



# Exploring Today's Risk Management and Insurance Landscape





# Exploring Today's Risk Management and Insurance Landscape

Edition Here Edition • Printing Here Printing

**The Institutes**

720 Providence Road, Suite 100

Malvern, Pennsylvania 19355-3433

© Copyright Year Here  
American Institute For Chartered Property Casualty Underwriters

All rights reserved. This book or any part thereof may not be reproduced without the written permission of the copyright holder.

Unless otherwise apparent, examples used in The Institutes materials related to this course are based on hypothetical situations and are for educational purposes only. The characters, persons, products, services, and organizations described in these examples are fictional. Any similarity or resemblance to any other character, person, product, services, or organization is merely coincidental. The Institutes are not responsible for such coincidental or accidental resemblances.

This material may contain internet website links external to The Institutes. The Institutes neither approve nor endorse any information, products, or services to which any external websites refer. Nor do The Institutes control these websites' content or the procedures for website content development.

The Institutes specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials.

The Institutes materials related to this course are provided with the understanding that The Institutes are not engaged in rendering legal, accounting, or other professional service. Nor are The Institutes explicitly or implicitly stating that any of the processes, procedures, or policies described in the materials are the only appropriate ones to use. The advice and strategies contained herein may not be suitable for every situation.

Edition Here Edition • Printing Here Printing • Print Month Here 2022

Library of Congress Control Number: LOC Here

ISBN: ISBN Here

# Welcome

To complement the online course, this course book is designed as a study aid. The online course provides the richest, and fullest, M-AB 134 course experience and best allows students to master the material and prepare for the credentialing exam.





# Contents

## 1

|                                                  |            |
|--------------------------------------------------|------------|
| <b>How Are Key Loss Exposures Managed?</b>       | <b>1.1</b> |
| Managing Personal Property Exposures             | 1.3        |
| Managing Personal Liability Exposures            | 1.8        |
| The Residential Risk Management Environment      | 1.12       |
| The Personal Vehicle Risk Management Environment | 1.17       |
| Summary                                          | 1.23       |

## 2

|                                                                     |            |
|---------------------------------------------------------------------|------------|
| <b>How Critical is Cyber Risk Management?</b>                       | <b>2.1</b> |
| Evaluating Cyber Risk Property Exposures                            | 2.3        |
| Assessing Cyber Risk Business Income Exposures                      | 2.7        |
| Evaluating Exposures Related to Data Breaches and Reputational Risk | 2.11       |
| Assessing Data Liability Exposures                                  | 2.16       |
| Summary                                                             | 2.22       |

## 3

|                                                      |            |
|------------------------------------------------------|------------|
| <b>How Can You Use Data to Your Advantage?</b>       | <b>3.1</b> |
| Strategic Opportunities From Big Data and Technology | 3.3        |
| Data Science                                         | 3.8        |
| Data-Driven Decision Making                          | 3.12       |
| <Enter Concept LO title here>                        | 3.15       |
| <Enter Concept LO title here>                        | 3.16       |
| Understanding Parametric Coverage and Why It Matters | 3.16       |
| Summary                                              | 3.21       |
| <b>Index</b>                                         | <b>1</b>   |





# How Are Key Loss Exposures Managed?



## Educational Objectives

- ▶ Analyze the techniques used by individuals and families to manage property loss exposures.
- ▶ Analyze the techniques used to manage personal liability loss exposures.
- ▶ Examine how homeowners insurance addresses personal risk management needs.
- ▶ Examine how auto insurance addresses personal risk management needs.

## Outline

Managing  
Personal Property  
Exposures

Managing  
Personal Liability  
Exposures

The Residential  
Risk Management  
Environment

The Personal  
Vehicle Risk  
Management  
Environment

Summary



# How Are Key Loss Exposures Managed?



## MANAGING PERSONAL PROPERTY EXPOSURES

Nearly all individuals and families have property that is subject to **property loss exposures** that can result in serious financial consequences. For example, a family's home could be destroyed by a windstorm, or an individual's belongings could be damaged in a flood. To protect themselves from these exposures, individuals and families and the insurance professionals they work with need to understand the sources of these exposures and the techniques used for managing them.

Property may be destroyed, damaged, stolen, or lost, or may otherwise suffer a decrease in value because of a particular cause of loss (or peril). Individuals and families face countless situations in their daily lives that present the possibility of a property loss that can harm them financially. However, by properly identifying and analyzing the property loss exposures they have and the risk management techniques that can be applied to them, individuals and families can employ the techniques that will best treat their unique exposures and shield themselves from potentially devastating financial consequences of loss.

### Property Loss Exposures

Individuals and families own two main categories of property that are exposed to loss: **real property (realty)** and **personal property**. Think of real property as real estate—it encompasses land; buildings; and things embedded in the land, like trees and plants. Personal property, on the other hand, is any other movable belonging that isn't attached to real property (although it may be on real property). To learn more, see "Examples of Property Exposed to Loss."

Individuals and families face loss exposures by owning or having a legal interest in any type of property. Selecting an appropriate risk management technique to treat these exposures requires understanding the sources and potential financial consequences of property losses.

#### Property loss exposure

A condition that presents the possibility that a person or an organization will sustain a loss resulting from damage (including destruction, taking, or loss of use) to property in which that person or organization has a financial interest.

#### Real property (realty)

Tangible property consisting of land, all structures permanently attached to the land, and whatever is growing on the land.

#### Personal property

All tangible or intangible property that is not real property.

---

### What Do You Know?

What are some financial consequences individuals and families can face if their property is damaged or destroyed?



[DA13543\_1]

*Feedback* : Damaged or destroyed property can result in any of these outcomes:

- Reduction in property value—The difference between the value of the property before the loss (pre-loss value) and after the loss (post-loss value)
- Increased expenses—Expenses in addition to normal living expenses that are necessary because of the loss, such as the cost of renting a hotel room following a house fire
- Lost income—Loss of income that results when property is damaged or destroyed, such as the loss of rent that can be collected on a property that is damaged by a hurricane


---

The sources of property loss exposures can be broken down into two general categories: natural risk sources and human risk sources.

As the term suggests, natural risks occur randomly in nature. Natural risk sources can be natural disasters that affect whole communities or isolated events that affect just one building, such as snow accumulation that causes a house's roof to collapse. Meanwhile, human risks are those created by human actions (either intentionally or unintentionally). To learn more, see "Natural Risk Sources Versus Human Risk Sources."


**Natural Risk Sources Versus Human Risk Sources**





**Natural Risk Sources**

Cave-in, drought, earthquake, erosion, evaporation, extreme humidity/temperature, fire, flood, hail, ice, landslide/mudslide, lightning, meteors, mildew, mold, rot, rust, vermin, volcanic activity, water, wind (for example, tornadoes, hurricanes, and typhoons)


**Human Risk Sources**

Arson, chemical leakage, collapse, electrical overload, explosion, fire and smoke, human error, machinery breakdown, mischief, molten materials, pollution, power outage/surge, riot, terrorism, theft, vandalism, vibration

[DA13543\_2]

## Risk Management Techniques for Property Loss Exposures

Individuals and families can use the **risk management process** to evaluate their property loss exposures and the best ways to manage them. Although this process was developed for organizations, individuals and families also can follow its steps to guide their risk management decisions. To learn more, see “Process for Managing Risk.”

### Risk management process

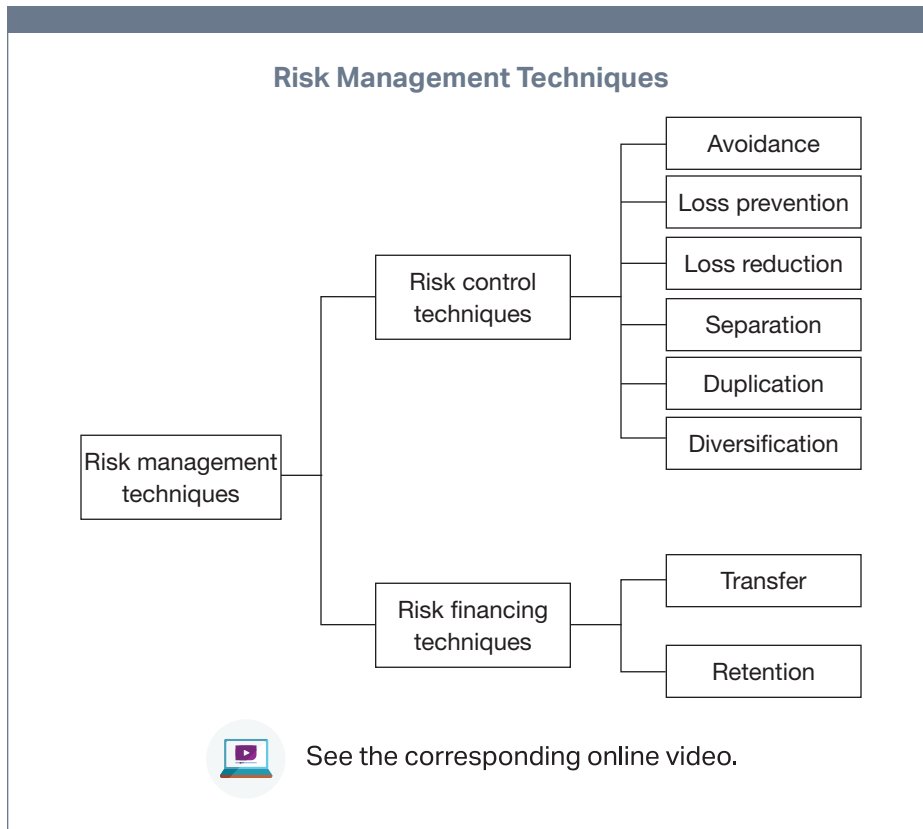
The method of making, implementing, and monitoring decisions that minimize the adverse effects of risk on an organization.



[DA13040\_1]

Five activities make up the process:

- Scan the environment—Loss exposures can be created by federal, state, and local laws, homeowners associations, condominium associations, the types of property owned, and various other factors present in the environment in which people live and work. Individuals, families, and the insurance professionals with which they work need to evaluate these (and other) environmental factors to determine where current exposures originate and where new ones may crop up.
- Identify risks—A comprehensive list of loss exposures that could affect an individual or a family needs to be developed. An insurance professional, such as a producer, can assist by providing checklists for this purpose. Friends or family members may help to identify risks by sharing their own loss histories and experience. It's not feasible or practical to identify all exposures, but it's essential to identify key and emerging exposures.
- Analyze risks—Risk analysis involves determining the source, likelihood, and potential consequences of each of the identified exposures and weighing them against the risk tolerance of the individual or family.
- Treat risks—Based on the analysis of each loss exposure, a treatment is selected for that exposure based on its ability to protect the financial security of the individual or family.
- Monitor and review—Effective risk management involves ongoing monitoring to determine the effectiveness of each selected treatment and



[DA00137]

whether changes need to be made. For example, if a family purchases a secondary vacation home, it almost certainly will also decide to purchase property insurance for the home.

Rather than a step-by-step process, this is instead a set of interconnected activities that occur simultaneously. To learn more, see “Risk Management Techniques.”

To learn more, see “Examples of Risk Management Techniques for Property Loss Exposures.”



Learn more from an expert in the online video.

### Examples of Risk Management Techniques for Property Loss Exposures

| Risk Management Technique | Property Loss Exposure                                     | Treatment                                                                            |
|---------------------------|------------------------------------------------------------|--------------------------------------------------------------------------------------|
| • Avoidance               | Theft of watercraft                                        | Do not purchase boat                                                                 |
| • Loss prevention         | Damage to building by vandalism                            | Put a fence around the building                                                      |
| • Loss reduction          | Home burglary                                              | Install burglar alarm                                                                |
| • Separation              | Theft of jewelry                                           | Keep only some valuables at home, while others are kept in off-site safe deposit box |
| • Duplication             | Destruction or theft of valuable documents                 | Make copies or store electronically                                                  |
| • Diversification         | Destruction of investment properties by a single hurricane | Purchase properties in different areas of the country                                |
| • Retention               | Wear and tear on clothing                                  | Budget for replacements                                                              |
| • Transfer                | Property damage resulting from fire                        | Purchase an insurance policy that transfers the risk to an insurer                   |

[DA00136]

## MANAGING PERSONAL LIABILITY EXPOSURES

### Liability loss exposure

Any condition or situation that presents the possibility of a claim alleging legal responsibility of a person or business for injury or damage suffered by another party.

### Damages

Money claimed by, or a monetary award to, a party who has suffered loss or injury for which another party is legally responsible.

All individuals and families have personal **liability loss exposures** that can reduce their financial assets. They stem from the possibility of being sued or held responsible for someone else's injury or for damage to their property. Knowing the legal bases for and financial consequences of these loss exposures is critical to selecting the personal liability risk management techniques that will best ensure the financial security of an individual or a family.

Owning property, driving a car, entering into contracts with others, and many other actions create personal liability loss exposures that can produce a financial loss. Even if people are successfully able to defend themselves against liability claims—and therefore don't have to pay **damages**—they will incur legal defense costs and other claim-related expenses. They can also face potentially adverse publicity, which can harm an individual's personal or professional reputation.



This section examines the different types of personal liability loss exposures individuals and families face and the risk management techniques they can use to protect themselves from financially devastating liability losses.

## Personal Liability Loss Exposures

Liability loss typically results from the breach of a legal duty with regard to the ownership or use of property, as well as from contractual agreements (contractual liability) and statutory or regulatory requirements (statutory liability). The cause of loss associated with a liability loss exposure is the claim of liability or the filing of a lawsuit.

For example, if a houseguest falls off a homeowner's deck and is injured, the guest might sue the homeowner, who then may be required to pay damages for the resulting medical expenses and wages the guest loses during recuperation. This is because the homeowner has a legal duty to ensure the deck is safe. As another example, if a renter breaches a lease agreement (breach of contract), the landlord can sue the renter for lost rental income.

---

### What Do You Know?

What types of financial consequences can individuals or families face as a result of a liability claim against them?

*Feedback* : When a liability claim occurs, an individual or a family can suffer two major financial consequences:

- Costs of a legal investigation and defense
- Money damages awarded if the defense isn't successful or if the claim is settled out of court

In theory, the financial consequences of a liability loss exposure are limitless. In practice, financial consequences are limited to the total wealth of the responsible party. Although some jurisdictions limit the amounts that can be taken in a claim, liability claims can result in the loss of most or all of a person's assets, as well as in a claim on future income.

---

Often, damages awarded in a liability judgment take the form of **special damages** or **general damages**. To learn more, see "Special Damages and General Damages."

**Punitive, or exemplary, damages** can also be imposed against individuals and families, but it's more common for them to be levied against companies.

The resolution of liability disputes between individuals and the indemnification for wrongs committed against individuals are within the scope of **civil law**. By contrast, criminal law deals with conduct that endangers the public

#### Special damages

A form of compensatory damages that awards a sum of money for specific, identifiable expenses associated with the injured person's loss, such as medical expenses or lost wages.

#### General damages

A monetary award to compensate a victim for losses, such as pain and suffering, that do not involve specific, measurable expenses.

#### Punitive damages (exemplary damages)

A payment awarded by a court to punish a defendant for a reckless, malicious, or deceitful act to deter similar conduct; the award need not bear any relation to a party's actual damages.

#### Civil law

A classification of law that applies to legal matters not governed by criminal law and that protects rights and provides remedies for breaches of duties owed to others.

### Special Damages and General Damages



#### Special Damages

- Also called particular damages or out-of-pocket losses
- Can include amount spent to restore lost property, hospital and doctor bills and related expenses for bodily injury, and loss of wages and earnings



#### General Damages

- Also called direct damages or necessary damages
- Often presumed when special damages are proved
- Can include compensation for pain and suffering; future effect of disfigurement, loss of a limb, sight, or hearing; as well as emotional distress

 See the corresponding online video.

