MILITARY COLLEGE OF SIGNALS

NETWORK SECURITY

Assignment 1

Submitted to:

Maj Sohaib Khan

Submitted by:

ASC Muhammad Uzair

Course:

BETE-54 (B)

Date:

27th Dec,2020

LifeLabs Data Breach

LifeLabs is a privately owned Canadian healthcare company established in 1958 by Dr. Cam Coady. LifeLabs is one of the largest healthcare companies in Canada with 16 Laboratories all over Canada, performing different diagnostics tests. On 17th December,2019, LifeLabs posted a newsletter on their website notifying their patients about a cyberattack which breached their computers and database. A large amount of their patient's data, their lab results, national health car numbers, their names, date of births, addresses, emails, login IDs, and passwords were stolen. Although the company was hacked in 1st November but the LifeLabs administration did not told the patients about the hack until December 17th. Almost 15 million Canadians were affected by this cyberattack, that's 40% of Canada's total population. The attack was of "Ransomware" nature and company paid the attackers to retrieve their patient's data. This was the second largest healthcare data breach of 2019.

After the incident LifeLabs took necessary steps to avoid such misadventure again but a sudden patient outburst happens and they filled lawsuits against the testing giant LifeLabs saying they failed to protect their patient's private data, violating consumer and privacy protection laws. The patients are asking for $1.1 Billion in compensation for settlement. An investigation was launched by Ontario and British Columbia Information and Privacy Commissioners to address public concerns and to find the actions which led to this disastrous cyberattack.

Officials found out that LifeLabs lacked adequate information technology security policies and information practices and they were collecting more personal data than required in violation of country's health privacy laws. The officials also pointed out that LifeLabs took necessary steps to contain and investigate the breach and they have also addressed that security shortcomings.

Since the incident, LifeLabs appointed Chief Information Security Officer, Chief Privacy Officer and Chief Information Officer. They are also enhancing their Information Security management program and have invested $50 Million in the program. LifeLabs also employed a third-party to evaluate its cyberattack response and efficiency of its security program. LifeLabs have also implemented additional cybercrime detection technology and going to arrange privacy and security awareness training programs for its workforce.

Officials ordered LifeLabs to clarify their terms under which it provides laboratory services to other healthcare entities and to improve specific practices regarding IT security, by formally putting written IT security practices and policies. The officials also ordered LifeLabs to stop collecting specified data from patients and dispose of the data which has already been taken. Regarding the late notification from LifeLabs about the cyberattack, official asked LifeLabs to improve their notification processes.