CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #5 - Option A

Team: 1

Participants: Jacob Forcht, Trevor Hagel, Zack Graas

Logistics

A. Get together with other students on your assigned **Team** in person and/or virtually.

B. Review the two options available and decide on only one to pursue as a team.

C. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning and may impact your performance on assessments, especially with respect to the essay questions.

D. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the names of the two required files to denote the number of your assigned **Team**.

Problem 1 *(15 points)*

Complete Exercise 1 from pp. 320 of your text with the following changes. *Switch L47's* hardware failure has an expected rate of occurrence of once every five years and when that happens it is a 100% failure of the device. The *SNMP buffer overflow* has an expected rate of occurrence of once every five years but only 50% of those attacks are successful. When it is successful, 100% of the asset would be lost or compromised. For server *WebSrv6*, the invalid Unicode vulnerability is attempted to be exploited once a year but only 10% of those attacks are successful. When those attacks succeed, existing controls keep the loss down to 25% of the asset. For the *MGMT45 control console*, the estimated rate of occurrence of unlogged misuse by the operators is once every ten years but when it happens, there are no controls in place to reduce the impact, so 100% loss of the asset is likely.

Perform the risk calculations (as shown on p. 287) and determine in what order each of the threat vulnerabilities should be addressed based on the relative risk. Show your work.

Switch L47 Hardware: failure once every five years, 100% failure, 75% certain, 90 impact rating, 100% loss

Risk: (20% * 100%) * (90 * 100%) + 25%

(.2 * 1) * (90*1) + .25

.2 * 90 + .25

18+(.25*18)=22.5

Risk = 22.5

SNMP Buffer Overflow: once every five years, 50% success rate, when success 100% loss, 75 certain, 90 impact rating

Risk: (20% * 50%) * (90 * 100%) + 25%

(.2 * .5) * (90 * 1) +.25

.1 * 90 + .25

9 + (.25*9)=11.25

Risk = 11.25

WebSrv6: once a year, 10% success, 25% loss, 80% certain, impact value of 100

Risk: (100% * 10%) * (100 * 25%) +20%

(1 * .1) * (100 * .25) +.2

.1 * 25 +.2

2.5+(.2*2.5) = 3

Risk = 3

MGMT46 Console: once every ten years, 100% loss, impact rating of 5, 90% certain

Risk: (10% * 100%) * (5 * 100%) + 10%

(.1 * 1) * (5 * 1) + .1

.1 * 5 + .1

.5+ (.10*.5)= .55

Risk = .55

According to the risk calculations, the order in which vulnerabilities should be addressed is first Switch L47 Hardware, then the SNMP Buffer Overflow, then the WebSrv6, and finally the MGMT46 Console.

Problem 2 *(15 points)*

Complete Exercise 3 from p. 320 of your text. You should create a worksheet using Microsoft Excel to support your calculations, then paste an image of the table with column headings and rows just below. Also attach the Excel workbook file when submitting your solution document for grading.