### Tort

A wrongful act or an omission, other than a crime or a breach of contract, that invades a legally protected right.

### Negligence

The failure to exercise the degree of care that a reasonable person in a similar situation would exercise to avoid harming others.

### Intentional tort

A tort committed by a person who foresees (or should be able to foresee) that his or her act will harm another person.

### Strict liability (absolute liability)

Liability imposed by a court or by a statute in the absence of fault when harm results from activities or conditions that are extremely dangerous, unnatural, ultrahazardous, extraordinary, abnormal, or inappropriate.

[DA13294]

welfare, such as the crimes of murder, rape, and fraud. Because such criminal acts are generally not the subject of insurance, civil law provides the legal foundation of insurance. The most common personal liability claims that fall under civil law involve **tort** liability, contractual liability, and statutory liability.

An individual may face a claim for tort damages based on an act of **negligence**, **intentional tort**, or **strict liability**. To learn more, see “Types of Torts.”

## Risk Management Techniques for Personal Liability Loss Exposures

Individuals and families can use the risk management process to evaluate and manage liability loss exposures in the same way they can for property loss exposures. To learn more, see “Activities in the Risk Management Process.”

Similarly, the risk management techniques used for treating liability loss exposures mirror those used for property loss exposures—that is, individuals and families use risk control or risk financing techniques (or a combination

## Types of Torts

|                   | Description                        | Element(s)                                                                                                                                                                                           | Examples                                                                                                                                                                  |
|-------------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Negligence        | Failure to act in a prudent manner | <ul style="list-style-type: none"> <li>• Duty owed to another</li> <li>• Breach of that duty</li> <li>• Breach of duty is proximate cause of injury or damage</li> <li>• Injury or damage</li> </ul> | <ul style="list-style-type: none"> <li>• Driving while intoxicated and causing an accident</li> <li>• Allowing a pet dog to run loose and bite a child</li> </ul>         |
| Intentional Torts | Deliberate acts that cause harm    | Deliberate act (other than a breach of contract) that causes harm to another person                                                                                                                  | <ul style="list-style-type: none"> <li>• Assault</li> <li>• Battery</li> <li>• Libel</li> <li>• Slander</li> <li>• False arrest</li> <li>• Invasion of privacy</li> </ul> |
| Strict Liability  | Inherently dangerous activities    | Inherently dangerous activities or dangerously defective products that result in injury or harm                                                                                                      | <ul style="list-style-type: none"> <li>• Owning a wild animal</li> <li>• Blasting operations</li> </ul>                                                                   |



See the corresponding online video.

[DA02532]

of both) to manage their liability loss exposures and ensure their well-being and financial security. To learn more, see “Examples of Risk Management Techniques for Liability Loss Exposures.”

It’s important to note that if people do not identify or plan to treat loss exposures, they retain them by default. Unplanned retention is the inadvertent assumption of a loss exposure that has not been identified or accurately analyzed. For example, an individual or a family may unintentionally retain losses if they select inadequate insurance policy limits. To illustrate, if an insured with an auto liability limit of \$100,000 is at fault in an auto accident that seriously injures another party, the insured may be liable for more than \$100,000 in damages and required to pay the amount in excess of that figure. The excess amount, therefore, represents an unplanned retention.



Learn more from an expert in the online video.



[DA13547\_1]

## THE RESIDENTIAL RISK MANAGEMENT ENVIRONMENT

Individuals and families have a variety of personal risk management needs related to their property and liability loss exposures. Homeowners insurance addresses many of these needs and can help ensure the financial security and well-being of policyholders. But homeowners insurance forms differ based on types of property eligible for coverage and types of coverage provided. Selecting appropriate insurance requires an examination of the different forms available as well as how the risk environment is evolving.

To address the risk management needs of homeowners, people who rent or lease their residence, and those who own private condominium units used for residential purposes, a variety of homeowners coverage forms have been created. The most prominent are those in the Insurance Services Office, Inc. (ISO) Homeowners (HO) insurance program. This section examines the different types of forms offered under the ISO HO program, as well as how emerging technology is changing the homeowners insurance environment.

### Examples of Risk Management Techniques for Liability Loss Exposures

| Risk Management Technique | Liability Loss Exposure                            | Treatment                                                          |
|---------------------------|----------------------------------------------------|--------------------------------------------------------------------|
| • Avoidance               | Injury/drowning in a swimming pool                 | Do not install pool                                                |
| • Loss Prevention         | Liability suit caused by injury on slippery floors | Install nonslip rugs                                               |
| • Loss Reduction          | Being held liable for damage to a rental property  | Include a limit of liability in contract                           |
| • Retention               | Serious injury to someone on your property         | Relying on savings to cover damages above insurance policy limit   |
| • Transfer                | Dog will bite and injure a pedestrian              | Purchase an insurance policy that transfers the risk to an insurer |

[DA13547\_2]

## Homeowners Insurance Forms

The ISO HO program offers six policy forms:

- Homeowners 2—Broad Form (HO-2)
- Homeowners 3—Special Form (HO-3)
- Homeowners 4—Contents Broad Form (HO-4)
- Homeowners 5—Comprehensive Form (HO-5)
- Homeowners 6—Unit-Owners Form (HO-6)
- Homeowners 8—Modified Coverage Form (HO-8)

Each of these forms varies based on who is eligible for them and the types of coverage they provide. To learn more, see “Homeowners Policy Forms and Covered Perils.”

The HO-3 is a widely used policy form because it provides valuable coverage for the majority of owner-occupied dwellings. As a result, insurance professionals typically study the HO-3 to develop a basis for understanding a variety of HO forms.

The HO-3 is designed for the owner-occupants of a one- to four-family dwelling, as opposed to owners who do not occupy the dwelling. It provides coverage for a house, its contents, and the occupants’ liability and is designed to be broad enough to cover the property and liability insurance needs of most families.

### Homeowners Policy Forms and Covered Perils

| Policy Form                    | Coverage Provided                                                                                                                                                                                                                                                        | Covered Perils                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HO-2<br>Broad Form             | This form provides coverage for owner-occupants of dwellings. It provides Section I coverages on a named perils basis and provides Section II coverage.                                                                                                                  | Fire or lightning; windstorm or hail; explosion; riot or civil commotion; aircraft; vehicles; smoke; vandalism or malicious mischief; theft; volcanic eruption                                                                                                                                                                                                       |
| HO-3<br>Special Form           | This form provides coverage for owner-occupants of dwellings. It insures the dwelling and other structures on an open perils basis and personal property on a named perils basis. Section II coverage is also provided.                                                  | For dwelling and other structures: open perils. For personal property: Broad Form covered perils, plus falling objects; weight of ice, snow, or sleet; accidental discharge or overflow of water or steam; sudden and accidental tearing apart; cracking, burning, or bulging; freezing; sudden and accidental damage from artificially generated electrical current |
| HO-4<br>Contents Broad Form    | This form is designed for tenants and other occupants of dwellings or apartments. It insures a tenant's personal property on a named perils basis (no dwelling coverage is included). Section II coverage is also provided.                                              | Broad Form covered perils                                                                                                                                                                                                                                                                                                                                            |
| HO-5<br>Comprehensive Form     | This form is designed for owner-occupants of dwellings. It provides the broadest coverage of all the homeowners forms. It insures the dwelling, other structures, and personal property on an open perils basis. Loss of use and Section II coverages are also provided. | Open perils on dwelling, other structures, and personal property (loss of use coverage based on loss sustained under Coverages A, B, and C)                                                                                                                                                                                                                          |
| HO-6<br>Unit-Owners Form       | This form is designed for the owners of residential condominium units. It insures personal property on a named perils basis, with limited dwelling coverage (unit improvements and betterments). Loss of Use and Section II coverages are also provided.                 | Broad Form covered perils                                                                                                                                                                                                                                                                                                                                            |
| HO-8<br>Modified Coverage Form | This form is a more limited form of coverage for owner-occupants of dwellings. Insures the dwelling, other structures, and personal property on a limited, named perils basis.                                                                                           | Fire or lightning, windstorm or hail, explosion, riot or civil commotion, aircraft, vehicles, smoke, vandalism or malicious mischief, theft, volcanic eruption                                                                                                                                                                                                       |



See the corresponding online video.

[DA00460]

Many endorsements are available to modify HO policies to further enable them to meet the specific needs of individuals and families. Endorsements can increase or decrease limits, add or remove coverages, change definitions, clarify policy intent, or recognize specific characteristics that require a premium increase or decrease. To learn more, see “Selecting Appropriate ISO Homeowners Policy Forms.”

### Selecting Appropriate ISO Homeowners Policy Forms

Which HO form would be most appropriate for an apartment tenant who needs personal property coverage but does not require dwelling coverage?

- HO 3—Special Form
- HO 4—Contents Broad Form (correct)
- HO 5—Comprehensive Form
- HO 6—Unit-Owners Form

Which HO form would be most appropriate for a condominium unit owner who needs personal property coverage and limited dwelling coverage?

- HO 3—Special Form
- HO 4—Contents Broad Form
- HO 5—Comprehensive Form
- HO 6—Unit-Owners Form (correct)



See the corresponding online video.

[DA13545]

## How the Environment Is Evolving

Traditionally, home insurers have depended on past claims data to assess risk and set prices for large groups of customers. In addition, they've used detailed (and sometimes long) investigative processes to adjust claims. Now, the insurance model is shifting to a more proactive risk management model, thanks to the use of the **internet of things (IoT)** and smart devices in insureds' homes. Not only does this technology provide detailed, real-time data about the systems and appliances within homes, but it can also detect hazards and protect against loss.

For example, risk control techniques such as leak sensors deployed near water heaters, washing machines, sinks, and toilets can alert homeowners and insurers to potential flood hazards and trigger remediation measures. If a smart valve is installed on the main water line for a house, a sensor could trigger the valve to shut off the water supply to prevent water damage. The data that can then be provided to insurers from scenarios like this can aid in everything from personalized pricing to claims handling.



Learn more from an expert in the online video.

### Internet of Things (IoT)

A network of objects that transmit data to each other and to central hubs through the internet.








**Blockchain**

A distributed digital ledger that facilitates secure transactions without the need for a third party.

Sensors are also facilitating the use of smart contracts, which create efficiencies in the insurance process. Smart contracts are self-executing contracts that use **blockchain** technology to perform insurance functions, such as issuing claim payments, as soon as the terms of a contract are met. To learn more, see “Sensors in the Home.”

**Sensors in the Home**

Examples of technology used for prevention and reduction of property and liability loss exposures:

-  **Motion detectors/lighting**  
Turn on exterior lights for guests and deter thieves
-  **Wi-Fi cameras**  
Detect children and pets approaching a swimming pool, as well as fire, smoke, flood, snow, and thieves
-  **Water sensors**  
Prevent flooding
-  **Smoke and carbon monoxide detectors**  
Reduce fire losses and prevent injuries to occupants
-  **Heat sensors**  
Detect when a stovetop burner is left on or a fire is smoldering in a fireplace
-  **Smart speakers/microphones**  
Monitor for sounds of intrusion
-  **Connected appliances/heating and cooling systems**  
Monitor operating systems and detect malfunctions

[DA13544]

One potential drawback to the growing use of IoT and smart devices: The data collected from them exposes homeowners and insurers to data breaches. As a result, insurers need to have safeguards in place to protect customer privacy and ensure they are abiding by any data security regulations to which they are subject.



### Apply Your Knowledge

How might a smart contract be beneficial to a homeowner and an insurer?

*Feedback :* Smart contracts benefit insureds by providing them with a claim payment immediately after a loss occurs that satisfies terms within the contract. They benefit insurers by eliminating the need for adjuster involvement in a claim.

Suppose a smart contract promised that an insured would receive an agreed-upon claim payment if the insured's basement was flooded with a foot of water. If a sensor in the insured's basement detects a foot of water there, that data would be collected and transmitted using blockchain technology and automatically trigger the claim payment.

## THE PERSONAL VEHICLE RISK MANAGEMENT ENVIRONMENT

Operating an automobile creates a variety of property and liability loss exposures. For example, suppose Byron is driving his car, runs through a stop sign at a high speed, and collides with a car carrying a family of four. The family's car is damaged beyond repair, and three family members are taken to the hospital with significant injuries. Byron may be held responsible for compensating the family for the damage to their car and their injuries. The financial consequences for Byron may be significant, and he may not be able to afford to cover them on his own.

For situations such as this, several types of auto insurance were created to provide coverage for the loss exposures of those who operate automobiles and to provide a means of compensation to those who are injured or incur property damage resulting from auto accidents that are the fault of other drivers. Selecting the appropriate level of coverage for an insured requires an understanding of how auto insurance functions and is regulated.

In the United States, people who are injured or have property damaged in auto accidents that are the fault of others are entitled to compensation. The tort liability system, which is based on fault, is the traditional and most commonly used method of seeking compensation for injured auto accident victims. Under this system, injured auto accident victims must prove that another party was at fault before they can collect damages from that party.

To ensure at-fault drivers have a means to compensate auto accident victims, most states have enacted **compulsory auto insurance laws** that require motorists to obtain auto liability insurance in order to be permitted to drive legally within the state. Other states have enacted **financial responsibility**

#### Compulsory auto insurance law

Law that requires the owners or operators of automobiles to carry automobile liability insurance at least equal to certain minimum limits before the vehicle can be licensed or registered.

#### Financial responsibility law

Law enacted to ensure that motorists have the financial ability to pay for any property damage or bodily injury they might cause as a result of driving or owning an auto.

**laws** requiring motorists to provide proof that they have a means (such as liability insurance) to pay for damages resulting from motor vehicle accidents.

In either case, purchasing auto insurance is the primary way motorists comply with these regulations. However, there can be subtle differences in the way auto insurance functions based on where it's purchased, whether it's purchased by a high-risk driver, how it's regulated, and what technology insurers have adopted.

### Variations in State Law

Auto insurance laws vary by state. Most states are at-fault states, while others are no-fault states. Insurance professionals and drivers need to know the differences between these two broad categorizations of auto insurance law to know how a particular policy will apply to an accident.

---

#### **What Do You Know?**

What's the difference between at-fault and no-fault automobile laws?

*Feedback :* At-fault states use the tort liability system to determine who is responsible for the financial consequences of an auto accident. Typically, each insurer pays for damages according to the degree that the insured person is at fault (subject to policy limits). If the party that is not at fault doesn't agree with the payout from the at-fault driver's insurer, it can file a lawsuit to seek additional damages, both economic (such as medical expenses and lost wages) and noneconomic (such as pain and suffering, emotional distress, and disfigurement).

In no-fault states, an injured person does not need to establish fault and prove negligence to collect payment for bodily injuries. Automobile insurance covers accident victims on a first-party basis, allowing them to collect damages from their own insurers regardless of who was at fault. Most no-fault laws apply only to bodily injury and not to property damage.

---

#### **Personal injury protection (PIP) coverage**

Coverage that pays benefits, regardless of fault, for medical expense, income loss, and other benefits, resulting from bodily injury to occupants of a covered auto.

No-fault laws authorize or mandate the use of **personal injury protection (PIP) coverage** and define the benefits that insurers can or must provide in those states. They tend to remove small bodily injury claims from the court system.



Learn more from an expert in the online video.

No-fault states have enacted no-fault laws to differing degrees, which have resulted in three types of no-fault plans:

- **Modified no-fault plans**—These place some restrictions on the right to sue an at-fault driver but do not entirely eliminate this right. Under a modified no-fault plan, injured motorists collect economic losses from their own insurers through the PIP benefits mandated by the plan. They then have the ability to sue at-fault drivers for any economic losses that exceed the no-fault coverage limits and for noneconomic losses if their injuries exceed a threshold stated in the law.
- **Add-on plans**—These add no-fault benefits to auto insurance policies but place no restrictions on the injured person's right to sue a negligent party for damages.
- **Choice no-fault plans**—Under these plans, insureds can choose whether to be covered on a modified no-fault basis. In most states with choice no-fault plans, insureds who choose not to be covered on a modified no-fault basis must purchase add-on no-fault coverages.

