Risk Analysis

- The process by which the goals of risk management are achieved is known as *risk analysis.*

- Risk analysis includes:
  - ➢ Examining an environment for risks
  - ➢ Evaluating each threat event as to its likelihood of occurring
  - ➢ Evaluating the cost of the damage it would cause if the threat did occur
  - ➢ Assessing the cost of various countermeasures for each risk
  - ➢ Creating a cost/benefit report for safeguards to present to upper management

Risk Terminology

- **Asset.** An asset is anything within an environment that should be protected.

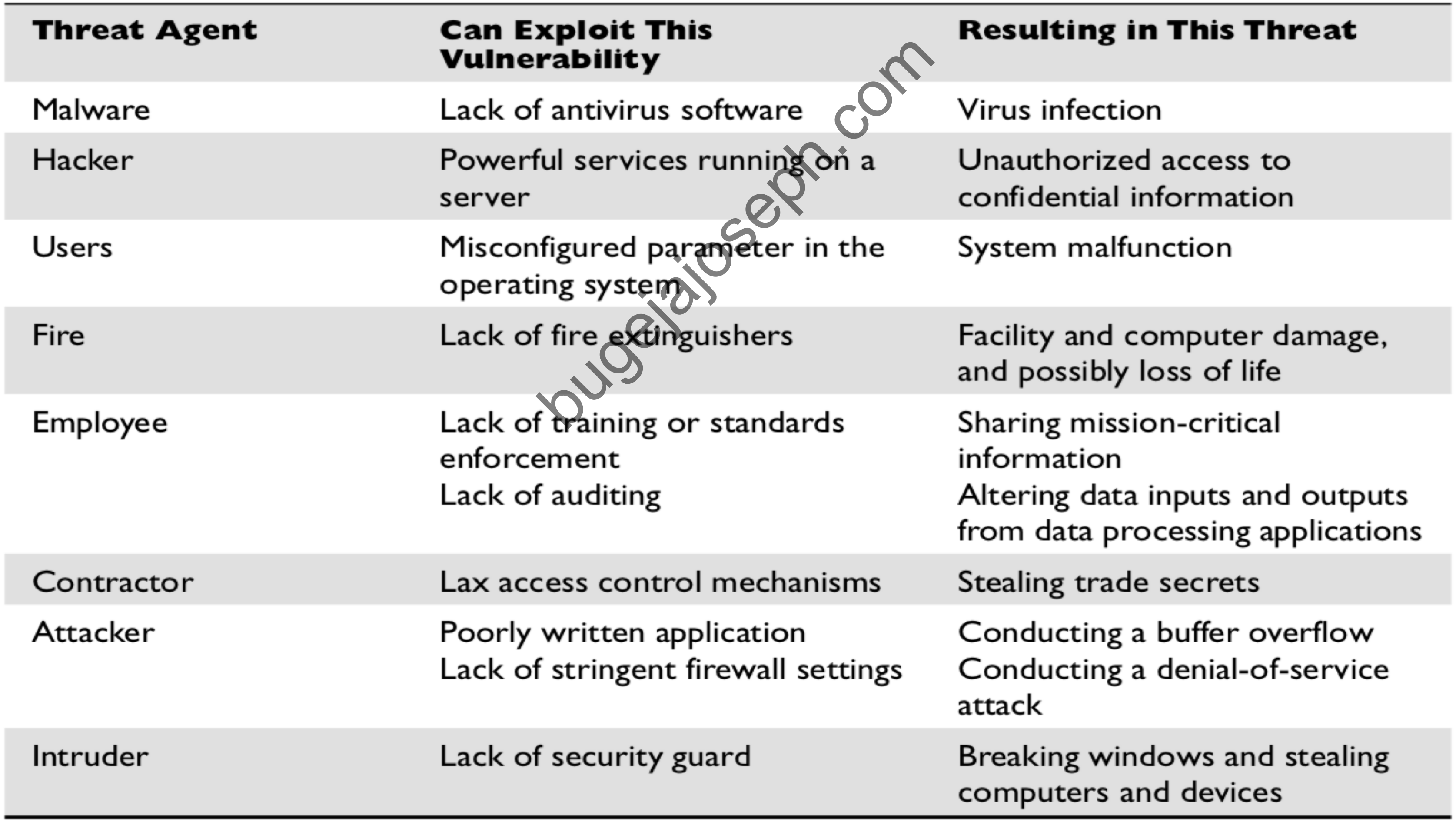
- **Asset Valuation.** The monetary value of asset based on actual cost (e.g., replacement costs) and nonmonetary expenses.

- **Threats**. Any potential occurrence that may cause an undesirable or unwanted outcome for an organization or for a specific asset.

- **Vulnerability**. The weakness in an asset or the absence or the weakness of a safeguard or countermeasure.

