Overview:

1. Risk

2. Chance of loss

3. Classification

4. Major commercial risks

5. Types of IT risks

6. Burden of risk on society

RISK

- is everywhere

• origin from Italian word "risco"(17th century)

• no single definition of risk – economists, behavioural scientists, risk theorists, statisticians, actuaries, and historians each have their own concept of risk

• based on the concept of uncertainty, definition of risk: **uncertainty concerning the occurrence of a loss**

Risk vs uncertainty

- **risk** = situations where probabilities of possible outcomes are known or can be estimated with some degree of accuracy

    - e.g. probability of hacker attack can be estimated with considerable accuracy

- **uncertainty** = situations such probabilities cannot be estimated

    - e.g. probability of destruction of your firm by a meteorite from outer space is only a guess and generally cannot be accurately estimated

Definitions of risk

- variability in future outcomes;

- chance of loss;

- possibility of an adverse deviation from a desired outcome that is expected or hoped;

- variation in possible outcome that exist in a given situation;

- possibility that a sentient entity can incur a loss.

IT risk

- is basically any threat to the business data, critical systems and business processes

- is the risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an organization

- IT risks have the potential to damage business value and often come from poor management of processes and events

- IT risks vary in range and nature

Categories of IT risk

IT risk spans a range of business-critical areas:

- security - compromised business data due to unauthorised access or use

- availability - inability to access your IT systems needed for business operations

- performance - reduced productivity due to slow or delayed access to IT systems

- compliance - failure to follow laws and regulations (e.g. data protection)

Loss exposure

Corporate risk managers use the term **loss exposure** to identify potential losses.

- any situation or circumstance in which a loss is possible, regardless of whether a loss actually occurs.

- e.g.: hardware that can be damaged by an earthquake or flood, defective products that may result in lawsuits against the manufacturer, possible theft of company property because of inadequate security, and potential injury to employees because of unsafe working conditions

Decisions

Decisions can be made under:

1. Certainty

2. Uncertainty - no insight into the future

3. Risk

- Objective - based on statistics and calculations, probability distribution is known

- Subjective - based on experience and guesswork, probability distribution is unknown

Objective risk (OR)

- degree of risk

- the relative variation of actual loss from expected loss

- e.g.: Assume that 10 000 companies are insured against cyber attacks and hacking attacks over a long period, and on average 1%, 100 companies are hacked each year (in some years, as few as 90 companies may be hacked, in others years as 110 companies may be hacked). Thus, there is a variation of 10 companies from expected number of 100, or a variation of 10% (10/100).

Objective risk (OR)

- OR varies inversely with the square root of the number of cases under observation.

- e.g.: OR was 10/100 or 10%. Now assume that 1 million companies are insured. The expected number of companies that will be hacked is now 10 000, but variation of actual loss from expected loss is only 100. OR is now 100/10 000 or 1%. Thus, as the square root of the number of companies increased from 100 in the first example to 1 000 in the second example (10 times), OR decline to one-tenth of its former level.

Objective risk (OR)

- OR can be statistically calculated by some measure of dispersion (standard deviation or the coefficient of variation). This is purpose, why it is an extremely useful concept for an insurer or a corporate risk manager. As the number of exposures increases, an insurer can predict its future loss experience more accurately because it can rely on the **law of large numbers** (as the number of exposure units increases, the more closely the actual loss experience will approach the expected loss experience).

- e.g.: As the number of companies under observation increases, the greater is the degree of accuracy in predicting the proportion of companies that will be hacked.

Subjective risk (SR)

- perceived risk, uncertainty based on a person's mental condition or state of mind

- e.g.: Assume that a driver with several convictions for drunk driving is drinking heavily in a neighborhood bar and foolishly attempts to drive home. The driver may be uncertain whether he will arrive home safely without being arrested by the police for drunk driving. This mental uncertainty or perception is called SR.

- The impact of SR varies depending on the individual. 2 persons in the same situation can have a different perception of risk, and their behaviour may be altered accordingly. If an individual experiences great mental uncertainty concerning the occurrence of a loss, that person's behaviour may be affected.

Subjective risk (SR)

- High SR often result in conservative and prudent behaviour, whereas low SR in less conservative behaviour.

- e.g.: Assume that a motorist previously arrested for drunk driving is aware that he has consumed too much alcohol. The driver may then compensate for the mental uncertainty by getting someone else to drive the car home or by taking a cab. Another driver in the same situation may perceive the risk of being arrested as slight. This second driver might drive in a more careless and reckless manner; a low SR results in less conservative driving behaviour.