## Auto Insurance for High-Risk Drivers

Although drivers in many states are required by law to purchase auto insurance, insuring high-risk drivers is extremely difficult for private insurers. These include drivers who habitually violate traffic laws; have been responsible for an excessive number of traffic accidents; and/or have been convicted of certain serious offenses, such as reckless driving, driving with a suspended license, or driving under the influence of alcohol or drugs.

High-risk drivers usually don't meet private insurers' underwriting standards. For drivers who cannot obtain insurance from private insurers in the voluntary market, states have created a **residual market** (also called a shared market).

Various programs exist for high-risk drivers in the residual market, including these:

- **Automobile insurance plans**—Programs for insuring high-risk drivers in which all auto insurers doing business in the state are assigned their proportionate share of such drivers based on the total volume of auto insurance written in the state.
- **Joint underwriting associations (JUAs)**—Organizations to which a limited number of insurers are designated as servicing insurers to handle high-risk drivers. All auto insurers in the state are then assessed a proportionate share of the losses and expenses based on their percentage of the voluntary auto insurance premiums written in the state.
- **Reinsurance facility**—A pool arrangement in which insurers accept all auto insurance applicants who have a valid driver's license and assign the premiums and losses for high-risk drivers to the pool. All insurers in the

### Residual market

The term referring collectively to insurers and other organizations that make insurance available through a shared risk mechanism to those who cannot obtain coverage in the admitted market.

pool share the losses and expenses of the facility in proportion to the total auto insurance they write in that state.

## Auto Insurance Rate Regulation

States regulate auto insurance rates. While states' rating laws can vary, they generally require insurers to use rates that are adequate to pay all claims and expenses, reasonable (not excessive) for the exposure presented, and not unfairly discriminatory.

---

### **What Do You Know?**

What constitutes unfair discrimination in auto insurance rating?

*Feedback* : Unfair discrimination occurs when an insurer applies different standards or treatment to insureds that present objectively similar loss potential. For example, charging higher-than-normal rates for an applicant based solely on the applicant's race, religion, or ethnic background is unfair discrimination.

---

Primary rating factors are the major factors that most states and insurers use for determining the cost of personal auto insurance. Although these factors have been used for many years in rating auto insurance, several states no longer permit the use of some factors that they consider unfairly discriminatory, such as age and gender.

In addition to primary rating factors, other factors also affect loss statistics. Typically, these factors are not essential in determining the rating classification. To learn more, see "Primary and Other Rating Factors."

Using rating factors, insurers often divide auto insurance applicants into homogeneous classes, or rating categories, such as "preferred," "standard," and "nonstandard," that reflect different levels of exposure to loss. For example, applicants with good driving records and rating factors that suggest they present minimal loss exposure are categorized as preferred. By offering lower rates to this category, insurers hope to attract and retain good customers.

Some insurers also give discounts or credits for certain automobile features or practices of the insured that reduce insurer costs. To learn more, see "Potential Sources of Discounts and Credits."

## How the Environment Is Evolving

Auto insurance rates are increasingly being affected by technology. Internet of Things (IoT) devices, such as in-car sensors, telematics instruments, smartphones, and global positioning systems (GPS), allow driving behavior data

## Primary and Other Rating Factors

### Primary Rating Factors:

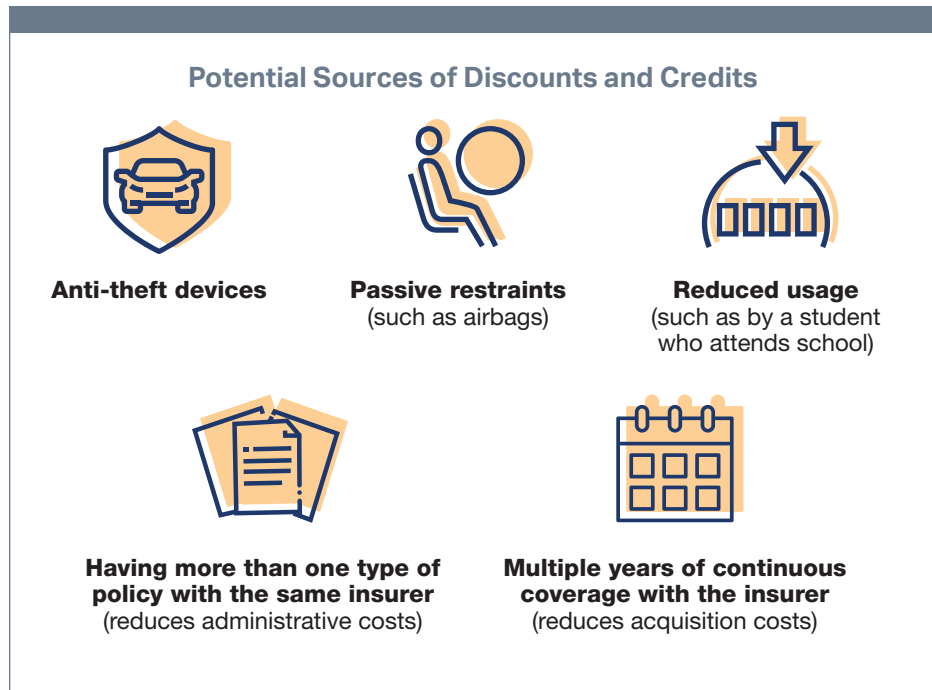
- Territory—Usually defined by the location of the insured's residence. Rural territories often have lower rates than urban territories because loss frequency and claim expenses tend to be higher in cities.
- Use of the auto—Typical "use" categories include pleasure, driving to work or school, business, and farm use. Rates are generally lowest for farm and highest for business use.
- Age—Young drivers have less driving experience and tend to be involved in accidents more frequently than older drivers.
- Gender—In the past, women tended to have fewer accidents than men in the same age categories, particularly among youthful drivers, so rates are often lower for women.
- Marital status—Young married men tend to have fewer accidents than young unmarried men, and rates often reflect this tendency.

### Other Rating Factors:

- Driving record—Almost all insurers use an applicant's driving record to determine whether the individual presents an acceptable exposure.
- Driver education—A discount may be provided for drivers who complete an approved driver education or training course.
- Good student—Students who maintain good grades may be offered premium discounts because, theoretically, they have fewer accidents than poor or average students.
- Multi-car policy—Most insurers give a multi-car discount based on the assumption that two or more autos owned by the same insured will not be driven as often as a single auto.
- Years of driving experience—Generally, drivers with more years of experience make fewer mistakes and have fewer accidents.
- Credit-based insurance score—These scores are based on an individual's financial history (without income data). Research indicates that insureds with low insurance scores submit more claims than insureds with high insurance scores. (Some states consider insurance scores unfairly discriminatory and do not allow them as a rating factor.)
- Type of auto—The performance, age, and damageability of an auto can affect the rates for physical damage coverage on it.
- Deductibles—Insureds who choose higher deductibles for collision and other physical damage coverage on their autos can receive a credit because the insured retains a portion of covered losses.
- Liability limits—Rates are generally based on the minimum liability limits required by the state, and premiums increase if the insured chooses higher limits.



See the corresponding online video.



[DA13571]

to be monitored and transmitted to third parties and insurers. IoT devices can report data on a vehicle's speed, acceleration, deceleration, location, miles driven, and more. The ability to collect and analyze this data has given rise to usage-based insurance, in which premiums are linked to driving history and performance.



Learn more from an expert in the online video.

In addition to the ability to track driving behavior, in-car sensors and radar systems can be used to prevent accidents. This technology facilitates the use of driver-assistance and semiautonomous systems that can perform a variety of functions to help prevent accidents, such as apply brakes, alert drivers to lane departures and potential collisions, and switch a vehicle's headlights from high to low beams when oncoming vehicles approach.



Learn more from an expert in the online video.

## SUMMARY

Individuals and families who own real or personal property are subject to property loss exposures. When property is damaged or destroyed by natural or human risk sources, it can result in a reduction in property value, increased expenses, and lost income. Risk control and risk financing are the two broad categories of risk management techniques. Risk control techniques include avoidance, loss prevention, loss reduction, separation, duplication, and diversification. Risk financing techniques include retention and transfer.

Individuals and families can be sued for injuring another party or damaging another party's property. As a result, they have liability loss exposures that can reduce their financial assets. When involved in a liability lawsuit, people may be responsible for paying legal defense costs, as well as special, general, and/or punitive damages. Risk control or risk financing techniques (or a combination of both) can be used manage liability loss exposures.

Homeowners insurance helps protect the financial security of policyholders by addressing many of their property and liability loss exposures. A variety of homeowners coverage forms are available, which vary by the types of property they cover and the types of coverage they provide. The most prominent forms are those in the ISO Homeowners insurance program. The growing use of IoT and smart devices in insureds' homes is causing insurers to adopt an increasingly proactive approach to risk management.

In the U.S., people are entitled to compensation when they suffer property damage or injury as a result of an auto accident that was the fault of others. For this reason, driving a vehicle creates numerous property and liability loss exposures. Several types of auto insurance provide coverage for these exposures. However, auto insurance can function differently based on where it's purchased, whether it's purchased by a high-risk driver, how states regulate insurance rates, and what technology insurers have adopted.





# How Critical is Cyber Risk Management?

# 2

## Educational Objectives

- ▶ Evaluate cyber risk loss exposures associated with an organization's tangible and intangible property.
- ▶ Evaluate these aspects of the business income loss exposure:
  - Measurement of business income loss
  - Effect on expenses
  - Property and perils involved
- ▶ Evaluate cyber loss exposures related to data breaches and organizational reputation.
- ▶ Propose a set of best practices for an organization to assess its third-party liability loss exposures that can result from a cyber incident.

## Outline

Evaluating Cyber Risk Property Exposures

Assessing Cyber Risk Business Income Exposures

Evaluating Exposures Related to Data Breaches and Reputational Risk

Assessing Data Liability Exposures

Summary



# How Critical is Cyber Risk Management?

# 2

## EVALUATING CYBER RISK PROPERTY EXPOSURES

To create an effective cyber risk management program, organizational leaders and risk managers need to consider all the potential cyber loss exposures their businesses face. This process starts by evaluating property exposures. Failing to adequately account for and protect against these exposures can lead to catastrophic financial loss.

Most business activities are conducted using computer systems. As a result, nearly all organizations have some **cyber risk**. When data processing, storage, and communication systems are compromised accidentally or through a **data breach**, the financial consequences can be devastating, particularly when property is affected.

**Tangible property** and **intangible property** alike are susceptible to cyber risk, so effective cyber risk management begins by considering both. This section will provide examples of these types of property.

---

### What Do You Know?

What type of property is associated with losses that are the most difficult to quantify but likely the most significant?

*Feedback :* The most difficult losses to quantify, which are typically the most significant, are associated with intangible property, such as data assets and intellectual property.

---

### Tangible Property

To determine the most effective risk control techniques, an organization's risk manager needs to assess all of the tangible property that is exposed to cyber risk. The form of tangible property most commonly associated with cyber risk is physical media and the hardware by which it is stored or processed.

Physical media and associated hardware refer to the physical materials, devices, or tools used to store, process, and transmit data. These can be computers, servers, phones, smart tablets, routers, modems, portable storage

#### Cyber risk

The possibility that data will end up in the possession of a party who is not authorized to have that data and who can use it in a manner that is harmful to the individual or organization that is the subject of the data and/or the party that collected and stored the data.

#### Data breach

An incident in which confidential or privileged information that is stored in a computer system is accessed or obtained by an unauthorized party.

#### Tangible property

Property that has a physical form.

#### Intangible property

Property that has no physical form.

### Malware

Malicious software, such as a virus, that is transmitted from one computer to another to exploit system vulnerabilities in the targeted computer.

drives, and more. The hardware and software in these devices can be damaged by a data breach, employee negligence, or third-party saboteurs using **malware** or other means. Damage to physical media is the most readily discernable and quantifiable type of property loss related to cyber risk loss exposures.

Tangible property susceptible to cyber risk also includes more traditional property, such as physical structures and equipment. People don't often associate damage to this type of property with cyberthreats, but as organizations become more reliant on computer systems to control operations, cyberattacks are becoming increasingly more destructive.

Here are some ways cyberattacks have resulted in damage to structures and equipment:

- Cyberattackers hacked into a German steel mill's control system and prevented a blast furnace from shutting down properly. The emergency shutdown that had to be performed resulted in significant damage.
- Hackers tapped into a power grid in Ukraine and caused a widespread blackout.
- A single hacker was able to gain access to the operational network of a water treatment and waste management facility in Australia. The hacker then used this access to spill hundreds of thousands of gallons of raw sewage into local waterways and parks.

Cyberattacks can also cause bodily injuries and damage to goods and equipment by tricking sensors and shutting down safety features. For example, hackers can potentially feed false data to or shut down sensors located along a gas pipeline so that operators don't know when pressure inside the pipeline reaches an unsafe level. This can lead to an undetected gas leak or explosion.

## Intangible Property

Implementing proper risk controls also requires a thorough assessment of all the intangible property exposed to cyber risk, such as the data assets of an organization. The most significant direct costs associated with cyber risk typically stem from liability loss exposures related to an organization's protection of consumer data. A large-scale data breach that results in consumers' **personally identifiable information** being exposed to or acquired by an untrusted third party can result in significant financial and reputational damage for an organization.

Potentially devastating direct costs related to a data breach are also associated with cyberextortion, a cybercrime in which a third party demands a ransom in exchange for the restoration of data it has stolen or compromised. To learn more, see "Calculating the Cost of a Data Breach."

**Intellectual property** (such as trade secrets, proprietary data about competitors, and creative output), which often resides in the same media and

### Personally identifiable information (PII)

Unique identifying information, such as name, address, or Social Security number, used separately or in conjunction with other information, that requires safeguarding and confidentiality.

### Intellectual property

The product of human intelligence that has economic value.

### Calculating the Cost of a Data Breach

The average cost of a data breach is generally expressed as a cost per compromised record. The calculation combines an analysis of factors such as these:

- Cause of the breach—Certain types of breaches are easier to contain than others, and the fines and penalties associated with different types of breaches vary.
- Number of records exposed—The larger the scale, the higher the cost.
- Types of information exposed—This is important for estimating fines and penalties, as well as remediation costs.
- How quickly it was contained—The longer it takes to detect and contain a breach, the more data that's compromised and the harder it is to investigate.
- Number of prior breaches—There may be additional fines and penalties for subsequent breaches.
- Damage to physical media—Did the breach occur because of lost or stolen equipment that needs to be replaced? Are any essential systems damaged?
- Investigation requirements—The more complex a network or a breach is, the more costly it is to investigate.
- Communication requirements—What activities are necessary to report the breach to appropriate personnel?
- Notification requirements—How is the organization required to notify affected individuals?
- Industry and location—Fines and penalties also vary based on what an organization does, its geographic location, and its global reach.
- Redress activities—How is the organization helping affected individuals recover from the breach? For example, is it providing a customer hotline and/or paying for credit monitoring?
- Business restoration plans—How is the organization replacing, reconstructing, or restoring compromised data and resuming operations?
- Media coverage—The more publicity a breach receives, the more it hurts a company's reputation.
- Lost opportunities—Negative publicity around a data breach causes reputational damage that results in higher customer churn, and it makes it more difficult and more expensive to acquire new customers.

[DA13203]

repositories as an organization's business-transaction data, is the least quantifiable type of intangible property subject to cyberloss. But it can prove to be the most costly type if it's compromised or lost.

Intellectual property derives its value from the right of its owner to exclude others from using it. But even intellectual property that is protected by copyright, trademark, patent, or trade-secret status is still vulnerable to infringement by third parties—particularly as technology makes it easier to be stored, transferred, and transmitted.