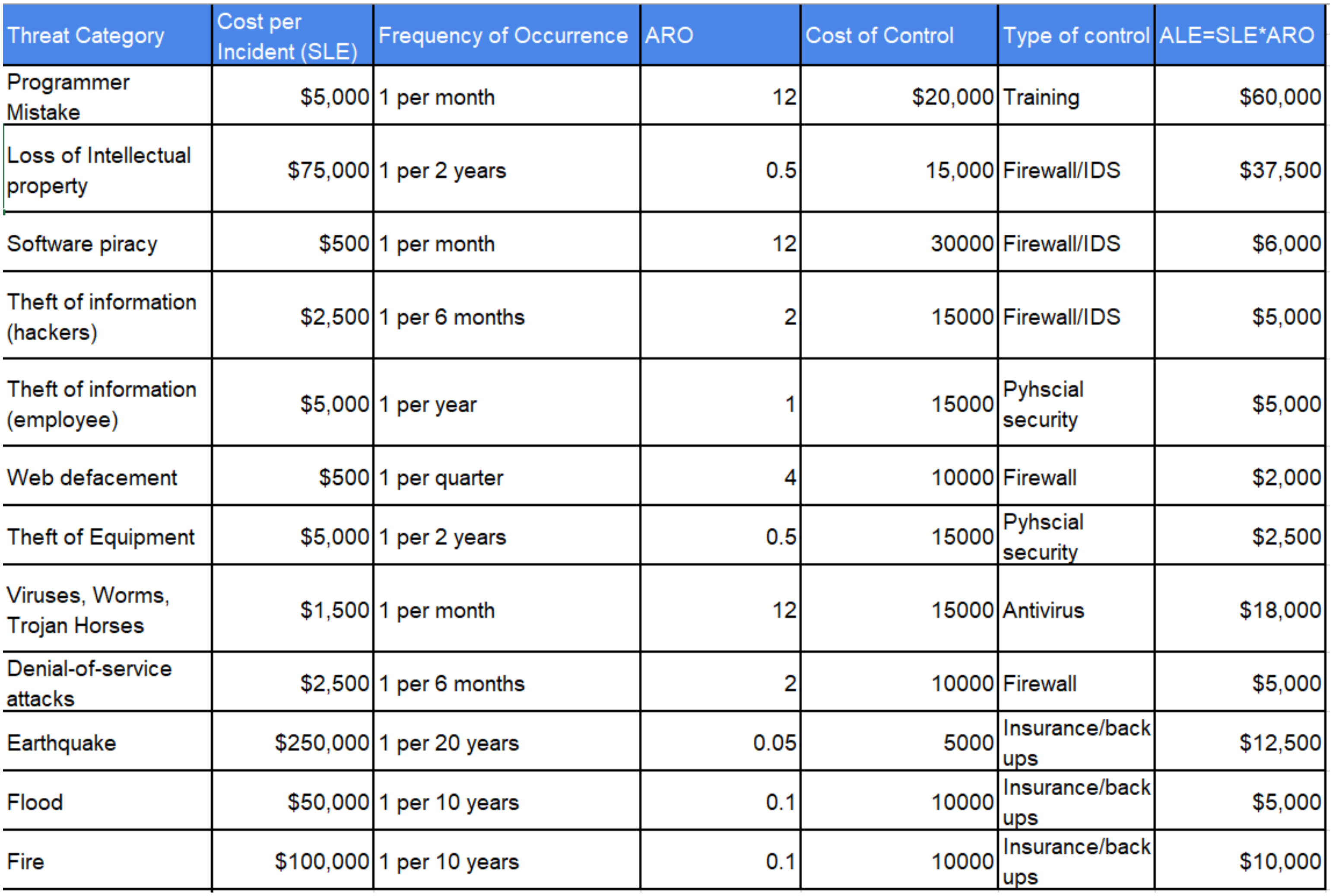
Prior ALE:

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence	ARO	SLE * ARO	ALE
Programmer Mistake	$5,000	1 per week	52 weeks	$5,000 x 52	$260,000
Loss of Intellectual property	$75,000	1 per year	1 year	$75,000 x 1	$75,000
Software piracy	$500	1 per week	52 weeks	$500 x 52	$26,000
Theft of information (hackers)	$2,500	1 per quarter	4 quarters	$2,500 x 4	$10,000
Theft of information (employee)	$5,000	1 per 6 months	2 months	$5,000 x 2	$10,000
Web defacement	$500	1 per month	12 months	$500 x 12	$6,000
Theft of Equipment	$5,000	1 per year	1 year	$5,000 x 1	$5,000
Viruses, Worms, Trojan Horses	$1,500	1 per week	52 weeks	$1,500 x 52	$78,000
Denial-of-service attacks	$2,500	1 per quarter	4 quarters	$2,500 x 4	$10,000
Earthquake	$250,000	1 per 20 years	1/20 = 0.05	$250,000 x 0.05	$12,500
Flood	$250,000	1 per 10 years	1/10 = 0.1	$250,000 x 0.1	$25,000
Fire	$500,000	1 per 10 years	1/10 = 0.1	$500,000 x 0.1	$50,000

