The Assignment on Information Security

(UE19CS347)

Documented by Anurag.R.Simha

SRN	:	PES2UG19CS052
Name	:	Anurag.R.Simha
Date	:	12/03/2022
Section	:	A

1. What's your diagnosis of the breach at Target? Was Target particularly vulnerable or simply unlucky?

   A. The cataclysmic data breach on Target was, alas, an atrocious incident. I reckon that Target was vulnerable to also simple data beaches. For, a mere phishing email performed a gargantuan breach on the company's data. All this is unequivocally by no means a case of luck. Despite having over 300 employees devoted to information security, Target desperately failed to provide rudimentary protection to their data. It's too bad that this company had made information about their vendors publicly accessible, hence making it facile for nefarious hackers to access their database. The worst part was that the employees failed to act on security warnings. I presume that these points should make it crystal clear that the data breach on Target was purely not a case of luck. But an instance of ignorance and weakness.

2. What, if anything, might Target have done better to avoid being breached? What technical or organizational constraints might have prevented them from taking such actions?

   A. Preferably, Target could have opted for security by 'defence in depth'. The fundamental cause of the data breach was the phishing mail that Target received. The company could have a DMZ installed into their infrastructure, thus advancing the onerousness to attack the servers/systems. A proficient mail examining software could be the chosen choice to thwart their servers from being agonised by data breaches. Another wise yet imperative option is to ensure impeccable authentication of their vendors. They could also train their employees to react swiftly to security warnings.

3. What's your assessment of Target's post-breach response? What did Target do well? What did they do poorly?

   A. Target put all its efforts to recover from the losses it underwent. They had to face lawsuits, the media and many such oppositions. With their strenuous attempts, the company took a stab in protecting the confidential data from the breach. The consequence of the assault posed great arduousness to Target. According to the Senate report, although the security team had pinpointed the hazardous vulnerabilities, Target ignored it and poured light upon preparing for a Black Friday. The CEO and the board of directors were highly irresponsible during the attack. It was at these points Target had failed. I appreciate that Target agreed to settle the lawsuits it faced by the customers aiding their (customers) losses. It also cooled the issues it had with Visa. But, proper authentication from its vendors was a vital sine qua non to Target, where it had failed.

4. To what extent is Target's board of directors accountable for the breach and its consequences? As a member of the Target board, what would you do in the wake of the breach? What changes would you advocate?

   A. The blame here is upon the board of directors. The directors are responsible for the welfare of a company. But they were negligent during the attack. They completely ignored all the warning signals and got least bothered about the breach. In the wake of the breach, I would first take notice of the most recent mail received and order for a forthwith activation of all the firewalls in the company. All the employees must adhere to the law and be principled workers of the company. So, I would consider educating them about the law. Thus, they get aware of all consequences of any nefarious and satanic acts they dare to proceed. Advancing with a firewall, I would get a DMZ installed in the company, thwarting any foreign cyberattacks that dwindle the company's profits. Deployment of a well-arranged security team would help in keeping the company safe.

5. What lessons can you draw from this case for prevention and response to cyber breaches?

   A. Quite a few points that strike into my observation are:
   - a. Responsibility:
     - i. One can never neglect his duties.
     - ii. It's imperative to take complete responsibility for the job assigned.
   - b. Zero ignorance:
     - i. If there's any sign of danger, it must get treated at once.
   - c. Trust
     - i. Customers bestow immense trust upon a company.
     - ii. Maintaining that trust is of great importance.

6. How would you characterize your role as a director in relation to cybersecurity at your organization? What are some concrete things that you can do as a director to oversee this domain?

   A. Being a cyber security director of the company, I would guarantee the authentication of every vendor and install an efficient firewall system in the company. Training each employee about the law would be an unavoidable requirement. It's taken care that all the emails that arrive at the company's mail servers do not contain any spam content and pose zero harm to the company. Authentication of every employee is also a sine qua non. An efficient and proficient cyber security team must serve the company 24/7.

7. What do you think companies can do better today to protect themselves from cyber breaches and in their post-breach response?

A. With the advancement of technology, there are ample security resources in the market today. Companies can install an efficient DMZ on their servers and worthy anti-virus programs. During the post-breach response, companies can prove their innocence in a court of law. In case of any data loss, they all must be recovered and kept highly confidential, veiled from the public. Performing a deep investigation of the data breach is advised. If possible, removing breached data from the internet is a considered option.

****