## 2.6 Exploring Today's Risk Management and Insurance Landscape

---

Because intellectual property is key to an organization's identity, market share, competitive strategies, and overall worth, its value must be determined before it is subject to compromise or a cyberattack. The value of intellectual property is used to determine the proportion of risk management resources devoted to it.

### Business interruption

Loss of revenue that a business or another organization sustains because its operations are suspended as a result of physical injury to its property.

**Business interruption** is another threat generally considered with property exposures. Restoration of operations following a cyberattack may require an organization to invest resources in the replacement and/or reconstruction of the damaged or otherwise compromised data. This may be accomplished in several ways, including by:

- Accessing a copy of the data—If an organization stores a copy of the data in either an on-site repository or an external repository (for example, a business partner's repository) that was not compromised, it may be able to seamlessly resume normal operations following a data breach.
- Using a third-party data-recovery service—An organization may engage a third party to recover data entombed on a compromised medium or to reconstruct data that is only partially recoverable.
- Collaborating with business partners—An organization that shares data with a business partner (for example, a third-party order-fulfillment facility) may be able to use the third party's data to reconstruct elements of data lost in a breach.

---

### Check Your Understanding

KraftToyy, Inc., is a successful toy retailer. Half of its business is generated online through KraftToyy's website, and half is generated in its brick-and-mortar retail location. Monica, the organization's risk manager, has discovered that the personally identifiable information of the company's online customers, which was stored on a single server, may have been exposed to an untrusted third party in a data breach. Describe some cyber risk property exposures KraftToyy may have as a result of this breach.

*Feedback* : KraftToyy may have to repair or replace tangible property in the form of physical media and associated hardware, such as the company's server if it was damaged as a result of the data breach. The company may also have liability loss exposures related to the intangible data assets, such as customers' personal information, that were exposed to an untrusted third party. In addition, it may suffer from business interruption on its website if the server is inoperable.

---

## ASSESSING CYBER RISK BUSINESS INCOME EXPOSURES

Threats to business income can be some of the biggest cyber risk exposures an organization faces—yet they are some of the least understood. Business income cyber losses occur when a data breach or some other cyberattack renders a business unable to function and generate revenue for a period of time.

Let's say that EntelliChip, Inc., is a microprocessor manufacturer that runs all of its production and order-fulfillment systems on the same network. A hacker penetrates the network and infects the interconnected systems with malware that damages essential software and hardware. As a result, EntelliChip has to stop operations for three weeks, which of course leads to business income losses. To select and apply the risk management techniques that best prepare the company for such an attack, the risk manager must understand how to assess and calculate business income loss exposures.

While quantifying the damage to tangible property (such as computers and equipment) after a cyberattack is fairly straightforward, calculating losses from a cyber-related business interruption tends to be more nuanced. However, calculating business income exposures accurately is just as important as getting property valuations correct because income losses can sometimes be even more devastating.

To select the best way to treat cyber exposures, risk managers will need to know how to accurately measure business income losses, how business interruption affects expenses, and what property and perils business income losses can involve. In this section, we'll discuss each of these considerations.

---

### What Do You Know?

How are business income losses calculated following a business interruption?

*Feedback* : Total business income loss is determined by subtracting the net income an organization actually earned during the interruption from the net income that the firm could reasonably have been expected to earn during the same period had no interruption occurred.

---

### Measurement of Business Income Loss

Business income losses are measured in terms of **net income**. One way to get to know how an organization's income losses can be calculated following a cyberattack is to study how an insurer would calculate a business income claim payment under a **business income insurance** policy. An insurer would calculate the income loss as the reduction in the organization's net income caused by a peril.

#### Net income

The difference between revenues (such as money received for goods or services) and expenses (such as money paid for merchandise, rent, and insurance).

#### Business income insurance

Insurance that covers the reduction in an organization's income when operations are interrupted by damage to property caused by a covered peril.

## 2.8 Exploring Today's Risk Management and Insurance Landscape

---

Here's a simplified example: After a malware attack, EntelliChip shut down its production line for three weeks while it repaired its hardware and software. During this interruption, EntelliChip could not make or sell microprocessors, its revenue was reduced to nil, and the company incurred some additional expenses (such as overtime labor) to get the production and fulfillment systems running again. However, the business interruption did temporarily reduce or eliminate some ordinary expenses (payroll, electricity, and so on). To learn more, see "Calculating EntelliChip's Business Income Loss."

| Calculating EntelliChip's Business Income Loss |                |                              |
|------------------------------------------------|----------------|------------------------------|
|                                                | Expected       | Actual (during interruption) |
| Revenue                                        | \$800,000      | \$0                          |
| Expenses                                       | <u>500,000</u> | <u>220,000</u>               |
| Net income (profit or loss)                    | \$300,000      | -220,000                     |

EntelliChip's business income loss is the \$520,000 difference between the \$300,000 profit it expected and the \$220,000 loss it actually experienced.

[DA13204]

What information is used to calculate business income may depend on the nature of the business. Here's how several types of businesses may choose to measure business income:

- Retailers and wholesalers depend on sales for income; some service businesses are in the same position. Interruption of sales interrupts business. The extent to which a loss reduces sales is the best measure of their income loss.
- Some service businesses, such as medical and legal practices, are reluctant to describe their income as sales. In these situations, the best measure is income itself. This is especially appropriate for businesses whose employees earn commissions, such as insurance agents and brokers. As a measure of loss, income is analogous to sales.
- Manufacturers rarely sell goods as they're produced, placing them instead into inventory from which they subsequently fulfill orders. As a result, stopping the manufacturing process causes a loss, but sales might not reflect that loss for several weeks. Manufacturers shut down by a direct loss for weeks or even months might recover with no reduction in sales. The manufacturers could meet orders from inventory until repairs are complete, then replenish their stock by increasing production. When this is the case, the proper measure of their business income is the net sales value of the goods they produce.



- Processing is very similar to manufacturing. So, as with manufacturers, the proper measure of a processor's business income is the net sales value of production.
- In real estate, rental value is an appropriate measure of income. Rental value includes actual rent due during the period of restoration. Forms of income also include other charges that are the landlord's obligation but that the tenant would have paid had no loss occurred, such as property taxes.

## Effect on Expenses

During a business interruption, some of the organization's expenses (often called **continuing expenses**) will continue, and others (**noncontinuing expenses**) won't. A business can also incur **extra expenses** during an interruption. All potential changes in expenses should be considered when assessing business income loss exposures.

If, for example, EntelliChip generates no revenue during its business interruption, its business income loss will be its lost profit for the period of interruption plus the continuing expenses and any extra expenses for that period.

### Continuing Expenses

Continuing expenses are normally a significant part of business income losses. If business is interrupted for a short time, payroll of key employees, debt repayments, taxes, insurance, and many other expenses typically continue during the interruption. However, if an interruption lasts longer, some expenses can be reduced or eliminated. For example, workers might be laid off, and income taxes and insurance premiums might decrease. Any reduction in expenses during an interruption lessens the severity of the resulting business income loss.

While it can be difficult to predict which expenses will continue and which will not, it's important to get a good handle on expenses that are likely to continue and those that won't while the business isn't operating. In many cases, a company's continuing expenses exceed the profit that the company would have earned during the period of interruption.

### Extra Expenses

Incurring extra expenses often pays for itself by reducing the business income loss. For example, the extra cost of overtime labor and overnight delivery of equipment needed to restore EntelliChip's network may be considerably less than the income that would have been lost had such measures not been taken.

Some organizations will incur extra expenses even when they exceed any reduction in the business income loss. The decision to incur such extra expenses depends on the organization's objectives. For some organizations, maintaining continuous service to customers may be more important than

#### Continuing expenses

Expenses that continue to be incurred during a business interruption.

#### Noncontinuing expenses

Expenses that will not continue during a business interruption.

#### Extra expenses

Expenses, in addition to ordinary expenses, that an organization incurs to mitigate the effects of a business interruption.

reducing the business income loss because it promotes customer retention and can help maintain a strong reputation. For example, a hospital might incur substantial extra expenses to maintain essential services for its patients even if such expenses increase its business income loss.

These are examples of extra expenses:

- After an assembly line is shut down because a computer virus damaged a machine, the factory owner pays the additional cost to have the machine replaced the next day rather than wait for it to be repaired.
- After a data breach exposes customers' credit card information, a retail organization pays for a credit monitoring service for affected customers.
- A hospital pays the perpetrators of a ransomware attack to regain access to critical medical systems and data before patients are harmed.

---

### Check Your Understanding

First Haul, an on-demand ridesharing service, conducts most of its business through an online app. Hackers breached the app, causing First Haul to shut down service for most of its customers for two weeks. During those two weeks, it generated just \$50,000 in revenue against an expected \$300,000 it would've generated had the app not been breached. However, First Haul's expenses dropped during the period of business interruption from \$150,000 to \$100,000. Describe how to calculate First Haul's business income loss.

*Feedback :* First Haul's business income loss is obtained by subtracting the net income that an organization actually earned in a period of interruption from the net income that the firm could reasonably have been expected to earn during the same period had no interruption occurred. First Haul's expected net income if no interruption occurred was \$150,000 ( $\$300,000 - \$150,000$ ). First Haul's net income during the interruption period is  $-\$50,000$  ( $\$50,000 - \$100,000$ ). As a result, First Haul's business income loss is \$200,000 (the difference between the \$150,000 profit it expected and the \$50,000 loss it experienced).

---

## Property and Perils Involved

Business income losses typically result from damage to the affected organization's own equipment, buildings, or property. However, a cyber risk at one organization can lead to a business interruption at another.

For example, suppose that EntelliChip's supply warehouse sits directly next to a chemical plant. A cyberattack disables the plant's safety systems and causes an explosion that severely damages EntelliChip's warehouse. As a result, EntelliChip cannot access the supplies it needs to maintain production of its microprocessors.

Organizations can also suffer business income losses if the operations of critical partners are interrupted. For example, an attack on an off-premises utility provider, such as an electricity or water company, could force EntelliChip to close.

Alternatively, one business may depend on another as a major customer or key supplier. A business can even experience business income losses simply because of a cyberattack on a nearby key facility or anchor store that attracts customers to the area (the way a popular department store draws customers to a mall). This is referred to as a contingent business interruption.

One of the most common cyber-related contingent business interruptions occurs when an organization suffers lost income because of an interruption of a shared computer system, such as a cloud service.

## EVALUATING EXPOSURES RELATED TO DATA BREACHES AND REPUTATIONAL RISK

If your organization collects, stores, or shares digital data pertaining to its operations, customers, or vendors, it's susceptible to a data breach and the resulting reputational risk. The financial fallout from even a small breach to an organization's data, a breach to a business partner, or a perceived breach can be financially crippling. Therefore, organizations must be prepared for any breach scenario. To effectively manage risk, organizational leaders need to know the data-breach and reputation exposures the organization faces and how costly they can be.

A data breach can be particularly troublesome for organizations of any size. Resources earmarked for growth, marketing, or acquisitions may have to be diverted to absorb costs associated with containing the breach, conducting a post-breach investigation, notifying affected parties, restoring operations after a business interruption, and paying any related fines.

Even more troubling, an organization doesn't need to have its systems attacked to be affected by a breach. Breaches to business partners—or public perceptions that a breach occurred even when it didn't—can also have significant financial consequences for an organization.

One of the most significant **cyber risk loss exposures** a company faces from a data breach is damage to its **reputation**. Even a company with a stellar reputation built over time can see that reputation permanently tarnished if customers or business partners lose faith in the organization's ability to protect their data.

### Cyber risk loss exposure

Any condition that presents the possibility of financial loss to an organization from property, net income, or liability losses as a consequence of advanced technology transmissions, operations, maintenance, development, or support.

### Reputation

An intangible asset, a key determinant of future business prospects, resulting from a collection of perceptions and opinions, past and present, about an organization that resides in the consciousness of its stakeholders.

---

### **What Do You Know?**

What are some general ramifications of a data breach?

*Feedback* : Ramifications of a data breach can include tangible and intangible property losses; income losses from business interruptions; increased costs associated with containment, notification, and business restoration; liability to third parties; punitive measures from regulatory and governmental bodies; and reputational damage and lost business.

This section highlights many of the data breach exposures organizations have, paying particular attention to reputational risk.

---

## **Data Breach Exposures**

An organization should have a plan for managing a data breach before a compromise ever occurs. To establish that plan, the organization's leaders and risk manager must first take a holistic approach to identifying and assessing all of the data breach exposures to the business. Appropriate risk management techniques can then be selected after this process is completed.

Organizations typically face these major data breach exposures, which must be accounted for in any risk management plan:

- Property losses—Tangible property, such as physical media and structures, as well as intangible property, such as data assets and intellectual property, can be lost or damaged following a breach.
- Immediate post-breach expenses—An organization's first priorities after discovering it's the victim of a data breach are containing the breach, investigating what happened, notifying affected parties, and repairing or restoring any critical systems that were damaged. Typically, considerable costs are tied to each of these actions.
- Liability loss—The greatest direct costs associated with a data breach often stem from liability loss exposures. When customers believe an organization had a legal obligation to protect their personally identifiable information and failed to do so, they may bring legal action against the organization. This can generate substantial legal costs and damages.
- Lost/stolen equipment—Data breaches aren't always the result of a cybercriminal hacking into an organization's computer system; they can also result from equipment ending up in the wrong hands. Organizations will then need to account for replacing this equipment in addition to the fallout from the breach itself.
- Employee error—Breaches can also result from employee mistakes or negligence. For example, an employee may infect a computer system with malware by clicking on a malicious link in an email, visiting a risky website, or plugging a portable storage device into an infected computer.

- **Business income losses**—An organization may lose significant revenue if it's forced to shut down operations after a data breach.
- **Third-party operations**—An organization can suffer a loss from a breach not only to its systems, but also to a third party with which it shares a system or data. For example, if an organization uses a third-party cloud storage provider, it could sustain a costly data breach if that provider is breached. Organizations are typically held responsible for the data security actions/processes of the third parties they use. In addition, an organization could suffer significant consequences if a third party it relies on, such as a utility company, experiences a business interruption because of a breach. For these reasons, an organization's entire operational network must be assessed for data breach exposures.
- **Global, national, and local regulations**—The regulatory landscape is constantly changing, and organizations need to stay abreast of the data privacy and data protection regulations they're subject to. Nearly every state has enacted some form of data privacy, security, or breach notification regulations. Failing to abide by them can result in considerable fines or penalties.
- **Reputational risk**—An organization's reputation is so important to its success that it needs to be managed as diligently as any other asset or risk. When customers lose trust in an organization, business dries up quickly. This can also happen if customers perceive that their information isn't safe in the organization's hands, whether or not a breach occurred.

#### Reputational risk

The risk that negative publicity, whether true or not, will damage a company's reputation and its ability to operate its business.

The financial consequences of a data breach can be significant. This may be especially true for a small to midsize business, which isn't likely to possess the financial reserves that a larger organization might have to undertake the necessary forensic investigation. Planning may mitigate the financial impact of a data breach, but it's unlikely to ever eliminate it entirely. To learn more, see "Financial Consequences of Data Breach Investigation and Resolution."

## Reputational Risk Exposures

A critical part of maintaining a good reputation is meeting or exceeding customer expectations. Customers want to know that it's safe to continue to do business with an organization. Otherwise, they will take their business elsewhere and may never come back.

Because an organization is a steward of its customers' sensitive personal data, its long-term health depends on protecting that data and, when it's breached, on effectively containing the breach, notifying affected parties, conducting an investigation to identify the source of the breach, and taking steps to eradicate the underlying vulnerability that caused it.

