Module 12

Cyber Risk, Terrorism, and International Insurance

Cyber Risk, Terrorism, and International Insurance

Module 12
Chapter 12

1

1

Objectives

- Obj I: Cyber Risk Loss Exposures
- Obj II: Controlling and Financing Cyber Risk Loss Exposures
- Obj III: Cyber Risk Insurance Policies
- Obj IV: Terrorism Insurance
- Obj V: International Insurance Solutions

2

2

Cyber Risk Loss Exposures

Objective I

3

3

Cyber Risk Loss Exposures

- An organization may rely on a computer network, digital devices, and a website.
  - These systems can be compromised or damaged.
- The use of such systems increases the exposure to:
  - Property loss.
  - Net income loss.
  - Liability loss.

4

4

Property Loss

- Property exposed to loss:
  - Tangible property – has a physical form.
  - Intangible property – no physical form.
    - Electronic data is an especially valuable and vulnerable type of intangible property.
- Commercial property forms usually limit electronic data coverage to a small amount.
  - Commercial liability forms often only cover tangible property, which excludes electronic data.

5

5

Net Income Loss

- Organizations can suffer a reduction in or cessation of normal business operations due to a computer network security breach.
  - Reductions in business operations are commonly known as business interruptions.
- Any possible business interruption that decreases revenues and/or increases expenses should be considered by an organization.

6

6

Net Income Loss

- Net income exposed to loss can be evaluated in terms of loss of business income and extra expenses.
  - Extra expenses could include cost of hiring a contractor to restore a computer network.
- Contingent business income loss exposures relate to income dependent on a network not owned or operated by the organization.
  - Can also result from events affecting the networks of suppliers, utilities, or vendors.

7

7

Liability Loss

- Organizations must guard against bodily injury and property damage exposures generated by technology-related activities.
  - Bodily injury liability can occur because of software development.
  - Property damage loss exposures can occur because of overall technology operations.

8

8

Liability Loss

- Coverage B of the CGL covers liability for personal and advertising injury.
  - Excludes coverage for activities such as designing websites, internet searches, and providing internet service.
  - Also excludes injury arising out of an electronic chat room or bulletin board the insured owns, hosts, or controls.
- Organizations face liability exposures for product advertising on their website.

9

9

Liability Loss

- Organizations also are subject to cyber risk intellectual property liability loss exposures.
  - Can affect an organization's copyrights, trademarks, patents, or trade secrets.
- Cyber risk errors and omissions (E&O) liability also exists.
  - Organizations should consider the scope of their daily business operations and how their actions could result in E&O liability.

10

10

Practice

- Which one of the following statements is correct regarding cyber risk loss exposures?
  - A. Net income exposed to cyber risk loss can be evaluated in terms of loss of operating systems and website functionality.
  - B. Cyber risk intellectual property loss exposures can affect a company's trademarks.
  - C. Bodily injury losses are not a concern with respect to cyber risk loss exposures.
  - D. Cyber risk property loss exposures only apply to tangible property.

11

11

Controlling and Financing Cyber Risk Loss Exposures

Objective II

12

12

Risk Control Measures

- Specialized risk control measures are usually necessary to control cyber risk loss exposures.
  - Physical controls.
  - Procedural controls.
  - Personnel controls.
  - Managerial controls.
  - Investigation and prosecution of cyber crimes.
  - Post-cyber incident rapid recovery program.

13

13

Physical Controls

- Physical controls place barriers between cyber criminals and their targets.
  - Organizations should provide physical protection such as alarms and locked doors.
- Access to sensitive areas should be controlled through ID badges or through biometrics.
  - Biometrics are methods of biological identification, such as fingerprints.

14

14

Procedural Controls

- Procedural controls specify tasks be performed in secure ways that prevent or reduce losses.
  - Apply to how a computer system and all of its associated data are protected.
- Protection from hackers is a critical reason for organizations to create, implement, and update procedural controls.
  - Controls include passwords, antivirus software, data encryption, and firewalls.

15

15

Personnel Controls

- Some employees are inadvertently the source of cyber losses.
  - Controls include preemployment screening, training, outlining unacceptable behavior, and termination procedures.
  - Personnel controls can also extend to how the organization deals with its customers, suppliers, and neighbors.

16

16

Managerial Controls

- Managerial controls establish an environment that detects or prevents cyber losses.
  - Include centralizing responsibility for cyber security.
  - Also involve ensuring systems are monitored and followed to control cyber loss exposures.
- An organization should continually evaluate and revise its risk control measures.

