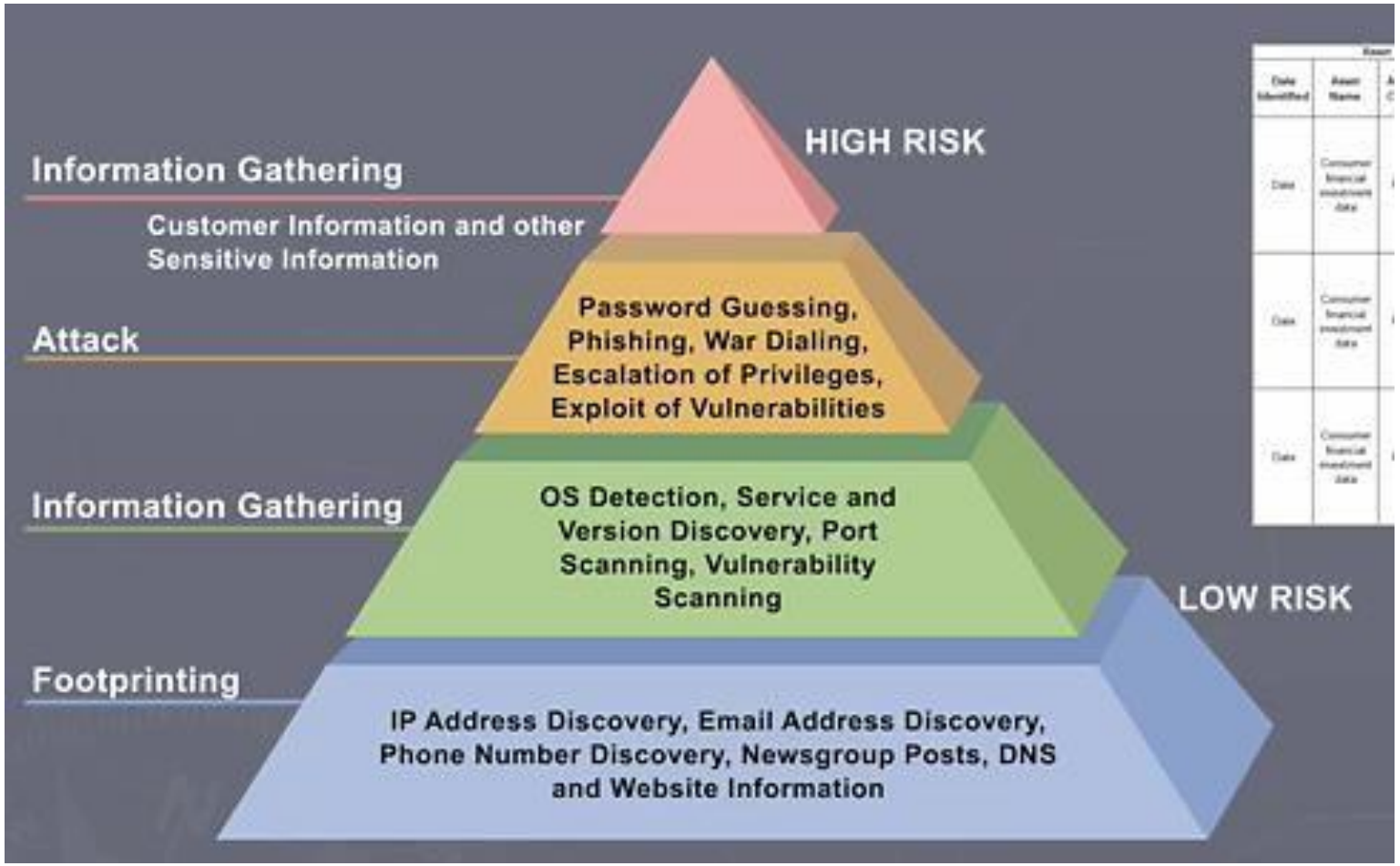
LECTURE 9
RISK MANAGEMENT

Dr WarusiaMohamed Yassin

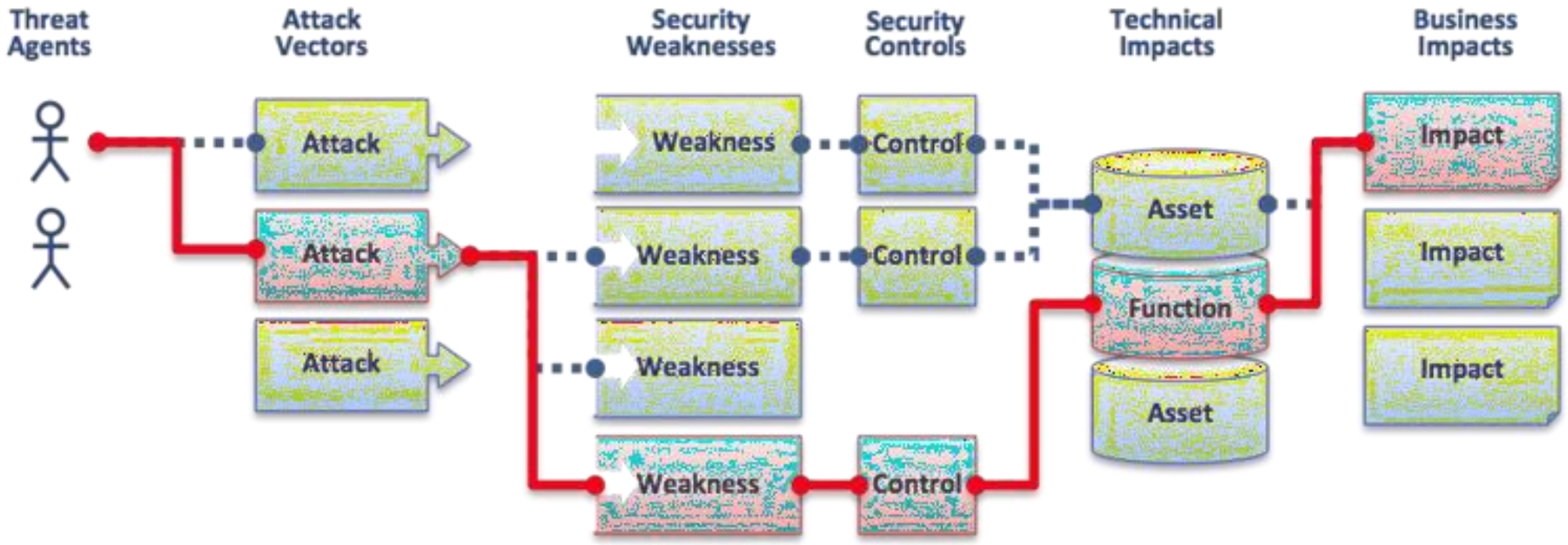
Topics

- Background Assessment
- Risk Management
- Risk Control Strategies
- Categories Of Control
- Cost Benefit Analysis
- Benchmarking

Understanding Risk Assessment



Risk Terminology



Asset Identification: Asset Ranking

- Assets should be ranked so that most valuable assets get highest priority when managing risks
- Questions to consider when determining asset value / rank:

Which info. asset is most critical to overall success of org.?

Example: Amazon's ranking assets Amazon's network consists of regular desktops and web servers.

Web servers that advertise company's products and receive orders 24/7 - critical.

Desktops used by customer service department – not so critical.

Which info. asset generates most revenue?

Which info. asset generates highest profitability?

Example: Amazon's ranking assets

At Amazon.com, some servers support book sales (resulting in highest revenue), while others support sales of beauty products (resulting in highest profit).

Risk Within Service Provider Environments

- A risk may have the same Risk Description but two separate impacts dependent on the Owner

- e.g. Risk: patching may fail to complete in a timely manner
  1. Impact on IT Service Provider: Potential Commercial Penalties, Damage to Reputation
  2. Impact on Client: Loss of Systems, loss of information, loss of revenue etc. etc.

