (such as forensics, public relations, notification of customers/banks, and credit/identity monitoring) as a result of the data breach suffered by the company.

Chapter 9
Cyber and Privacy Insurance: Third-Party Liability Insuring Agreements

Overview

This chapter will examine the insuring agreements written to cover the five major types of third-party cyber and privacy liability loss exposures, which include the following.

1. Information security and privacy liability
2. Regulatory defense and penalties
3. Payment card industry fines and assessments
4. Website media content liability
5. Cyber-related bodily injury and property damage liability coverage

Chapter Objectives

This chapter discusses the four major types of third-party liability loss exposures. On completion of this chapter, you should be able to do the following.

- Recognize the nature of the insuring agreement commonly used to cover each exposure.
- Identify the manner in which the insuring agreement applies to given claims scenarios.
- Recognize the key coverage limitations and extensions associated with each of these insuring agreements.

Information Security and Privacy Liability Coverage

This insuring agreement covers the insured's liability for the following.

- Failure to prevent the *loss, theft, or unauthorized disclosure* of personally identifiable information (PII) that is (a) in its own care, custody, or control or (b) is in the care, custody, or control of a third party for which the insured is responsible. An example of the latter instance could involve a corporate wellness plan vendor that collects the data produced by annual employee health screenings. If such data were to be breached, the information security and privacy liability insuring agreement would cover an insured corporation's *vicarious liability* for the negligence of the wellness plan vendor in allowing the data to be accessed.
- Failure to prevent (a) damage to data *stored* on the insured's computer systems, (b) the *transmission of malicious code* from the insured's computer to a third party's computer, or (c) the *denial of service* to a third party's computer system.
- Failure to timely disclose a data breach incident in violation of any *breach notification law.*
- Failure to comply with its own privacy policy that prohibits or restricts (a) the *disclosure, sharing, or selling* of a person's personally identifiable nonpublic information, (b) *failure to correct* incomplete or inaccurate personally identifiable nonpublic information after a request is made by a person, or (c) *failure to prevent the loss* of personally identifiable nonpublic information.
- Failure to administer an *identity theft prevention program* required by governmental statute or regulation or failure to take necessary actions to prevent identity theft, including phishing.

The key point to recognize with regard to the information security and privacy liability insuring agreement is that it applies *only* when the legal liability of the insured is *either* established by a court of law *or* to pay on behalf of an insured business that has entered into a settlement with a claimant. This is in contrast to the notification and crisis management expense insuring agreement (discussed previously in Chapter 8), which makes payments to claimants on a *voluntary basis* (i.e., prior to receiving a legal demand) for items such as credit and identity monitoring. In effect, coverage under the information security and privacy liability insuring agreements is driven by the insured's legal liability rather than by the insured's voluntary actions.

Claim Scenario

A hacker gains access to a retailer's computer system. As a result, she obtains the names, addresses, Social Security numbers, and driver's license numbers (all of which constitute PII) belonging to 100,000 of the company's customers. After the breach becomes public knowledge, a class action lawsuit is brought against the retailer by a number of the customers whose PII was obtained by the hacker. In this situation, the information security and privacy liability insuring agreement will provide coverage for

actual damages incurred by the customers (e.g., their PII is used for identity theft, which the thief uses to empty the customers' bank accounts). If the retailer is found legally liable for the breach and must pay a settlement or judgment to the plaintiffs (as well as the costs incurred in defending the claim), this insuring agreement will cover these items.

"Intrusion" but No Theft of Data: Does Coverage Apply?

A few insurers' information security and privacy liability insuring agreements provide coverage only when there is an actual theft of data, such as in a Target-type data breach (i.e., when credit and debit card numbers were stolen). On the other hand, such policies do not afford coverage when there is a mere "intrusion" with no actual theft.

Two examples of intrusions that *do not* involve theft include (a) the introduction of a virus into a computer system (with the intention of damaging or corrupting data stored within the system) and (b) a "spam" attack (in which a computer system is intentionally flooded with a massive number of emails intending to "crash" the system and shut it down).

In both cases, an insured's website could cease to function, producing various kinds of losses, such as a denial of service to subscribers to an online data service, yet without the actual theft of data.

From an insured's standpoint, it is, of course, preferable if the scope of coverage under the Information Security and Privacy Liability insuring agreement *also* includes loss resulting not only from theft, but also from electronic "intrusions" and "disruptions," such as those sustained in these last two examples.

Regulatory Defense and Penalties Coverage

This insuring agreement covers the costs of dealing with regulators who oversee state and federal data breach laws, as well as laws governing protected, personal health data, such as the Health Insurance Portability and Accountability Act (HIPAA).

The two key components of this insuring agreement include (1) coverage for the costs of the legal defense required by regulatory actions and (2) payment of the fines and penalties that may be levied against an insured by various regulators.

Dealing with Multiple Regulatory Agencies: An Insured's Worst Nightmare

Regulatory defense and penalties coverage is especially valuable because a data breach normally involves having to deal with multiple sets of regulators. This is because, at the time of writing, 47 of the 50 states have their own separate laws enumerating a business's obligations to its customers and the general public immediately following a data breach.

Recognize, too, that state regulatory authorities become involved in a data breach whenever residents of their state are affected. Thus, a business located in a given state will not merely be compelled to deal with regulators in the company's principal state of business. In addition, the company will be required to report the breach to state regulators in every state where its customers are located—a fact that vastly increases the number of state regulatory authorities, which a business must deal with after a major data breach.

In addition to state regulators, there are a number of federal regulatory agencies that oversee data breaches, including the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), and the Department of Justice (DOJ).

By purchasing the regulatory defense and penalties insuring agreement, an insured will benefit from its insurer's network of regulatory-savvy defense attorneys.

Affirmative Coverage for Fines and Penalties

It is also important to point out that the regulatory defense and penalties insuring agreement provides one of the few types of insurance that *affirmatively covers* fines and penalties; items otherwise considered uninsurable (and thus excluded) under most other kinds of insurance coverage. (Note that some insurers' policies offer coverage for fines and penalties, but only by endorsement, and for an additional premium.)

Claim Scenario

As an example of how costly data breach-related fines and penalties can be, one company agreed to pay a $25 million penalty to the Federal Communications Commission (FCC) for having exposed the PII of 280,000 of its customers. These are precisely the kinds of costs that are commonly covered under the Regulatory Defense and Penalties insuring agreement.

Payment Card Industry Fines and Assessments Coverage

This insuring agreement covers fines and penalties assessed against the insured (although only to the extent that such fines and penalties are insurable by law) incurred in conjunction with a claim made against the insured by a credit card company, alleging that the insured *did not* comply with payment card industry data security standards. Such claims most often arise in response to a wrongful act covered under

a cyber and privacy policy's information security and privacy liability insuring agreement (discussed in detail above).

Payment Card Industry Data Security Standards

Payment card industry data security standards are a set of proprietary information security standards for businesses that accept payment from the leading credit cards, including Visa, MasterCard, American Express, and Discover. Payment card industry fines and assessments coverage is offered by a minority of insurers, although its presence within cyber and privacy policies has been increasing.

Affirmative Coverage of Fines and Penalties

Just as the regulatory defense and penalties insuring agreement affirmatively covers fines and penalties, so too does the payment card industry fines and assessments insuring agreement. Once again, this insuring agreement is one of the few types of insurance that affirmatively covers fines and penalties; items otherwise considered uninsurable (and thus excluded) under most other kinds of insurance coverage.

Insuring Agreement also Covers Defense

This insuring agreement also covers the cost of defending the insured if the insured believes that it did not violate industry standards and that the loss suffered by the credit card issuer was not the result of a failure to follow such standards.

Claim Scenario

A merchant processes a $5,000 transaction that used a fraudulent credit card. (The card had been stolen and then used by the thief to make purchases.) As a result of having accepted the stolen card, the merchant is fined for having violated payment card industry standards. The payment card industry fines and assessments insuring agreement will cover the fine as well as the defense costs that the merchant incurs if the merchant decides to challenge the imposition of the fines (because she believes she followed applicable standards when processing the transaction).

Website Media Content Liability Coverage

This insuring agreement affords coverage when the insured incurs liability in conjunction with material published on its website. More specifically, it covers claims alleging four broad types of claim allegations.