Problem 3 *(20 points)*

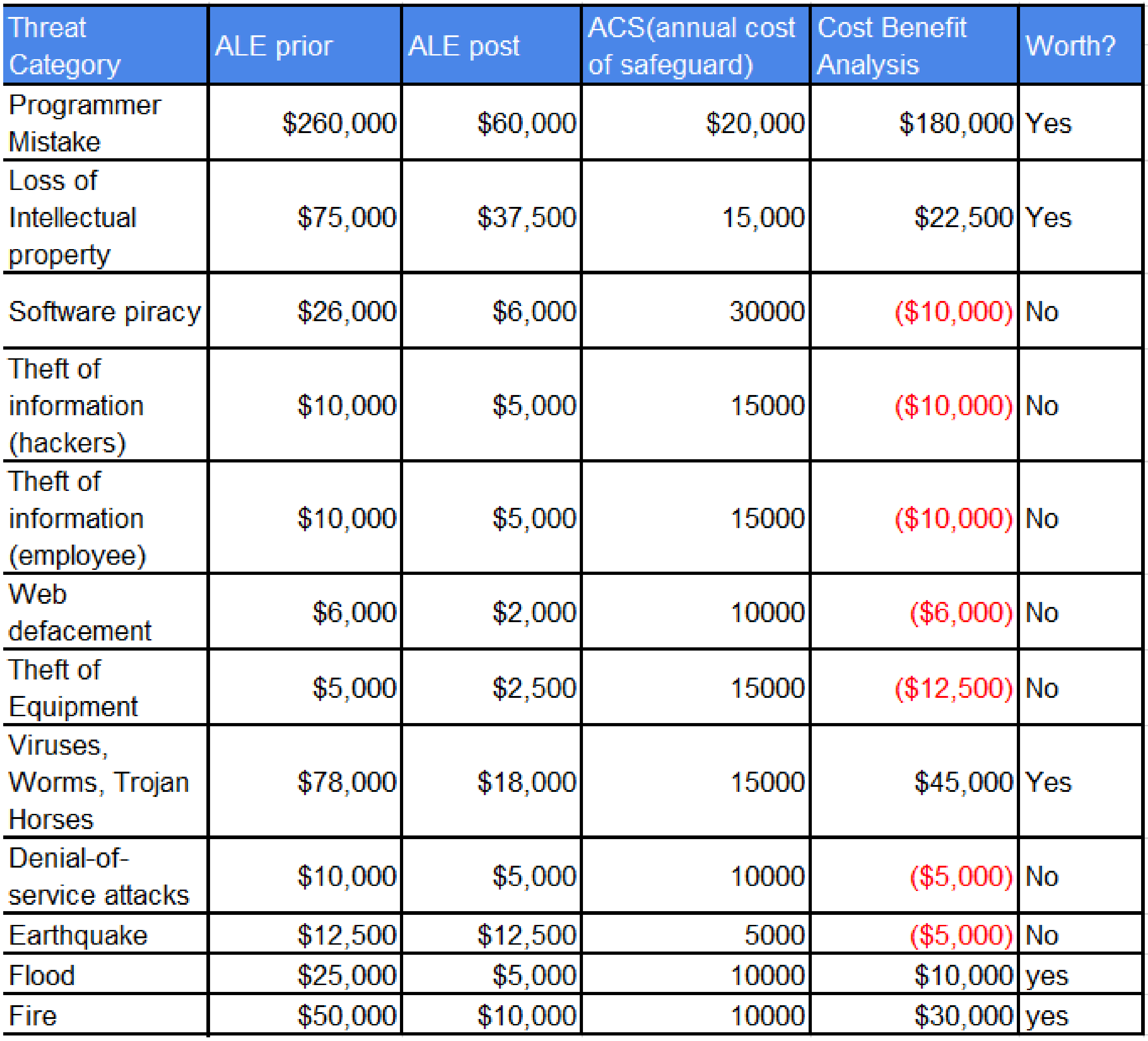
Complete Exercise 5 from p. 321 of your text. You should create a worksheet using Microsoft Excel to support your calculations, then paste an image of the table with column headings and rows just below. Attach the Excel workbook when submitting this document file for grading. Don't forget to address all of the questions at the end of Exercise 5.

