CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #5 - Option A

Team: Seven
Participants: Jackson Dillingham, Matt Jackson, Hilton Siaffa, Tabor Payne, and Emily Wantland

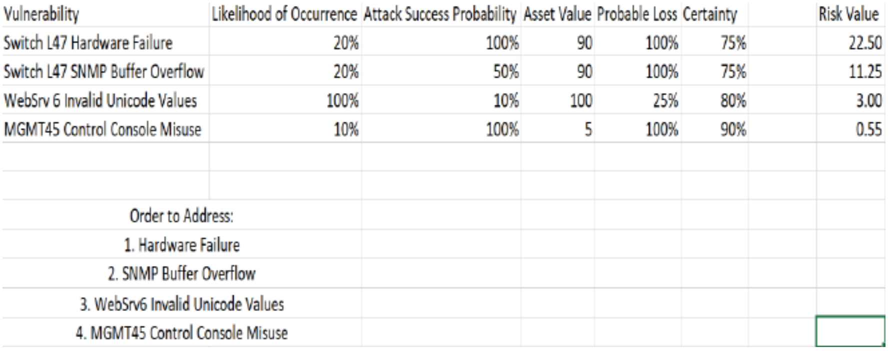
Logistics

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**.

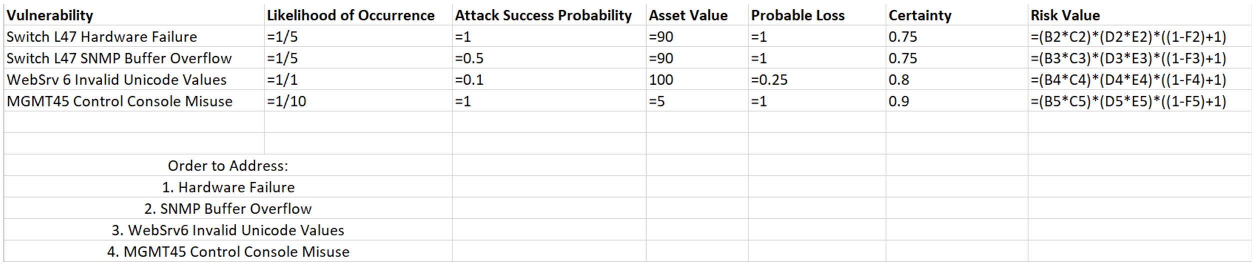
Problem 1

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)*



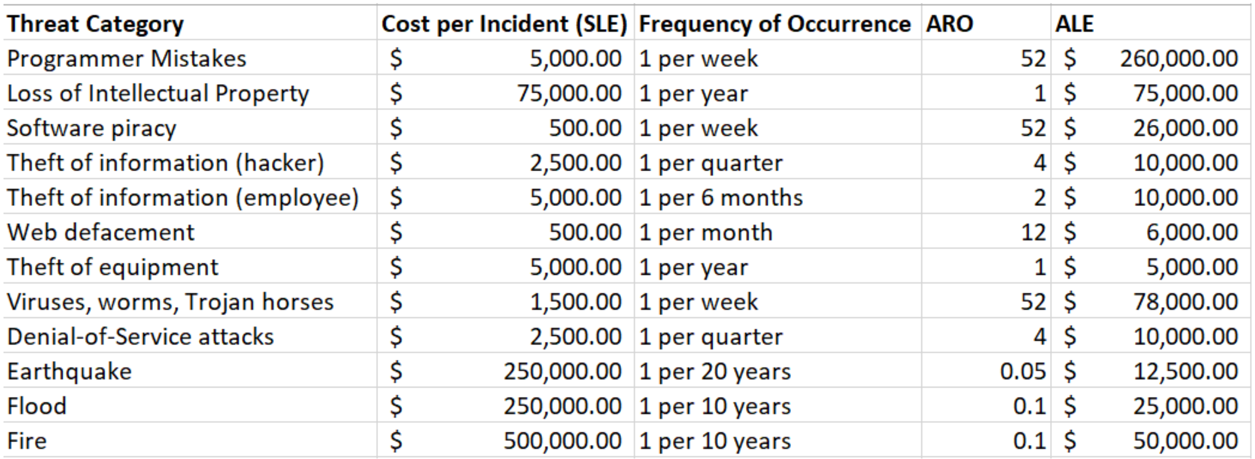
Vulnerability	Likelihood of Occurrence	Attack Success Probability	Asset Value	Probable Loss	Certainty		Risk Value
Switch L47 Hardware Failure	20%	100%	90	100%	75%		22.50
Switch L47 SNMP Buffer Overflow	20%	50%	90	100%	75%		11.25
WebSrv 6 Invalid Unicode Values	100%	10%	100	25%	80%		3.00
MGMT45 Control Console Misuse	10%	100%	5	100%	90%		0.55
Order to Address:							
1. Hardware Failure							
2. SNMP Buffer Overflow							
3. WebSrv6 Invalid Unicode Values							
4. MGMT45 Control Console Misuse							