- **Personal injury,** such as defamation, libel, slander, trade libel, infliction of emotional distress, and invasion of privacy, including an invasion or interference with an individual's right of publicity
- **Commercial/intellectual property violations,** including plagiarism; piracy; misappropriation of ideas under implied contract; copyright infringement; and infringement of domain name, trademark, trade name, trade dress, logo, title, meta-tag, slogan, service mark, or service name
- **Other improper Web-based activities,** including improper deep linking or framing within electronic content
- **Social media liability** resulting from activities engaged in on sites such as Facebook, LinkedIn, Twitter, Snapchat, and others

Claim Scenarios

The following claim scenarios illustrate potential claims in each of the aforementioned four categories.

Personal Injury

A health insurance company accidentally posts to its website private medical information about several patients without first obtaining a release from the patients. This would constitute an invasion of privacy, which is a type of personal injury.

Commercial/Intellectual Property Violations

An online retailer's website incorporates a photo from a commercial photographer. The commercial photographer brings a lawsuit against the retailer alleging copyright infringement on the basis that the retailer failed to license the material.

Other Improper Web-Based Activities

A publishing firm provides information on human resources policies and procedures to its customers. Its online material contains a number of links to a human resources consulting firm's website. The consulting firm sues the publishing firm, alleging that the links violate the consulting firm's intellectual property rights because the links enhance the publishing firm's website without providing compensation to the consulting firm. (This is known as "improper deep-linking.")

Social Media Liability

The president of a company posts a business-related "how to" article on LinkedIn that is virtually identical to an article published a year earlier by another author. The author brings a claim of plagiarism

against the company president.

Website Media Content Liability Coverage: Does Not Respond to Data Breaches

One oddity concerning the website media content liability insuring agreement is that unlike the other 12 insuring agreements discussed in this course, it is the only one that covers losses caused neither by data breaches nor by electronic intrusions.

Consider Buying a "Traditional" Media Liability Policy That Covers Website and Social Media Activities

In reality, the website media content liability insuring agreement functions much like a "traditional," stand-alone media liability policy, but with one key difference—it only covers media-type liability incurred from website activities. As a result, the website media content liability insuring agreement's main drawback is that it provides no coverage for nonwebsite media activities (e.g., paper publishing, broadcast media, public appearances). For this reason, it may be more advantageous for an insured to simply buy a traditional, comprehensive media liability policy that also includes coverage for liability incurred as a result of the company's website activities.

Only about half of all cyber and privacy insurers offer website media content liability coverage.

Cyber-Related Bodily Injury and Property Damage Liability Coverage

Coverage for cyber-related bodily injury (BI) and property damage (PD) liability is necessary because (as will be discussed in Chapter 13 of this course) cyber and privacy insurance policies universally exclude coverage for direct bodily injury and property damage liability caused by cyber intrusions.

An Example

A hospital's computer system is breached, causing it to shut down. As a result, for 8 hours, the hospital is unable to remotely monitor the patients in its cardiac unit. During this period of time, three patients suffer fatal heart attacks because changes in their conditions could not be ascertained, and thus, they were not given immediate, necessary treatments. Lawsuits are later brought by the patients' estates against the hospital, alleging that the hospital's negligence in failing to prevent the intrusion into its computer system caused the patients' injuries.

Although there is no coverage for cyber-induced BI and PD liability within cyber and privacy policy forms (given the bodily injury and property damage liability exclusion noted earlier), the hospital would have coverage for claims of this nature under its commercial general liability (CGL) and umbrella liability policies. This is because such forms affirmatively cover liability for bodily injury and contain no exclusions for cyber-induced claims of this type.

Why Is Coverage for Cyber-Related Bodily Injury and Property Damage Liability Necessary?

So why, then, is coverage for cyber-related bodily injury and property damage liability even necessary? There are two reasons, which are explained below.

First, it is very possible that in the future, CGL policy forms may begin to exclude coverage for bodily injury and property damage liability claims arising from cyber incidents. Or even if standard CGL wording continues to cover cyber-related BI and PD liability, underwriters may selectively add exclusionary wording to policies, especially those covering high-severity risks, such as those involving construction, healthcare, and energy-related businesses.

Second, even if a CGL form does not exclude such coverage, in a catastrophic claim situation (as in the hospital example above), typical $1–$5 million CGL policy limits (even when augmented by an umbrella policy) may not provide adequate coverage.

Cyber-Related Bodily Injury and Property Damage Liability Coverage Details

In April 2014, AIG introduced a policy form, known as CyberEdge PC, which provides coverage for

cyber-related BI liability and PD liability. (A handful of other insurers have introduced similar policy forms covering cyber-related BI and PD-related liability, and it is expected that additional carriers will do likewise in the near future.)

Yet another important feature of the AIG policy is that it applies on both (1) an excess and (2) a difference-in-conditions (DIC) basis. This means that first, the policy does not pay until underlying applicable policy limits (i.e., as afforded by CGL and/or umbrella policies) are exhausted. Second, the DIC coverage aspect means that the policy will "drop down" and, thus, provide coverage in the event that the underlying CGL and/or umbrella policies contain cyber-related BI and/or PD-related cyber exclusions or other coverage restrictions.

Summary

This chapter examined the insuring agreements found within cyber and privacy policies, written to cover four specific types of third-party liability exposures.

1. Information security and privacy liability
2. Regulatory defense and penalties
3. Payment card industry fines and assessments
4. Website media content liability
5. Cyber-related bodily injury and property damage liability

Each exposure is addressed by a separate insuring agreement found within cyber and privacy liability policies.

Chapter 10
Cyber and Privacy Insurance: First-Party Time Element Insuring Agreements

Overview

The two major types of first-party time element insuring agreements include the following.

- Business interruption
- Extra expense

Chapter Objectives

On completion of this chapter, you should be able to do the following.

- Identify the insuring agreement commonly used to cover first-party property time element loss exposures.
- Recognize the manner in which the insuring agreement applies to a given claims scenario.
- Recognize the key coverage limitations and extensions associated with each of these insuring agreements.

Cyber and privacy insurance policies provide two types of time element insuring agreements**:** business interruption (BI) and extra expense (EE)**.**

It is important to recognize, however, that many insurers do not offer time element coverages. This is because, philosophically, they view cyber and privacy insurance as a liability/third-party coverage and as a means of providing breach response cost coverage rather than first-party/property-type insurance. Other underwriters offer time element coverages, but by endorsement and not within their standard policy forms.

Business Interruption Coverage

This insuring agreement covers the insured's "business interruption loss" sustained during the "period of recovery" (or the "extended interruption period") that results from a "material interruption" caused by a "computer system disruption." A BI loss occurs when an insured sustains a loss of income if, for example, its order-taking system is unable to function because of a virus attack.

How the Policies Define "Business Interruption Loss"

BI loss is defined as the sum of the following.

- Net profit before income taxes that an insured sustains as a result of a service interruption
- Operating expenses that continue, despite the interruption (e.g., salaries, rent).

Dependent Business Interruption Coverage

Some, but not all, insurers' BI insuring agreements include *dependent business interruption coverage.*

Dependent business interruption coverage differs from "standard" business interruption coverage, in that the latter applies when an *insured's* computer system is unable to operate and, as a consequence, the insured suffers a loss of revenue. In contrast, dependent business interruption coverage is triggered when the computer system operated by a technology provider (who supplies services to the insured) cannot operate, and as a result, the insured sustains a revenue loss.

For example, assume a retailer outsources its order-taking function by hiring a technology company to host its website. In the event the service provider's computer system cannot operate because of a malicious virus, the retailer will be unable to process orders during the period of outage and, therefore, suffers a loss of revenue. Subject to the retailer's policy's limit available under its business interruption insuring agreement and the applicable deductible (a concept discussed later in this chapter), the insurer will indemnify the retailer for its "business interruption loss" during the period of time in which the technology service provider's computer system is unable to function.

Business Interruption Coverage Applies to Profits—Not Sales

The business interruption insuring agreement applies to *net profits* rather than *net sales*. Thus, if a computer disruption caused a business to lose $500,000 in sales, the covered loss would be the extent of the actual profit lost on $500,000 rather than on the full $500,000 in lost sales.

Extra Expense Coverage

This insuring agreement pays the *additional* costs expended to *expedite* repairs to an online system so as to minimize downtime. Such costs may include overtime labor expenses, the cost of hiring special computer experts, or the cost for express shipping of computer parts.

Extra Expense Coverage Applies Only to the Extent the Expenditure Reduces Loss

Under some policies, extra expense coverage applies *only* to the extent the extra expense actually reduces the loss (i.e., hastens a firm's return to operations). For example, assume an insured expends $50,000 to expedite return to full operations, but the expenditure only reduces the loss by $25,000. Under such policies, only $25,000 will be covered.

