جامعة البخاري الدولية

ALBUKHARY INTERNATIONAL UNIVERSITY

Cybersecurity Risk Management (CCS 3143)

Methodology for Cybersecurity Risk Management

"inspiring minds"

AQIDAH AKHLAQ ADAB AMANAH AMALAN

Course Learning Outcome

- Analyse the needs for cybersecurity risk management (C4, PLO1).
- Prepare a cybersecurity risk management plan (A4, PLO6).

Learning Objectives

- At the end of the chapter, students should be able to:
- Identify types of cybersecurity list methodologies
- Explain the types of cybersecurity list methodologies

Cybersecurity Risk Assessment Methodologies

- Identifying those security risks is critical to protect the information
- Some risks are bigger than others. Some mitigation options are more expensive than others
- Choosing the right decision is very important as it help IT personnel to identify the information that need to set priorities.

Cybersecurity Risk Assessment Methodologies

- Cybersecurity risk assessment methodology can be classified into two main categories, which is quantitative and qualitative.
- Other methodologies are semi-quantitative, asset based, vulnerability base and threat base.
- Each methodology can evaluate an organization’s risk posture, but they all require tradeoffs.

Quantitative Methodology

- Quantitative risk assessment methodology focuses on factual and measurable data to calculate probability and impact values
- The risk values are represented in monetary terms, e.g; loss of money is understandable for any business unit
- The problem with quantitative assessment is that, in most cases, there is no sufficient data about SLE and ARO, or obtaining such data costs too much.

Quantitative Methodology

- To reach a monetary result, quantitative risk assessment often makes use of these concepts:
- **SLE (Single Loss Expectancy):**money expected to be lost if the incident occurs one time.
- **ARO (Annual Rate of Occurrence):**how many times in a one-year interval the incident is expected to occur.
- **ALE (Annual Loss Expectancy):**money expected to be lost in one year considering SLE and ARO (ALE = SLE * ARO). For quantitative risk assessment, this is the risk value.

Quantitative Methodology

"inspiring minds"

- Database value: $2.5 million (SLE)
- Manufacturer statistics show that a database catastrophic failure (due to software or hardware) occurs one time every 10 years (1/10 = 0.1) (ARO)
- Risk value: $2,500,000 x 0.1 = $250,000 (ALE)
- That is, in this case, the organization has an annual risk of suffering a loss of $250K in the event of the loss of its database.

Qualitative Methodology

- Qualitative risk assessment methodology focus on the interested parties' perception.
- For example, the probability of a risk occurring and its impact on relevant organizational aspects (e.g., financial, reputational, etc.).
- This perception is represented in scales such as "low-medium-high" or "1-2-3-4-5," which are used to define the risk's final value.

Qualitative Methodology

- Qualitative risk assessment methodology is easy and quick to perform.
- It has little mathematical dependency (risk may be calculated through a simple sum, multiplication, or other form of non-mathematical combination of probability and consequence values)
- Qualitative assessment can be highly biased, both in terms of probability and impact definition, by those who perform it.

Semi Quantitative Methodology

- Semi-quantitative risk assessments work based on the combination of the quantitative and qualitative methodologies.
- Organizations will use a numerical scale, such as 1-10 or 1-100, to assign a numerical risk value.
- Risk items that score in the lower third are grouped as low risk, the middle third as medium risk, and the higher third as high risk.

Asset based Methodology

- Assets are composed of the hardware, software, and networks that handle an organization's information—plus the information itself.

- Assets are composed of the hardware, software, and networks that handle an organization's information—plus the information itself

Vulnerability based Methodology

- Vulnerability-based methodologies expand the scope of risk assessments beyond an organization's assets.
- This process starts with an examination of the known weaknesses and deficiencies within organizational systems or the environments those systems operate within.
- From there, assessors identify the possible threats that could exploit these vulnerabilities, along with the exploits' potential consequences.

Threat based Methodology

- Threat-based methods can supply a more complete assessment of an organization's overall risk posture.
- This approach evaluates the conditions that create risk.
- An asset audit will be part of the assessment since assets and their controls contribute to these conditions.

