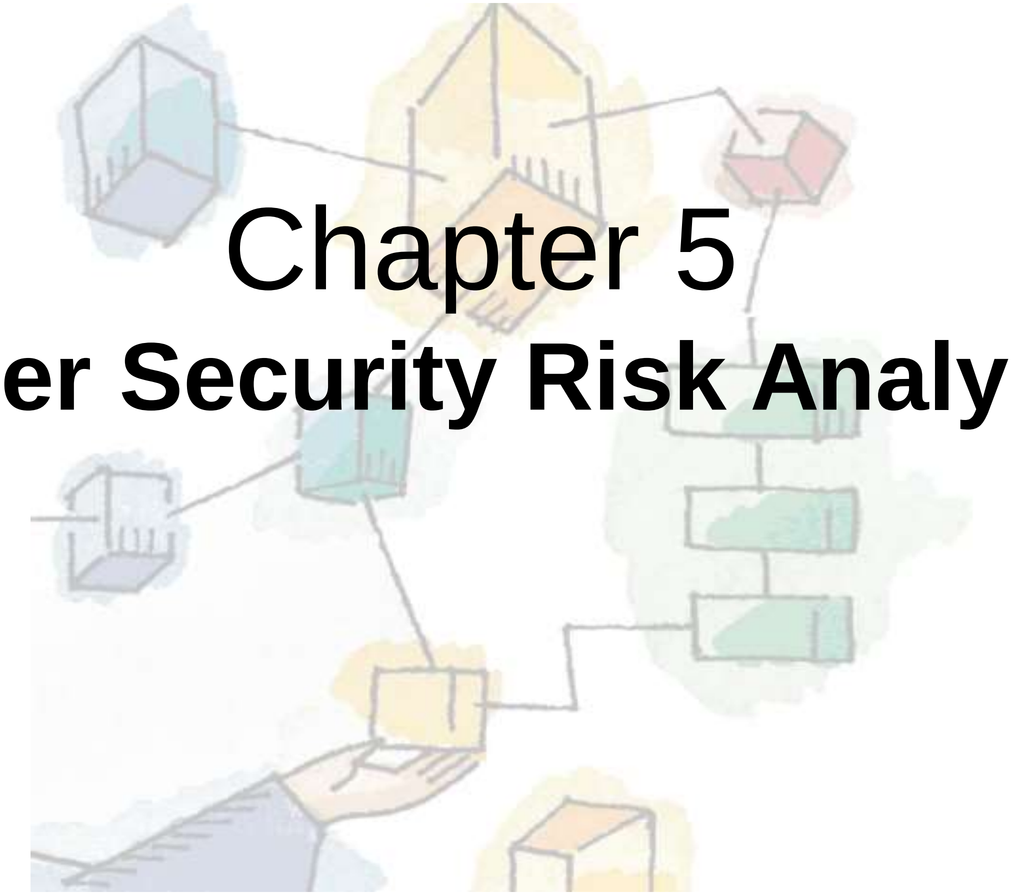
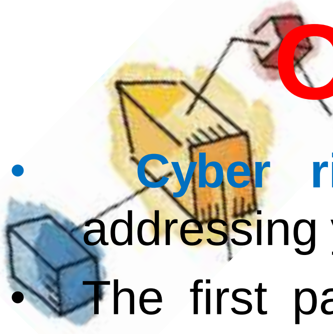


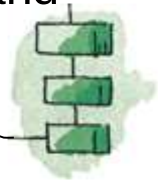
Chapter 5

Cyber Security Risk Analysis

Cyber Security Risk Analysis

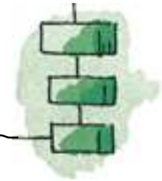


- **Cyber risk management** means identifying, analysing, evaluating and addressing your organisation’s cyber security threats.
- The first part of the cyber security risk management process is a cyber risk assessment. This risk assessment will provide a snapshot of the threats that might compromise your organisation’s cyber security and how severe they are.
- **Risk analysis** refers to the review of risks associated with the particular action or event. The risk analysis is applied to information technology, projects, security issues and any other event where risks may be analysed based on a quantitative and qualitative basis.
- Risks are part of every IT project and business organizations. The analysis of risk should be occurred on a regular basis and be updated to identify new potential threats. The strategic risk analysis helps to minimize the future risk probability and damage.
- **Cyber security Risk Management** must be continuous in order to maintain protections. Other factors beyond the changing threat landscape also affect existing cyber security risk planning. Regulations are often changed, or new ones introduced. The risks associated with these changes need to be analyzed, and cyber security policies and procedures changed to ensure compliance.