17

17

Prosecution of Cyber Crimes

- Organizations often do not report cyber crimes to authorities.
  - May fear negative publicity.
- Organization may experience PR benefit by releasing the news regarding a cyber crime.
  - Can describe the measures it is taking to prevent such an incident from recurring.
  - Restores consumer confidence.
- Reporting certain types of cyber crimes may not be optional for some organizations.

18

18

Rapid Recovery Program

- A post-cyber incident rapid recovery program aids in reducing the severity of cyber losses.
  - Restores operations as soon as possible.
  - Focuses on preservation of net income in the event of a cyber loss.
- Risk control measures include maintaining full backups of the computer system.
  - Also should include a public relations component.

19

19

Risk Financing Measures

- Risk financing measures include:
  - Insurance.
  - Noninsurance risk transfer.
  - Retention.
- Sources of risk financing can be secured before or after a loss occurs.

20

20

Noninsurance Risk Transfer

- A hold-harmless agreement, or indemnity agreement, is a type of noninsurance measure.
  - Organizations can receive reimbursement for cyber risk losses.
- Many software firms also use liability disclaimers.
  - Do not transfer risk or act as risk financing.
  - Can be used to limit the scope of liability.

21

21

Retention

- An organization may use retention to finance its cyber risk loss exposures.
  - Funds within the organization are used to pay for losses.
  - One advantage of retention is that it encourages risk control.
- An organization should limit its retention to a severity level at which it can tolerate the variability in the sum of its retained losses.

22

22

Practice

- At an amusement park in Florida, guests who exit the park often desire to return to the park later in the day. Upon returning to the park, the guests are asked to insert their finger into an electronic reader at the time of reentry so the park can ensure that a ticket is used by the same person from day to day. This is an example of which type of risk control measure?
  - A. Telematics.
  - B. Fintech.
  - C. Biometrics.
  - D. Procedural control.

23

23

Cyber Risk Insurance Policies

Objective III

24

24

Insuring Agreements

- Cyber risk insurance needs vary widely.
  - Some insurers allow their customers to supplement a basic product with the insuring agreements that are appropriate for them.
  - Others allow for full policy customization using insuring agreements.
  - Other insurers offer a standard package of insuring agreements.
- Insuring agreements apply to various coverage areas.

25

25

Insuring Agreements

Insuring Agreement	Covered Loss
Electronic Data Protection	Costs to recover or restore electronic data that have been altered, destroyed, deleted, or damaged.
Cyber Extortion	Expenses related to computer network kidnap or ransom events.
Cyber Crime	Theft of money and securities.
Notification or Remediation	Expenses related to crisis management during or after a loss (such as a security breach).
Business Interruption	Loss of business income resulting from network security breach or other cyber events.

26

26

Insuring Agreements

Liability Insuring Agreement	Covers Liability Arising From
Network Security Liability	Security breaches to insured's computer network.
Privacy Liability	Unauthorized disclosure or use of the private information of others.
Electronic Media Liability	Insured's electronic content.
Technology Errors & Omissions Liability	Any negligent act, error, or omission relating to an insured's products or services.
Intellectual property liability	Copyright or patent infringement claims.

27

27

Coverage Triggers

- Policies are usually subject to a claims-made or discovery coverage trigger.
  - Coverage is usually available for prior acts, subject to a retroactive date.
- Claim is typically made when the insured first becomes aware of facts that could cause a reasonable person to assume that a loss has occurred.

28

28

Exclusions

- Cyber risk policy exclusion categories:
  - General exclusions – exclusions that may also be found in other types of policies.
    - Intentional acts, fraud, SEC violations.
  - Product-related exclusions – apply to products produced by the insured and/or serviced and supported by the insured.
    - Product recall, defects in design, bodily injury, and breach of warranty.

29

29

Exclusions

- Cyber risk policy exclusion categories:
  - Service-related and security-related exclusions – found in policies purchased by technology services and support providers.
    - Performance delay, security breach.
  - Cyber risk-related exclusions – found in policies typically purchased by technology-oriented organizations with a website.
    - Advertising injury, copyright infringement.