Chance of loss

- is closely related to the concept of risk

- the probability that an event will occur

- can be distinguished from OR – chance of loss may be identical for 2 different groups, but OR may be quite different

- e.g.: Assume that 10 000 companies are insured against cyber attacks and hacking attacks in Berlin and 10 000 companies are insured in London and that the chance of a hacking attack in each city is 1%. Thus, on average, 100 companies should be hacked annually in each city. However, if the annual variation in losses ranges from 75 to 125 in Berlin, but only from 90 to 110 in London, OR is greater in Berlin even though the chance of loss in both cities is the same.

Objective probability (OP)

- the long-run relative frequency of an event based on the assumptions of an infinite number of observations, and of no change in the underlying conditions

- OP can be determined by:

  1. Deductive reasoning – a priori probabilities, e.g.: the probability of getting a head from the toss of a perfectly balanced coin is 1/2 because there are two sides and only one is a head; the probability of rolling a 6 with a single die is 1/6, since there are six sides and only one has six dots.

  2. Inductive reasoning – e.g.: the probability that a person age 21 will die before age 26 cannot be logically deduced. However, by a careful analysis of past mortality experience, life insurers can estimate the probability of death and sell a five-year insurance policy issued at age 21.

Subjective probability (SP)

- the individual's personal estimate of the chance of the loss

- SP need not coincide with OP

- e.g.: people who buy a lottery ticket on their birthday may believe it is their lucky day and overestimate the small chance of winning

Subjective probability (SP)

- A wide variety of factors can influence SP – a person's age, gender, intelligence, education, the use of alcohol or drugs, and of course, the way in which probability is perceived.

- e.g.: Assume that a slot machine in a casino requires a display of 3 lemons to win. The person playing the machine may perceive the P of winning to be quite high. However, if there are 10 symbols on each reel and only one is a lemon, the OP of hitting the jackpot with 3 lemons is quite small. Assuming that each reel spins independently of the others, the P that 3 lemons will simultaneously show a lemon is the product of their individual probabilities (1/10 x 1/10 x 1/10 = 1/1000). This knowledge is advantageous to casino owners.

Different terms

The concept of risk should not be confused with the terms:

1. Peril

- the cause of loss

- e.g.: if your company is hacked, the peril is the hacking attack. If company's car is damaged in a collision with another car, collision is a peril.

- Common perils that cause loss to property include fire, lightning, windstorm, hail, tornado, earthquake, flood, burglary, and theft.

2. Hazard

- a condition that creates or ↑ the frequency or severity of loss

- There are 4 major types

Hazard

1. Physical hazard:

   - a physical condition that ↑ the frequency or severity of loss

   - e.g.: icy roads (↑ the chance of an auto accident); defective wiring in a building (↑ the chance of fire); and a defective lock on a door (↑ the chance of theft)

2. Moral hazard:

   - dishonesty or character defects in an individual that ↑ the frequency or severity of loss

   - e.g. in insurance: faking an accident to collect benefits from an insurer; submitting a fraudulent claim; inflating the amount of a claim; and intentionally burning unsold merchandise that is insured; murdering the insured to collect the life insurance proceeds

   - because of moral hazard, insurance premiums are higher

   - it is difficult to control – insurers attempt to control by the careful underwriting of applicants for insurance and by various policy provisions, such as deductibles, waiting periods, exclusions, and rider

Hazard

3. Attitudinal hazard:

   - careless or indifference to a loss, which ↑ the frequency or severity of a loss

   - e.g.: leaving car keys in an unlocked car (↑ the chance of theft); leaving a door unlocked (allows a burglar to enter); and changing lanes suddenly on a congested expressway without signalling (↑ the chance of an accident)

4. Legal hazard:

   - characteristics of the legal system or regulatory environment that ↑ the frequency or severity of loss

   - e.g.: adverse jury verdicts or large damage awards in liability lawsuits; statutes that require insurers to include coverage for alcoholism; and regulatory action by state insurance departments that prevents insurers from withdrawing from a state because of poor underwriting results

Classification of risk

Risk can be classified into several distinct classes. The most important include the following:

1. Pure and speculative risk

2. Diversifiable and nondiversifiable risk

3. Enterprise risk

4. Systemic risk

Pure and speculative risk

1. Pure risk

   - a situation in which there are only the possibilities of loss or no loss

   - the only possible outcomes are adverse (loss) and neutral (no loss)

   - e.g.: premature death, job-related accidents, catastrophic medical expenses, and damage to property from fire, lightning, floor, or earthquake

2. Speculative risk

   - a situation in which either profit or loss is possible

   - e.g.: If you purchase 100 shares of common stock, you would profit if the price of the stock increases but would lose if the price declines.