Risk Management

- Competitive advantage vs. competitive disadvantage, or the need to avoid falling behind the competition
- To keep up with the competition, organizations must design and create a safe environment in which business processes and procedures can function
- This environment must maintain the confidentiality, privacy and integrity of organizational data
- These objectives are met through the application of the principles of risk management

Risk Management

- Risk management is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to assure the confidentiality, integrity, and availability of all the components in the organization's information systems

- The primary deliverable from risk assessment was a list of documented vulnerabilities, ranked by criticality of impact

Risk Control Strategies

- When risks from information security threats are creating a competitive disadvantage the information technology and information security communities of interest control the risks

- Four basic strategies are used to control the risks that result from vulnerabilities:

  - Apply safeguards (avoidance)
  - Transfer the risk (transference)
  - Reduce the impact (mitigation)
  - Inform themselves of all of the consequences and accept the risk without control or mitigation (acceptance)

Risk Control Strategies

- When risks from information security threats are creating a competitive disadvantage the information technology and information security communities of interest control the risks

- Four basic strategies are used to control the risks that result from vulnerabilities:

  - Apply safeguards (avoidance)
  - Transfer the risk (transference)
  - Reduce the impact (mitigation)
  - Inform themselves of all of the consequences and accept the risk without control or mitigation (acceptance)

Risk Control Strategies: Avoidance

- Avoidance attempts to prevent the exploitation of the vulnerability
- This is the preferred approach, as it seeks to avoid risk in its entirety rather than dealing with it after it has been realized
- Accomplished through countering threats, removing vulnerabilities in assets, limiting access to assets, and/or adding protective safeguards
- Three areas of control:
  - Policy
  - Training and education
  - Technology.

Risk Control Strategies: Transference

- Transference is the control approach that attempts to shift the risk to other assets, other processes, or other organizations
- If an organization does not already have quality security management and administration experience, it should hire individuals or firms that provide such expertise
- This allows the organization to transfer the risk associated with the management of these complex systems to another organization with established experience in dealing with those risks

Risk Control Strategies: Mitigation

- Mitigation attempts to reduce the impact of exploitation through planning and preparation
- Three types of plans:
  - disaster recovery planning (DRP)
  - business continuity planning (BCP)
  - incident response planning (IRP).
- The most common of the mitigation procedures is the disaster recovery plan or DRP
- The actions to take while the incident is in progress defined in the incident response plan or IRP
- Longer term issues are handled in the business continuity plan or BCP

Risk Control Strategies: Mitigation

TABLE 5.1 Summaries of Mitigation Plans

Plan	Description	Example	When deployed	Time frame
Incident response plan (IRP)	Actions an organization takes during incidents (attacks)	■ List of steps to be taken during disaster ■ Intelligence gathering ■ Information analysis	As incident or disaster unfolds	Immediate and real-time reaction
Disaster recovery plan (DRP)	Preparations for recovery should a disaster occur; strategies to limit losses before and during disaster; step-by-step instructions to regain normalcy	■ Procedures for the recovery of lost data ■ Procedures for the reestablishment of lost services ■ Shut-down procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business recovery plan (BCP)	Steps to ensure continuation of the overall business when the scale of a disaster requires relocation	■ Preparation steps for activation of secondary data centers ■ Establishment of a hot site in a remote location	Immediately after it is determined that the disaster affects the continued operations of the organization	Long-term recovery

Mitigation Summary

Risk Control Strategies: Mitigation

Mitigation Strategy Selection

- The level of threat and value of the asset play a major role in the selection of strategy

- The following rules of thumb can be applied in selecting the preferred strategy:
  - When a vulnerability can be exploited apply layered protections, architectural designs, and administrative controls to minimize the risk or prevent this occurrence
  - When the attacker's cost is less than his potential gain apply protections to increase the attacker's cost
  - When potential loss is substantial apply design principles, architectural designs, and technical and non-technical protections to limit the extent of the attack, thereby reducing the potential for loss

Risk Control Strategies: Acceptance

- Acceptance of risk is doing nothing to close a vulnerability and to accept the outcome of its exploitation
- Acceptance is valid only when:
  - Determined the level of risk
  - Assessed the probability of attack
  - Estimated the potential damage
  - Performed a thorough cost benefit analysis
  - Evaluated controls using each appropriate feasibility
  - Decided that the particular function, service, information, or asset did not justify the cost of protection
- Risk appetite describes the degree to which an organization is willing to accept risk as a trade-off to the expense of applying controls

Categories of Control

- Controlling risk through avoidance, mitigation or transference may be accomplished by implementing controls or safeguards.