Choosing the Right Methodology

- None of these methodologies are perfect. Each has strengths and weaknesses.
- Fortunately, none of them are mutually exclusive.
- Whether intentionally or by circumstance, organizations often perform risk assessments that combine these approaches

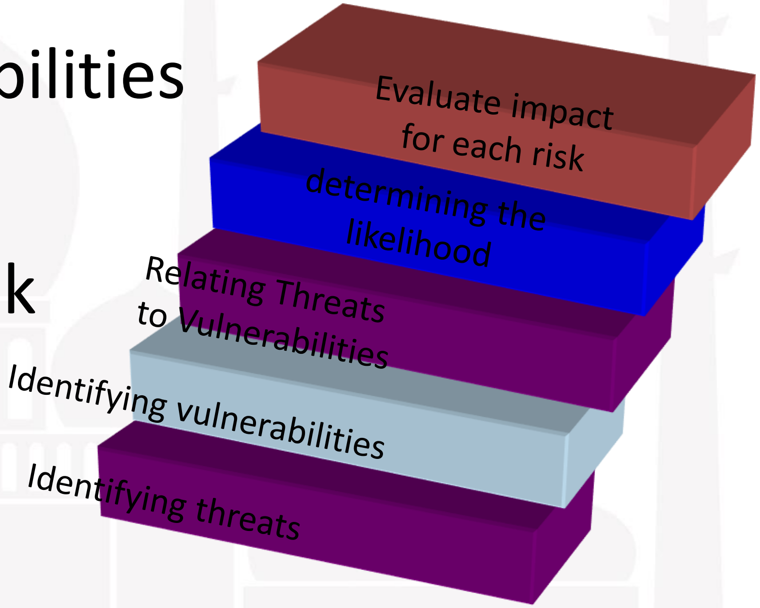
Choosing the Right Methodology

- When designing the risk assessment process, the methodologies use will depend on the need to achieve and the nature of the organization.
- If board-level and executive approvals are the most important criteria, then the approach will lean towards quantitative methods.
- More qualitative approaches might be better if there is a need to get support from employees and other stakeholders.
- Asset-based assessments align naturally with your IT organization while threat-based assessments address today's complex cybersecurity landscape.

How to assess the risks

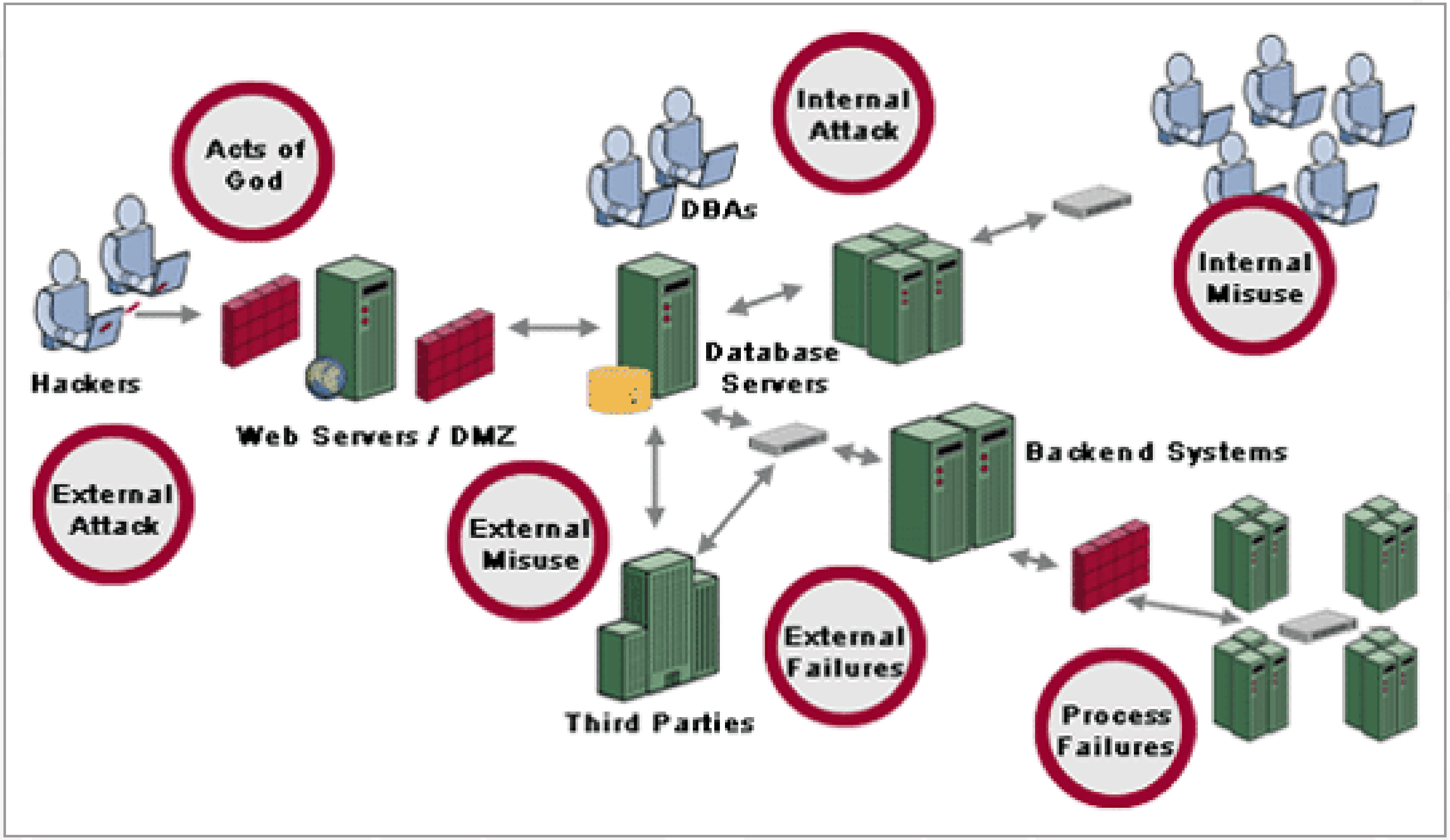
Risk is assessed by following the following steps:

- Identifying threats
- Identifying vulnerabilities
- Relating Threats to Vulnerabilities
- determining the likelihood
- Evaluate impact for each risk


Evaluate impact for each risk
determining the likelihood
Relating Threats to Vulnerabilities
Identifying vulnerabilities
Identifying threats

Identifying Risk

"inspiring minds"



Identifying Vulnerabilities

- **Identifying Vulnerabilities** : how each of the threats that are possible or likely could be perpetrated , and list the organization's assets and their vulnerabilities

- **Vulnerabilities can be identified by numerous means.**

- **Different methodologies for identifying vulnerabilities**.
  - start with commonly available vulnerability lists.
  - Then, working with the system owners or other individuals with knowledge of the system or organization, start to identify the vulnerabilities that apply to the system.
  - Specific vulnerabilities can be found by reviewing vendor web sites and public vulnerability archives, such as Common Vulnerabilities and Exposures (CVE - http://cve.mitre.org) or the National Vulnerability Database (NVD - http://nvd.nist.gov).

Relating Threats to Vulnerabilities

- Not every threat-action/threat can be exercised against every vulnerability.

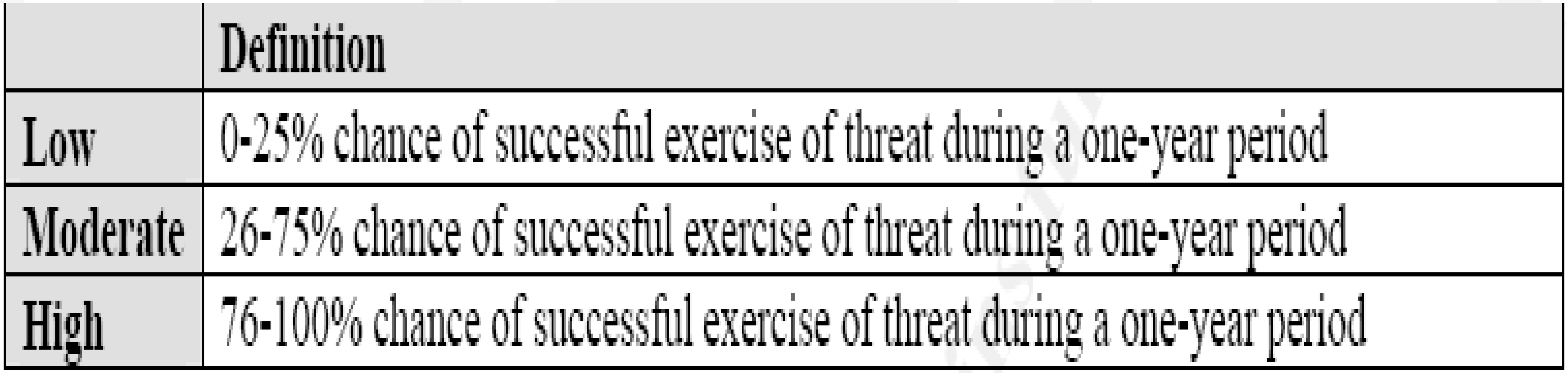
- For example, a threat of "flood" obviously applies to a vulnerability of "lack of contingency planning", but not to a vulnerability of "failure to change default authenticators."