   - e.g.: betting on a horse race, investing in real state, and going into business for yourself

Reasons to distinguish between pure and speculative risks

- private insurers generally concentrate on pure risks and do not emphasize the insurance of speculative risks (exceptions: insurance of institutional portfolio investments and municipal bonds against loss, enterprise risk management)

- the law of large numbers can be applied more easily to pure risks than to speculative risks (exception: speculative risk of gambling, where casino operators can apply the law of large numbers in a most efficient manner)

- society may benefit from a speculative risk even though a loss occurs, but is harmed if a pure risk is present and a loss occur (e.g.: A firm may develop new technology for producing inexpensive computers. As a result, some competitors may be forced into bankruptcy. Despite the bankruptcy, society benefits because the computers are produced at a lower cost.) - society normally does not benefit when a loss from a pure risk occurs, such as a flood or earthquake that destroys a town or area

Diversifiable risk

- a risk that affects only individuals, business firms or small groups and not the entire economy

- nonsystematic, particular risk

- e.g.: car thefts, robberies, and dwelling fires

- it can be reduced or eliminated by diversification

- e.g.: A diversified portfolio of stocks, bonds, and certificates of deposits is less risky than a portfolio that is a 100% invested in common stocks. Losses on one type of investment (stocks) may be offset by gains from bonds and certificates of deposits.

- e.g.: There is less risk to a property and liability insurer if different lines of insurance are underwritten rather than one line. Losses on one line can be offset by profits on other line.

Nondiversifiable risk

- a risk that affects the entire economy or large numbers of persons or groups within the economy

- fundamental risk

- e.g.: rapid inflation, cyclical unemployment, war hurricanes, floods, and earthquakes

- it cannot be eliminated or reduced by diversification (exceptions: state unemployment compensation programs and federal flood insurance program in the US)

Enterprise risk

- term that encompasses all major risks faced by a business firm, include pure, speculative, strategic, operational and financial risks

- **Strategic risk** - uncertainty regarding the firm's financial goals and objectives (e.g.: if a firm enters a new line of business, the line may be unprofitable)

- **Operational risk** - uncertainty results from the firm's business operations (e.g. a bank that offers online banking services may incur losses if hackers break into the bank's computer)

Enterprise risk

- **Financial risk** - uncertainty of loss because of adverse changes in commodity prices, interest rates, foreign exchange rates, and the value of money (e.g.: a computer company that agrees to deliver computers at a fixed price to a customer in 3 moths may lose money if prices of sound cards rise)

  - treatment of financial risks typically requires the use of complex hedging techniques, financial derivates, future contracts, options, and other financial instruments

  - some firms appoint a chief risk officer (CRO), such as the treasurer, to manage the firm's financial risks

Enterprise risk

- **Enterprise risk management** - combines into a single unified treatment program all major risks faced by the firm

    - Then the firm can offset one risk against another. As a result, overall risk can be reduced. As long as all risks are not perfectly correlated, the combination of risks can reduce the firm's overall risk. In particular, if some risks are negatively correlated, overall risk can be significantly reduced.

- 3 approaches of enterpreneuters/risk managers:

    - risk averse/avoiding - conversational strategy, avoid risk projects;

    - risk loving/seeking - look for risky projects;

    - risk neutral - balance between risk averse and risk seeking;

Systemic risk

- the risk of collapse of an entire system or entire market due to the failure of a single entity or group of entities that can result in the breakdown of the entire financial system

- an economic risk that is extremely important in the monetary policies of central banks, fiscal policies of governments

- economic downswings can be caused by systemic risk

Major commercial risks (pure risks)

Personal risks - risks that directly affects an individual or family (premature death, inadequate retirement income, poor health, unemployment, property risks, liability risks) **Commercial risks** – can financially cripple or bankrupt the firm if a loss occur

1. Property risks

    •   Business firms own valuable business property that can be damaged or destroyed by numerous perils, including fires, windstorms, tornadoes, hurricanes, earthquakes.

    •   Business property (recorded in the balance sheet) includes plants and other buildings; furniture, office equipment, and supplies; computers and computer software and data; inventories of raw materials and finished products; company cars, boats, and planes; and machinery and mobile equipment. The firm also has accounts receivable records and may have other valuable business records that could be damaged or destroyed and expensive to replace.

2. Liability risks

- Business firms often operate in highly competitive markets where lawsuits for bodily injury and property damage are common. The lawsuits range from small nuisance claims to multimillion-dollar demands.

- ⇒ a need for online dispute resolution

- Firms are sued for numerous reasons, including defective products that harm or injure others, pollution of the environment, damage to the property of others, injuries to customers, discrimination against employees and sexual harassment, violation of copyrights and intellectual property, and numerous other reason.

- Directors and officers may be sued by stockholders and other parties because of financial losses and mismanagement of the company.

- Commercial banks, other financial institutions, and other business firms are exposed to enormous potential liability because of cybersecurity and identity theft crimes that have occurred in recent years.

3. Loss of business income

- Another important risk is the potential loss of business income when a covered physical damage loss occurs. The firm may shut down for several months because of a physical damage loss to business property due to a fire, tornado, hurricane, earthquake, or other perils.