Reputational damage can cripple an organization, so reputational risk needs to be a key consideration in risk management planning. With today's instantaneous communication, a reputational crisis can compromise an

### Financial Consequences of Data Breach Investigation and Resolution

The financial consequences of an organization's investigation of a data breach and the resolution of regulatory action related to the breach can be catastrophic, particularly if the organization has not invested in an enterprise-wide approach to protecting its data. Smaller and midsize organizations, which frequently either lack the resources to implement cybersecurity measures or choose to spend money on more immediate concerns, are especially vulnerable. This is because they are unprepared for the aftermath of a breach and because cybercriminals are more likely to consider them to be "soft" targets.

For example, one such organization was victimized by a malware attack that led to theft of files that had been in the custody of a third-party vendor with whom the organization had subcontracted. The investigation (which required extensive forensic analysis because the cause of the breach was not immediately connected to the organization itself), resolution of Federal Trade Commission action (including fines), and measures to secure the source of the breach forced the organization to allocate funds to the breach that it would have used for other purposes, significantly jeopardizing its financial health and its long-term prospects in the marketplace. In total, the incident cost the organization a significant portion of its annual earnings and damage to its reputation that diminished its future earnings.

[DA11356]

organization's progress toward its strategic objectives in a matter of days, hours, or even minutes. Sales can drop markedly, causing liquidity problems. Ultimately, investors may take their funds elsewhere, bond ratings can be affected, and other sources of revenue can dry up. To learn more, see "Planning for a Data Breach."

### Planning for a Data Breach

News of data being mishandled—or news that data may have been exposed to a malicious party—can quickly go viral through the internet, social media, and television, severely damaging an organization's reputation. Planning immediate, appropriate responses to negative publicity can help mitigate the damage.

Planning for situations like this might include developing sample informative and compassionate responses that can be mobilized immediately after an issue goes viral. Some companies select a high-profile executive—even the president—to provide a personal, sympathetic response. As part of the response, the executive—while explaining the ramifications and expressing sympathy for victims—might also announce how the company will prevent future breaches and help make affected individuals whole. Some public relations firms provide media-interview training for executives in which they practice responding to tough and rapid-fire questions about potential reputation-damaging issues.

[DA13196]



Organizations can learn valuable lessons by looking at two well-publicized cases of data breaches and the experiences of the companies involved.

In 2013, Target Corporation was the victim of a data breach in which the credit card information of more than 40 million of the retailer's customers was compromised along with other personal information of about 70 million customers. The breach occurred because one of Target's third-party vendors, a heating and air conditioning company, was infected with malware. When the vendor connected to Target's network, the malware obtained the vendor's login credentials. Attackers then used those credentials to access Target's customer data.

Target was heavily criticized by the media and consumers for failing to protect shopper data and for not notifying affected individuals until weeks after the initial breach. Target reported that the breach cost it \$162 million across 2013 and 2014. But in reality, the breach was even more costly, as disgruntled customers avoided shopping at Target, and the company incurred additional expenses resulting from lawsuits and settlements related to the breach.

In 2017, Equifax Inc., one of the three largest consumer credit reporting agencies, reported that it was the victim of a data breach that exposed the personal information (including names, Social Security numbers, birthdates, and addresses) of more than 140 million individuals to cybercriminals. Equifax was heavily criticized for its security practices leading up to the breach and its post-breach response.

Before the breach, Equifax was informed of a vulnerability in one of its online applications. Equifax then took several months to apply a patch. In the meantime, hackers exploited the vulnerability to gain access to the data. In addition, Equifax's report came more than a month after it first detected suspicious activity.

Equifax's chairman and CEO issued a public apology for the breach, but it did little to quell consumers' and regulators' outrage. The Consumer Financial Protection Bureau (Bureau) accused Equifax of violating the Consumer Financial Protection Act of 2010, and the event proved extremely costly for the company. In 2019, the Bureau, in conjunction with the Federal Trade Commission, announced that a settlement had been reached with Equifax in which the company would pay up to \$425 million in monetary relief to consumers, a \$100 million civil money penalty, and other relief that could bring Equifax's total obligations to \$700 million.

---

### **Check Your Understanding**

Fluent Insurance Company provides its adjusters with tablets so they can take photos and notes when investigating insurance claims. The tablets contain third-party software that transmits claims data to another third-party cloud storage provider. Describe some of the data breach exposures Fluent has regarding employees and equipment.

*Feedback* : Some of the data breach exposures Fluent has include the adjusters' tablets being lost, stolen, or hacked, resulting in company and customer data being collected by cyber criminals. In addition, Fluent has exposures related to the third-party software and cloud storage provider it uses. If either the software or cloud storage provider is hacked, Fluent's data could be hacked as well.

---

## ASSESSING DATA LIABILITY EXPOSURES

Data is the asset most vulnerable to cyber risk, and organizations face substantial third-party cyber liability loss exposures from data breaches affecting their customers' and business partners' private information. Risk professionals and organizational leaders must be able to accurately assess these exposures to effectively manage the risk involved.

It's difficult to conduct business today without collecting at least some personal information from customers and business partners, such as their names, addresses, and credit card numbers. All organizations that conduct business online and store this private information are exposed to loss from a data breach. And the more data an organization stores, the more risk it's sitting on, the more likely it is to experience a data breach, and the more time it needs to spend assessing and mitigating its risk.

There are two types of cyber loss exposures: first-party expenses and third-party liability. To learn more, see "Distinguishing Between First-Party Expenses and Third-Party Liability."

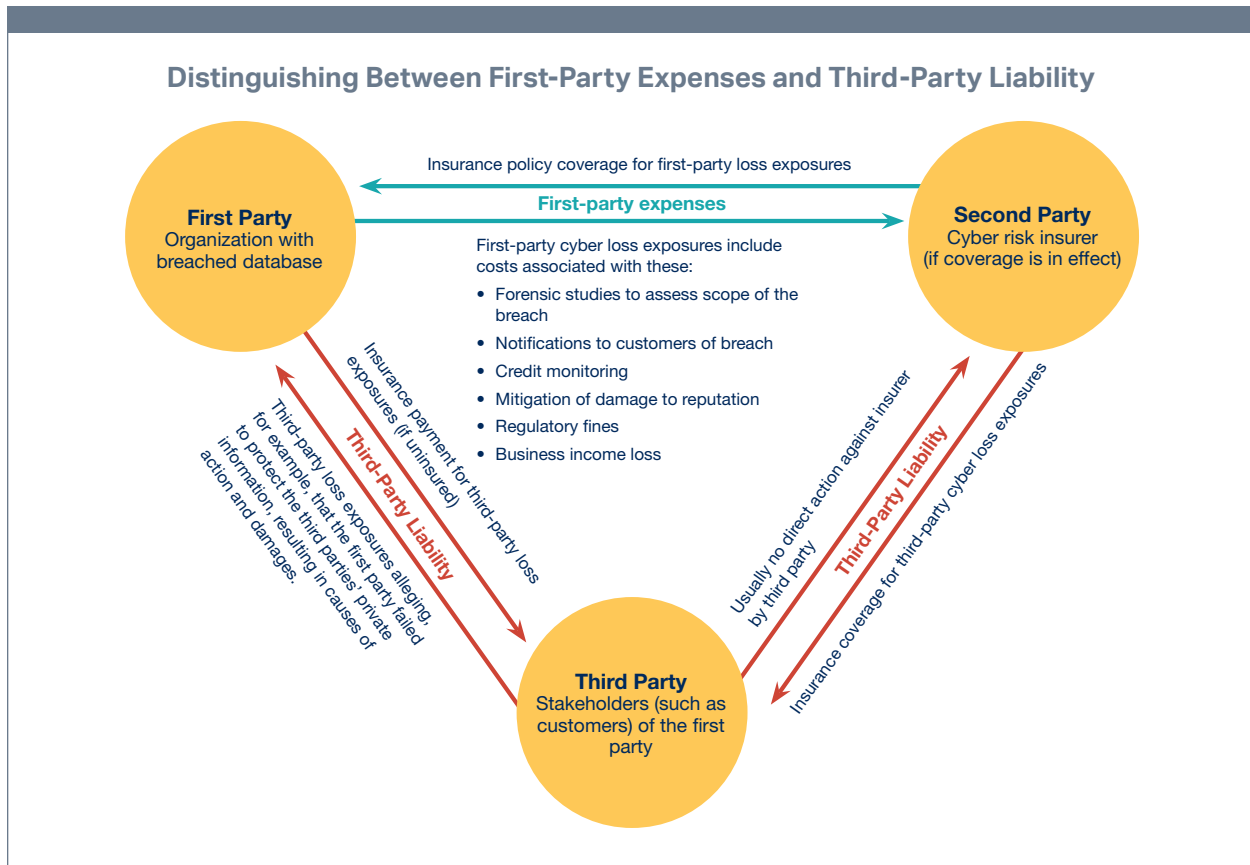
While first-party losses related to data-storage practices can occur more frequently, third-party losses are typically more severe, so this section focuses on the third-party data liability loss exposures organizations face in the wake of a data breach. Many of these loss exposures tend to fall into one of four categories: liability for customer data, business partner liability, network security liability, and directors and officers liability. An organization can follow several practices both before and after a data breach to accurately assess its data liability exposures.

---

### **What Do You Know?**

Sergio, the chief information officer of a midsize auto insurer, is negotiating a contract with a software vendor that provides claims database services. Naturally, he wants the software to meet the needs of his Claims Department, be compatible with other systems, and be easy to maintain. What else should Sergio think about, especially regarding cyber risk?





[DA13199]

*Feedback :* To protect his company and its third-party trading partners and their customers from possible data breaches or viruses originating in the vendor's system, Sergio will want assurance that the vendor has secure networks. Accordingly, the contract between the auto insurer and software vendor should stipulate responsibilities and remedies in the event of a breach or virus that originates in the vendor's network.

One question risk managers and organizational leaders should constantly ask themselves when reviewing the data liability exposures of their organization: Do the gains from storing certain information outweigh the liability exposures? After all, it can be easy to stockpile data on customers and business partners in hopes of making something useful out of it one day. But that stockpile is a target for cybercriminals. And the larger it grows, the bigger the liability exposure becomes, and the bigger the bull's-eye the organization puts on its back.

## Third-Party Data Liability Exposures

Let's examine some of the bigger third-party exposures an organization faces because of its data collection.

### Liability for Customer Data

An organization has a duty to take reasonable measures to prevent a breach of customers' personally identifiable information (PII). This duty cannot be delegated to another party. If PII is transferred to another party to perform, for example, a payroll accounting function, the original first-party organization retains responsibility for a breach that may occur. To learn more, see "Due Care and Due Diligence."

#### Due Care and Due Diligence

Creating a secure infrastructure and protecting the sensitive data of others requires organizational leaders and cybersecurity professionals to exercise due care and due diligence. Due care is the level of care a reasonable business or person would be expected to take under the given circumstances to avoid harming another party. Due diligence is the effort to demonstrate or make sure that due care is exercised. In other words, due care is the action being taken, and due diligence refers to the policies or procedures in place to make sure that action is taken.

If third parties can argue that the due care and due diligence to protect their data weren't followed, an organization's exposure to penalties and legal damages increases significantly.

Examples of exercising due care and due diligence include:

- Retraining or terminating employees who fail to follow established procedures to protect data and who are careless or negligent with data.
- Hiring independent auditors to assess whether third-party business partners are taking the necessary steps to apply due care and due diligence to protect data and systems that affect your organization.

[DA13198]

An organization's failure to protect PII obligates it to notify customers after a breach that their personal data may have been compromised. The organization may even be required to pay for credit monitoring services for those affected. The costs of a comprehensive approach to notification and monitoring can include a potentially substantial investment to create and maintain a customer contact database; to cover postal costs; and to hire public relations and forensic experts. These expenditures, however, can be offset by the long-term financial benefits of customer retention and goodwill.

When a first-party organization's database is breached, causing customers' private information to be released without permission, customers may be able

to sue for a variety of alleged transgressions, including, **breach of contract**, negligence, **fraud**, **conversion**, breach of **fiduciary duty**, and **invasion of privacy**. Transgressions such as these can often result in **class action lawsuits**.

Breach of contract is one of the most frequent allegations in lawsuits stemming from data breaches. Privacy allegations can also arise from an organization's failure to prevent unauthorized disclosure, deletion, or alteration of personal and corporate information. Federal and state regulations exist to safeguard customers' personal information, and failing to abide by these laws can result in substantial fines and penalties, as well as lawsuits.

Breach of contract claims can stem from a first-party organization's failure to fend off a cyberattack that results in damages. This is because a contract typically exists between business partners that includes a promise to protect confidential information that is in the partners' care, custody, or control. To learn more, see "Example of Liability to Customers Resulting From a Data Breach."

### Example of Liability to Customers Resulting From a Data Breach

A multinational organization in the entertainment industry had its database breached. It was eventually determined that over 100 million customer records were compromised.

Initially, the organization said that only the names, addresses, phone numbers, and email addresses of customers had been exposed. But investigators later discovered that the attackers also obtained the credit card data of over 20,000 customers in Europe.

Recently, the organization estimated its costs to resolve the claims from its customers at over \$150 million, which included defense costs and paying the settlement or judgment awards of over sixty class action lawsuits. The cost to resolve the claims was a small amount relative to the net worth of the organization. Of greater concern to this organization is the damage to its reputation, which may be far more substantial and long lasting.

[DA11353]

## Business Partner Liability

The third party is often the customer of the first-party organization, but it can also be, for instance, a business partner, such as a supplier or buyer, who receives a computer virus because of the first party's failure to manage cyber liability loss exposures. This can result in the first party owing damages to the third party if the third party experiences a business interruption because of the virus.

Additional damages may be incurred when a third-party trading partner becomes infected with a virus and has to stop being a supplier or buyer to the first party, at least temporarily. This could cause a drop in revenue and an

### Breach of contract

The failure, without legal excuse, to fulfill a contractual promise.

### Fraud

An intentional misrepresentation resulting in harm to a person or an organization.

### Conversion

The unlawful exercise of control over another person's personal property to the detriment of the owner.

### Fiduciary duty

The duty to act in the best interests of another.

### Invasion of privacy

The unauthorized disclosure of private information to another.

### Class action (class action lawsuit)

A lawsuit in which one person or a small group of people represent the interests of an entire class of people in litigation.

increase in costs for the first party as it searches for substitute suppliers and buyers.

### Network Security Liability

An organization can be held liable when its network security fails to prevent cyberattacks. Such attacks may result in, for example, unauthorized access to corporate information that allows the attacker to delete, corrupt, or steal data; denial of service, making the network unavailable for its authorized users; or the forwarding of a virus or other harmful code to another computer.

Other situations in which an organization can be held liable when its network security fails include:

- Liability for damage to a third-party network resulting from a data breach—A first party is liable if it fails to prevent the transmission of malicious code from its own network to connected third-party networks.
- Liability for libel, slander, and trademark and copyright infringements—Liability can be incurred when a cyberattack causes offensive content to be placed on a first party's website. If the content defames or portrays a third party unfavorably in written form, it's libel. If spoken or transmitted by sound, it's slander. A data breach can result in trademarked or copyrighted content displayed on a breached party's website in a manner that falsely indicates the party owns the intellectual property. Such infringement could cause the owner of the intellectual property to sue the party with the breached website.

### Directors and Officers Liability

When an organization's directors and officers fail to fulfill their responsibilities and duties as required under the law, they can be held liable for resulting losses. Corporate directors' top responsibility is to fulfill their fiduciary duties (most notably, duty of care, duty of loyalty, duty of disclosure, and duty of obedience) to the corporation and its stockholders. Directors and officers have fulfilled their duty of care if they act in good faith and in a manner they reasonably believe to be in the corporation's best interests. This may be accomplished, for example, by shifting the board's attention toward cyber liability loss exposures.

Further, directors and officers have the general duty to disclose significant and essential facts to all persons who have a right to know those facts and would not otherwise be able to obtain them. For example, directors and officers have a duty to make public disclosures of data breaches and their cost, to stockholders, bondholders, and potential investors.