In contrast, under other underwriters' versions of this insuring agreement, the insurer will cover the extra expenses incurred, even if they do not actually expedite an insured's return to full operating capacity. Thus, in the above example, the full $50,000 expenditure would be covered.

Coverage Limitations

There are several coverage limitations associated with cyber policy time element coverages.

- Some policies do not cover losses unless they involve theft of data.
- Coverage applies only to a failure of security, but not to computer malfunctions.
- The policies do not cover time element losses caused by "traditional" physical damage perils.

"Intrusion" but No Theft of Data: Does Coverage Apply?

Under some polices, and as is also the case with the four liability insuring agreements already discussed, for coverage to apply under time element insuring agreements, an "electronic disruption" *must* involve a theft of data. Yet, under other, broader forms, an actual theft is not required. For example, under such

policies, if an insured's website is rendered inoperable by a *spam attack* or by the *introduction of a virus*, a resulting BI/EE loss would still be covered.

Coverage Limited to Failure of Security—Not Computer Malfunction

Coverage is generally limited to a failure of computer security (e.g., virus transmission by a hacker or loss caused by a theft of data) and *does not* normally extend to a simple malfunction or failure *not* related to a security failure. Thus, a failure due to the fact that a computer part simply wore out, causing a malfunction and consequent shut down of a company's computer system, would not be covered.

No Coverage for Loss Caused by "Traditional' Physical Damage

Another important limitation associated with cyber-related time element coverages is that under all insurers' time element insuring agreements, coverage is triggered *only* by an "electronic disruption" (however, this term is defined within a given insurer's form). On the other hand, there is *never* any coverage for other types of "traditional" physical damage perils, such as fire, flood, windstorm, or earthquake. Thus, if a fire were to damage a business's computer system and disrupt operations as a result, no coverage would be available.

The rationale for this approach is that if a computer system is disabled by "traditional" physical damage perils and a BI or EE loss results, coverage is normally available (or could have been arranged) under standard property insurance policies.

Combined/Single Coverage Approaches

Some insurers "bundle" BI and EE coverages under a single insuring agreement. Others separate them into two insuring agreements. Still others offer business interruption, but *not* extra expense coverage.

Deductible Approaches

Both BI and EE insuring agreements are usually subject to a "time" deductible (rather than a "dollar" deductible) before coverage applies—most often 8, 12, or 24 hours. In contrast, as will be noted later in this course, all of the other insuring agreements are subject to a dollar amount deductible.

Summary

This chapter examined the insuring agreements found within cyber and privacy policies written to cover time element losses, including the following.

- Business interruption
- Extra expense

Each insuring agreement is subject to various limitations. Not all insurers offer time element coverages, while some provide only business interruption, but not extra expense coverage.

Some insurers that write business interruption coverage also provide (a) dependent business interruption and/or (b) extended business interruption coverages.

Time element coverages, unlike the other types of insuring agreements within cyber and privacy policies, contain time deductibles rather than dollar-denominated deductibles.

Chapter 11
Cyber and Privacy Insurance: First-Party Theft of Property Insuring Agreements

Overview

The five major types of first-party theft of property insuring agreements include the following.

- Data asset coverage
- Cyber extortion coverage
- Computer fraud coverage
- Funds transfer fraud coverage
- Social engineering/fraudulent instruction coverage

Chapter Objectives

On completion of this chapter, you should be able to do the following.

- Identify the insuring agreements commonly used to cover first-party theft of property loss exposures.
- Recognize the manner in which each insuring agreement applies to a given claims scenario.
- Recognize the key coverage limitations and extensions associated with each of these insuring agreements.

Data Asset Coverage

This insuring agreement covers the cost of *restoring* and *recovering* the data lost from the "failure of an insured's computer security," meaning situations where a computer system is breached by a hacker.

There is no coverage under this insuring agreement for the cost of research needed to recover lost data. In effect, the policies exclude coverage for the expense required to perform "pencil-and-paper" research to recapture lost data. Rather, the forms only cover the expense incurred by "electronic" recovery methods, such as locating seemingly lost data that has been backed-up within the insured's computer system, yet requires a high level of expertise to find and then restore the system to working order. It would also, for example, cover the cost of restoring a company's data by removing a virus that has corrupted the data. But, on the other hand, this insuring agreement would not cover the costs of recreating such data from scratch.

Important Coverage Limitations and Variations

A number of limitations and variations are found within the data asset coverage insuring agreement, as offered by various insurers, and are enumerated in Exhibit 11.1.

Exhibit 11.1
Restrictions and Variations within Data Asset Insuring Agreements

The following are among the most important limitations and variations found within the various insurers' policies.

Limitations

- **No Fidelity Coverage**. Coverage usually does not apply when loss of data assets is caused by *intentional* employee acts. The intent of this restriction is to avoid providing what would essentially be fidelity/employee dishonesty coverage. However, coverage does apply to unintentional employee acts, such as when an employee accidentally erases data.
- **No Coverage for Software Upgrades**. Nor does this insuring agreement cover the cost of *upgrading software* or other programs during the data restoration process. (Sometimes security breaches result because a system was not equipped with the latest security software.) The intent is to make the insured "whole" following a loss, but not to put the insured in a better position as a consequence of a data breach or disruption.

Variations

- **Preapproval Requirements**. Under some forms, the insurer must *preapprove* all data restoration expenditures, whereas under others, this is not required.
- **Variations in Covered Causes of Loss**. A number of policies only provide coverage for loss caused by an intentional "electronic disruption," such as a theft of data, the introduction of a virus, or the launching of a spam attack. Other broader policies cover these perils, as well as loss from additional causes, such as accidental erasure.

Data Asset Coverage Loss Scenarios

A hacker manages to gain access to an insured's entire customer database. Following the discovery of the breach, the database can no longer be accessed by the insured. This insuring agreement would cover the insured's cost to recapture the "lost" customer database that had been backed-up within the insured's computer system, but which requires time and other expenses to recover.

Cyber Extortion Coverage

This insuring agreement covers loss sustained from computer-aided extortion. Cyber extortion consists of threats to (1) commit an intentional computer attack, (2) damage or shut down a computer system, (3) disclose confidential information, (4) block access to a computer system, or (5) introduce a virus into a computer system unless the insured pays a specified sum of money to the extortionist.

There are three elements of loss covered by this insuring agreement.

Coverage for Cyber Extortion Demands

First, this insuring agreement covers ransom monies required to be paid as a result of extortion demands.

Coverage To Prevent Further Extortion

Second, this insuring agreement pays monies to a computer security systems expert to provide an assessment and report containing recommendations aimed at preventing future extortion attempts. It is important to note that under most insurers' policies, coverage of such costs first requires insurer approval of the expert who will perform the assessment.

Coverage for Expense Required in Dealing with the Cyber Extortionist

Third, this insuring agreement pays the cost of hiring the expert(s) required to negotiate with the cyber extortionist. Insurers have networks of such experts available to assist insureds under these circumstances. Availability of this service is perhaps the most valuable element of this insuring agreement, since few businesses have the expertise to deal successfully with ransom demands of this nature.

An Important Coverage Restriction: No Coverage of Employee Acts

One important aspect of cyber extortion coverage is that it usually *does not* apply to acts committed by employees. Thus, if an employee of the named insured attempts to extort monies from her employer by means of threats to shut down or damage a computer network, this insuring agreement will not normally apply. The rationale for this approach is that such losses fall more within the realm of fidelity/employee dishonesty coverage and, thus, should not be the subject of cyber and privacy insurance. The "spirit" of cyber and privacy policies is to address threats from outside of—rather than within—an organization. Note, however, that there is no universal insurer agreement on this coverage point, and thus, a minority of insurers' forms do cover employee extortion incidents.

Cyber Extortion Coverage Loss Scenario

An insured receives an email from an individual who threatens to shut down, damage/deface, introduce a virus into, disclose confidential information from, block access to, or attack in some other way a company's website unless the insured pays a $10 million ransom. (Note that historically, the majority of ransom demands have fallen within a range of $100,000 to $5 million.)

An insured is contacted by telephone and is told by the caller that its website will be shut down by a denial of service attack within 30 minutes and that the attack will continue until the insured wires $20 million to an offshore bank account. This insuring agreement would cover the ransom demand, the cost of hiring a negotiator to deal with the cyber extortionist, and the expense of bringing in a computer security

expert to provide an assessment and recommendations aimed at preventing future extortion attempts.