Post ALE calculations:



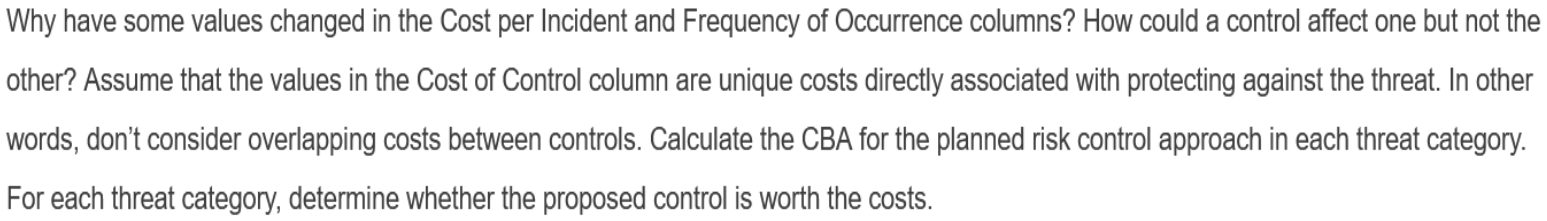
Threat Category	Cost per Incident (SLE)	Frequency of Occurrence	ARO	Cost of Control	Type of control	ALE=SLE*ARO
Programmer Mistake	$5,000	1 per month	12	$20,000	Training	$60,000
Loss of Intellectual property	$75,000	1 per 2 years	0.5	15,000	Firewall/IDS	$37,500
Software piracy	$500	1 per month	12	30000	Firewall/IDS	$6,000
Theft of information (hackers)	$2,500	1 per 6 months	2	15000	Firewall/IDS	$5,000
Theft of information (employee)	$5,000	1 per year	1	15000	Pyhscial security	$5,000
Web defacement	$500	1 per quarter	4	10000	Firewall	$2,000
Theft of Equipment	$5,000	1 per 2 years	0.5	15000	Pyhscial security	$2,500
Viruses, Worms, Trojan Horses	$1,500	1 per month	12	15000	Antivirus	$18,000
Denial-of-service attacks	$2,500	1 per 6 months	2	10000	Firewall	$5,000
Earthquake	$250,000	1 per 20 years	0.05	5000	Insurance/backups	$12,500
Flood	$50,000	1 per 10 years	0.1	10000	Insurance/backups	$5,000
Fire	$100,000	1 per 10 years	0.1	10000	Insurance/backups	$10,000

Cost Benefit Analysis:



Threat Category	ALE prior	ALE post	ACS(annual cost of safeguard)	Cost Benefit Analysis	Worth?
Programmer Mistake	$260,000	$60,000	$20,000	$180,000	Yes
Loss of Intellectual property	$75,000	$37,500	15,000	$22,500	Yes
Software piracy	$26,000	$6,000	30000	($10,000)	No
Theft of information (hackers)	$10,000	$5,000	15000	($10,000)	No
Theft of information (employee)	$10,000	$5,000	15000	($10,000)	No
Web defacement	$6,000	$2,000	10000	($6,000)	No
Theft of Equipment	$5,000	$2,500	15000	($12,500)	No
Viruses, Worms, Trojan Horses	$78,000	$18,000	15000	$45,000	Yes
Denial-of-service attacks	$10,000	$5,000	10000	($5,000)	No
Earthquake	$12,500	$12,500	5000	($5,000)	No
Flood	$25,000	$5,000	10000	$10,000	yes
Fire	$50,000	$10,000	10000	$30,000	yes

Problem 3 questions:



Why have some values changed in the Cost per Incident and Frequency of Occurrence columns? How could a control affect one but not the other? Assume that the values in the Cost of Control column are unique costs directly associated with protecting against the threat. In other words, don't consider overlapping costs between controls. Calculate the CBA for the planned risk control approach in each threat category. For each threat category, determine whether the proposed control is worth the costs.

After controls were implemented nearly all threat categories' frequency of occurrence was reduced. The outliers were earthquake, flood, and fire which are forces of nature; their frequency remained the same, as their frequency cannot be reduced by the current controls. Nearly all the costs per incident remained the same. The outliers here were flood and fire because the control type is insurance/backups so while these controls cannot reduce the frequency of these threats they can reduce the cost that they have on the company. Most of these controls returned a positive value on the cost-benefit analysis and these are the controls that should remain implemented because they are saving the company money. The positive controls that the company should keep were in the programmer mistake, Loss of Intellectual property, Viruses-Worms-Trojan Horses, Flood, and earthquake categories. The control categories that returned a negative value for the cost-benefit analysis were: software piracy, theft of information (hackers), theft of information (employee), web defacement, theft of equipment, denial-of-service attacks, and earthquake. All of the controls applied to this category resulted in a negative cost-benefit analysis and should be reevaluated to find different controls that are more cost-beneficial.