30

30

Limits of Insurance

- Several types of limits of insurance are available for cyber risk policies.
- The limits offered depend on whether the policy has an annual aggregate limit of insurance.
  - No aggregate limit – insuring agreements work independently, each with its own limit.
    - Most package or modular policies.
  - Aggregate limit – each insuring agreement will have an insuring agreement aggregate limit of insurance.

31

31

Coverage Territory

- Virtually all cyber risk insurers provide worldwide coverage.
  - May be contingent on whether a loss is a first-party loss or a third-party loss.
  - May be contingent on what geographic location a suit for damages is brought.

32

32

Practice

- A company that needs coverage for expenses related to computer network kidnap and/or ransom events should choose which one of the following insuring agreements in a cyber risk insurance policy?
  - A. Electronic data protection.
  - B. Electronic media liability.
  - C. Cyber extortion.
  - D. Cyber crime.

33

33

Terrorism Insurance

Objective IV

34

34

TRIA

- Under the Terrorism Risk Insurance Act (TRIA), the federal government shares responsibility for terrorism losses with the insurance industry.
  - Insurers writing lines of business subject to TRIA are required to make coverage available for certified acts of terrorism on the same terms as coverages applicable to non-terrorism events.
  - ISO has developed terrorism endorsements to help insurers comply with TRIA.

35

35

TRIPRA

- The Terrorism Risk Insurance Program Reauthorization Act reauthorized TRIA.
  - Designed to provide stability in the insurance market regarding terrorism coverage.
- The Act gradually increases the insurance industry's participation in payment of losses.
  - Reduces federal government's participation.
- The Act retains many provisions of TRIA.

36

36

TRIPRA

- TRIPRA requires all commercial property insurers to make coverage available for terrorism losses.
  - Secretary of the Treasury certifies acts of terrorism.
  - Acts of a war declared by Congress are not acts of terrorism.
  - Acts with aggregate losses less than or equal to $5,000,000 are not acts of terrorism.

37

37

TRIPRA

- The federal government only participates in losses if act results in aggregate insured losses greater than program trigger.
  - TRIPRA trigger starts and $100,000,000.
  - Increased in increments of $20,000,000 per year until cap of $200,000,000 is reached.
- Not all commercial lines of insurance are eligible for loss-sharing program.
  - Personal lines are never eligible.

38

38

TRIPRA

- TRIPRA requires property insurers to offer terrorism coverage without terrorism-specific exclusions or limitations.
  - Coverage cannot be materially different than non-terrorism coverage.
- Insurer is responsible for all terrorism losses until losses exceed 20% of direct premiums.
  - Federal government enters into cost sharing for excess losses.
- Overall cap on covered losses is $100 billion.

39

39

Disclosure Endorsements

- TRIA requires insurers to disclose to insureds:
  - Portion of premium attributed to certified acts of terrorism.
  - Federal share of compensation for certified acts of terrorism.
  - Amount of program cap ($100 billion).
    - Must explain if program cap is exceeded, coverage for losses may be reduced at discretion of the Secretary of the Treasury.

40

40

ISO Endorsements

- ISO contains the following endorsements:
  - Cap endorsement – insurer must attach a cap endorsement when policyholder accepts certified acts of terrorism coverage.
    - Describes certified acts of terrorism.
  - Certified Acts Exclusion endorsement – excludes coverage for acts of terrorism.
    - Applies when insured declines insurer's offer of coverage.

41

41

ISO Endorsements

- ISO contains the following endorsements:
  - Aggregate Limit Endorsement – limits the insurer's exposure and provides limited liability coverage for certified acts.
  - Other Acts Exclusion Endorsement – excludes acts committed outside the U.S.
  - Automobile endorsement – excludes coverage for commercial auto policies.
  - Nuclear, biological, chemical, or radiological endorsement – excludes NBCR acts.

42

42

NCCI Endorsements

- Insurers must include coverage for certified acts of terrorism in any workers compensation policies they write.
  - Therefore, few terrorism endorsements are needed for workers compensation insurance.
- NCCI endorsement discloses the portion of workers compensation premium attributed to certified acts.
  - Acts of war are covered under the endorsement.

43

43

Practice

- Which one of the following statements is correct regarding terrorism endorsements?
  - A. The workers compensation endorsement developed by NCCI includes acts of war among the losses that are covered.
  - B. Acts of terrorism that are not certified under the federal program are specifically excluded from coverage under the certified acts exclusion endorsement.
  - C. The main purpose of the aggregate limit endorsement is to provide a different means of marketing terrorism insurance coverage.
  - D. A $50,000,000 cap is placed on annual aggregate losses paid by the federal government and all insurers for certified acts of terrorism.