Defining Likelihood

Likelihood is :

- the estimation of the probability that a threat will succeed in achieving an undesirable event
- is the overall rating - often a numerical value on a defined scale (such as 0.1 – 1.0) - of the probability that a specific vulnerability will be exploited

- **Sample Likelihood Definitions**

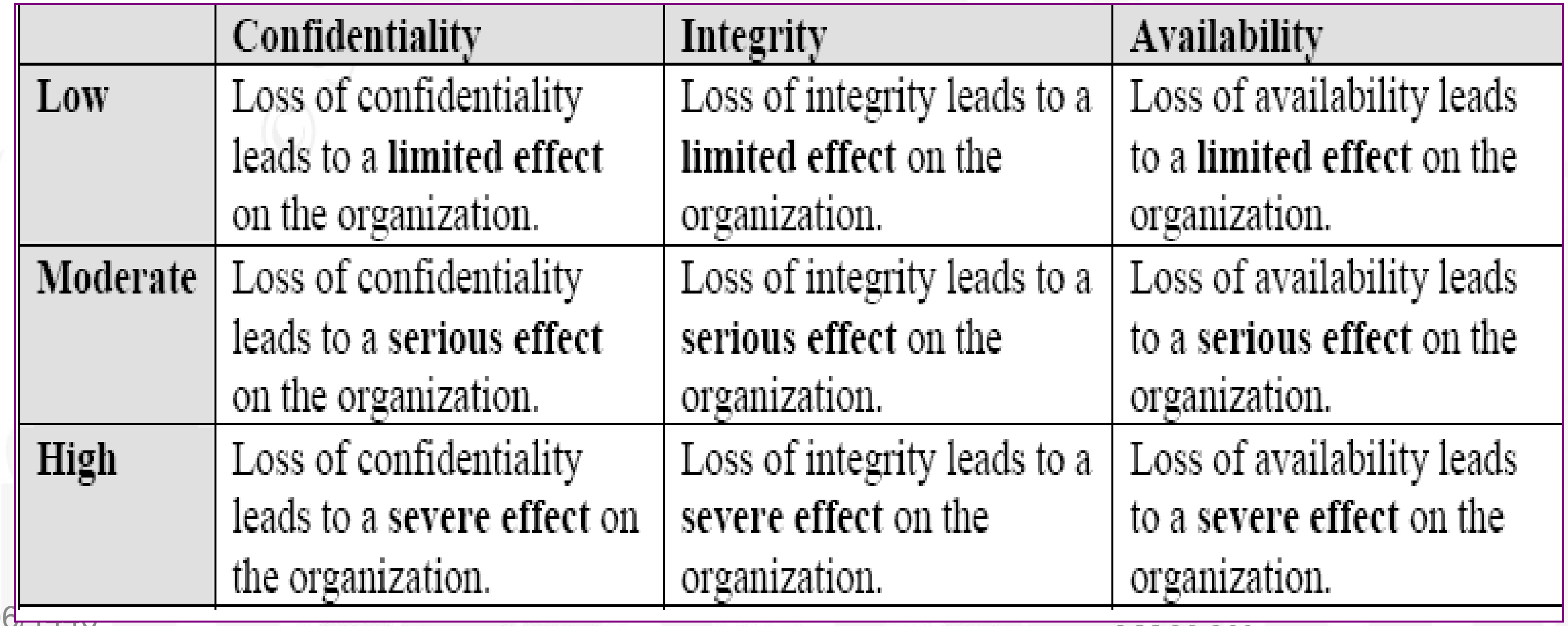


	Definition
Low	0-25% chance of successful exercise of threat during a one-year period
Moderate	26-75% chance of successful exercise of threat during a one-year period
High	76-100% chance of successful exercise of threat during a one-year period

Defining Impact

- Impact (Value)
  - Using the information documented during the risk identification process, assign weighted scores based on the value of each information asset, i.e.1-100, low-med-high, etc