However, directors and officers must refrain from discussing confidential or market-sensitive matters with others. For example, they can't publicly discuss the specifics of a corporation's cybersecurity strategy because that would compromise the organization's cybersecurity.

## Assessing Liability Exposures

A risk manager should take several concrete steps both before and after a breach to accurately assess an organization's data liability exposures. For starters, the risk manager should break down and document all the data the organization is storing, including the amount of data it's collecting and what that data consists of. Using this information, the risk manager can determine which laws apply to the data and, as a result, the types of fines and penalties that can be associated with noncompliance.

Secondly, the risk manager should evaluate the data security practices of the organization's third-party business partners with which it shares sensitive data. If possible, the risk manager should conduct regular audits of what happens to data within the third-party's system. Contracts should stipulate that the first-party organization retains the right to an independent audit of the third-party's system. The goal is to find out how third parties handle the organization's data and what, if any, risks that data faces. This can also provide opportunities to create additional barriers to protect data or contain a breach that occurs in part of the data storage infrastructure.

Additionally, any contracts with third-party partners should clearly stipulate the data security responsibilities of each party. However, it's important to remember that the first-party organization retains responsibility for a breach, which is why it's important to constantly audit third parties' data practices.

Once these analyses are conducted, the risk manager and organizational leaders should determine what data the organization no longer needs to collect. Allowing unused PII to lie around is a huge liability risk with no upside.

Following a breach, the best way for an organization to assess its liability exposures and how costly they may be is to document as much information about the breach as possible, as quickly as possible. These are some of the essentials that should be documented and analyzed:

- When the breach occurred (including specific dates or the best estimate of the period during which the data was compromised)
- The cause of the breach
- The number of data records exposed
- The types of information those records contained
- What, if any, systems are connected to the breached system and how
- What laws apply to the industry and the exposed records
- Which, if any, law enforcement agencies need to be notified
- How quickly notifications can be sent
- What redress activities will be provided for customers (such as credit monitoring)
- Revisions that will be made to the organization's security protocols

### **Check Your Understanding**

At the board meeting of Eastern Minnesota Farm & Ranch Insurance (Eastern), the directors inquired about cyber risk to the company. In response, the risk manager shared cyber risk insurance policy quotes from several insurers. After some directors objected to the cost of the insurance, the chief information officer (CIO) told the board that Eastern has a secure network, and all of its data is backed up off-site daily. As a result, the CIO noted that Eastern is “safe from a cyberattack because even if our systems are breached, we can use our backups to be fully operational again within hours.” Describe some of the liability exposures Eastern faces and what could go wrong if the board opts not to purchase cyber risk insurance.

*Feedback :* The CIO and the board shouldn't regard the first-party threat to Eastern's data and systems as the only cyber risk to manage. Eastern has third-party liability exposures regarding its customers and business partners. The risk manager should be actively mitigating those third-party exposures, and the board should be fulfilling its fiduciary duties, which include attempting to control the risk of third-party cyber liability exposures. By failing to transfer some of those exposures through insurance, Eastern faces significant financial consequences if a breach occurs.

---

## **SUMMARY**

Nearly all organizations have at least some cyber risk—and the potential consequences of a cyberattack or data breach can be devastating. Creating an effective cyber risk management program begins by evaluating and accounting for tangible and intangible property loss exposures susceptible to a cyberattack. Tangible property includes physical media and traditional structures. Intangible property includes data assets and intellectual property.

An organization can lose income when a cyberattack interrupts its business activities. Business income loss exposures can be as devastating as property exposures, if not more so. A common way to calculate a business income loss is to subtract the net income that an organization actually earned during the interruption from the net income that the firm could reasonably have been expected to earn during the same period had no interruption occurred. Risk managers must also account for a business interruption's effect on continuing, noncontinuing, and extra expenses, as well as the fact that a cyber risk at one organization can lead to business interruption losses at another.

Organizations must be prepared for any number of scenarios regarding a data breach because even a small breach to their data, a breach to a business partner, or even a perceived breach can be financially devastating. Some of the most significant data breach exposures organizations face include property losses, post-breach expenses, liability loss, lost/stolen equipment, employee

error, business income losses, third-party operations, regulations, and reputational risk. Damage to its reputation is often one of the greatest exposures an organization faces because it can result in losing a substantial amount of business.

Any organization doing business online and collecting information about customers and partners is exposed to data breach loss. Third-party losses are typically the most severe and tend to fall into one of four categories: liability for customer data, business partner liability, network security liability, and directors and officers liability. Before a breach, a risk manager needs to analyze all of the data the organization stores, as well as the data security practices of the organization's partners. If a breach occurs, numerous aspects of it must be documented, such as the cause, number of records exposed, and applicable laws.





# How Can You Use Data to Your Advantage?

# 3

## Educational Objectives

- ▶ Explain how big data and technology influence risk management and insurance strategy.
- ▶ Explain how data science applies to risk management and insurance and the role of the data scientist.
- ▶ Explain how data-driven decision making applies to risk management and insurance.
- ▶ <State the learning objective.>
- ▶ <State the learning objective.>
- ▶ Explain why parametric insurance has emerged and how it works in the industry.

## Outline

Strategic Opportunities From Big Data and Technology

Data Science

Data-Driven Decision Making

<Enter Concept LO title here>

<Enter Concept LO title here>

Understanding Parametric Coverage and Why It Matters

Summary



# How Can You Use Data to Your Advantage?

# 3

## STRATEGIC OPPORTUNITIES FROM BIG DATA AND TECHNOLOGY

As technology evolves, it changes almost every aspect of our lives—especially how we communicate, learn, and do business. In this, the insurance industry is no exception. The convergence of **big data** and technology is transforming the property-casualty insurance business.

Data allows insurers, through the **law of large numbers**, to provide coverage for a variety of risk exposures. Traditionally, the data insurers use has come from loss histories. By analyzing large numbers of claims, insurers can reasonably predict the probable cost of future claims.

However, as technology evolves, the sources and amount of data available to insurers are increasing rapidly. As such, they have to develop new, more efficient methods of processing and analyzing it.

---

### **What Do You Know?**

Why would claims, underwriting, or risk management professionals study data analytics?

*Feedback* : Claims or underwriting professionals typically study data analytics because they increasingly use the results of analytics in their decision making, and insurance professionals will want to be able to more effectively communicate with data scientists in their organizations.

---

## Opportunities Presented by Big Data and Technology

Why would an insurance professional who is not an actuary or a data scientist want to learn about data analytics? Succinctly, big data and technology are central to the future of the insurance industry. The evolution of this area has already disrupted the traditional ways in which insurers market, underwrite, and analyze their products, and this disruption will only grow as future technology, such as autonomous vehicles, comes online.

### **Big data**

Sets of data that are too large to be gathered and analyzed by traditional methods.

### **Law of large numbers**

A mathematical principle stating that as the number of similar but independent exposure units increases, the relative accuracy of predictions about future outcomes (losses) also increases.

However, a more practical reason is simply that insurance professionals, such as those in underwriting and claims, must be able to communicate with the data scientists in their organizations. As the application of data analytics to insurance continues to evolve, analysis of the new techniques that result will rely on professionals in areas such as underwriting and claims. Communication and collaboration between those who perform the daily work of an insurer and those designing data analytics will be important for success.

Decision making driven by big data can also provide better results than more traditional decision making. For example, the credit industry was using data obtained from loss histories to select clients and determine credit lines based on the probability of default. When Capital One was known as Signet Bank, it wanted to determine which potential clients would be profitable but did not have that data available. Signet decided to obtain a base amount of data by providing credit randomly. Losses increased significantly as a result, but the bank saw this as the cost of data acquisition. Once enough data was collected, however, the bank's data scientists were able to create predictive models that identified the characteristics of the most profitable clients. The bank then used the results to develop a strategy regarding which credit products should be offered to which and at what level of credit and interest rate.

#### Big Data

Although insurers have always gathered and analyzed large amounts of data to make business decisions, the amount of data available has increased exponentially and is therefore referred to as big data. The advent of the use of big data came when organizations began using the internet to conduct business and compile data about their customers. Insurers developed online insurance applications and used data from these applications, as well as claims history, to improve underwriting efficiency, product development, and marketing. Other industries have put big data to similar use. For example, retail investment firms, such as E\*Trade, used the internet to create new products for consumers, and stock traders began using computers to execute transactions and bond trades much more efficiently than was previously possible.

Since that beginning stage, organizations have improved their methods of obtaining and aggregating vast amounts of data very quickly and extracting useful knowledge from it. For example, investment firms have computers that can scan the internet instantly for news and information about products, prices, economic and geopolitical developments, and consumer trends. This data is then entered into computer trading algorithms that conduct automated trading of stocks and bonds at high speeds. This newest evolution of big data, sometimes referred to as big data 2.0, allows organizations to process and analyze data from such sources as vehicles, homes, and wearable technology. A common example is sensors that can be placed in an automobile to voluntarily track an insured's driving habits, providing information that could be the basis for a lower premium.

Two types of big data available to insurers are their own internal data and data from external sources. It might seem odd to consider an insurer's own data as an advancement that might require new methods of analysis, considering that the data was already in its possession. But just because the insurer already had the data does not mean that it was accessible. New techniques of data analysis, such as **data mining** and **text mining**, can provide new understandings of old information.

For example, data mining could take the biographical data of a group of insureds and, based on the information they provided, group them by characteristics they have in common, such as age or geographical location. This is a very simple example, but as the mining applications become more complex, the groupings could be based on more obscure information that previously would have been too time-intensive to analyze. And text mining can analyze adjusters' notes to identify common fraud indicators, such as insureds noted as having made late loan payments.

Much like the methods of analyzing internal data, external sources of big data are constantly evolving. For example, some insurers use **telematics** to gather data that helps identify both safe and unsafe driving patterns. If used properly (and with the insured's consent), telematics can provide the basis for real-time changes in premium. A safe driver could receive a discount, while an unsafe driver may receive a premium increase or be required to attend a remedial driving program.



Learn more from an expert in the online video.

## Technology

Technological innovations are constantly changing risk management and insurance. Similar to telematics devices, the **Internet of Things (IoT)** allows machine-to-machine communication and **machine learning**, both of which could have potential uses in risk management. For example, the IoT may eventually be able to identify the next asbestos-type problem before it occurs by analyzing data from wearables, sensors, and text mining.

Another area under development that could affect how insurers do business is **artificial intelligence (AI)**. For example, Google uses AI to find answers to rare search inquiries. As AI becomes more refined, it will be able to provide and analyze information from voice recordings, photos, and videos, which could hold significant potential for insurers. Consider claims adjusters, who often take recorded statements from claimants: AI techniques could be applied to recognize voice patterns that may indicate the possibility of fraud. There could also be applications related to photos of accidents or natural catastrophes.

### Data mining

The analysis of large amounts of data to find new relationships and patterns that will assist in developing business solutions.

### Text mining

Obtaining information through language recognition.

### Telematics

The use of technological devices in vehicles with wireless communication and GPS tracking that transmit data to businesses or government agencies; some return information for the driver.

### Internet of Things (IoT)

A network of objects that transmit data to computers.

### Machine learning

Artificial intelligence in which computers continually teach themselves to make better decisions based on previous results and new data.

### Artificial intelligence (AI)

Computer processing or output that simulates human reasoning or knowledge.

For underwriting and claims management, drones have become another important source of information. Instead of sending adjusters to a disaster scene, insurers are now testing the use of drones to provide detailed data about property damage. Additionally, drones can assist in gathering risk data for underwriting property coverage in wildfire-prone areas.

### Data Science

#### Data science

An interdisciplinary field involving the design and use of techniques to process very large amounts of data from a variety of sources and to provide knowledge based on the data.

**Data science** arose from the need to link big data and technology in ways that provide useful knowledge. Because big data, by definition, is an amount of data too large to be analyzed by traditional methods, data scientists developed various techniques to organize and analyze it. Traditional techniques, such as probability, are often combined with newer techniques, such as machine learning, to obtain the most relevant knowledge from the data.

While a major tenet of data science is that data organization and analysis are automated rather than performed by an individual, human evaluation of automated data analysis is critical. First, computer analyses are not always accurate. Just look at weather forecasting—different models interpret meteorological data differently and can produce contradictory forecasts. Experienced meteorologists must evaluate all the model analyses and use their professional judgment to make a final decision on what the forecast should be. Second, the automated analysis may be correct but irrelevant to a given business problem. For example, an automated analysis of claims information indicating that teenaged male drivers are more likely to have accidents would not be relevant to a deeper understanding of auto accident risk because that information about teenaged male drivers is already known. And third, just as technology is rapidly evolving, so are the physical, political, economic, and business environments. Unless the automated method can take those factors into account, the results of the automated analysis may not be helpful if the environment suddenly changes.

For data science to be useful to an insurer or to specific functional areas, such as underwriting or claims, it is usually important to define the business problem to be solved, such as improving claims or underwriting results. Although data analytics may be used to forecast unforeseen events in the future, this is still an area for exploration rather than application to business decisions.

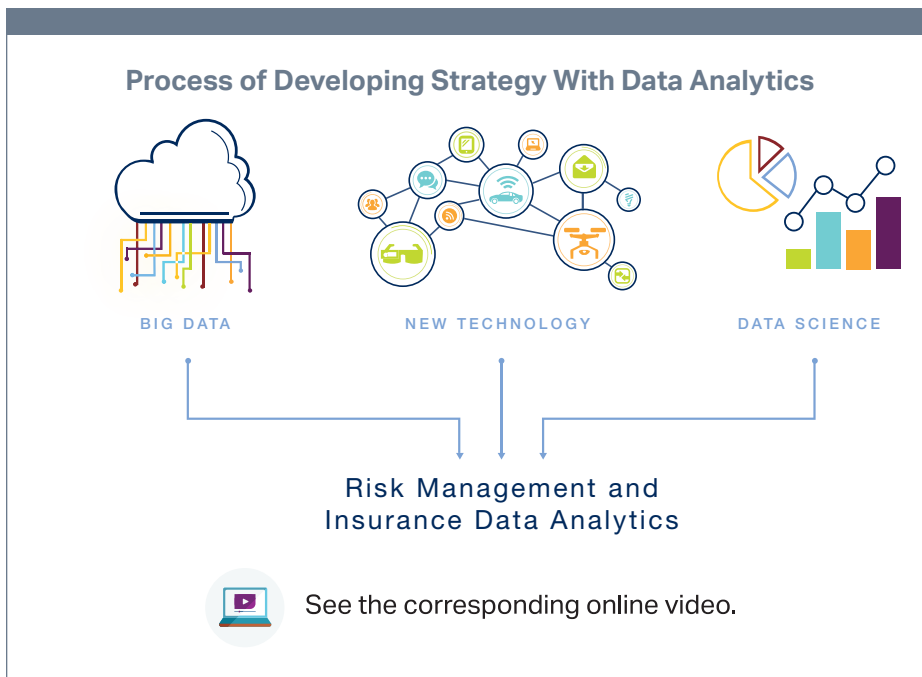
### Strategic Applications to Insurance

Insurers and risk managers need to determine which investments in big data and technology will provide the best fit for their business. For example, an insurer that provides only personal lines of coverage may not be interested in wearable sensors that help prevent workers compensation claims. A company that operates a fleet of vehicles may be more interested in telematics than sensors that detect the risk of fire or collapse in a building.

After data has been obtained and processed, insurance analytics must be applied to make data-driven decisions and develop strategy. This involves not

only the big data, technology, and data science techniques, but also people who can evaluate the results of the analytics. Insurance professionals in areas such as underwriting, claims, and risk management should have input regarding the types of data that they know would be helpful to their decision making, such as fraud indicators. These professionals should also have input into how well the analytics are working to produce relevant and practical information or to improve efficiency.

