SIT284 Cyber Security Management – Assignment 2

Group Members

Name

Rory
Ruslan
John
Justin

1. Assets Identification

Asset Name	Asset Type	Department	Value	Priority
Market Strategies and Marketing Analysis	Information	Marketing		60
This asset generates revenue for the law firm making it a very valuable information asset				
Legal Documents	Knowledge	Legal		100
This asset is valuable to the firm as it contains knowledge of clients, potential clients and any legal information that is made public by other law firms				
Market Trends	Liquid Asset	Finance		54
This asset being a liquid asset it has to have some value in terms of money or credit. This information of market trends can be sold to other companies for money or more information about a certain thing??				
Oracle E-Business Suite	System Asset	e-Solution		57
This asset helps store and manage clients contact details, administrative records and personal information				

Asset valuation: Use the cost-based approach or the market value-based approach to calculate the relative value of the selected assets. You must justify any assumptions you make.

Asset Prioritisation Weighted Factor Analysis

Asset	Impact on Revenue	Impact on Public Image	Impact on Profitability	Weighted Score
Market Strategies and Marketing Analysis	80	30	70	**60**
Legal Documents	100	100	100	**100**
Market Trends	70	30	60	**54**
Oracle E-Business Suite	60	60	50	**57**

2. Threat and Vulnerability Analysis

	Asset 1	Asset 2	Asset 3	Asset 4
Threat 1	Software attacks	Compromises to intellectual property	Human error or failure	Technological obsolescence
Threat 2	Missing, inadequate, incomplete controls	Data Theft	Espionage or trespass	Software attacks
Threat 3	Espionage	Vandalism	Software attacks	Technical Software Failures

We have selected the threats for Asset 1 (market strategies and analysis) using the Threat analysis table "pg 254" and the assets that we have chosen to be the most likely to harm or damage the law firm are as follows (Threat 1software attacks) on the marketing strategies attempting to gain some information or trying to stop the law firm from gathering any more valuable information. (Threat 2 Human error and failure) is also a very possible threat even at such a big law firm such as Chowdhury-Lim as they oversee a lot of staff and if a mistake is not caught it could create false information about the company or what it wants information on. And lastly (Threat 3 espionage) which a big law firm like Chowdhury-Lim should be very cautious of as they undoubtedly have many competitors and they will want to have access to anything they can have a competitive edge

The threats for asset 2(legal documents) using the Same threat analysis table(Threat 1 Theft) as most legal firms have legal documents they are required to have copies of them in digital and physical form, and physical documents are very open to theft if there is not enough security or precautions to prevent someone from accessing them (Threat 2 missing, inadequate, incomplete controls) this could occur from Non legal professionals filling out documents and creating mistakes which may not be caught by professionals. (Threat 3, Vandalism) this again could occur to both the physical documents that are kept and the digital documents and if it was allowed to happen then documents could be altered or destroyed without any one knowing.

Threats for Asset 3 (market trends) using the Threat analysis Table (threat 1 Human error or failure) since people are used to analyse market trends errors can occur since they are using highly complicated programs that help analyse. people can accidently create the wrong information providing a liquid asset that is worth no money or value to the company. (Threat 2 espionage or trespassing) market trends are very valuable and Chowdhury-Lim is a very big law firm so many other companies will want to steal or have access to the liquid assets that market trends create. (threat 3 Software attack)
The information on market trends can be also acquired via software attacks, i.e hackers breaking into the system.

Threats for asset 4 (Oracle E-Business Suite) using the threat analysis table (threat 1 technical obsolescence) in the description of the Oracle E-Business Suite they state that the last patch was January 1st and the official website states "Apply the appropriate patch according to the April 2019 Oracle Critical Patch Update advisory". this leaves the company to a huge possible data breach since the Oracle E-Business Suite handles all personal details and contact details that the company has access to. (threat 2 software attack) as stated before since the Oracle E-Business Suite hasn't updated its software it leaves it open to an attack that could steal or alter lots of personal information. (threat 3 technical software failure) again the Oracle E-Business Suite being out of date leaves it with a chance of failing to perform its job in organizing and keeping personal data potentially creating a bug or an error that causes the loss or corruption of data.

