IS4231 Information Security Management, Sem1, AY21/22

Tutorial 3: Cyber Breach at Target

Case Background

"On December 19, 2013, Target, the second-largest retailer in the United States, announced a breach involving the theft of data from over 40 million credit and debit cards used to make purchases in its U.S. stores between November 27 and December 18.

On January 10, 2014, it reported that the cybercriminals had also stolen personal data, including the names, telephone numbers, home addresses and email addresses of up to 70 million additional customers."

Recommended reading (but not limited to):

a. Hacking Timeline: What Did Target Know and When?
https://www.youtube.com/watch?v=M5tl4Yf92Nk

b. Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed For The Giant Retailer
http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056

c. Anatomy of the Target data breach: Missed opportunities and lessons learned
http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

d. Target Breach Costs: $162 Million
http://www.databreachtoday.com/target-breach-costs-162-million-a-7951

e. Breaking the Target: An Analysis of Target Data Breach and Lessons Learned
https://arxiv.org/pdf/1701.04940.pdf

Research on this data breach case and answers the following questions:

1) What hacking techniques have been used in this breach case? (Pls select all the correct options)
   a. Phishing
   b. Hardware Keylogging
   c. Memory scraping
   d. DDOS

2) What law would be applied to the hackers if it happened in Singapore?
   a. Cybersecurity Act
   b. PDPA
   c. Computer Misuse Act
   d. None of the above

3) What law would be applied to Target if it happened in Singapore?
   a. Cybersecurity Act
   b. PDPA
   c. Computer Misuse Act
   d. a&b

4) What are the consequences of this cyber breach?

Data: The breach exposed 40 million payment cards and personal information on 70 million customers.

5) Reflected from this incident, what are the problems/weaknesses existed in Target's information security management program (e.g., technical, process, people)?

Technical - Vendors not properly secured with latest anti-malware softwares / Internal network too exposed

People - Vendor staff not properly trained to prevent phishing

Process - Early warnings not treated seriously

6) What security controls (e.g., technical, managerial) Target has implemented after this cyber breach happened? Such implementation represents what kind of implementation approach?

Improved monitoring and logging of system activity
Installed application whitelisting POS systems and
Implemented POS management tools
Improved firewall rules and policies
Limited or disabled vendor access to their network
Disabled, reset, or reduced privileges on over 445,000 Target personnel and contractor accounts
Expanded the use of two-factor authentication and password vaults
Trained individuals on password rotation

- These represent a _____ implementation approach