Tutorial 9: InfoSec Risk Management

1. The WORST problem with risk analysis is that ________.
   a) protections often protect multiple resources
   b) resources often are protected by multiple controls/safeguards
   c) we cannot accurately estimate the annualized rate of occurrence
   d) costs and benefits are not the same each year

   d is a fact but not a problem

2. True or False question.

   Considering the following risk scenario description, it is a complete risk scenario description:

   Unauthorized employee accesses the student data server and exports sensitive student data.

   False - missing vulnerability which enable the unauthorized employee to access the data

3. Assume that you are the information security manager in an organization. If your organization has three information assets to evaluate for risk management purposes, as shown below:
   - Switch L47 connects a network to the Internet. It has two vulnerabilities: (1) susceptibility to hardware failure, and such hardware failure occurs once every 5 years, and (2) susceptibility to an SNMP buffer overflow attack estimated at one attack every 10 years. This switch has no current controls in place.
   - Server WebSrv6 hosts a company Web site and performs e-commerce transactions. It has Web server software that is vulnerable to attack via invalid Unicode values. Such an attack is likely to occur once every 2 years. A control has already been implemented that reduced the impact of the vulnerability by 90 percent.
   - Operators use the MGMT 45 control console to monitor operations in the server room. It has no password and is susceptible to unlogged misuse by the operators. A misuse is likely to occur once every 4 years. There is no control in place on this asset.

   a) As part of the risk assessment process, three criterion have been selected to determine the value of the information asset to the organization. You have been tasked to value and prioritize the three information assets by preparing the Weighted Factor Analysis Worksheet as shown below. Complete **all four missing values** in the worksheet correctly.

Information Asset	Criterion 1: Impact on Revenue	Criterion 2: Impact on Profitability	Criterion 3: Impact on Public Image	Weighted Score
Criterion weights	30	40	30	
Switch L47	0.8	0.8	0.3	65
Server WebSrv6	1.0	1.0	1.0	100
MGMT 45	0.8	0.5	0.2	50

b) After deriving the Weighted Factor Analysis Worksheet, you have been further tasked to calculate the risk for each information asset and document the results in a Ranked Vulnerability Risk Worksheet as shown below. Here you should assume that the impact of a successful attack or failure is 100%. Complete **all twelve missing values** in the worksheet correctly.

Information Asset	Asset Impact	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Switch L47	65	Susceptibility to hardware failure	0.2	13
Switch L47	65	Susceptibility to an SNMP buffer overflow attack	0.1	6.5
Server WebSrv6	100	Subject invalid Unicode values attack	0.5	50
MGMT 45	50	No effective assess control and is susceptible to unlogged misuse by the operators	0.25	12.5

c) Continue risk assessment, which vulnerability should be addressed first and why? Which vulnerability should be addressed last and why?

The assumptions that an attack is 100% should not hold anymore.

And since it is talking about vulnerability must be specifc to the vuln instead of the info asset

must consider information background - to check if there are any current mitigations

4. *Discussion*

Read the recommended materials and answer the following questions.

- Mondelez sues Zurich in test for cyber hack insurance
  - *https://www.ft.com/content/8db7251c-1411-11e9-a581-4ff78404524e*
- Insurance Circular Letter No. 2, (2021), the New York Department of Financial Services
  - https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02
- Ransomware Guidance, the New York Department of Financial Services
  - https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210630_ransomware_guidance

a. Mondelez, owner of dozens of well-known food brands like Cadbury chocolate and Philadelphia cream cheese, was hit by the NotPyetya cyberstrike in 2017. What were the challenges it faced when it tried to claim reimbursement from its cybersecurity insurer Zurich Insurance?

denied because exclusion in the policy for a "hostile or warlike action" by a government or sovereign power or people acting for them

b. Explain what "non-affirmative" or "silent" risk in insurance policies is.

insurance companies will face alot of trouble and cost if they do not define this well

- risks not explicitly granted or excluded from insurance policies that do not explicitly grant or exclude cyber coverage

c. Which of the following cybersecurity related losses is least likely to be covered under cybersecurity insurance in the future?

a) System failure and dependent system failure
b) Cyber fraud and social engineering
[✓ c) Ransomware cyber extortion]
d) Forensic investigation expenses
e) Civil fine and penalties associated with PCI