At more senior levels of an insurer, the information obtained from data analytics can guide such decisions as which lines of coverage the insurer wants to increase or decrease, countries where it would like to expand or reduce operations, and even which investment options it acts upon. To learn more, see “Process of Developing Strategy With Data Analytics.”



[DA11928]

### Check Your Understanding

A risk manager for a large organization that delivers food products is considering whether new technology could help improve driver safety and reduce accidents. Describe a type of new technology that could help this risk manager.

*Feedback :* Telematics could help the risk manager. Data about the driving behavior of each driver could be transmitted to a computer and then analyzed to determine which drivers are driving safely and, potentially, the cause of accidents.

# DATA SCIENCE

Big data and new technology can offer an organization a great many business solutions via data analytics, but seizing that opportunity requires a combination of unique skills.



Learn more from an expert in the online video.

In order to gain a competitive advantage from data analytics, insurers need to have people with the necessary skills to manage the ever-increasing amounts of data and its rapidly evolving types and sources. Insurers have typically employed individuals with the education and skills to evaluate data and determine specific results, such as prices for products and claim reserves. However, without additional training in data science, these people may not be able to effectively apply data analytics to big data.

---

### **What Do You Know?**

Although data science is a fairly new field, some fundamental concepts have been established. Can you identify any?

*Feedback :* These are four fundamental concepts of data science:

- Systematic processes can be used to discover useful knowledge from data.
- Information technology can be applied to big data to reveal the characteristics of groups of people or events of interest.
- Analyzing data too closely can result in interesting findings that are not generally applicable.
- The selection of data mining approaches and evaluation of the results must be thoughtfully considered in the context in which the results will be applied.

---

## Data Science Concepts

Data science emerged as a new field at the frontier of data analytics. As such, it is rapidly developing, often by making use of the scientific method. To learn more, see “The Scientific Method.”

Data science involves experimenting with data using rapidly evolving methods. Its purpose, as with all sciences, is to increase knowledge of the world and provide solutions to complex problems. Data science is able to leverage big data and new methods available to analyze it.



## The Scientific Method

The scientific method consists of these seven steps:

1. A question or problem is raised.
2. Research is conducted regarding the subject.
3. A hypothesis is developed, based on the research, regarding the answer to the question, the cause of the problem, or the solution.
4. Experiments are performed to test the hypothesis.
5. Data from the experiments is analyzed.
6. A conclusion is reached.
7. The conclusion is communicated.



See the corresponding online video.

[DA13194]

These are four fundamental concepts of data science:

- Systematic processes can be used to discover useful knowledge from data—Insurers can benefit from a framework that forms a foundation for data-analytical processes. For example, if analysis of a dataset indicates that an insurer's auto rates are too high to compete in the market, the insurer must have a process to evaluate whether that conclusion is accurate. If it is, the insurer may be able to develop solutions to gain market share.
- Information technology can be applied to big data to reveal the characteristics of groups of people or events of interest—For example, insurers can learn the characteristics of insureds who do not renew their policies. Risk managers can identify the characteristics of employees who avoid injury. Underwriters can determine the characteristics of building construction that make a home or business less vulnerable to fire loss.
- Analyzing data too closely can result in interesting findings that are not generally applicable—For example, an insurer may discover that drivers between the ages of thirty-five and forty are more likely to purchase red cars. This may be an interesting fact, but it is unlikely to lead to an actionable conclusion.
- The selection of data mining approaches and evaluation of the results must be thoughtfully considered according to how the results will be applied—For example, if an insurer discovers specific characteristics that are shared by insureds who do not renew their policies, how will the insurer use that information? Can the insurer find a way to increase retention among insureds with these characteristics? Could the insurer more efficiently limit its marketing to customers who are more likely to renew?

Unless one or more actions can be taken to provide better business results, pursuing a particular data mining project may not be worthwhile.

## The Data Scientist

Traditional data is usually numerical or categorical. But, beyond these types, data scientists must be able to analyze increasingly large amounts of new types of data, including text, geolocation data, sensor data, images, and social network data.

### Actuary

A person who uses mathematical methods to analyze insurance data for various purposes, such as to develop insurance rates or set claim reserves.

Traditionally, **actuaries** have been the professionals who analyze data and make predictions based on those analyses for insurers. With strong backgrounds in mathematics and statistics, they focus primarily on pricing, ratemaking, and claim reserving.

Data scientists, meanwhile, explore previously underutilized sources of data, such as social networks and new technology. Rather than being concerned directly with pricing and reserving, their work may lead to new insurance products and risk management techniques, as well as the refinement of existing products. There is no clear division between the roles of actuary and data scientist, however. Many actuaries are acquiring advanced computer programming skills by using new data analysis programming languages, such as R or Python, to supplement their mathematical and statistical knowledge.

Having a strong base of knowledge in mathematics, statistics, and computer programming isn't all it takes to navigate the field of data science. Data scientists must also have **domain knowledge**, or knowledge related to the context of the information they are working with, to be effective. To learn more, see "Necessary Skills for a Data Scientist."

### Domain knowledge

Information related to the context of the information a data scientist is working with.

## The Data Science Team

Results produced through data science are useful only if they are relevant to the business context. For example, unless insurers gain knowledge that helps them compete more effectively, they aren't receiving any benefits from data science. Similarly, to make data science a worthwhile endeavor for risk managers, they must be able to realize the benefits of employing new technologies, such as wearable devices, to improve safety or obtain insights about risk that will help them manage it more efficiently.

Risk management and insurance professionals can be valuable members of data science teams. They help provide the context for the goals of data mining projects and how results can be applied to generate business solutions. For example, underwriters may inform the insurer that it is losing commercial business to competitors. The data science team may design a data mining project to try to determine the reasons. Likewise, claims professionals may find that use of opioid medications is rising, and the data science team may be able to perform data mining to analyze the characteristics of medical provid-



[DA12705]

ers and claimants involved in excessive opioid use. Risk managers may have information regarding an increase in repetitive motion injuries; data mining may provide more detailed information on how and where those injuries are occurring, and that information may lead to a solution, such as wearable safety devices.

### **Check Your Understanding**

A national package-delivery organization wants to develop a predictive model for locations and drivers that are most likely to be involved in accidents in order to develop accident-prevention solutions. The organization has employed several data scientists to assist with various business problems. Explain whether another professional in the organization, in addition to the data scientists, should be involved in a team to develop a predictive model and solutions for the accident problem.

*Feedback* : A risk management professional should be involved in the team along with the data scientists to develop a model and potential solutions

for the accident problem. Risk managers have domain knowledge and can assist with providing information for development of a predictive model and analyzing the results of the model's application. After results are obtained, the risk management professional should be involved with proposing solutions.

---

### Data-driven decision making

An organizational process to gather and analyze relevant and verifiable data and then evaluate the results to guide business strategies.

## DATA-DRIVEN DECISION MAKING

Although risk management and insurance professionals have long based their decisions on internal and external data, modern data analytics has both broadened and improved the types of data, methods of analysis, and results attained by applying **data-driven decision making**.

Risk management and insurance were previously dependent on human analysis of data. For example, if a risk manager or underwriter wanted to know the previous year's losses at a particular location before renewing a policy, they would obtain the information from computer records and then analyze it before making their decision. Data science provides more advanced methods of aggregating and analyzing data.

---

### *What Do You Know?*

Data-driven decision making can solve a variety of business problems. Differing approaches may be required, however, depending on whether the problem to be solved will be recurring or a one-time-only event. Can you name the types of approaches used in each of these instances?

*Feedback* : There are two basic approaches to data-driven decision making—descriptive and predictive. The descriptive approach is used when solving a business problem that is likely to be a one-time-only event, while predictive approaches are used for problems that will likely recur.

---

## Data Science and Data-Driven Decision Making

Data science, through data-driven decision making, helps insurers and risk managers improve their business results in these ways:

- Automating decision making for improved accuracy and efficiency—Providing online quotes for personal auto insurance based on a computer algorithm has become commonplace.
- Organizing large volumes of new data—For example, an insurer could organize data according to multiple characteristics, such as the informa-

tion provided by telematics, which can include speed, braking patterns, left turns, and distance traveled.

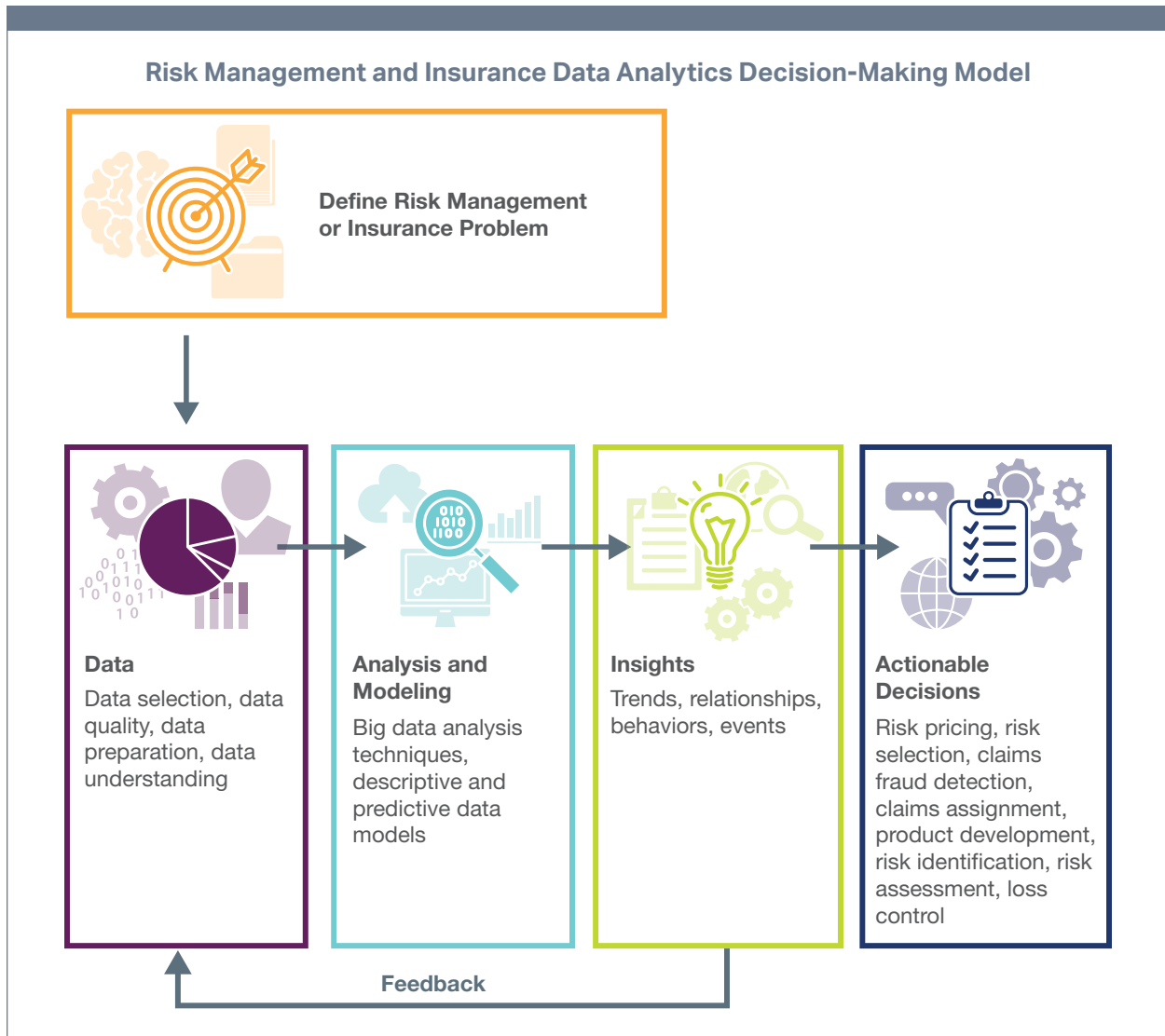
- Discovering new relationships in data—For example, a risk manager could identify the characteristics of workers who have never had a workplace accident and use that information to improve safety for all workers.
- Exploring new sources of data—An insurer could use text mining to analyze claims adjusters’ notes for various purposes, such as developing an automated system to predict a claim’s severity and assign the appropriate resources to those claims predicted to become severe.

Data-engineering and data-processing technology allows insurers to manage data that is too large for most conventional systems. Models are developed to gather and analyze data in the context of an insurer’s areas of interest, with results ultimately provided to the data analytics team or the manager who requested the data analysis. The appropriate person can then make data-driven decisions accordingly. To learn more, see “Risk Management and Insurance Data Analytics Decision-Making Model.”

Data-driven decision making can be applied across an insurer’s or risk manager’s enterprise to solve a variety of business problems, achieve greater efficiency, and provide a competitive advantage. There are two basic approaches to data-driven decision making—descriptive and predictive.

The descriptive approach is applied when an insurer or risk manager has a specific problem that could be solved through data science. Once the specific problem is solved, such as deciding whether accepting a particular type of risk is a sound business decision, the approach is no longer used. For example, let’s say that an insurer changed its underwriting guidelines for auto insurance to reduce applicants’ required time period without an accident to be accepted for coverage from five years to three. In this scenario, the insurer may use a descriptive approach to decision making the following year to determine whether reducing the accident-free time requirement was a sound business decision, and once it had an answer, it likely would not use that approach again.

The predictive approach to data analytics involves providing a method that can be used repeatedly to provide information for data-driven decision making by humans, computers, or both. For example, automated underwriting for personal auto insurance is a predictive approach that is used each time a person applies for insurance. The computer makes the underwriting decision and issues a price quote. In another example, a risk manager may receive data from sensors regarding which employees are using required safety equipment. The risk manager will make a decision about how to address the problem of employees who are not using their safety equipment.



[DA11978]

## A Model for Data-Driven Decision Making in Risk Management and Insurance

Following the process outlined in the decision-making model will help ensure the best results. The important first step is to define the risk management or insurance problem. Without a business context, it's unlikely that modeling and analyzing data will be effective. To learn more, see "Data-Driven Decision Making Using the Descriptive Approach."

## Data-Driven Decision Making Using the Descriptive Approach



See the online video.

[DA13177]

### <ENTER CONCEPT LO TITLE HERE>

<Begin with an interesting fact, thought-provoking question, or a one sentence scenario to illustrate why the learning object (content) is important.>

<Begin with a definition, if required. Then, provide an example.>

<Next, provide an overview of the key concepts to be taught as they relate to each other. The following are some options available to you:>

- <A numbered list>
- <A bulleted list>
- <A table>
- <An infographic (a visual representation of information; the graphic portrays the message; some labeling may be included)>

### <Concept 1>

<Provide a description of the first concept as outlined in the list, table, or infographic.>

<Provide an example, if required.>

### <Concept 2>

<Provide a description of the first concept as outlined in the list, table, or infographic.>

<Provide an example, if required.>

### <Concept 3>

<Provide a description of the first concept as outlined in the list, table, or infographic.>

<Provide an example, if required.>

## **<ENTER CONCEPT LO TITLE HERE>**

<Begin with an interesting fact, thought-provoking question, or a one sentence scenario to illustrate why the learning object (content) is important.>

<Begin with a definition, if required. Then, provide an example.>

<Next, provide an overview of the key concepts to be taught as they relate to each other. The following are some options available to you:>

- <A numbered list>
- <A bulleted list>
- <A table>
- <An infographic (a visual representation of information; the graphic portrays the message; some labeling may be included)>

### **<Concept 1>**

<Provide a description of the first concept as outlined in the list, table, or infographic.>

<Provide an example, if required.>

### **<Concept 2>**

<Provide a description of the first concept as outlined in the list, table, or infographic.>

<Provide an example, if required.>

### **<Concept 3>**

<Provide a description of the first concept as outlined in the list, table, or infographic.>

<Provide an example, if required.>

## **UNDERSTANDING PARAMETRIC COVERAGE AND WHY IT MATTERS**

As vital as they are, traditional property-casualty insurance products aren't perfect. The claims process can be time-consuming and labor-intensive, claimants don't know what their total claim payments will be until settlement, and insurers can opt not to cover certain risks.



