Three UK (a leading UK telecommunications company) were subjected to a cyber attack in 2016. What IT professional issues were raised by this incident?

Introduction

As technology grows faster and faster, the probability of cyber- attack crimes increases as well. This is a constantly growing threat that affects business and society. One of the biggest cyber-attack targets are telecommunications companies as they store large amounts of sensitive data. For example, Three UK, one of the biggest mobile companies, was a subject to a significant cyber-attack on November, 2016. The affected reputation of the company caused a share price fall but apart from the direct financial consequences, there a legal and ethical issues that arise.

What Happened?

According to several sources the huge mobile phone company Three admitted 'a major cyber-security breach which could have exposed six million customers' personal data at risk' [1].
Three Mobile also admitted that the hackers successfully accessed their database after using an employee login credentials. The data that was stolen included customers' names, addresses, date of births and phone numbers. The reason for gaining access to the mobile giant's computer systems was to order and then steal hundreds of new handsets [2]. Furthermore, by the same time when eight devices have been illegally obtained through the upgrade scheme, a large number of high-value handsets have been stolen as well.
In statement regarding consumer's concerns of the stolen data, Three UK said that 'This upgrade system does not include any customer payment, card information or bank account information' [3].

Privacy Issue

One of the major issues ,which arises after the cyber-attack regards the privacy of data. According to the Data Protection Act 1998, Three UK is obliged to perform appropriate technical and organisational measures against unauthorised or unlawful processing of personal data. Therefore, Three UK violated the Act by not improving their security in order to protect the privacy rights of their customers against frauds. As a result, names, date of births, addresses and phone numbers were being accessed.

On the other hand, there are not clearly defined standards that exist in order to protect against cyber-attacks. The Data Protection Act 1998 enforces measures to be taken but how do we know if those measures are sufficient? Without explicit rules and procedures to be followed, the targeted institutions can always claim that they have done everything possible to secure their systems, but the attacks were too sophisticated and unavoidable. Currently, there are government schemes such as Cyber Essentials that provide support to organisations against cyber-attacks. A step forward would be to oblige every company that stores sensitive data to be certified

by Cyber Essentials or another authorised institution. But are all those prevent leak of information from an employee login as in the cyber-attack that affected Three UK?

However, there are some official governmental institutions that regulate the actions of companies operating with personal data like the Information Commissioner's Office (ICO). It is a national data protection authority that deals with the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003 across UK. The telecommunication companies are required to report any kind of data breaches to ICO. Therefore, as it has been stated, Three UK informed ICO for the breach: 'the ICO told IT Pro it was aware of the situation and was investigating' [4].

Furthermore, no matter that the stolen data from the cyber-attack against Three UK did not contain bank or credit details of the customers, it clearly exposes them to risk of identity theft. This is the reason why hackers target large companies with millions of customers. The accessed details could be sold on the global black market for stolen data. Consequently, the victims of the Three UK data breach are facing an ongoing threat of identity theft, scam or phishing, which pose a challenge for the company regarding the trust and loyalty.

Consequences for the Company

A company's reputation is strongly related to the levels of security it provides to its customers. Therefore, Three UK must significantly improve its security policies after the attack in order to cope with the issue of customers' mistrust.
Nevertheless, Three UK was a crime victim, according to the Computer Misuse Act 1990. Cybercrimes cause huge financial losses for the affected companies, which has a huge negative impact on the economy.

How Could the Cyber-Attack have been Prevented?

The attackers accessed the database using a stolen employee credentials, which allowed them to login to the system without Three UK noticing. This brought them valuable time before anyone noticed the unusual behavioural. Once in, they tricked it into sending high-end upgrade handsets to an address where they could intercept them. [5] How did hackers gain access to an employee's credentials in the first place? Was it a hacker from outside, or just an employee from inside the company? As Hans Zandbelt, Senior Technical Architect suggested, 'organisations must implement and invest in two-factor and multi-factor authentication to safeguard data and maintain customer loyalty'. [6] 'The Three data breach demonstrates that perimeter defences are not enough. Any organisation that handles customer data is at risk from insider threats. The way that files are managed, monitored and shared is key. An authorised login will enable someone with malicious intent to download data to a disc or USB key, unless there are safeguards built in to the infrastructure that flag this movement of data.'[6]

Conclusion

In conclusion, Three UK was responsible for the attack since they had not applied standard security measures which was a violation of the Data Protection Act 1998. This exposed the customers to huge risks of frauds. Although there are no specific requirements for security, there are government schemes that help organisations protect from cyber-attacks. On the other hand, Three UK was a victim of a crime that caused significant damages to the company. Every company could be attack regardless of their security levels. This is a major issue that need to be addressed in today's society. Companies must be supported and monitored by security experts in order to verify that it is safe for them to store sensitive personal data. Data is the new modern currency and the challenge is to protect it.

REFERENCES:

[1] http://www.informationsecuritybuzz.com/expert-comments/three-mobile-cyber-attack-six-million-customers-details-exposed/

[2] https://www.thesun.co.uk/news/2208831/thieves-target-mobile-phone-network-three-putting-9million-customers-personal-data-at-risk/

[3] http://www.cityam.com/253912/three-mobile-becomes-latest-high-profile-victim-cyber-hack

[4] http://www.itpro.co.uk/hacking/27594/over-133000-three-mobile-customers-hit-by-data-breach

[5] http://www.telegraph.co.uk/technology/2016/11/17/three-hack-how-to-protect-yourself-if-youve-been-affected/

[6] http://www.informationsecuritybuzz.com/expert-comments/three-mobile-cyber-attack-six-million-customers-details-exposed/

http://www.telegraph.co.uk/news/2016/11/17/three-mobile-cyber-hack--six-million-customers-private-data-at-r/