Vulnerability	Likelihood of Occurrence	Attack Success Probability	Asset Value	Probable Loss	Certainty	Risk Value
Switch L47 Hardware Failure	=1/5	=1	=90	=1	0.75	=(B2*C2)*(D2*E2)*((1-F2)+1)
Switch L47 SNMP Buffer Overflow	=1/5	=0.5	=90	=1	0.75	=(B3*C3)*(D3*E3)*((1-F3)+1)
WebSrv 6 Invalid Unicode Values	=1/1	=0.1	100	=0.25	0.8	=(B4*C4)*(D4*E4)*((1-F4)+1)
MGMT45 Control Console Misuse	=1/10	=1	=5	=1	0.9	=(B5*C5)*(D5*E5)*((1-F5)+1)
Order to Address:						
1. Hardware Failure						
2. SNMP Buffer Overflow						
3. WebSrv6 Invalid Unicode Values						
4. MGMT45 Control Console Misuse						

Problem 2

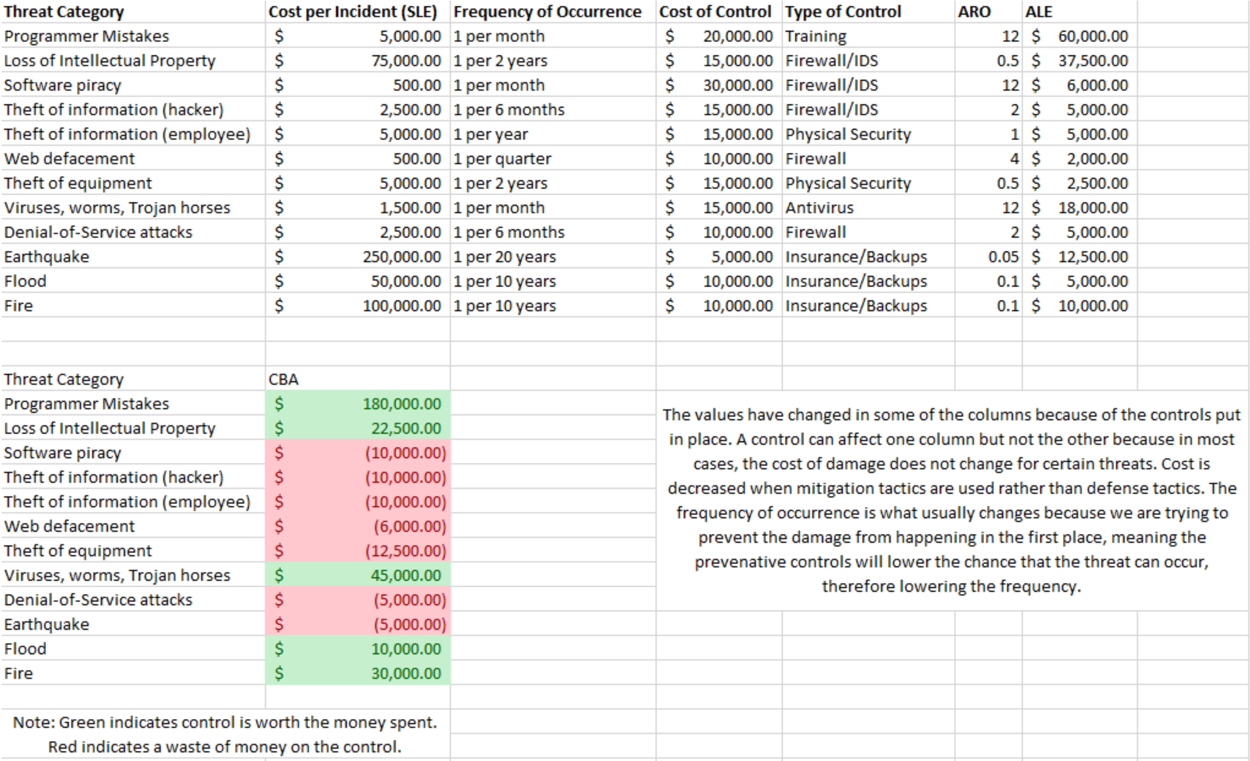
Complete Exercise 3 from p. 320 of your text. You should create a worksheet using Microsoft Excel to support your calculations, then paste an image of the table with column headings and rows just below. Attach the Excel workbook when submitting this document file for grading. *(15 points)*