Identify three different most probable threat agents

Threat	Threat Agent	Threat Agent			
		Size	Skill	Motive	Opportunity
Technological obsolescence	Organised cybercriminal groups	Anonymous Internet users (9)	Some Technical Skills (3)	High reward (9)	Special access or resources required" (4)
Vandalism	Disgruntled Staff / Client	Anonymous Internet users (9)	Some Technical Skills (3)	Possible Rewards (4)	Special access or resources required (4)
Data Theft	Undetermined	Anonymous Internet users (9)	Security Penetration Skills (9)	Some Access or Resources Required (7)	Special access or resources required (4)

Vulnerability Factors

Asset	Vulnerability Name	Vulnerability Factors			
		Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
Market Strategies and Marketing Analysis					
Legal Documents					
Market Trends					
Oracle E-Business Suite					

3. Estimating Risk

Asset Name	Vulnerability	Threat	Risk Likelihood	Risk Impact		Risk Rating	Priority
				Technical	Business		
Market Strategies and Marketing Analysis		Sabotage	4.37(Med)	5.25(Med)	4.00(Med)	4.54(Med)	Medium
Legal Documents	Loss	Theft	6.37(High)	8.00(High)	7.50(High)	7.59(High)	High
Market Trends		Espionage	4.62(Med)	1.25(Low)	4.25(Med)	3.75(Med)	Medium
Oracle E-Business Suite		Software attacks	4.12(Med)	5.50(Med)	4.75(Med)	4.79(Med)	Medium

Risk Formulas and Justification			
Asset Name	*Market Strategies and Marketing Analysis*		
	Risk Likelihood	*Likelihood*	(6 + 7 + 4 + 5) / 4 = 5.50
		Vulnerability	(3 + 3 + 6 + 1) / 4 = 3.25
		Risk Likelihood	0.5 * (5.50 + 3.25) = 4.37
	Technical	(6 + 3 + 5 + 7) / 4 = 5.25	
	Business	(3 + 4 + 2 + 7) / 4 = 4.00	
	Risk Rating		
	Justification	Something Goes Here	
Asset Name	*Legal Documents*		
	Risk Likelihood	*Likelihood*	(6 + 9 + 9 + 9) / 4 = 8.25
		Vulnerability	(3 + 3 + 9 + 3) / 4 = 4.50
		Risk Likelihood	0.5 * (8.25 + 4.50) = 6.37
	Technical	(9 + 9 + 7 + 7) / 4 = 8.00	
	Business	(7 + 9 + 7 + 7) / 4 = 7.50	
	Risk Rating		
	Justification	Something Goes Here	
Asset Name	*Market Trends*		
	Risk Likelihood	*Likelihood*	(1 + 1+ 9 + 9) / 4 = 5.00
		Vulnerability	(9 + 1 + 2 + 5) / 4 = 4.25
		Risk Likelihood	0.5 * (5.00 + 4.25) = 4.62
	Technical	(2 + 1 + 1 + 1) / 4 = 1.25	
	Business	(9 + 1 + 2 + 5) / 4 = 4.25	
	Risk Rating		
	Justification	Something Goes Here	
Asset Name	*Oracle E-Business Suite*		
	Risk Likelihood	*Likelihood*	(5 + 4 + 0 + 9) / 4 = 4.50
		Vulnerability	(3 + 3 + 6 + 3) / 4 = 3.75
		Risk Likelihood	0.5 * (4.50 + 3.75) = 4.12
	Technical	(7 + 5 + 3 + 7) / 4 = 5.50	
	Business	(3 + 4 + 7 + 5) / 4 = 4.75	
	Risk Rating		
	Justification	Something Goes Here	

4. Risk Treatment Strategy

This section involves the identification and selection of appropriate risk treatment strategies for managing the risks identified in the previous section. Note that selecting the most appropriate risk treatment option involves organisation's risk appetite and residual risk as well as balancing the costs and efforts of implementation against the benefits derived. Use the following template to record the results.

Risk	Treatment	Residual Risk	Cost-Benefit Analysis

For each risk, select a security control and briefly describe how the selected security control sufficiently reduces the risk to a desired level. You need to research online to address this question. As you perform research, make sure that you collect certain parameters and values (e.g., the amount of risk mitigated by the control) about the selected security control. This information will be useful to determine if the new security control you propose is worthwhile to use it.

For each risk, perform a cost-benefit analysis to determine if the cost of protecting the asset against the risk outweighs the benefits from implementing the security control. From online sources, you will need to collect statistics on parameters such as the frequency with which a threat (you identified threats in section 2) is expected to occur in a particular year and the percentage of the asset value lost due to the security incident. Briefly explain, why you think the values for the parameters you collected correspond to the particular threat. You must justify and show step by step your work and include all the formulas required to arrive at your answer.

For each risk, determine the residual risk and the appropriate treatment strategy. Provide a brief explanation of why you consider the treatment strategy you selected is appropriate for managing the risk.