- One approach to selecting controls is by category:
  - Control Function
  - Architectural Layer
  - Strategy Layer
  - Information Security Principle

Categories of Control: Control Function

- Controls or safeguards designed to defend the vulnerability are either preventive or detective
- Preventive controls stop attempts to exploit vulnerability by implementing enforcement of an organizational policy or a security principle, such as authentication or confidentiality
- Detective controls warn of violations of security principles, organizational policies, or attempts to exploit vulnerabilities
- Detective controls use techniques such as audit trails, intrusion detection, or configuration monitoring

Categories of Control: Architectural Layer

- Some controls apply to one or more layers of an organization's technical architecture

- Among the architectural layer designators in common use are:
  - organizational policy
  - external networks
  - extranets (or demilitarized zones)
  - Intranets (WAN and LAN)
  - network devices that interface network zones (switches, routers, firewalls, and hubs)
  - systems (computers for mainframe, server or desktop use)
  - applications

Categories of Control: Strategy Layer

- Controls are sometimes classified by the risk control strategy they operate within:
  - avoidance
  - mitigation
  - transference
  - acceptance

Categories of Control: Information Sec. Principle

- Controls operate within one or more of the commonly accepted information security principles:
  - Confidentiality
  - Integrity
  - Availability
  - Authentication
  - Authorization
  - Accountability
  - Privacy

Cost Benefit Analysis (CBA)

- The most common approach for a project of information security controls and safeguards is the economic feasibility of implementation
- Begins by evaluating the worth of the information assets to be protected and the loss in value if those information assets are compromised
- It is only common sense that an organization should not spend more to protect an asset than it is worth
- The formal process to document this is called a cost benefit analysis or an economic feasibility study

Cost Benefit Analysis (CBA): Cost Factor

- Some of the items that impact the cost of a control or safeguard include:
  - Cost of development or acquisition
  - Training fees
  - Cost of implementation
  - Service costs
  - Cost of maintenance

Cost Benefit Analysis (CBA): Benefits

- Benefit is the value that the organization recognizes by using controls to prevent losses associated with a specific vulnerability

- This is usually determined by valuing the information asset or assets exposed by the vulnerability and then determining how much of that value is at risk

Cost Benefit Analysis (CBA): Asset Valuation

- Asset valuation is the process of assigning financial value or worth to each information asset

- The valuation of assets involves estimation of real and perceived costs associated with the design, development, installation, maintenance, protection, recovery, and defense against market loss for each set of information bearing systems or information assets

- There are many components to asset valuation

Cost Benefit Analysis (CBA): Loss Estimates

- Once the worth of various assets is estimated examine the potential loss that could occur from the exploitation of vulnerability or a threat occurrence
- This process results in the estimate of potential loss per risk
- The questions that must be asked here include:
  - What damage could occur, and what financial impact would it have?
  - What would it cost to recover from the attack, in addition to the costs above?
  - What is the single loss expectancy for each risk?

Cost Benefit Analysis (CBA): Loss Estimates

- Once the worth of various assets is estimated examine the potential loss that could occur from the exploitation of vulnerability or a threat occurrence
- This process results in the estimate of potential loss per risk
- The questions that must be asked here include:
  - What damage could occur, and what financial impact would it have?
  - What would it cost to recover from the attack, in addition to the costs above?
  - What is the single loss expectancy for each risk?

Benchmarking

- An alternative strategy to the cost benefit analysis is to approach risk management from a different angle

- Rather than use the financial value of information assets review peer institutions to determine what they are doing to protect their assets (benchmarking)
- When benchmarking, an organization typically uses one of two measures:
  - Metrics-based measures are comparisons based on numerical standards, such as:
  - Process-based measures examine the activities performed in pursuit of its goal, rather than the specifics of how goals were attained