CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #5 - Option A

Team: 3
Participants: Brandon Crosier, Aaron Gordon, Kitrina Justus, Sam Steele, Marvin Weaver

Logistics

A. Get together with other students on your assigned team in person and 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.
D. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1
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 5 years and when that happens it is 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 console, the estimated rate of occurrence of unlogged misuse by the operators is once every 10 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. *(15 points)*

Switch L47- two vulnerabilities: hardware failure and SNMP buffer

Hardware Failure

1/5 = 20% likelihood, 100% success, 90 asset value, 100% failure, 25% uncertainty

(20% * 100%) * (90*100%) ± 25% = 20% * 90 ± 25% = 18 ± (25%*18) = 18 + 4.5 = *22.5*

SNMP Buffer

1/5 = 20% likelihood, 50% attack success, 90 asset value, 100% failure, 25% uncertain

(20% * 50%) * (90*100%) ± 25% = 10% * 90 ± 25% = 9 ± (25%*9) = 9 + 2.25 = *11.25*

WebSrv6 – Unicode Vulnerability

1/1 = 100% likelihood, 10% success, 100 asset value, 25% failure, 20% uncertain
(100% * 10%) * (100 * 25%) ± 20% = 10% * 25 ± 20% = 2.5 + (25%*2.5) = 2.5 + 0.5 = *3*

MGMT45 – Operator Misuse

1/10 = 10% likelihood, 100% attack success, 5 asset value, 100% failure, 10% uncertain

(10% * 100%) * (5*100%) ± 10% = 10% * 5 ± 10% = 0.5 ± (10%*0.5) = 0.5 + 0.05 = *0.55*

The order the threat vulnerabilities should be addressed based on relative risk is a hardware failure of Switch L47, SNMP buffer of Switch L47, WebSrv6 Unicode vulnerability, then MGMT45 operator misuse vulnerability.

Problem 2
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. Attach the Excel workbook when submitting this document file for grading. *(15 points)*

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence	ARO	ALE
Programmer mistakes	$5,000	1 per week	52/1=52	52*$5,000=$260,000
Loss of intellectual property	$75,000	1 per year	1/1=1	1*$75,000 = $75,000
Software piracy	$500	1 per week	52/1=52	52*$500=$26,000
Theft of information (hacker)	$2,500	1 per quarter	4/1=4	4*$2,500 = $10,000
Theft of information (employee)	$5,000	1 per 6 months	2/1=2	2*$5,000=$10,000
Web defacement	$500	1 per month	12/1=12	12*$500=$6,000
Theft of equipment	$5,000	1 per year	1/1=1	1*$5,000=$5,000
Viruses, worms, Trojan horses	$1,500	1 per week	52/1=52	52*$1,500 = $78,000
Denial-of-service attacks	$2,500	1 per quarter	4/1=4	4*$2,500 = $10,000
Earthquake	$250,000	1 per 20 years	1/20=.05	.05*$250,000 = $12,500
Flood	$250,000	1 per 10 years	1/10=.1	.1*$250,000 = $25,000
Fire	$500,000	1 per 10 years	1/10=.1	.1*$500,000= $50,000

ARO = annualized occurance
ALE= SLE * ARO

Problem 3
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. *(20 points)*

Threat Category	Cost per Incident	Frequency of Occurrence	Cost of Control	Type of Control	ARO	ALE
Programmer mistakes	$5,000	1 per month	$20,000	Training	12/1=12	12*$5,000=$60,000
Loss of intellectual property	$75,000	1 per 2 years	$15,000	Firewall/IDS	1/2=.5	.5*$75,000=$37,500
Software piracy	$500	1 per month	$30,000	Firewall/IDS	12/1=12	12*$500=$6,000
Theft of information (hacker	$2,500	1 per 6 months	$15,000	Firewall/IDS	2/1=2	2*$2,500= $5,000
Theft of information (employee)	$5,000	1 per year	$15,000	Physical security	1/1=1	1*$5,000=$5,000
Web defacement	$500	1 per quarter	$10,000	Firewall	4/1=4	4*$500=$2,000
Theft of equipment	$5,000	1 per 2 years	$15,000	Physical security	1/2=.5	.5*$5,000=$2,500
Viruses, worms, Trojan horses	$1,500	1 per month	$15,000	Antivirus	12/1=12	12*$1,500=$18,000
Denial-of-service attacks	$2,500	1 per 6 months	$10,000	Firewall	2/1=2	2*$2,500=$5,000
Earthquake	$250,000	1 per 20 years	$5,000	Insurance/backups	1/20=.05	.05*$250,000=$12,500
Flood	$50,000	1 per 10 years	$10,000	Insurance/backups	1/10=.1	.1*$50,000=$5,000
Fire	$100,000	1 per 10 years	$10,000	Insurance/backups	1/10=.1	.1*$100,000=$10,000

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.

Some of the values have changed because controls have been applied. These controls affect some of the final values but have no effect on other values.

A control could affect the cost per incident but not frequency of occurrence because the control may affect how much damage the attack does, but may not be able to do anything to prevent it. An example of this would be insurance.

A control could affect the frequency of occurrence but not cost per incident if the control only protects the asset from certain attacks, but if the attack goes through, it will do the same amount of damage. An example of this would be training.

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.

CBA = ALE(prior) - ALE(post) - cost

Programmer Mistakes
260,000 - 60,000 - 20,000= 180,000 - Yes, it was worth the cost

Loss of Intellectual Property
75,000 - 37,500 - 15,000 = 22,500 - Yes it was worth the cost

Software Privacy
26,000 - 6,000 - 30,000 = -10,000 - No it was not worth the cost

Theft of information (hacker)
10000 - 5000 - 15000 = -10,000- No it was not worth the cost

Theft of information(employee)
10000 - 5000 - 15000 = -10,000 - No it was not worth the cost

Web Defacement
6000 - 2000 - 10000 = -6,000 - No it was not worth the cost

Theft of Equipment
5,000 - 2,500 - 15,000 = -12,500 - No it was not worth the cost

Viruses, worms, Trojan horses

78000 - 18000 -15000 = 45,000 - Yes it was worth the cost

Denial-of-service attacks
10,000 - 5,000 - 10,000 = -5,000 - No it was not worth the cost

Earthquake
12500 -12500 - 5000 = -5,000 - No it was not worth the cost

Flood
25,000 - 5,000 - 10,000 = 10,000 - Yes it was worth the cost

Fire
50,000 - 10,000 - 10,000 = 30,000 - Yes it was worth the cost