Threat Category	Cost per Incident (SLE)	Frequency of Occurrence	ARO	ALE
Programmer Mistakes	$ 5,000.00	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 (employee)	$ 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 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 (SLE)	Frequency of Occurrence	Cost of Control	Type of Control	ARO	ALE
Programmer Mistakes	$ 5,000.00	1 per month	$ 20,000.00	Training	12	$ 60,000.00
Loss of Intellectual Property	$ 75,000.00	1 per 2 years	$ 15,000.00	Firewall/IDS	0.5	$ 37,500.00
Software piracy	$ 500.00	1 per month	$ 30,000.00	Firewall/IDS	12	$ 6,000.00
Theft of information (hacker)	$ 2,500.00	1 per 6 months	$ 15,000.00	Firewall/IDS	2	$ 5,000.00
Theft of information (employee)	$ 5,000.00	1 per year	$ 15,000.00	Physical Security	1	$ 5,000.00
Web defacement	$ 500.00	1 per quarter	$ 10,000.00	Firewall	4	$ 2,000.00
Theft of equipment	$ 5,000.00	1 per 2 years	$ 15,000.00	Physical Security	0.5	$ 2,500.00
Viruses, worms, Trojan horses	$ 1,500.00	1 per month	$ 15,000.00	Antivirus	12	$ 18,000.00
Denial-of-Service attacks	$ 2,500.00	1 per 6 months	$ 10,000.00	Firewall	2	$ 5,000.00
Earthquake	$ 250,000.00	1 per 20 years	$ 5,000.00	Insurance/Backups	0.05	$ 12,500.00
Flood	$ 50,000.00	1 per 10 years	$ 10,000.00	Insurance/Backups	0.1	$ 5,000.00
Fire	$ 100,000.00	1 per 10 years	$ 10,000.00	Insurance/Backups	0.1	$ 10,000.00

Threat Category	CBA
Programmer Mistakes	$ 180,000.00
Loss of Intellectual Property	$ 22,500.00
Software piracy	$ (10,000.00)
Theft of information (hacker)	$ (10,000.00)
Theft of information (employee)	$ (10,000.00)
Web defacement	$ (6,000.00)
Theft of equipment	$ (12,500.00)
Viruses, worms, Trojan horses	$ 45,000.00
Denial-of-Service attacks	$ (5,000.00)
Earthquake	$ (5,000.00)
Flood	$ 10,000.00
Fire	$ 30,000.00

The values have changed in some of the columns because of the controls put in place. A control can affect one column but not the other because in most cases, the cost of damage does not change for certain threats. Cost is decreased when mitigation tactics are used rather than defense tactics. The frequency of occurrence is what usually changes because we are trying to prevent the damage from happening in the first place, meaning the prevenative controls will lower the chance that the threat can occur, therefore lowering the frequency.

Note: Green indicates control is worth the money spent.
Red indicates a waste of money on the control.