Computer Fraud Coverage

This insuring agreement covers loss from intentional, fraudulent, unauthorized entry into a computer system resulting in a theft of money or data.

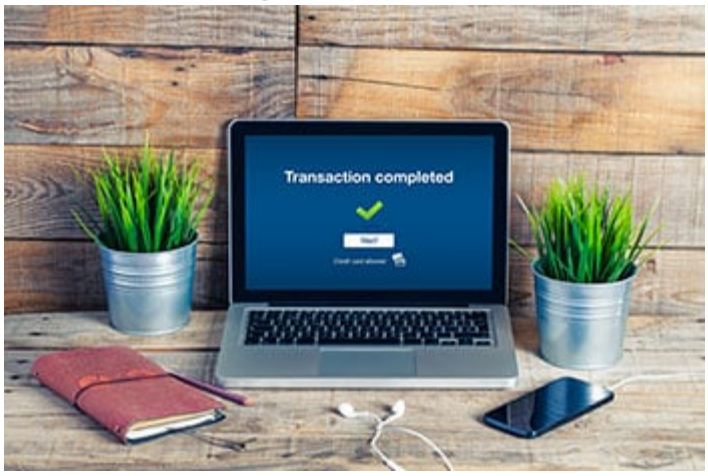
An Important Coverage Restriction: No Coverage for Employee Acts

As is also the case with respect to cyber extortion coverage, computer fraud coverage *does not* apply to acts committed by employees since they more appropriately fall within the scope of fidelity/employee dishonesty coverage and, thus, should not be addressed by cyber and privacy insurance.

Computer Fraud Loss Scenario

A cyber thief obtains the savings account numbers and passwords belonging to various customers of Bank X by hacking into X's computer system. The thief then uses this information to withdraw $500,000 from the customers' accounts by using Bank X's ATM machines.

Funds Transfer Fraud Coverage



This insuring agreement covers loss sustained when funds are fraudulently *transferred* from one financial institution to another.

Funds Transfer Fraud Loss Scenario

A representative loss scenario would involve a situation where a stock brokerage firm in the United States receives an email that "appears" to be from a US bank (but is not). The broker's employee opens the email, which activates a virus, allowing the thief to access the account numbers and passwords of the brokerage's customers. The hacker then uses this information to transfer monies from the brokerage accounts to her bank in Eastern Europe.

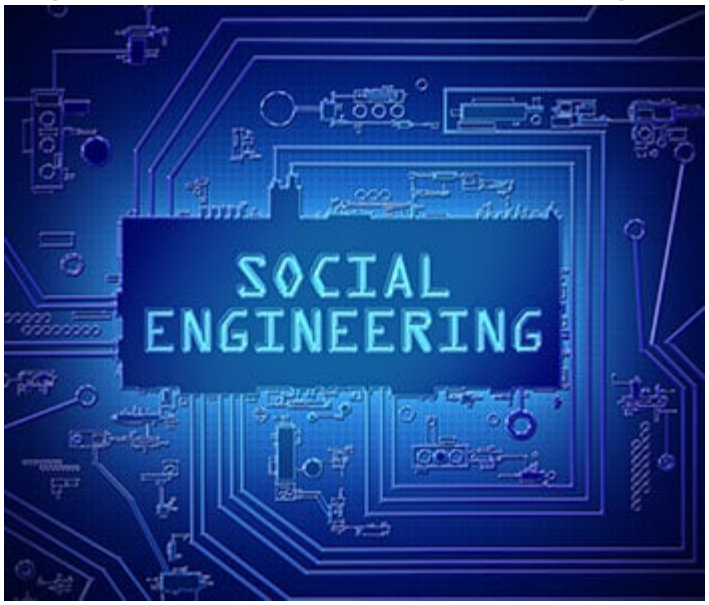
An Important Coverage Restriction: No Coverage for Employee Acts

Again, given the distinct possibility that otherwise covered losses could be caused by employees (as is also the case regarding computer fraud and cyber extortion insuring agreements, discussed above), this insuring agreement does not apply to losses caused by employees.

Computer Fraud Coverage versus Funds Transfer Fraud Coverage

The key difference between coverage applicable under the *computer fraud* insuring agreement and the *funds transfer fraud* insuring agreement is that the latter involves transfer of monies from one financial institution to another. In contrast, the example illustrating a computer fraud incident in which the hacker obtained savings account numbers and passwords and used this information to withdraw $500,000 did not entail the fraudulent transfers of monies *between* two financial institutions. Rather, the fraud was perpetrated by computer and resulted in the theft of money by means of ATM machines.

Social Engineering/Fraudulent Instruction Coverage



This insuring agreement provides coverage for losses resulting from attempts to have insureds transfer monies (usually by means of wire transfers) based on instructions (typically in the form of an email) in which the recipient is instructed to transfer funds from one financial institution to another. For this reason, a number of insurers' policies refer to this insuring agreement as "fraudulent instruction" coverage.

Important Coverage Restrictions

There are two important coverage restrictions associated with social engineering/fraudulent instruction coverage.

First, coverage applies *excess of* any applicable crime insurance that the insured has available.

Second, no coverage applies to any loss involving a fraudulent instruction that was not verified using an *out-of-band authentication*. The latter term refers to a type of two-factor authentication process that makes hacking difficult because it requires two separate and unconnected authentication channels to gain access to a system. For example, such a system might require (1) a personalized password *and* (2) the entry of an ever-changing passcode that an employee may have on a physical "token" she keeps on her person at all times.

Social Engineering Coverage versus Funds Transfer Fraud Coverage

The key difference between coverage applicable under the *funds transfer fraud* insuring agreement and the *social engineering/fraudulent instruction* insuring agreement, is that the latter involves a *voluntary* transfer of monies from the insured to another party. In contrast, the example illustrating a computer fraud incident (in which the hacker obtained savings account numbers and passwords and then used this information to withdraw $500,000) did not entail the *voluntary* transfer of monies. Rather, the fraud was perpetrated by an *involuntary* transfer of monies by the hacker from the individual accounts to the ATM machines and, ultimately, to the hacker.

Social Engineering/Fraudulent Instruction Loss Scenario

The treasurer at Company X receives an email from what appears to be Security National Bank requesting an immediate transfer of $25,000 to cover an outstanding check, which seems appropriate and legitimate. Accordingly, per the instructions contained in the email, the treasurer wire transfers $25,000 (from another bank in which Company X has an account), as requested. In fact, the $25,000 ends up in the phisher's offshore bank account, rather than in Company X's account at Security National Bank.

Many Insurers Do Not Offer Theft of Property Coverages

A substantial minority of insurers do not offer *any* of the five theft of property coverages discussed above. This is, as already noted, because these insurers philosophically view cyber and privacy insurance as coverage for (1) notification and crisis management costs, (2) regulatory defense and penalties, and (3) third-party/liability losses rather than for first-party/property losses.

Insurers also avoid providing theft of property coverages because a number of the losses these insuring agreements address can also be covered under other types of policies, such as kidnap and ransom (i.e., cyber extortion) and crime (i.e., computer fraud, funds transfer fraud, and social engineering) forms.

Summary

This chapter examined the insuring agreements written to cover the five major types of first-party property loss exposures, which include the following.

- Data asset coverage
- Cyber extortion
- Computer fraud
- Funds transfer fraud
- Social engineering/fraudulent instruction coverage

The chapter explained the nature of each insuring agreement, provided a loss scenario indicating where and how the insuring agreement applies, and described the various coverage limitations applying to several of these insuring agreements.

Chapter 12
Cyber and Privacy Insurance: Limits, Retentions, and Other Important Policy Provisions

Overview

The manner in which limits and retentions provisions of a cyber and privacy policy apply has an important effect on the extent of coverage the policies afford.

A number of other policy provisions also have a material effect on the extent to which a cyber and privacy policy will respond to a loss. Such provisions include the following.

- Limits/deductibles
- Insured persons/insured organizations
- Covered defense costs
- Settlement provisions
- Coverage trigger provisions

Chapter Objectives

On completion of this chapter, you should be able to do the following.

- Recognize how the limits and retentions provisions apply within cyber and privacy policies.
- Recognize how these other provisions function within a cyber and privacy policy.
- Recognize how the provisions operate within a given loss scenario.
- Identify important variations between these provisions on an insurer-to-insurer basis.
- Identify key limitations that are a part of such provisions.

Limits and Deductibles

The policies are written with both of the following.

