CIS 481 – Intro to Information Security

IN-CLASS EXERCISE # 5

Names of team members: Volodymyr Bestiyanets, Nick Cunningham, Timothy Mahan, and Shawn Nasr.

Logistics

A. Get into your regular team
B. Discuss and complete the assignment together. Don't just assign different problems to each teammate! That defeats the purpose of team-based learning.
C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

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 MGMT-45 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 these vulnerabilities should be addressed based on relative risk. Show your work. (15 pts.)

(likelihood X attack success probability) **x** (asset value **x** probable loss) + Uncertainty

Switch L47:
1/5 years, 100% attacks successful, impact rating of 90, 100% probable loss, 75% accurate.
(.2 x 100%) x (90 x 100%) = (.2 x 90) = 18 * 1.25 = **22.5 risk rating = highest risk rate and highest priority for evaluation.**
SNMP buffer overflow:
1/5 years, 50% attacks successful, impact rating of 90, 100% probable loss, 75% accurate.
(.2 * 50%) x (90 x 100%) = (.1 x 90) = 9 * 1.25 = **11.25 risk rating. Should be addressed after Switch L47 hardware failure.**
Server WebSrv6:
1/year, 10% attacks successful, impact value = 100, 25% lost, 80% accurate.
(1 x 10%) x (100 x 25%) = 2.5 * 1.2 = **3 risk rating. Evaluate after SNMP buffer.**
MGMT-45:
1/10 years, 100% attacks successful, impact rating = 5, 100% probable loss, 90% accurate.
(.1 x 100%) x (5 x 100%) = .5 * 1.10 = **.55 risk rating = lowest risk rate and should be addressed last.**

Problem 2

Complete Exercise 3 from p. 320 of your text. You may create a spreadsheet to support your work and paste results into a table here. Be sure to attach spreadsheet, as well, if you choose to use one. (15 pts.)

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence	ARO	ALE
Programmer Mistates	$ 5,000.00	1 per week	52	$260,000.00
Loss of Intellectual property	$ 75,000.00	1 per year	1	$ 75,000.00
Software Piracy	$ 500.00	1 per week	52	$ 26,000.00
Theft of Information (hacker)	$ 2,500.00	1 per quarter	4	$ 10,000.00
Theft of Information (employe	$ 5,000.00	1 per 6 months	2	$ 10,000.00
Web Defacement	$ 500.00	1 per month	12	$ 6,000.00
Theft of equipment	$ 5,000.00	1 per year	1	$ 5,000.00
Viruses, worms, Trojan horses	$ 1,500.00	1 per week	52	$ 78,000.00
Denial-of-service attacks	$ 2,500.00	1 per quarter	4	$ 10,000.00
Earthquake	$ 250,000.00	1 per 20 years	0.05	$ 12,500.00
Flood	$ 250,000.00	1 per 10 years	0.1	$ 25,000.00
Fire	$ 500,000.00	1 per 10 years	0.1	$ 50,000.00

Problem 3

Complete Exercise 5 from p. 321 of your text. You may create a spreadsheet to support your work and paste results into a table here. Be sure to attach spreadsheet, as well, if you choose to use one. Be sure to address the questions at the end of the problem. The calculations alone are not sufficient. (20 pts.)

Frequency of Occurrence	Cost of Control (ACS)	Type of Control	ARO	ALE	CBA	Benefit
1 per month	$ 20,000.00	Training	12	$ 60,000.00	$ 180,000.00	YES
1 per 2 years	$ 15,000.00	Firewall/IDS	0.5	$ 37,500.00	$ 22,500.00	YES
1 per month	$ 30,000.00	Firewall/IDS	12	$ 6,000.00	$ (10,000.00)	NO
1 per 6 months	$ 15,000.00	Firewall/IDS	2	$ 5,000.00	$ (10,000.00)	NO
1 per year	$ 15,000.00	Physical Security	1	$ 5,000.00	$ (10,000.00)	NO
1 per quarter	$ 10,000.00	Firewall/IDS	4	$ 2,000.00	$ (6,000.00)	NO
1 per 2 years	$ 15,000.00	Physical Security	0.5	$ 2,500.00	$ (12,500.00)	NO
1 per month	$ 15,000.00	Antivirus	12	$ 18,000.00	$ 45,000.00	YES
1 per 6 months	$ 10,000.00	Firewall/IDS	2	$ 5,000.00	$ (5,000.00)	NO
1 per 20 years	$ 5,000.00	Insurance/Backups	0.05	$ 12,500.00	$ (5,000.00)	YES
1 per 10 years	$ 10,000.00	Insurance/Backups	0.1	$ 5,000.00	$ 10,000.00	NO
1 per 10 years	$ 10,000.00	Insurance/Backups	0.1	$ 10,000.00	$ 30,000.00	NO

The implementation of controls affected both the ARO or frequency of occurrence and the SLE or cost per incident. By lowering both the ARO and the SLE the calculated ALE is affected significantly reducing the cost attributed to the possibility of each threats. A control may only affect the frequency or may only lower the cost if the threat were to happen, in some cases a control may affect both the cost and frequency. Not all controls are beneficial when put into place as the spreadsheet benefit column suggests. Some controls have greater cost attributed to their implementation then the cost of the incident if it were to happen.