Homework 1 Name: Abbas Shamshi Email: as10608n@pace.edu

The assignment consists of 2 parts. Part 1 (80%) and Part 2 (20%)

Papers:

1. IB4803_PrivateSectorCyberIncidents.pdf *(Private Sector Cyber Incidents in 2017 - Riley Walters)*
2. IB4804_FederalCyberBreaches.pdf *(Federal Cyber Breaches in 2017 - Riley Walters)*

The above PDF's can be found under blackboard document section.

Part 1 (Individual):

This must be completed individually.

Please choose one cyber incident of your choice from each paper (Pick one incident from IB4803 and one breach from IB4804 for CIA triad impact analysis)

Do additional web research to learn more about the attack. Now, using the concept of CIA traid in Week1 lecture, assign a low, moderate, or high impact level for the loss of confidentiality, integrity, and availability respectively in the affected system. **Provide as much as details as possible to justify your analysis rating.**

Since the students in this class have varied levels of network security background I am only looking for you to give a sincere effort at this point. We will learn much more about these topics in the coming weeks so no discussion is planned this week.

Upload your document with the name HW_"LastName".pdf **by replying to the HW for Weeks 1and 2 Thread**. Do not create new thread.

Limit your submission: 3 to 4 pages
List all external references you researched.

Part 2 (Blackboard discussion):

Review and Comment on at least 1 of your classmate's HW1 assignment in blackboard by replying inside their reply.

Possible topics for commenting: State your opinion about whether the analysis and the CIA impact level assigned is reasonable. Feel free to share any other information pertaining to Cyber-attacks/Prevention from your corporate or personal experience.

<Selected Private Sector incident > (40 points)\

IB4803 Private Sector Cyber Incidents

Hyatt (hotel chain).

Report**.**

Point of Sales System at Hayatt was breached, its cyber security team discovered signs of unauthorized access to payment card information at certain Hyatt-managed locations worldwide, 41 places across 11 countries were affected with this breach. The nation with the largest number of Hyatt properties impacted was China.
Hackers were able to collect credit card numbers, expiration dates, cardholder names, and "internal verification code," presumably the three-digit one on the back, from cards manually entered or swiped at the front desk of certain Hyatt-managed locations.
This was a major breach which resulted in various credit card scams. Statement from hayatt mentioned only small percentage of card details were stolen, but no specific number was mentioned

Self-Analysis

By reading various articles, I would assign **High** level impact

- It was detected after 4 months of first incident, it has affected 41 location in 11 countries, leaving customers credit card at risk

Confidentiality: **High**

- The Data, which was stolen consisted of credit card number expiration date and the security pin which is on back of the card. It affected 41 location in 11 countries. Credit card details of the customers was compromised and customers were at risk of credit card scam. Impact **High**

Integrity: **High**

- Breach consisted of all the detail of credit card which were used at Hayatt location, Card details which should not be stored or made available to anyone was exposed to attacker which resulted to the user at very high impact of integrity breach. Impact **High**

Availability: Medium

- The available stolen data was not easily available on the dark web. Impact **Medium**

Reference:
https://techcrunch.com/2017/10/12/hyatt-breach-exposed-customer-payment-data-at-41-hotels/

https://thegate.boardingarea.com/credit-card-security-breach-at-41-hyatt-hotel-properties-in-eleven-countries/

https://krebsonsecurity.com/2017/10/hyatt-hotels-suffers-2nd-card-breach-in-2-years/

<Selected Fed Breach > (40 points)

IB480 Federal Cyber Breaches.

Department of Defense (DOD).

Report.

Hack the Pentagon was the bug bounty program which was initiated by Department of Defense (DOD) launched on 2016 through the efforts of Hacker-one platform, through this innovative effort, hackers were provided legal consent to perform specific hacking techniques on various websites of DOD.
Goal behind this program was to find vulnerability and improve departments security

Bug Bounty Program:

bug bounty program organizations, software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities. The entire cost of the Hack the Pentagon pilot was $150,000, with about half going to the hackers themselves.

Self-Analysis:
I have read various articles on this bug bounty program, and from my point of view I would assign **Low** impact to this data breach

- This bounty program was focus to improve the security of the department; vulnerability was discovered so that It can be fixed by the department.
- No data was stolen/made public as this was done under the supervision of the department

Confidentiality: **Low**

- Confidentiality was preserved; No data was misused or made public. Impact was **Low**

Integrity: **Low**

- The data or system was not been manipulated; data remained in its original form. Impact was **Low**.

Availability: **Low**

- As this was bug bounty program no data was made public. Impact **Low**

Reference

https://dod.defense.gov/Portals/1/Documents/Fact_Sheet_Hack_the_Pentagon.pdf

https://www.usds.gov/report-to-congress/2017/fall/hack-the-pentagon

https://www.securityweek.com/expert-hacks-internal-dod-network-army-websit