- A *per claim limit* for *each* of the individual insuring agreements that the insured has purchased
- An *annual aggregate limit* that applies across *all* of the different insuring agreements that the insured has purchased (The annual aggregate limit is typically the total of the per-claim limits for the individual insuring agreements the insured has purchased.)
- A *per claim deductible* for each of the insuring agreements the insured has purchased

Implications of Limits and Deductibles Provisions

The fact that the policies contain insuring agreement-specific limits and deductibles, coupled with an annual aggregate limit, has several implications. First, it requires the insured to make multiple decisions when buying cyber and privacy insurance. Second, it constricts the true extent of coverage that a cyber and privacy policy actually provides. Lastly, it adds complexity to the overall purchasing process.

Exhibit 12.1 offers a case study of how deductibles and limits apply under a cyber and privacy policy.

Exhibit 12.1 Application of Limits and Deductibles: A Case Study			
Insuring Agreement	**Per-Loss Limit**	**Covered Loss**	**Deductible**
Privacy Notification and Crisis Management	$10 million	$5 million	$10,000
Regulatory Defense and Penalties	$5 million	$2 million	$5,000
Information Security and Privacy Liability	$20 million	$15 million	$25,000
Aggregate Limit: $35 million			

Assume that a covered loss involved each of the three insuring agreements noted in Exhibit 12.1 in the amounts of $5 million, $2 million, and $15 million, respectively. In this situation, the insurer will pay the sum of these losses, or $22 million, less $40,000 (the total of the respective deductible amounts applicable under each of the three insuring agreements).

Also recognize that $13 million remains available to pay any additional covered losses sustained during the current policy term (i.e., $35 million aggregate limit less $22 million already paid = $13 million remaining limits).

Other Approaches to the Application of Deductibles

Although Exhibit 12.1 presents one common approach to the application of deductibles in cyber and privacy policies, other insurers offer slightly different options. For example, one leading underwriter's form contains a separate deductible for the notification/crisis management insuring agreement, one for the liability insuring agreements purchased by the insured, and one for the policy's first-party coverages. Alternatively, other insurers provide a "single highest retention" endorsement under which only one deductible would apply to a given loss (i.e., the largest one applicable to all of the insuring agreements that have been purchased).

Selecting Limits and Deductibles

Expert broker advice is essential in choosing appropriate limits and deductibles. Brokers often have databases to assist in arriving at these amounts. Specifically, they can use the limits/deductibles purchased by "comparable" businesses to guide them in recommending limits/deductibles to an individual insured. Business interruption work sheets (used in purchasing property insurance policies) are also an effective tool in estimating potential time element losses and selecting appropriate limits.

Exhibit 12.2 lists a number of key factors in arriving at optimal limits and deductibles.

Exhibit 12.2
Key Factors in Selecting Limits and Deductibles

- **Business/Industry Type.** "Data-rich" industries, such as health care, are especially vulnerable to cyber losses (e.g., thieves can use personally identifiable information (PII) to commit Medicare/Medicaid fraud).
- **Business Size/Number of Electronic Records.** Typically, the higher a business's gross sales, the larger its number of different customers. And since data breach costs are roughly $200 per electronic file (under the privacy notification and crisis management insuring agreement), the total number of electronic records maintained by a business has a substantial effect on the size of the cyber loss it can be expected to sustain.
- **Geographical Dispersion of Customers.** The more jurisdictions (i.e., states) in which a business's customers are located, the larger the number of involved regulatory authorities (and thus, the higher the potential costs under the regulatory defense and penalties insuring agreement) can be following a loss.
- **Loss Control Program.** An effective loss control program can both reduce the *likelihood* of a breach and also lower the *potential costs* of a breach.
- **Loss History.** A prior loss may actually be a "positive," if it impels an insured company to implement robust loss control measures.
- **Contractual Risk Transfer Arrangements.** Outside vendors (e.g., data storage firms) and technology consultants with which an insured does business should be required to sign hold harmless agreements and provide evidence of technology errors and omissions (E&O) coverage. Such arrangements will, in theory at least, reduce the policy limits an insured needs to maintain. However, such firms should not be permitted to limit their liability to the amount of their insurance coverage.
- **Cash Position.** This is especially important in determining deductible amounts for time element coverages, since many small businesses cannot continue to operate for long if their cash flow is interrupted by an electronic shutdown.

Insured Organization and Insured Individuals

Cyber and privacy policy forms are designed to cover a broad range of individuals and organizations.

Named Insured and Subsidiaries

The policies cover the entity named on the declarations page known as the "named insured." In addition, coverage also applies to "subsidiaries" of the "named insured," which is generally defined as entities in which the "named insured" holds a majority ownership interest.

Insured Individuals

A wide range of persons are insureds under the policies, including the following.

- Directors, officers, and managers
- Partners and principals (and often, but not always, stockholders)
- Employees (often, but not always, including temporary, part-time, and leased employees)
- Former/past insured persons
- Estates, heirs, executors, administrators, assigns, and legal representatives
- Spouses (often, but not always, including domestic partners)

Coverage of Independent Contractors

A minority of forms cover independent contractors as insureds. Such coverage is qualified, however, by the fact that it extends only to independent contractors "for whom the insured organization is legally

responsible." Thus, no coverage applies to independent contractors unless they are, in effect, working in tandem with the insured organization, such as on a specific project.

Defense Cost Provisions

The defense provisions in cyber and privacy forms are among the most important contained within the policies. The two key concepts relating to the payment of defense costs under the policies are (1) defense costs *(as well indemnity payments; i.e., settlements and judgments)* reduce policy limits, and (2) retentions under the policy also apply to defense costs—as well as to indemnity payments—so that there is no "first dollar" defense coverage provided.

Defense Cost Payments Reduce Policy Limits

Unlike commercial general liability (CGL) insurance policies, which pay defense costs on an unlimited basis, payment of defense costs under cyber and privacy forms reduces available limits (this is also known as a "shrinking limits" policy).

For example, assume a policy contained a $5 million information security and privacy liability limit. Further assume that as a result of a covered claim, indemnity (i.e., settlement and judgment) payments totaled $3 million, and defense costs were $2 million. In this situation, no additional monies would be available because defense and indemnity payments (i.e., $3 million + $2 million) have already exhausted the policy's $5 million limit.

Deductibles Apply to Defense Costs

Under cyber and privacy policies, insurers do not offer so-called first-dollar defense coverage. For example, assume a claim required $250,000 to defend, but no indemnity payments were involved. If the policy was written with a $50,000 deductible, the insurer and the insured would pay $200,000 and $50,000, respectively.

Implications for Policy Limit Selection

Given the fact that (1) in many claims, defense costs far exceed indemnity payments, (2) insurers do not offer first-dollar defense, and (3) defense costs reduce policy limits, insureds should bear these facts in mind when selecting policy limits.

Defense and Settlement Procedures

The defense and settlement procedures contained within the policies have a substantial effect on the insured's rights in a claim situation.

Duty To Defend versus Non-Duty To Defend Policies

Cyber and privacy policies written with duty to defend wording require the insurer to assume the defense of all claims made against the insured under a policy. Accordingly, the insurer has the right to (1) select counsel, (2) control the process of settling a claim, and (3) determine the amount of a settlement. In contrast, under non-duty to defend policies (also known as "reimbursement" policies), the insurer's sole obligation is to reimburse the insured for the defense and indemnity costs the insured has incurred in settling a claim covered by the policy.

Most cyber and privacy forms are written on a duty to defend basis, especially those designed for private companies and nonprofit organizations. However, some policies give the insured the option of selecting *either* duty to defend *or* non-duty to defend coverage.

Benefits of Duty To Defend Policies

Duty to defend provisions are preferable for most insureds because few businesses have had the experience of defending a data breach claim. For this reason, they are usually better served by delegating claims management responsibilities to a more knowledgeable insurer.

Coverage Triggers

As is the case with nearly all types of professional and E&O policy forms, the liability coverage sections of cyber and privacy policies are written on a claims-made basis, meaning that for coverage to apply, a claim must be both (1) made against the insured during the policy period and (2) made on or after the policy's retroactive date.

In contrast, the property coverage sections of the policies are written on an occurrence basis, meaning that coverage is triggered whenever a loss "occurs," so that unlike a claims-made policy, claims can be made under an occurrence policy that has long since expired.

Because cyber and privacy insurance policies are written with two different types of coverage triggers, various foreseeable complications can result in the event that a single loss involves the application of *both* claims-made *and* occurrence coverage triggers. Even greater complexity might ensue under these circumstances because the use of both occurrence and claims-made coverage triggers could conceivably involve two different policy periods. Fortunately, while possible, the likelihood of this happening is low.