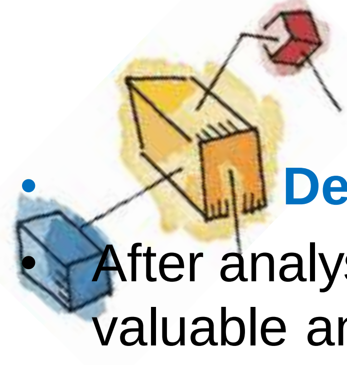


Steps in the risk analysis process

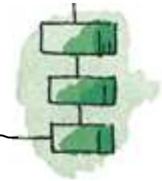
- The basic steps followed by a risk analysis process are:
- **Conduct a risk assessment survey:**
- Getting the input from management and department heads is critical to the risk assessment process. The risk assessment survey refers to begin documenting the specific risks or threats within each department.
- **Identify the risks:**
- This step is used to evaluate an IT system or other aspects of an organization to identify the risk related to software, hardware, data, and IT employees. It identifies the possible adverse events that could occur in an organization such as human error, flooding, fire, or earthquakes.
- **Analyse the risks:**
- Once the risks are evaluated and identified, the risk analysis process should analyse each risk that will occur, as well as determine the consequences linked with each risk. It also determines how they might affect the objectives of an IT project.



Steps in the risk analysis process



- **Develop a risk management plan:**
- After analysis of the Risk that provides an idea about which assets are valuable and which threats will probably affect the IT assets negatively, we would develop a plan for risk management to produce control recommendations that can be used to mitigate, transfer, accept or avoid the risk.
- **Implement the risk management plan:**
- The primary goal of this step is to implement the measures to remove or reduce the analyses risks. We can remove or reduce the risk from starting with the highest priority and resolve or at least mitigate each risk so that it is no longer a threat.
- **Monitor the risks:**
- This step is responsible for monitoring the security risk on a regular basis for identifying, treating and managing risks that should be an essential part of any risk analysis process.



Types of Risk Analysis

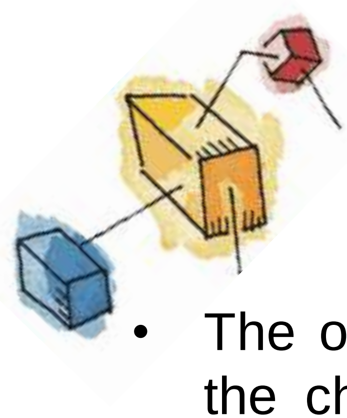
- The essential number of distinct approaches related to risk analysis are:

Quantitative

Qualitative

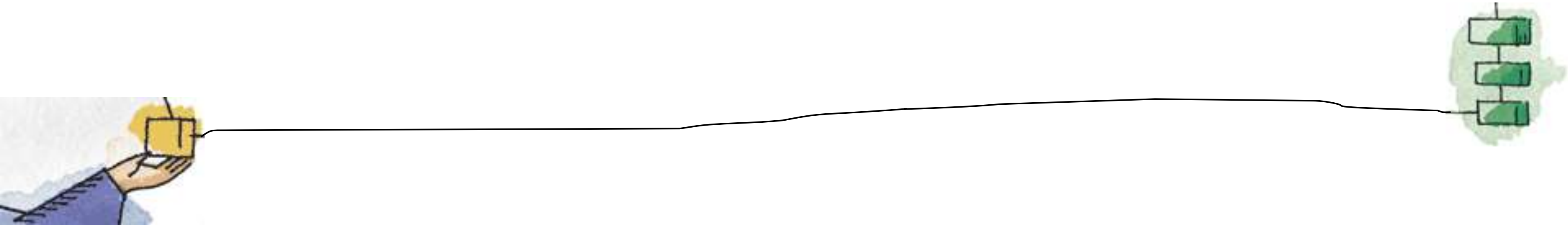
Types of Risk Analysis

- **Qualitative Risk Analysis**
- The qualitative risk analysis process is a project management technique that prioritizes risk on the project by assigning the probability and impact number. Probability is something a risk event will occur whereas impact is the significance of the consequences of a risk event.

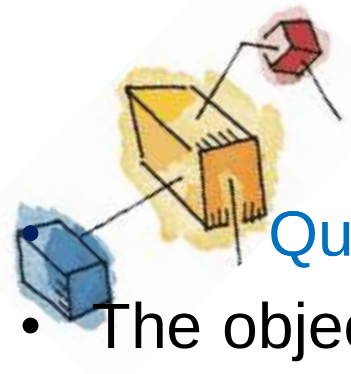


Qualitative Risk Analysis

- The objective of qualitative risk analysis is to assess and evaluate the characteristics of individually identified risk and then prioritize them based on the agreed-upon characteristics.
- The assessing individual risk evaluates the probability that each risk will occur and effect on the project objectives. The categorizing risks will help in filtering them out.
- Qualitative analysis is used to determine the risk exposure of the project by multiplying the probability and impact.

