**Module 4 (30 points) – Chapter 5**

1. (Whitman & Mattord, 2016, p. 290) What is risk management? Why is the identification of risks and vulnerabilities to assets so important in risk management? Why is an enterprise architecture and documented business processes important?

Risk management is the process used to access the risk and the level of how bad it is then what can be done to reduce the level of the risk. The identification of risks and vulnerabilities is important to risk management as it helps identify future problems and the level of detriment they can cause. This helps with accessing the time until potential risk, the severity, and how long it would take to resolve. The enterprise architecture and documented business processes are important because they are used to help keep information private and safe which can help reduce some threats.

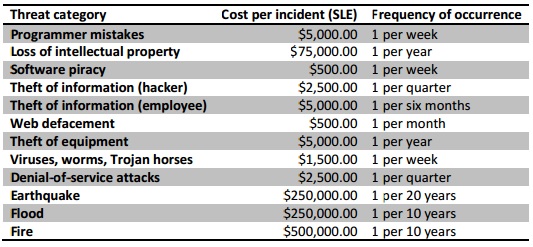
1. (Whitman & Mattord, 2016, p. 291) What five strategies for controlling risk are described in this chapter? What other ways can an organization control risk?

The five risk control strategies are defense, transference, mitigation, acceptance, and termination. Other ways an organization can control the risk is to do tests using white hat hackers to test their systems prior to storing the more important information. If they are protecting files, they could use test files in the system that hold no real value and have the hired hackers try to access the files then put how they go into it in the files so the company can protect against more malicious threats.

1. (Whitman & Mattord, 2016, p. 291) What is a cost benefit analysis? Are there times that security costs need to be incurred even if the cost recovery is not immediate? Give an example.

A cost benefit analysis is the calculated graph that determines at which price the company would be achieving the greatest benefit. For instance, a company in manufacturing will look at multiple suppliers and determine which will be the best cost, provide the best service, the most product, and how long this agreement would last. There are times that the security costs are needed even if there is not an immediate cost recovery. An instance of this would be if there is a known problem with people hacking the medical field. The hospitals would pay to increase the security and not see immediate cost recovery as they are weighing the options of long-term protection over the chance of the hackers leaking important information. There are some companies that chose not to upgrade their security and were unable to recover when there was a security leak.

1. (Whitman & Mattord, 2016, p. 292) Suppose XYZ Software company has a new application development project with projected revenues of $1,200,00.00. Using the following table, calculate the ARO and ALE for three threat categories that XYZ Software Company faces for this project.



Looking at the threat categories I chose the natural disasters of Earthquake, Flood, and Fire.

Earthquake: ARO = 1/20 ALE = 1/20 of $250000.00 = $12500.00

Flood: ARO = 1/10 ALE = 1/10 of $250000.00 = $25000.00

Fire: ARO = 1/10 ALE = 1/10 of $500000.00 = $50000.00

1. (Whitman & Mattord, 2016, p. 293) Assume a year has passed and XYZ has improved security by applying a number of controls. Using the information from question 4 and the following table, calculate the post-control ARO and ALE for each threat category listed.

ARO = mistakes per year, ALE = SLE \* ARO

Programmer Mistakes: ARO = 12/1 ALE = 12 \* $5000 = $60000

Loss of intellectual property: ARO = 1/2 ALE = ½ \* $75000 = $37500

Software Piracy: ARO = 12/1 ALE = 12\*$500 = $6000

Theft of info(hacker): ARO = 6/1 ALE = 6\*$15000 = $90000

Theft of info(employee): ARO = 1 ALE = 1\*$15000 = $15000

Web Defacement: ARO = 4/1 ALE = 4\*$500 = $2000

Theft of equipment: ARO = 1/2 ALE = ½ \* $5000

Viruses…: ARO = 12/1 ALE = 12\*$1500 = $18000

Denial-of-service: ARO = 2/1 ALE = 2\*$2500 = $5000

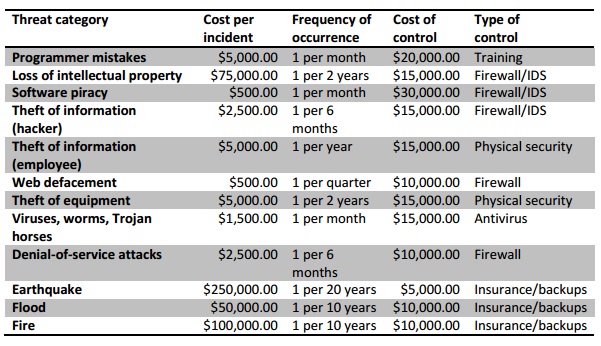
Earthquake: ARO = 1/20 ALE = 1/20 of $250000 = $12500

Flood: ARO = 1/10 ALE = 1/10 of $50000= $5000

Fire: ARO = 1/10 ALE = 1/10 of $100000 = $10000

**Bibliography**

Whitman, M. E., & Mattord, H. J. (2016). *Principles of Information Security*. Course Technology.



Why have some values changed in the columns “Cost per incident” and “Frequency of occurrence?” How could a control affect one but not the other?

Assume that the values in the “Cost of control” column presented in the table are those unique costs directly associated with protecting against the threat. In other words, don’t consider overlapping costs between controls. Calculate the Cost Benefit Analysis (CBA) for the planned risk control approach for three threat categories. For each threat category selected determine whether the proposed control is worth the costs.

The controls can have different affects based on the type of threat. For instance, adding the firewall will help against threats through the internet and the software but will not be able to protect the hardware against a natural threat like a fire.

Earthquake: ALE = $12500 cost is $5000 CBA:12500/5000

Control is worth the cost.

Flood: ALE = $5000 cost is $10000 CBA:5000/10000

Control is not worth the cost.

Fire: ALE = $10000 cost is $10000 CBA:10000/10000

Control is equal to cost so it is not worth it.

**Bibliography**

Whitman, M. E., & Mattord, H. J. (2016). Principles of Information Security. Boston: Course Technology.