Summary

The manner in which limits and retentions provisions of a cyber and privacy policy apply has an important effect on the extent of an insured's recovery under a cyber and privacy form. This chapter examined both types of provisions and provided examples of how limits and retentions not only apply, but also interact in various claim scenarios. This chapter also analyzed the effect of the all-important aggregate limit that is found within cyber and privacy forms.

The other provisions analyzed in this chapter are also a key element in determining whether and to what extent a claim will be covered under a cyber and privacy policy. These provisions include the following.

- Limits/deductibles
- Insured persons/insured organizations
- Covered defense costs
- Settlement provisions
- Coverage trigger provisions

Chapter 13
Cyber and Privacy Insurance Policy Exclusions

Overview

This chapter examines the exclusions that are commonly found within cyber and privacy policy forms.

Chapter Objectives

On completion of this chapter, you should be able to do the following.

- Identify key exclusions within cyber and privacy policies.
- Recognize how these exclusions operate and affect the extent of coverage under the policies.
- Recognize differences among various insurers' versions of these exclusions.
- Identify the so-called exceptions contained within these exclusions.

Fraud, Criminal, Dishonest Acts

Although coverage for fraudulent, criminal, and dishonest acts is excluded by nearly all of the policies, this exclusion should only apply when these acts are committed by an insured and not when caused by third parties. Thus, if a nonemployee hacker causes an insured's computer system to crash because he launched a spam attack, this exclusion would not apply. On the other hand, if the spam attack were the work of an employee (an insured under virtually all cyber and privacy policy forms), no coverage would be available.

Key Exception Wording

The wording of this exclusion should include (1) defense coverage for "innocent insureds" and (2) "final adjudication" defense coverage wording.

For example, the innocent insured's wording would apply in the event three employees were charged with instigating a data breach, yet only one of the three were actually involved. Innocent insured wording within this exclusion would provide defense coverage to the two employees who played no role in the data breach.

Final adjudication wording would provide defense coverage for the two innocent insureds until *either* a verdict was rendered against them *or* they admitted to having committed the data breach. A favorable variation of the final adjudication provision is one that defines "final adjudication" as "including all appeals." Such wording is valuable if, for example, a trial court's verdict is rendered against an insured, but the insured appeals the verdict. Such wording would cover the defense costs required by the appeal, an extension not available within standard "final adjudication" language.

Bodily Injury and Property Damage

The policies exclude cyber-related claims alleging bodily injury and property damage because such losses are covered under commercial general liability (CGL)/property insurance policies. However, the broadest policies "except"—and thus cover—"mental anguish," "shock," "emotional distress," and "humiliation." This wording is valuable because in addition to alleging financial losses, lawsuits (covered under the information security and privacy liability insuring agreement) also sometimes include these types of allegations.

Employment-Related Claims

Employment-related claims are excluded by cyber and privacy policy forms because employment practices liability (EPL) policies are designed to cover such exposures. However, the policies should except—and thus cover—employee suits alleging employment-related privacy violations, such as when personally identifiable information (PII) is removed from human resources (HR) files or employee PII is obtained via hacking.

ERISA Act Exposures

The policies exclude coverage for exposures relating to an employer's responsibilities enumerated by the Employee Retirement Income Security Act (ERISA) of 1974. This is because these exposures are covered by fiduciary liability policies. However, cyber and privacy forms should except, and thus cover, claims involving data breaches that impact employee benefit programs, such as when a hacker obtains information about an employee's medical condition that is stored in an electronic file pertaining to the health insurance coverage purchased and administered by an employer-insured.

War, Invasion, Insurrection

Nearly all of the policies exclude coverage for claims caused by war, invasion, and insurrection. Furthermore, a handful of insurers also exclude coverage for "terrorism" within such wording. Yet, language excluding "terrorism" is problematic because virtually *every* intentionally caused cyber-related hacking or intrusion event could be considered "terrorism," thus affording the insurer an opportunity for a coverage denial. One means of moderating the scope and effect of this wording is for insureds to request that it be modified to except, and thus cover, "electronic terrorism." Wording of this kind would at least preserve coverage for hacking/intrusion-driven losses, although it still might preclude coverage if, for example, an insurer were to assert that an individual who stole paper files containing PII had engaged in an act of "terrorism."

Patent, Software Infringement

Patent infringement claim exposures are excluded by the policies because they can be covered by intellectual property (IP) insurance forms. Nevertheless, the broadest cyber and privacy policies affirmatively cover infringement claims if they are caused by non-management employees or by third parties such as technology contractors with whom an insured may be working.

Mechanical or Electrical Breakdown/Failure

The policies exclude coverage for losses caused by mechanical or electrical failures and related breakdowns for two reasons. First, such failures do not usually result from data breaches. Second, when these kinds of breakdowns do cause business interruption, the resulting losses are insurable under standard property policies.

Yet, some mechanical failures can be caused by hackers who, for example, overload a system (i.e., by generating a "spam attack" *or* by introducing a virus that shuts down a system). As a consequence, insureds should request wording that excepts, and thus covers, mechanical/electrical failures that are *intentionally* caused by hackers.

Loss Involving Portable Electronic Devices

This exclusion (while somewhat unusual) is often referred to as the "laptop exclusion." It is typically added as an exclusionary endorsement, rather than being included within the regular provisions of cyber and privacy policy forms. Insurers will sometimes remove it if the insured agrees to encrypt (i.e., "scramble" to make unreadable) all data contained on portable devices.

Failure To Follow Minimum Required Security Practices

Applications for cyber and privacy insurance policies routinely contain detailed questions regarding the steps the applicant is currently taking to protect its electronic data. Accordingly, a growing minority of policies exclude coverage in the event it can be established that a claim was caused by failure to follow the described procedures (e.g., not regularly checking and maintaining security patches).

Since this exclusion is common, although not (yet) universal, an insured can avoid it by selecting a policy that does not contain an exclusion for failing to follow minimum security practices. If this is not possible, the insured should, first, take great care when completing a coverage application, making sure not to overstate the nature of its current cyber security measures. Second, insureds should closely and continuously monitor the extent to which the procedures enumerated within the application are actually being implemented once coverage is in place.

Professional Services

This exclusion eliminates coverage for what are essentially technology errors and omissions (E&O) exposures (i.e., providing technology products and services to others for a fee), rather than losses resulting from data protection issues—the essence of cyber and privacy policy.

If, for instance, a third-party contractor engaged by the insured committed an error that exposed the insured's customers' PII, this exclusion would eliminate coverage for the insured. The solution to this coverage gap is for insureds to insist that all of its third-party technology providers buy technology E&O coverage as a condition of working with the organization.

Exhibit 13.1 presents a recap of the key exceptions and modifications that buyers of cyber and privacy policies should seek or request within the exclusions sections of their policies.

Exhibit 13.1 Exclusion "Exceptions" and Modifications: A Recap	
Exclusion	**But Coverage Applies if/for Actions**
Fraud, Criminal Acts	"Innocent Insureds," "Final Adjudication"
Bodily Injury/Property Damage	Shock, distress, mental anguish, humiliation
Employment-Related Claims	Violations of employee privacy
War, Invasion, Insurrection	"Electronic Terrorism"
ERISA Act	Violations of employee privacy
Software, Patent Infringement	Non-management employees, third parties
Mechanical or Electrical Failure	Caused by hackers
Portable Electronic Devices	Data on such devices is encrypted
Failure To Follow Minimum Security Procedures	Periodically verify that application procedures are being followed
Professional Services	Require third-party contractors to buy technology E&O coverage

Summary

Cyber and privacy policy forms contain a number of standard exclusions. However, there is considerable variation within these exclusions. Accordingly, insureds should attempt to select policies containing the most favorable versions of such exclusions and/or attempt to negotiate with insurers to modify existing exclusionary wording, as explained in this chapter.

Glossary

accessible website—An Internet website that has login capabilities allowing access to secure or restricted content.

aggregate limit—An insurance contract provision limiting the maximum liability of an insurer for a series of losses in a given time period (e.g., a year or for the entire period of the contract). Sometimes called "annual aggregate limit."

annual aggregate limit—See aggregate limit.

business interruption loss—Loss that results when a breach or malfunction of a business's computer systems causes a loss of income to the firm.