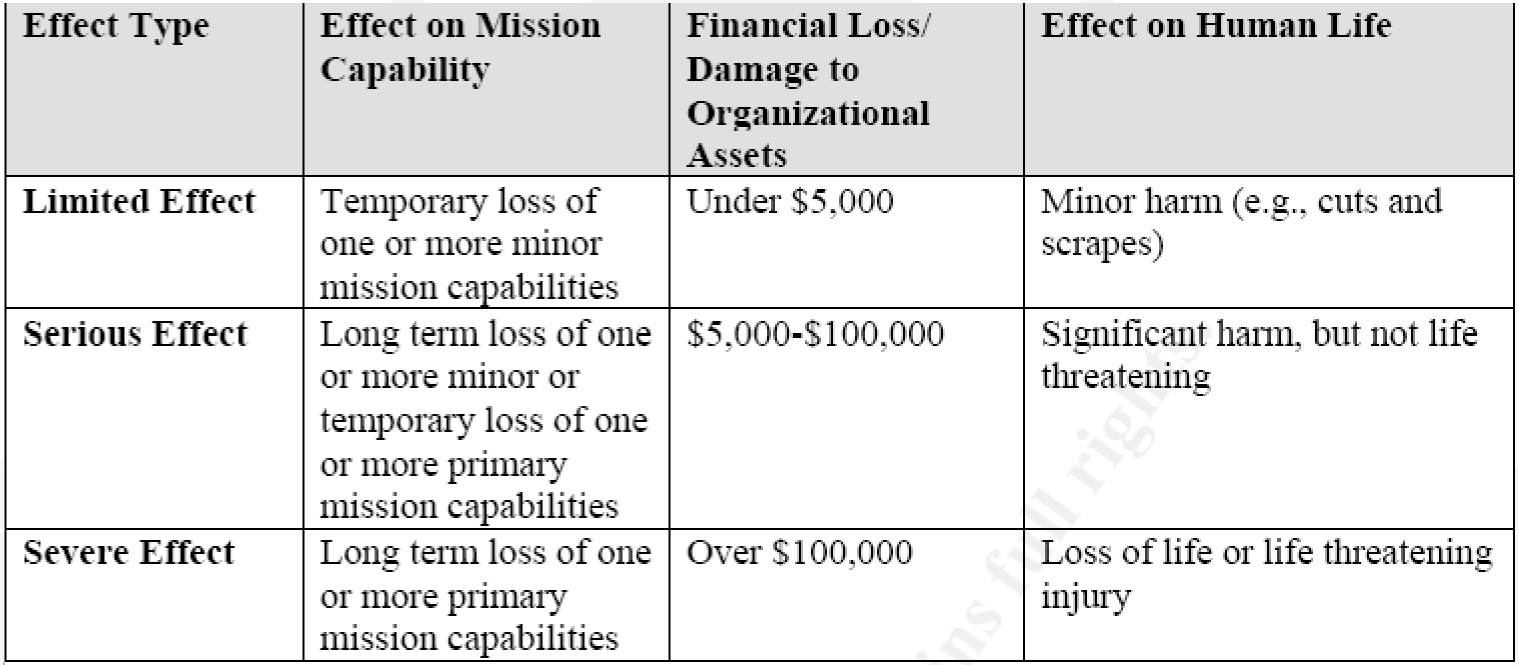
Sample Impact Definitions



	Confidentiality	Integrity	Availability
Low	Loss of confidentiality leads to a **limited effect** on the organization.	Loss of integrity leads to a **limited effect** on the organization.	Loss of availability leads to a **limited effect** on the organization.
Moderate	Loss of confidentiality leads to a **serious effect** on the organization.	Loss of integrity leads to a **serious effect** on the organization.	Loss of availability leads to a **serious effect** on the organization.
High	Loss of confidentiality leads to a **severe effect** on the organization.	Loss of integrity leads to a **severe effect** on the organization.	Loss of availability leads to a **severe effect** on the organization.

Defining Impact

- However, in order the risk assessment to be meaningful, reusable and easily communicated, specific ratings should be produced for the entire organization as below example .



Effect Type	Effect on Mission Capability	Financial Loss/ Damage to Organizational Assets	Effect on Human Life
Limited Effect	Temporary loss of one or more minor mission capabilities	Under $5,000	Minor harm (e.g., cuts and scrapes)
Serious Effect	Long term loss of one or more minor or temporary loss of one or more primary mission capabilities	$5,000-$100,000	Significant harm, but not life threatening
Severe Effect	Long term loss of one or more primary mission capabilities	Over $100,000	Loss of life or life threatening injury

References

- https://drata.com/blog/risk-assessment-methodologies
- https://www.just.edu.jo/~tawalbeh/aabfs/iss6753/presentations/RiskAssesment.ppt

ALBUKHARY INTERNATIONAL UNIVERSITY

Thank You

"inspiring minds"

AQIDAH AKHLAQ ADAB AMANAH AMALAN