44

44

International Insurance Solutions

Objective V

45

45

International Exposures

- As an organization's international operations grow, new loss exposures are faced.
  - Insurance solutions change as organization's international exposures change.
- Common methods of addressing exposures:
  - Territorial endorsements to U.S. policies.
  - International package policies.
  - Local placements.
  - Controlled master programs (CMPs).

46

46

Territorial Endorsements

- CGL Coverage Form provides international coverage for a limited number of exposures.
  - Persons making short foreign trips.
  - Products liability coverage for goods made or sold in U.S. or Canada.
    - Not completed operations coverage.
  - Personal and advertising injury claims related to the Internet.
- CGL coverage only applies to a settlement, or suit brought about in the U.S. or Canada.

47

47

Territorial Endorsements

- Amendment of Coverage Territory-Worldwide Coverage endorsement extends CGL coverage.
  - Coverage applies anywhere in the world.
  - Covers suits brought in foreign courts.
  - Exception for country subject to trade sanctions by U.S.

48

48

Territorial Endorsements

- Commercial umbrella liability policies typically cover losses occurring anywhere in the world, if suit is brought in U.S. or Canada.
  - By endorsement, policies can be extended to handle overseas claims.
- Commercial property policies generally do not cover losses outside the U.S. or Canada.
  - Endorsements can provide limited international coverage for property losses or business income losses.

49

49

Territorial Endorsements

- Standard workers compensation policy covers employee injured while working temporarily overseas.
  - Voluntary Compensation Endorsement – covers injuries outside U.S. or Canada.
  - Repatriation expense coverage – pays expenses to bring injured employees to U.S. hospitals.

50

50

Territorial Endorsements

- Advantages of territorial endorsements:
  - Adequate coverage for minimal exposures.
  - Low premiums and convenience.
- Disadvantages of territorial endorsements:
  - Nonadmitted coverage issues – local courts and governments do not recognize coverage provided by these endorsements.
  - Coverage differences.
  - Deficient claim services – many U.S. insurers have little experience with international claims.

51

51

International Package Policies

- International package policies bundle property and casualty coverages.
  - Cover only overseas exposures.
  - Typically issued by U.S. insurers.
  - Nonadmitted insurance in other countries.
- Advantages:
  - Broad coverages at low prices.
  - Flexibility – can be easily modified.
  - International expertise.

52

52

Local Placements

- Local policies are most often purchased from insurers based in the host country.
- Advantages:
  - Compliance with local laws.
  - Coverage match.
  - Claim services – local insurers can provide knowledgeable in-country claims support.
  - Image – working with local insurers maintains a "good citizen" image.
  - Familiarity with coverages.

53

53

Local Placements

- Disadvantages:
  - Solvency issues.
  - Home office unfamiliarity – policies may be written in a foreign language, making it difficult for home office managers to determine the adequacy of protection.
  - Lack of economies-of-scale – policies in individual markets do not offer economies of scale & provide no leverage during disputes.
  - Lack of control.

54

54

Controlled Master Program

- A controlled master program (CMP) links policies in an organization's home country with foreign policies where they do business.
  - Managers work with a global broker and a global insurance provider.
  - Premiums paid to purchase policies overseas reduce premium under master policy.
- CMP fully covers all international exposures.
  - Claims are adjusted in the countries where they occur.

55

55

Controlled Master Program

- Property losses not covered by the local policy can be covered under the master policy.
  - Master policy also acts as excess policy if claim exceeds local policy limits.
- Master policies usually contain additional coverages that cannot be included in local policies.
  - Can include political risk coverage and workers compensation coverage for employees working overseas.

56

56

Controlled Master Program

- Advantages of writing a CMP:
  - Economies of scale – results in better prices.
  - Admitted coverage.
  - Claim services.
  - Centralized control.
  - Seamless coverages – local coverage plus master program that fills coverage gaps.
  - Tax coordination.

57

57

Practice

- Which one of the following statements is correct regarding international package policies as an international insurance solution?
  - A. They cover both the insured's domestic and international loss exposures.
  - B. Coverage is provided on an admitted basis, thus satisfying local regulations.
  - C. They are typically sold to companies headquartered in the United States.
  - D. They link master policies written in the insured's home country with local policies written in countries where the insured does business.

58

58