CGL—See commercial general liability (CGL) policy.

claims-made policy—A policy providing coverage that is triggered when a claim is made against the insured during the policy period, regardless of when the wrongful act that gave rise to the claim took place. (The one exception is when a retroactive date is applicable to a claims-made policy. In such instances, the wrongful act that gave rise to the claim must have taken place on or after the retroactive date.) Most professional, errors and omissions (E&O), directors and officers (D&O), and employment practices liability insurance (EPLI) are written as claims-made policies.

claims-made trigger—A type of coverage trigger that obligates an insurer to defend and/or pay a claim on an insured's behalf if the claim is first made against the insured during the period in which the policy is in force. (The term "made" means notification to an insured that a demand for money or services is being requested.)

cloud computing—A method of delivering information technology services (i.e., hardware and software) in which resources are hosted and retrieved from the Internet through Web-based tools and applications rather than a direct connection to a local server. The cloud computing structure allows access to information as long as an electronic device has access to the Web. The word "cloud" is used as an analogy for the "Internet" because many network diagrams use the image of a cloud to represent the Internet.

commercial general liability (CGL) policy—A standard insurance policy issued to business organizations to protect them against liability claims for bodily injury (BI) and property damage (PD) arising out of premises, operations, products, and completed operations; and advertising and personal injury (PI) liability. The CGL policy was introduced in 1986 and replaced the "comprehensive" general liability policy.

computer crime—See computer fraud.

computer fraud—In a computer fraud situation, after gaining access to a company's network, the criminal uses such access to obtain valuable data or information.

computer network—A term that includes not only servers and web applications regularly accessed by desktop, mobile phone, and laptop users, but also credit card processors, mobile apps, and other devices connected to the Internet in some capacity.

computer virus—A hidden, self-replicating software program, usually containing malicious logic, that propagates by inserting copies of itself into and becoming part of another host program. It is designed to infect and gain control over vulnerable systems without the user's knowledge or consent and is activated when a user runs or opens its host program. Computer viruses can cause frequent computer crashes or pop-up messages, corrupt or delete data on a computer, reformat the hard drive, use an email program to spread the virus to other computers, or flood a network with traffic, ultimately making it impossible to

perform any Internet activity.

computer worm—A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. Unlike computer viruses, worms do not require human involvement to propagate. Worms can do damage by reproduction, consuming internal disk and memory resources within a single computer, exhausting network bandwidth, deleting files, or making it impossible to send documents via email.

coverage trigger—The event that must occur before a particular liability policy applies to a given loss. Under an occurrence policy, the occurrence of injury or damage is the trigger; liability will be covered under that policy if the injury or damage occurred during the policy period. Under a claims-made policy, the making of a claim triggers coverage. Coverage triggers serve to determine which liability policy in a series of policies covers a particular loss.

credit monitoring—Service that detects situations where a "bad actor" attempts to open new or use existing credit lines.

cyber and privacy insurance—A type of insurance designed to cover consumers of technology services or products. More specifically, the policies are intended to cover a variety of both liability and property losses that may result when a business engages in various electronic activities, such as selling on the Internet or collecting data within its internal electronic network.

Most notably, but not exclusively, cyber and privacy policies cover a business's liability for a data breach in which the firm's customers' personal information, such as Social Security or credit card numbers, is exposed or stolen by a hacker or other criminal who has gained access to the firm's electronic network. The policies cover a variety of expenses associated with data breaches, including notification costs, credit monitoring, costs to defend claims by state regulators, fines and penalties, and loss resulting from identity theft.

In addition, the policies cover liability arising from website media content, as well as property exposures from (1) business interruption, (2) data loss/destruction, (3) computer fraud, (4) funds transfer loss, and (5) cyber extortion.

Cyber and privacy insurance is often confused with technology errors and omissions (E&O) insurance. In contrast to cyber and privacy insurance, technology E&O coverage is intended to protect providers of technology products and services, such as computer software and hardware manufacturers, website designers, and firms that store corporate data on an off-site basis. Nevertheless, technology E&O insurance policies do contain a number of the same insuring agreements as cyber and privacy policies.

cyber extortion—A type of online crime in which a criminal threatens to damage or shut down a company's website, email server, or computer system or threatens to expose electronic data or information belonging to the company unless the company pays the criminal a specific ransom amount.

cyber extortion coverage—An insuring agreement contained within some policies written to cover claims associated with data breaches. Such policies are most often termed "cyber and privacy insurance," "information security and privacy insurance," and "cyber security insurance."

This insuring agreement covers the costs associated with a cyber extortion event (e.g., an insured receives an email stating that the extortionist will introduce a virus into the insured company's website unless the company pays a $10 million ransom). The costs covered by this insuring agreement include (1) monies paid to meet extortion demands, (2) the cost of hiring computer security experts to prevent future extortion attempts, and (3) the expenses charged by professionals to deal/negotiate with cyber extortionists.

data asset coverage—An insuring agreement in a cyber and privacy policy that covers the cost of *restoring* and *recovering* the data lost from the "failure of an insured's computer security," meaning situations where a computer system is breached by a hacker.

denial of service attack—A deliberately planned attack on a computer system or network that causes a loss of use of the computer system or network to legitimate users. Examples of denial of service attacks

include flooding network connections to prevent legitimate network traffic, denying communication between systems, preventing a particular individual from accessing an Internet-based service, and disrupting service to a specific system or individual.

dependent business interruption loss—Dependent business interruption loss, as defined by those insurers whom offer this coverage within their cyber and privacy forms, typically results from the failure of *service providers'* computer systems (rather than the insured's systems). This failure, in turn, leads to an interruption in the insured's business and a subsequent loss of revenue.

discrimination—Unfair or illegal treatment of or denial of rights to persons on the basis of certain arbitrarily chosen attributes or characteristics, including race, gender, religion, creed, age, medical condition, pregnancy, sexual orientation/preference, physical appearance, marital status, physical or mental disability, or national origin.

Employment Retirement Income Security Act (ERISA) of 1974—Federal law that established rules and regulations to govern employer-provided pensions and other employee benefits provided to US employees.

ERISA—See Employment Retirement Income Security Act (ERISA) of 1974.

extra expense coverage—Insurance that pays for additional costs in excess of normal operating expenses that an organization incurs to continue operations while its property is being repaired or replaced after having been damaged by a covered cause of loss.

funds transfer fraud—A situation that occurs when a cyber criminal accesses a computer network and then uses such access to fraudulently transfer monies from one account to another.

GDPR—See General Data Protection Regulation (GDPR).

General Data Protection Regulation (GDPR)—A regulation aimed at improving security for all companies processing personal data for subjects in the European Union regardless of the company's location. GDPR states that organizations can be fined "up to 4% of annual global turnover or €20 million (whichever is greater)" for the most serious violations.

identity theft monitoring—A service that can detect fraudulent uses of personally identifiable information (PII).

information-only website—An Internet website that provides general information about the applicant's products/services.

Internet of Things (IoT)—Collectively refers to the everyday devices that are connected in some way to the Internet. Many of these devices are referred to as "smart" devices—smartphones, smart homes (e.g., Internet-capable thermostats, appliances, and so on), smart televisions, and many more devices. Through Bluetooth, Wi-Fi, and other means of wireless communication, users of smart devices are able to control them and often times connect them functionally with *other* smart devices. Connections to the Internet allow these devices to track usage habits, provide helpful recommendations (e.g., a refrigerator that sends an alert to a home owner's smartphone when a visit to the grocery store is needed), and generally offer users a more interactive and feature-rich experience.