- During the shutdown period, the firm would lose business income, which includes the loss of profits, the loss of rents if business property is rented to others, and the loss of local markets. Certain expenses may still continue such as rent, utilities, leases, interest, taxes, some salaries, insurance premiums, and other overhead costs. Fixed costs and continuing expenses that are not offset by revenues can be sizeable if the shutdown period is lengthy.

- The firm may incur extra expenses during the period of restoration that would not have been incurred if the loss had not taken place. Examples include the costs of relocating temporarily to another location, increased rent at another location, and the rental of substitute equipment.

4. Cybersecurity and identity theft

- Cybersecurity and identity theft by thieves breaking into firms' computer system and database are major problems for many firms.

- Computer hackers have been able to steal hundreds of thousands of consumer credit records, which have exposed individuals to identity theft and violation of privacy. As a result, commercial banks, financial institutions, and other business are exposed to enormous legal liabilities.

- Other crime exposures include robbery and burglary; shoplifting; employee theft and dishonesty; fraud and embezzlement; piracy and theft of intellectual property, and computer crimes.

5. Other risks

Business firms must cope with a wide variety of additional risks:

1. Human resources exposures

    - These include job-related injuries and diseases of workers; death or disability of key employees; group life and health and retirement plan exposures; and violation of federal and state laws and regulations.

2. Foreign loss exposure

    - These include acts of terrorism, political risks, kidnapping of key personnel, damage to foreign plants and property, and foreign currency risks.

5. Other risks

3. Intangible property exposures

- These include damage to the market reputation and public image of the company, the loss of goodwill, and loss of intellectual property.

- For many companies, the value of intangible property is greater than the value of tangible property.

4. Government exposures

- Government may pass laws and regulations that have a significant financial impact on the firm.

- Examples include laws that increase safety standards, laws that require reduction in plant emissions and contamination, and new laws to protect the environment that increase the cost of doing business.

Types of IT risks

Threats to IT systems can be external, internal, deliberate and unintentional.

Most IT risks affect one or more of the following:
- business or project goals
- service continuity
- bottom line results
- business reputation
- Security
- Infrastructure

Looking at the nature of risks, there are the examples of IT risks:

1. Physical threats - resulting from physical access or damage to IT resources - e.g.: the servers. These could include theft, damage from fire or flood, or unauthorised access to confidential data by an employee or outsider.

Types of IT risks

2. **Electronic threats** - aiming to compromise the business information - e.g.: a hacker could get access to your website, your IT system could become infected by a computer virus, you could fall victim to a fraudulent email or website. These are commonly of a criminal nature.

3. **Technical failures** - such as software bugs, a computer crash or the complete failure of a computer component. A technical failure can be catastrophic if you cannot retrieve data on a failed hard drive and no backup copy is available.

4. **Infrastructure failures** - such as the loss of your internet connection can interrupt your business - e.g.: you could miss an important purchase order.

5. **Human error** - is a major threat - e.g.: someone might accidentally delete important data, or fail to follow security procedures properly

Burden of risk on society

The presence of risk results in certain undesirable social and economic effects. Risk entails 3 major burden on society:

1. The size of an emergency fund must be increased. It is prudent to set aside funds for an emergency. However, in the absence of insurance, individuals and business firms would have to ↑ substantially the size of their emergency fund to pay for unexpected losses. E.g.: assume you have purchased a 6 000 000 CZK home and want to accumulate a fund for repairs if the home is damaged by fire, hail, windstorm, or some other peril. Without insurance, you would have to save at least 1 000 000 CZK annually to build up an adequate fund within a relatively short period of time. Even then, an early loss could occur, and your emergency fund may be insufficient to pay for the loss. If you are a middle- or low-income earner, you would find such saving difficult. In any event, the higher the amount that must be saved, the more current consumption spending must be reduced, which results in a lower standard of living.

Burden of risk on society

2. **Society is deprived of certain goods and services**.
   - E.g.: because of the risk of a liability lawsuit, many corporations have discontinued manufacturing certain products. Some 250 companies in the world once manufactured childhood vaccines; today, only a small number of firms manufacture vaccines, due in part to the threat of liability suits. Other firms have discontinued the manufacture of specific products, including asbestos products, football helmets, silicone-gel breast implants, and certain birth-control devices, because of fear of legal liability.

3. **Worry and fear are present**.
   - Numerous examples illustrate the mental unrest and fear caused by risk. Parents may be fearful if a teenage child departs on a ski trip during a blinding snowstorm because the risk of being killed on an icy road is present. Some passengers in a commercial jet may become extremely nervous and fearful if the jet encounters severe turbulence during the flight. A college student who needs a grade of C in a course to graduate may enter the final examination room with a feeling of apprehension and fear.

Thank you for your attention!