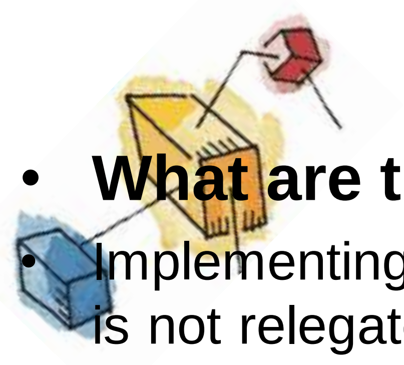


Quantitative Risk Analysis

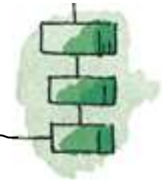


- Quantitative Risk Analysis
- The objectives of performing quantitative risk analysis process provide a numerical estimate of the overall effect of risk on the project objectives.
- It is used to evaluate the likelihood of success in achieving the project objectives and to estimate contingency reserve, usually applicable for time and cost.
- Quantitative analysis is not mandatory, especially for smaller projects. Quantitative risk analysis helps in calculating estimates of overall project risk which is the main focus.

Benefits of risk analysis

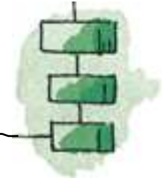


- **What are the Benefits of Cyber security Risk Management?**
- Implementing Cyber security Risk Management ensures that cyber security is not relegated to an afterthought in the daily operations of an organization. Having a Cyber security Risk Management strategy in place ensures that procedures and policies are followed at set intervals, and security is kept up to date. Cyber security Risk Management provides ongoing monitoring, identification, and mitigation of the following threats:
- **Phishing Detection**
- **VIP and Executive Protection**
- **Brand Protection**
- **Fraud Protection**
- **Sensitive Data Leakage Monitoring**
- **Dark Web Activity**
- **Automated Threat Mitigation**
- **Leaked Credentials Monitoring**
- **Malicious Mobile App Identification**
- **Supply Chain Risks**



Benefits of risk analysis

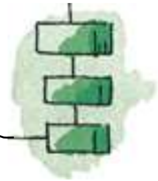
- Every organization needs to understand about the risks associated with their information systems to effectively and efficiently protect their IT assets. Risk analysis can help an organization to improve their security in many ways. These are:
- **Concerning financial** and organizational impacts, it identifies, rate and compares the overall impact of risks related to the organization.
- **It helps to identify** gaps in information security and determine the next steps to eliminate the risks of security.
- **It can also enhance** the communication and decision-making processes related to information security.
- **It improves security policies** and procedures as well as develop cost-effective methods for implementing information security policies and procedures.
- **It increases employee awareness** about risks and security measures during the risk analysis process and understands the financial impacts of potential security risks.



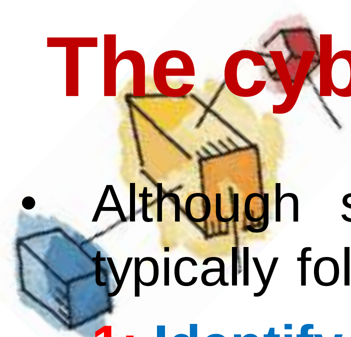
Enterprise and organization used risk analysis:

Enterprise and organization used risk analysis:

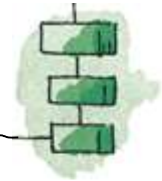
- To anticipates and reduce the effect of harmful results occurred from adverse events.
- To plan for technology or equipment failure or loss from adverse events, both natural and human-caused.
- To evaluate whether the potential risks of a project are balanced in the decision process when evaluating to move forward with the project.
- To identify the impact of and prepare for changes in the enterprise environment.



The cyber security risk management process



- Although specific methodologies vary, a risk management programme typically follows these steps:
- **1: Identify the risks** that might compromise your cyber security. This usually involves identifying cyber security vulnerabilities in your system and the threats that might exploit them.
- **2: Analyse the severity** of each risk by assessing how likely it is to occur and how significant the impact might be if it does.
- **3: Evaluate how each risk** fits within your risk appetite (your predetermined level of acceptable risk).
- **4: Prioritise the risks**.
- **5: Decide how to respond to each risk**. There are generally four options:
- **Treat** – modify the risk's likelihood and/or impact typically by implementing security controls.
- **Tolerate** – make an active decision to retain the risk (e.g., it falls within the established risk acceptance criteria).



The cyber security risk management process

- **Terminate** – avoid the risk entirely by ending or completely changing the activity causing the risk.
- **Transfer** – share the risk with another party, usually by outsourcing or taking out insurance.

- **6: Since cyber risk management** is a continual process, monitor your risks to ensure they are still acceptable, review your controls to ensure they are still fit for purpose, and make changes as required. Remember that your risks continually change as the cyber threat landscape evolves, and your systems and activities change.