IoT—See Internet of Things (IoT).

malicious code—Any virus, Trojan horse, malware, worm, or other similar software program, code, or script intentionally designed to insert itself into computer memory or onto a computer disk and spread itself from one computer to another

management liability insurance—Insurance that covers exposures faced by directors, officers, managers, and business entities that arise from governance, finance, benefits, and management activities (also called "executive liability insurance"). This includes (1) directors and officers (D&O) liability insurance, (2) employment practices liability (EPL) insurance, (3) fiduciary liability insurance, and (4) "special crime" insurance (covering kidnap, ransom, and extortion exposures). These coverages may be written as stand-alone insurance policies or combined into a single "package" policy. Management

liability policy "package" policies usually contain a set of common conditions applying to all of the coverage lines purchased. In most cases, an insured must select a minimum of two types of coverage to be eligible to purchase a management liability "package" policy. This arrangement offers meaningful premium discounts because much of the same data is needed to underwrite EPL, D&O, fiduciary, and special crime coverages. Management liability "package" policies are usually available only to privately held firms, not-for-profit organizations, and small publicly traded companies (i.e., those with annual sales of under $25 million). Large publicly traded firms generally purchase stand-alone policies.

network breach—A situation that occurs when someone gains access to a computer network, despite not being authorized to do so; transmits malicious code (e.g., a virus) to a computer network; or prevents a third party, who is authorized to do so, from gaining access to a computer network (i.e., a denial of service attack).

occurrence trigger—For coverage to be provided, the act giving rise to a claim needs to occur within the policy period. The claim does not need to be reported during the policy period. Used with liability policies.

payment card industry fines and assessments coverage—An insuring agreement found within cyber and privacy insurance policy forms that covers (1) fines and penalties assessed against the insured for failing to comply with Payment Card Industry Data Security Standards and (2) defense costs incurred, if the insured challenges the imposition of such penalties because the insured believes that it complied with requisite security standards. Payment Card Industry Data Security Standards are a set of proprietary information security standards that have been promulgated for businesses that accept payment from the leading credit card issuers, including Visa, MasterCard, American Express, and Discover. Coverage under this insuring agreement would apply under the following circumstances. A retailer reports that the personally identifiable information (PII) (including credit and debit card information) belonging to its customers was stolen by a hacker. An investigation reveals that the breach occurred because the retailer's computer system did not comply with Payment Card Industry Data Security Standards. In the event the retailer was fined $100,000 for failure to comply with applicable standards, this insuring agreement would cover the fines. Furthermore, if the retailer incurred costs to dispute the imposition of the $100,000 fine (because it felt that it did, in fact, comply with standards), this insuring agreement would cover those required defense costs.

personally identifiable information (PII)—Any information that can be used to uniquely identify, contact, or locate an individual, either alone or in conjunction with other sources, such as their name, Social Security number, driver's license number, date of birth, place of birth, mother's maiden name, and genetic information.

phishing—A message, usually delivered via email (and less frequently via telephone), that falsely claims to be from a lawful business or otherwise legitimate entity or person. The message attempts to entice the recipient into providing personal information, such as Social Security, credit card, and bank account numbers. This information, if obtained, is later used to commit identity theft. In addition to phishing that targets personal information, many phishing attacks are aimed at obtaining sensitive business information, like corporate bank account numbers. "Fraudulent instruction" (e.g., a message claiming to be from a company's CEO and instructing a mid-level employee to wire transfer a sum of money to a certain account) can also be considered a form of phishing.

PII—See personally identifiable information (PII).

privacy liability—Liability a company incurs when its computer system is breached by a hacker and, as a consequence, personally identifiable information (PII) is released to unauthorized persons.

privacy notification and crisis management expense coverage—An insuring agreement contained within policies written to cover claims caused by data breaches. Such policies are most often termed "cyber and privacy insurance," "information security and privacy insurance," or "cyber security insurance."

Privacy notification and crisis management expense coverage includes the cost of (1) hiring a forensics expert to determine the cause of the breach and suggesting measures to secure the site and prevent future

breaches, (2) hiring a public relations agency to assist the insured in dealing with the crisis, (3) setting up a post-breach call center, (4) notifying affected individuals whose personally identifiable information (PII) has been compromised, (5) monitoring these individuals' credit (usually for 1 year), and (6) paying the costs to "restore" stolen identities as a result of a data breach (e.g., expenses of notifying banks and credit card companies).

Privacy notification and crisis management expense coverage addresses the so-called immediate response costs associated with a data breach. This insuring agreement makes payments on a "no fault" basis and without admission of liability (as is the case under "medical payments" coverage, included in a homeowners or personal auto policy (PAP)). The intent of such payments is to discourage affected customers from making claims associated with a data breach. In contrast, the information security and privacy liability insuring agreement is the true "liability" coverage element of a cyber and privacy policy since it responds to lawsuits and pays liability losses from claims made against the insured by various parties.

Similar to other cyber and privacy insurance policies, privacy notification and crisis management expense coverage is subject to an annual aggregate limit and an annual aggregate deductible.

ransomware—A technique in which hackers typically replace an organization's website home page with a ransom demand.

sexual harassment—Conduct involving unwelcome sexual advances; requests for sexual favors; and verbal, visual, or physical conduct of a sexual nature. There are two types of sexual harassment: quid pro quo sexual harassment, in which sexual contact is made a condition of employment, and hostile environment sexual harassment, in which such conduct creates an intimidating, hostile, or offensive working environment. Lawsuits against businesses that allege sexual harassment have increased significantly during the past decade. Accordingly, around 1990, the insurance market began offering employment practices liability (EPL) policies, a specialized form of insurance covering claims of sexual harassment as well as other employment-related torts.

social engineering/fraudulent instruction coverage—Coverage for losses resulting from attempts to have insureds transfer monies (usually by means of wire transfers) based on instructions (typically in the form of an email), in which the recipient is instructed to transfer funds from one financial institution to another.

social media—Web-based and mobile-based technologies that are used to turn communication into interactive dialogue between organizations, communities, and individuals.

spam, spamming—Sending unwanted and unsolicited email to an individual's or corporation's computer system. A massive spam attack on a company's email system can take up so much space on its server that it causes the system to crash. Such risks can be insured against under Internet/online policy forms that cover business interruption losses.

spear phishing—Phishing aimed at specific individuals and/or companies, relying on the use of personal information to make emails appear convincing and trustworthy. See also phishing.

technology errors and omissions (E&O) insurance—A type of insurance designed to cover providers of technology services or products. For example, data storage companies and website designers provide technology services, while computer software and computer manufacturers offer technology products.

Technology E&O policies cover both liability and property loss exposures. Major liability insuring agreements include losses resulting from (1) technology services, (2) technology products, (3) media content, and (4) network security breaches. Key property insuring agreements provide coverage for extortion threats, crisis management expense, and business interruption.

Technology E&O insurance is often confused with cyber and privacy insurance. In contrast to technology E&O coverage, cyber and privacy insurance is intended to protect consumers of technology products and services. Nevertheless, cyber and privacy insurance policies do offer a number of the same insuring agreements as technology E&O policies.

transactional website—Internet website that accepts orders or purchase using credit/debit cards, accepts bill payment, or allows customers to view account balances or transfer funds between accounts.

Trojan horse—A type of malicious software (malware) named after the wooden horse the Greeks used to infiltrate Troy that masquerades as a legitimate computer program, such as a game, image file, disk utility, or even an antivirus program. Users are typically tricked into downloading Trojan horses on their systems because they appear in the form of benign, useful software or files from a legitimate source. Once activated, Trojan horses can perform a number of attacks on a computer system that can cause pop-up windows to delete files, steal data, give malicious users access to a system, or activate and spread other malware, such as viruses. Unlike computer viruses and worms, a Trojan horse does not reproduce by infecting other files, nor do they self-replicate.

website media content liability coverage—Coverage that applies when the insured incurs liability in conjunction with material published on its website.

wrongful termination—The act of terminating an employee in a manner that is against the law. In recent years, erosion of the employment-at-will doctrine has been the factor most responsible for the increase in claims alleging wrongful termination. Coverage for this exposure is provided under employment practices liability (EPL) policies.

End Notes

[1] Forrester Analytics Business Technographics Security Survey, 2020..

[2] As reported in Robyn Sterling's April 30, 2012, article in *JD Supra Business Advisor,* "First Data Breach Settlement under HITECH—$1.5 Million."

[3] Anna D. Kraus and Tara Carrier, "HHS Announces Multiple HIPAA Settlements Related to Data Breaches and the Right of Access Initiative," Covington Digital Health, October 6, 2020,

[4] Kevin LaCroix, "Guest Post: Cybersecurity Enforcement: The FTC Is Out There," *The D&O Diary*, April 21, 2015.

[5] "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," Securities and Exchange Commission, 2018.

[6] Sam Cook, "Malware Statistics and Facts for 2022," Comparitech, February 18, 2022.

[7] *Cost of a Data Breach Report 2021*, IBM Security, July 2021,.

[8] *2019 Global State of Cybersecurity in Small and Medium-Sized Businesses*, Ponemon Institute, October 2019.

[9] *2021 Data Breach Investigations Report*, Verizon, 2021, f

[10] Rob Sobers, "81 Ransomware Statistics, Data, Trends, and Facts for 2021," Varonis, July 2, 2021, **https://www.varonis.com/blog/ransomware-statistics-2021**.

[11] Brian Dean, "Social Network Usage and Growth Statistics: How Many People Use Social Media in 2022?," October 10, 2021, Backlinko.

[12] Daniel Ku, "Social Recruiting: Everything You Need To Know for 2022," PostBeyond, November 16, 2021.