Identifying Threats and Vulnerabilities

- Many types of threat agents can take advantage of several types of vulnerabilities, resulting in a variety of specific threats



Threat Agent	Can Exploit This Vulnerability	Resulting in This Threat
Malware	Lack of antivirus software	Virus infection
Hacker	Powerful services running on a server	Unauthorized access to confidential information
Users	Misconfigured parameter in the operating system	System malfunction
Fire	Lack of fire extinguishers	Facility and computer damage, and possibly loss of life
Employee	Lack of training or standards enforcement Lack of auditing	Sharing mission-critical information Altering data inputs and outputs from data processing applications
Contractor	Lax access control mechanisms	Stealing trade secrets
Attacker	Poorly written application Lack of stringent firewall settings	Conducting a buffer overflow Conducting a denial-of-service attack
Intruder	Lack of security guard	Breaking windows and stealing computers and devices

Risk Analysis

- To organize the process of risk analysis, we look at assets, vulnerabilities, and threats

- Risk is a function of assets, vulnerabilities, and threats:
  - Risk = Assets × Threats × Vulnerabilities

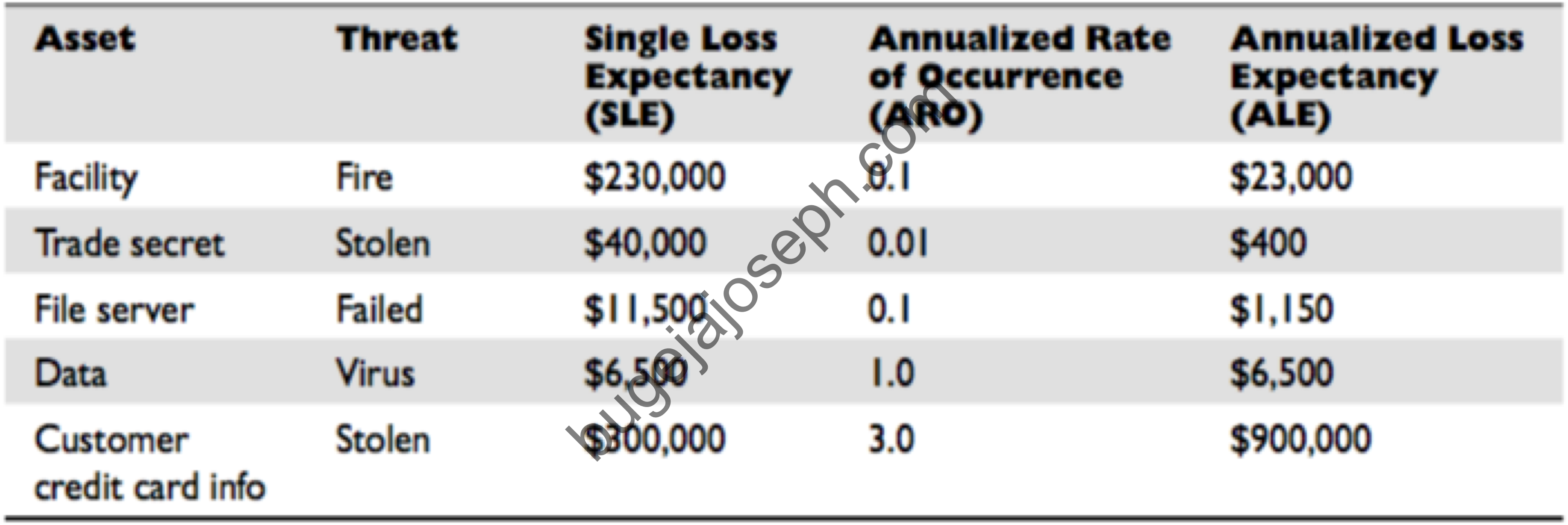
- During risk analysis values are assigned to assets, vulnerabilities, and threats.

Quantitative Risk Analysis Steps

1. Inventory asset, and assign a value.
2. Research each asset, and produce a list of all possible threats of each individual asset. For each, calculate the Exposure Factor (EF) and single loss expectancy (SLE).
3. Perform a threat analysis to calculate the likelihood of each threat being realized within a single year (ARO).
4. Derive the overall loss potential per threat by calculating the annualized loss expectancy (ALE).
5. Research countermeasures for each threat, and then calculate the changes to ARO and ALE based on an applied countermeasures.
6. Perform a cost/benefit analysis of each countermeasure for each threat for each asset. Select the most appropriate response to each threat.

Using SLE and ALE Values

- Example of outcome of a quantitative risk analysis.



Asset	Threat	Single Loss Expectancy (SLE)	Annualized Rate of Occurrence (ARO)	Annualized Loss Expectancy (ALE)
Facility	Fire	$230,000	0.1	$23,000
Trade secret	Stolen	$40,000	0.01	$400
File server	Failed	$11,500	0.1	$1,150
Data	Virus	$6,500	1.0	$6,500
Customer credit card info	Stolen	$300,000	3.0	$900,000

- With this data a company can make intelligent decisions of what threats must be addressed first because of the severity of the threat, the likelihood of it happening, and how much could be lost if the threat were realized.

Qualitative Risk Analysis

- The process of performing qualitative risk analysis involves judgement, intuition, and experience.

- Examples of techniques used for conducting this include:
  - Brainstorming
  - Delphi technique
  - Storyboarding
  - Focus groups
  - Interviews

- The basic process for all these mechanisms involves the creation of scenarios. A scenario is a written description of a single major threat.