

INFO-6027- Assignment 2

Bohan zhang



July 11, 2019

ID: 0814917

Section 2

Part 1:

**Question 1:**

**Policies:** Policies are formal statements which initialized by the senior management. Policies should reflect the company’s objectives for information security and it is a foundation before standards, procedures, and guidelines. [1]

**Standards:**  Standards are rules and actions in a company used for supporting the driven policies.[1]

**Procedures:** Procedures are the questions comes down to how do I do it. They are detailed processes to support mandate actions or standards.  [1]

**Guidelines:** Guidelines are the supplements for standards. If there are no standards come in place, then the guidelines will be best practices and recommendations for users to follow. [1]

**Question 2**: Policies are important because :

* They are used for internal audit
* They are used for the legal purpose regarding the management’s duel diligent
* They help companies to meet compliance
* They reflect management’s intent

**Question 3:** Policies should be developed when:

* Employees show confusion on what the appropriate way to behave is. For example dress code and personal devices.[2]
* To stay in compile with the laws for example hospitals should develop their policies to meet HIPPA as soon as possible
* There was a security breach and the issue has not been addressed before.
* The old policies outdated

**Question 4:** While developing policies, the following factors are considered:

* The policies should be easy to understand
* The policies should be well funded and bought in by senior management
* The policies should be enforceable [4]
* The policies should be complied with all current laws

Part 2:

**2-1** Marriot Hotel Inc core value statement is putting people first, pursuing excellence, adopting changes and staying in integrity and serve the world. [3]

**2-2**

Access Control defines who can access what in a computing environment. It categorized as physical control and logical control.

**General Policy on Access Control for Marriot International:**

* Accessing to information system will be limited to authorized users. Information on the system will be processed on behalf of only the authorized users.
* Marriot international will revoke users accessing to information system upon employment or partnership termination.
* Security awareness training will be provided to employees and customers to increase security awareness and mitigate security risk.

Since the breach happened last year, our company has lost hundred million dollars. The breach all comes down to our outdated policy and poor security awareness training on our employees and end users. The malware Mimikatz secretly sitting on Starwood network for years because of employees fall down to the phishing attack. The malware successfully used old accounts sitting on the system to gain access to our system. To mitigate the risk, we must educate our employees and end users to increase their security awareness. In addition, to prevent unauthorized access to our system, we must revoke all the user rights on our systems if they have terminated partnership with us.

Reference

1. Spoden. C. “BUILD FROM THE GROUND UP: DIFFERENTIATING BETWEEN POLICIES, STANDARDS, PROCEDURES, AND GUIDELINES”, *FRSECURE,* Aug 22, 2017. <https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/>

2. HEATHFIELD. S, “Why, When, and How to Develop a Company Policy”, June 25, 2019.

<https://www.thebalancecareers.com/how-to-develop-a-policy-1918870>

3. Marriot International. <https://www.marriott.com/culture-and-values/core-values.mi>

4. “info6027 information security planning lesson 9 slides”