Enter parametric insurance. It offers coverage options that effectively address some of the inherent flaws of traditional indemnity products. However, parametric insurance is meant to be a complement to—and not a replacement for—traditional indemnity products.

This discussion will help you understand the value that parametric insurance provides to both customers and insurers, and how it fits into personal and commercial risk management programs.

In a parametric policy, a predetermined payout is immediately triggered when a predetermined parameter for which there is reliable data is met or exceeded. The parameter is known as the parametric trigger. The loss payment is a specific, agreed-upon amount—and is not based on a true indemnity process. In addition, the loss payment is not intended to reimburse the claimant for any particular type of loss (such as for property damage or business income loss). Instead, it can be used at the insured's discretion to accommodate their needs.

---

### **What Do You Know?**

Can you think of a practical example of a parametric contract?

*Feedback* : A parametric contract can be written to pay an insured a set amount (such as \$50,000) when rainfall exceeds a certain amount (such as six inches in a single day) at a stated location, regardless of the type or severity of loss the insured sustains from flooding or water damage.

---

The payment typically isn't meant to completely indemnify the insured for a sustained loss. Often, it's intended to provide the insured with a quick lump sum of cash to jump-start the recovery process—or to provide some basic level of coverage for a risk for which the insured could not obtain insurance in the traditional market. As a result, parametric insurance isn't meant to replace, but rather to complement, traditional insurance policies.

---

### **Apply Your Knowledge**

Since parametric contracts aren't meant to cover an insured's total loss, what do you think would be the key to ensuring customer satisfaction and avoiding errors and omissions (E&O) exposures when selling or issuing parametric coverage?

*Feedback* : The key to maintaining customer satisfaction and avoiding E&O liability is clear communication during the sales process. It's important to convey to the customer what the parametric policy covers, exactly what the claim payment will be, and that it's not a suitable substitute for an indemnity policy.

---

## 3.18 Exploring Today's Risk Management and Insurance Landscape

---

### Smart sensor

A specialized sensor programmed to respond in a specific way when a threshold of detection or measurement is reached.

### Artificial intelligence (AI)

The ability of machines to simulate human intelligence.

### Cloud computing

Information, technology, and storage services contractually provided from remote locations, through the internet or another network.

### Predictive modeling

A process in which historical data based on behaviors and events is blended with multiple variables and used to construct models of anticipated future outcomes.

The parametric insurance concept isn't new; for example, crop insurance is written similarly. But it's starting to push its way to the forefront, thanks to emerging technology, an increasing number of triggers that can be linked to coverage, and a variety of benefits for insureds and insurers.

## Technology Fueling Growth

Parametric policies require clear, accurate, and real-time data on the triggering event. If robust data—such as that produced by extreme weather occurrences—exists, some level of parametric protection can often be structured around the event.

Emerging technology—such as **smart sensors**, the Internet of Things, smartphones, mobile apps, big data, **artificial intelligence**, **cloud computing**, advanced analytics, **predictive modeling**, smart contracts, and block-chain—is making it increasingly easier to collect, store, and assess event data and rapidly issue claim payments. This same technology also helps facilitate the design and use of parametric policies. To learn more, see “The Rise of Parametric Insurance.”



[DA13790\_3]

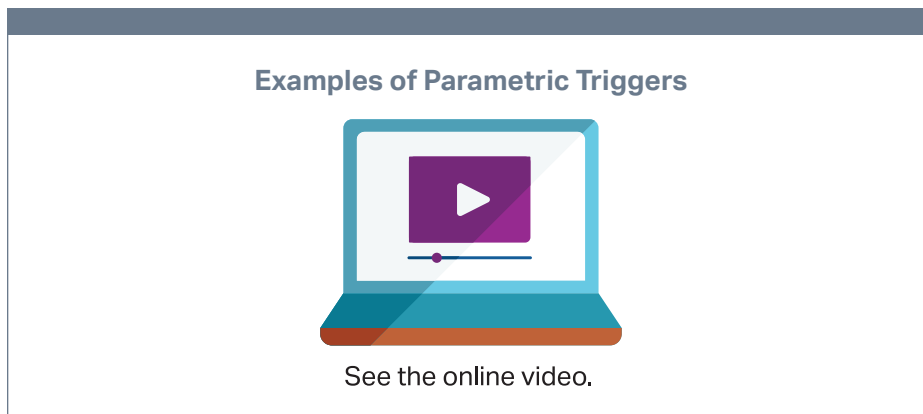
Emerging technology is making it easier to structure parametric coverage for both commercial and personal lines customers. For example, homeowners who have trouble obtaining affordable or adequate flood, windstorm, or earthquake coverage using traditional indemnity products may now be able to obtain some amount of parametric protection if the technology exists in their area to obtain accurate, real-time data on parameters such as rainfall, rising water levels, wind speed, and earth movement.

Blockchain technology is credited with being able to expedite claim payments under parametric contracts that use smart contract technology. Smart contracts can be automatically executed by verifying information provided by a neutral third party. The ability of the blockchain to reliably verify third-party data makes it an ideal instrument to administer parametric contracts.

Mobile technology makes it possible for individuals in communities and geographic areas that don't have access to traditional insurance products to obtain parametric coverage. As long as enough reliable data exists regarding the event for which coverage is sought, an individual in a remote area or an underserved market could potentially shop for a parametric policy, sign up for coverage, pay the premium, file a claim, and receive payment—all from a smartphone.

## Prevalent Triggers

The key to creating a parametric insurance product is the ability to identify an appropriate triggering event parameter and reliably establish when that parameter has been met or exceeded. If enough data can be obtained (preferably from a neutral third party) regarding a specific event to accurately determine whether the parameter has been met or exceeded, coverage can be established. To learn more, see “Examples of Parametric Triggers.”



[DA14363\_1]

A parametric contract must specifically delineate the loss payment, parameter, and party or mechanism responsible for verifying that the parameter was met or exceeded.

## Benefits

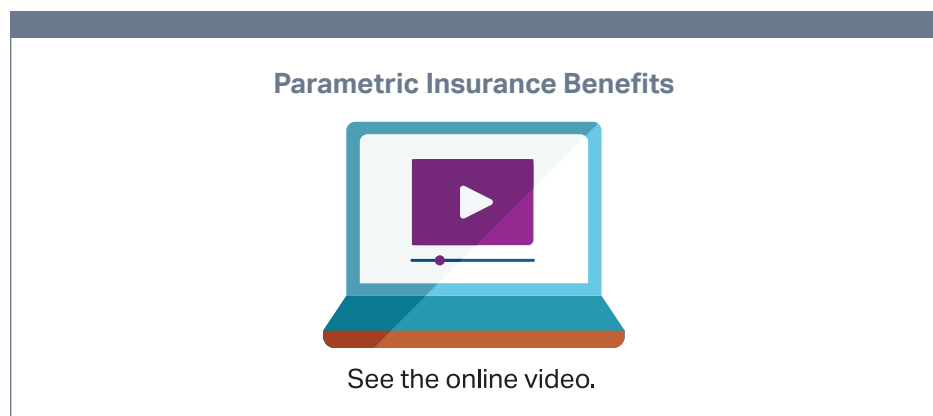
Parametric insurance offers many advantages to the parties involved. For starters, it can create a way to cover risks that may be difficult to insure (or are altogether uninsurable), such as weather-related business income loss exposures for an outdoor event's venue. Without parametric coverage, administering such policies could be entirely too cost-prohibitive.

The reduced administrative costs could also allow smaller transactions to take place, providing commercial customers and consumers with access to preset

policies via apps on their phones or through the internet. This, in turn, could provide insurance opportunities to customers in geographic locations that are too far removed from population centers for traditional insurance methods—which may require assessments or loss adjusting—to work.

Parametric coverage can also help policyholders by giving them a quick injection of cash to keep them afloat until they receive a claim payment from a traditional indemnity product.

It can take weeks (or longer) for claimants to receive settlement payments from traditional insurance policies following a major catastrophe, but expenses kick in immediately. With parametric insurance, the payment is triggered when a specific parameter is met or exceeded. Combine that with the fact that the exact payout was determined from the outset of the agreement, and a parametric policy eliminates the need for a lengthy claims process. All of this ultimately aids recovery and loss mitigation. To learn more, see “Parametric Insurance Benefits.”



[DA14363\_2]

---

#### **Apply Your Knowledge**

What risk is posed by parametric insurance, and how should an insurer (or a producer) address it when dealing with a potential customer?

*Feedback :* **Basis risk** is inherent in parametric contracts. For example, a parametric contract may call for the insured to receive \$20,000 if a specific loss occurs, but the actual damage could be greater (meaning that the insured would not be fully indemnified) or less (meaning that the insured would benefit from the parametric contract) than \$20,000. Also, if the parameters that would trigger the contract are just barely missed—such as a rainfall amount that falls just short of the trigger threshold—the insured may suffer damage but receive no compensation.

Because of the possibility that a parametric policy will not fully indemnify the insured for a loss, the insurer (or producer) must take great care to clearly explain to potential customers that a claim payment will be issued only once

#### **Basis risk**

The risk that the amount the organization receives to offset its losses may be greater than or less than its actual losses.

the agreed-upon parameter is reached, and the payment will not be increased or decreased based on the insured's actual losses (as it would be under a traditional insurance product). As a result, a parametric policy may not be a suitable substitute for other insurance.

---

## SUMMARY

Although insurance has always involved data analytics, technology and big data provide many more sources and a much larger quantity of data. Because the quantity of data now available cannot be organized and analyzed with traditional techniques, data science has developed methods to organize and analyze the data to provide relevant information. Organizations can then use that knowledge strategically to improve business decisions.

Data science emerged as a scientific field in response to the convergence of big data and technology. Because traditional skills and methods are insufficient to handle the rapid changes in the amounts and types of data, professionals with a unique combination of knowledge and skills are necessary to provide useful business solutions. Because domain knowledge is an important aspect of data science, insurance and risk management professionals are often important members of data science teams who provide a business context.

Although risk managers and insurers have traditionally made decisions based on data, the amount and sources of data have increased exponentially and will continue to do so. Additionally, the methods to gather, process, and analyze data have also increased and become more sophisticated. To gain competitive advantage and operate more effectively, insurers and risk managers must be able to frame business problems and questions and use the techniques of data science to perform analysis that will improve results.

- <Summarize the definition, if applicable.>
- <Provide bullet points of concepts.>
- <Follow up with a statement of the importance of the content taught in the module.>
- <Summarize the definition, if applicable.>
- <Provide bullet points of concepts.>
- <Follow up with a statement of the importance of the content taught in the module.>

Parametric insurance offers a predetermined payout that's triggered when a parameter, such as those produced by weather events, is met or exceeded. Emerging technology is making it easier to develop and deliver parametric products. Some of the most prominent benefits of a parametric policy are

### 3.22 Exploring Today's Risk Management and Insurance Landscape

---

its clear terms, the speed of the claims process, and the certainty of knowing exactly what the claim payment will be.

# Index

Page numbers in boldface refer to pages where the word or phrase is defined.

## SYMBOLS

<Concept 1>, 3.15, 3.16  
<Concept 2>, 3.15, 3.16  
<Concept 3>, 3.15–3.16  
<Enter Concept LO title here>, 3.15, 3.16

## A

Actuary, **3.10**  
Artificial intelligence (AI), **3.5, 3.18**  
Assessing Cyber Risk Business Income Exposures, 2.7–2.8  
Assessing Data Liability Exposures, 2.16–2.19  
Assessing Liability Exposures, 2.20–2.23  
Auto Insurance for High-Risk Drivers, 1.19  
Auto Insurance Rate Regulation, 1.20

## B

Basis risk, **3.20**  
Benefits, 3.19–3.21  
Big data, **3.3**  
Big Data, 3.4  
Blockchain, 1.16  
Breach of contract, **2.18**  
Business income insurance, 2.7  
Business interruption, 2.6  
Business Partner Liability, 2.19

## C

Civil law, 1.9  
Class action (class action lawsuit), **2.18**  
Cloud computing, **3.18**  
Compulsory auto insurance law, **1.18**  
Continuing expenses, 2.9  
Continuing Expenses, 2.9  
Conversion, **2.18**  
Cyber risk, 2.3  
Cyber risk loss exposure, 2.11

## D

Damages, 1.8  
Data breach, 2.3  
Data Breach Exposures, 2.12  
Data-driven decision making, **3.12**  
Data-Driven Decision Making, 3.12–3.14  
Data mining, 3.5  
Data science, 3.6

Data Science, 3.6, 3.8–3.10  
Data Science and Data-Driven Decision Making, 3.12–3.13  
Data Science Concepts, 3.8  
Data Science Team, 3.10  
Data Scientist, 3.10  
Directors and Officers Liability, 2.20  
Domain knowledge, **3.10**

## E

Effect on Expenses, 2.9  
Evaluating Cyber Risk Property Exposures, 2.3  
Evaluating Exposures Related to Data Breaches and Reputational Risk, 2.11  
Extra expenses, 2.9  
Extra Expenses, 2.9–2.10

## F

Fiduciary duty, **2.18**  
Financial responsibility law, **1.18**  
Fraud, **2.18**

## G

General damages, 1.9

## H

Homeowners Insurance Forms, 1.13  
How the Environment Is Evolving, 1.15–1.17, 1.22

## I

Intangible property, 2.3  
Intangible Property, 2.4–2.6  
Intellectual property, 2.4  
Intentional tort, 1.10  
Internet of Things (IoT), 1.15, 3.5  
Invasion of privacy, 2.18

## L

Law of large numbers, **3.3**  
Liability for Customer Data, 2.18  
Liability loss exposure, 1.8

## M

Machine learning, 3.5  
Malware, 2.4

## 2 Exploring Today's Risk Management and Insurance Landscape

---

Managing Personal Liability Exposures, 1.8–1.9  
Managing Personal Property Exposures, 1.3–1.7  
Measurement of Business Income Loss, 2.7  
Model for Data-Driven Decision Making in Risk Management and Insurance, 3.14

### N

Negligence, 1.10  
Net income, 2.7  
Network Security Liability, 2.19–2.20  
Noncontinuing expenses, 2.9

### O

Opportunities Presented by Big Data and Technology, 3.3

### P

Personal injury protection (PIP) coverage, 1.18  
Personal Liability Loss Exposures, 1.9  
Personally identifiable information (PII), 2.4  
Personal property, 1.3  
Personal Vehicle Risk Management Environment, 1.17–1.18  
Predictive modeling, 3.18  
Prevalent Triggers, 3.19  
Property and Perils Involved, 2.10  
Property loss exposure, 1.3  
Property Loss Exposures, 1.3  
Punitive damages (exemplary damages), 1.9

### R

Real property (realty), 1.3  
Reputation, 2.11  
Reputational risk, 2.13  
Reputational Risk Exposures, 2.13  
Residential Risk Management Environment, 1.12  
Residual market, 1.19  
Risk management process, 1.5  
Risk Management Techniques for Personal Liability Loss Exposures, 1.10  
Risk Management Techniques for Property Loss Exposures, 1.5

### S

Smart sensor, 3.18  
Special damages, 1.9  
Strategic Applications to Insurance, 3.6  
Strategic Opportunities From Big Data and Technology, 3.3  
Strict liability (absolute liability), 1.10

### T

Tangible property, 2.3  
Tangible Property, 2.3–2.4

Technology, 3.5  
Technology Fueling Growth, 3.18–3.19  
Telematics, 3.5  
Text mining, 3.5  
Third-Party Data Liability Exposures, 2.17–2.18  
Tort, 1.10

### U

Understanding Parametric Coverage and Why It Matters, 3.16–3.17

### V

Variations in State Law, 1.18