CIS-481: Introduction to Information Security

In-Class Exercise #5 - Option A

IQ Team: 4
Names of team members: Daniel Kearl, Mohammed Al Madhi, Yuxuan Chen, Joseph Baxter

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 **IQ 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 these vulnerabilities should be addressed based on relative risk. Show your work. *(15 points)*

Switch L47: ((0.2 * 1) + (0.2 * 0.5)) * (90 * 1) + 75% = 27 + 6.75 = 33.75
WebSrv6: (1 * 0.1) * (100 * 0.25) + 20% = 2.5 + 0.5 = 3
MGMT45: (0.1 * 1) * (5 * 1) + 10% = 0.5 + 0.05 = 0.55

Switch L47 should absolutely be addressed first, followed by WebSrv6, and finally MGMT45.

When doing this problem, we considered multiplying the two vulnerabilities for the switch rather than adding, which results in 2.25. We decided against this because despite the number looking like something that would be expected of the answer, adding the two together is the solution that made sense to us (both vulnerabilities could happen, and both do not have to happen at once).

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 points)*

Table 2

Threat Category	Cost per Incident (SLE)	Freq. of Occurrence	ARO	Annualized Loss Expectancy
Programmer mistakes	$5,000	Weekly	**52**	**$260,000**
Loss of intellectual property	$75,000	Yearly	**1**	**$75,000**
Software piracy	$500	Weekly	**52**	**$26,000**
Theft of information (hacker)	$2,500	Quarterly	**4**	**$10,000**
Theft of information (employee)	$5,000	Biannually	**2**	**$10,000**
Web defacement	$500	Monthly	**12**	**$6,000**
Theft of equipment	$5,000	Yearly	**1**	**$5,000**
Viruses, worms, Trojan horses	$1,500	Weekly	**52**	**$78,000**
Denial-of-service attacks	$2,500	Quarterly	**4**	**$10,000**
Earthquake	$250,000	Vicennially	**0.05**	**$12,500**
Flood	$250,000	Decennially	**0.1**	**$25,000**
Fire	$500,000	Decennially	**0.1**	**$50,000**
Total				**$567,500.00**

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 points)*

Table 3-1

Threat Category	Cost per Incident	Freq. of Occurrence	Cost of Control	ARO	Annualized Loss Expectancy
Programmer mistakes	$5,000	Monthly	$20,000	**12**	**$60,000.00**
Loss of intellectual property	$75,000	Biennially	$15,000	**0.5**	**$37,500.00**
Software piracy	$500	Monthly	$30,000	**12**	**$6,000.00**
Theft of information (hacker)	$2,500	Biannually	$15,000	**2**	**$5,000.00**
Theft of information (employee)	$5,000	Yearly	$15,000	**1**	**$5,000.00**
Web defacement	$500	Quarterly	$10,000	**4**	**$2,000.00**
Theft of equipment	$5,000	Biennially	$15,000	**0.5**	**$2,500.00**
Viruses, worms, Trojan horses	$1,500	Monthly	$15,000	**12**	**$18,000.00**
Denial-of-service attacks	$2,500	Biannually	$10,000	**2**	**$5,000.00**
Earthquake	$250,000	Vicennially	$5,000	**0.05**	**$12,500.00**
Flood	$50,000	Decennially	$10,000	**0.1**	**$5,000.00**
Fire	$100,000	Decennially	$10,000	**0.1**	**$10,000.00**
Total			**$170,000.00**		**$168,500.00**

Controls can both reduce the frequency of threat occurrence and the impact a threat may have. This results in the cost per incident decreasing while the frequency of occurrence also becomes less common. A control could reduce one of these things by focusing its effort or impact. For example, improving physical security for equipment may prevent theft from occurring, but may not improve the impact of potential theft.

Table 3-2

Threat Category	ALE (Prior)	ALE (Post)	Cost of Control (ACS)	Cost-Benefit Analysis (CBA)	Result
Programmer mistakes	$260,000	$60,000.00	$20,000	**$180,000**	**Worth it!**
Loss of intellectual property	$75,000	$37,500.00	$15,000	**$22,500**	**Worth it!**
Software piracy	$26,000	$6,000.00	$30,000	**-$10,000**	**Not worth it.**
Theft of information (hacker)	$10,000	$5,000.00	$15,000	**-$10,000**	**Not worth it.**
Theft of information (employee)	$10,000	$5,000.00	$15,000	**-$10,000**	**Not worth it.**
Web defacement	$6,000	$2,000.00	$10,000	**-$6,000**	**Not worth it.**
Theft of equipment	$5,000	$2,500.00	$15,000	**-$12,500**	**Not worth it.**
Viruses, worms, Trojan horses	$78,000	$18,000.00	$15,000	**$45,000**	**Worth it!**
Denial-of-service attacks	$10,000	$5,000.00	$10,000	**-$5,000**	**Not worth it.**
Earthquake	$12,500	$12,500.00	$5,000	**-$5,000**	**Not worth it.**
Flood	$25,000	$5,000.00	$10,000	**$10,000**	**Worth it!**
Fire	$50,000	$10,000.00	$10,000	**$30,000**	**Worth it!**
Total				**$229,000.00**	