On 18th November 2016, Hutchison 3G UK CEO David Dyson confirmed that the company had been victim of a cyber attack. Employee logins belonging to employees of Three UK were used to gain unauthorised access to the company's customer upgrade database, allowing the hackers to intercept handset upgrades of 8 customers, steal over 400 from stores, as well as steal sensitive information relating to over 130,000 others. Among the information stolen were full names, home addresses, dates of birth and phone numbers.[1] The nature of this attack raises several questions in regards to the professional issues involved. This essay will explore said issues as well as other examples of situations in which they have arisen.

A major issue that could arise for Three depending on what happens with the stolen data is the issue of legal proceedings. Evidently, the hackers are in violation of the UK Computer Misuse Act 1990 purely for gaining unauthorised access to the system[2], however the company is also in violation of the Data Protection Act, which states that any sensitive data must be "kept safe and secure".[3] On top of this, Three may be liable for negligence charges. This is exactly the situation that is happening to Yahoo in the US. In 2013, Yahoo suffered one of the largest data breaches to date when 1 billion records of customer data was stolen from it's servers. This happened after the company told its customers it would step up its security following previous breaches. As well as this, Yahoo only publically disclosed the attack in December 2016, something that they had previously done with an attack that occurred in 2014 and was announced in September 2016. Ronald Schwartz, a Yahoo user, sued the company on behalf of Yahoo users in the US on the grounds of gross negligence and not taking customer security seriously.[4] If people are affected by Three's stolen data, a similar case may be brought up in the UK and would seriously harm Three's reputability.

As previously stated, the hack was carried out by someone illegitimately using an employee login to access the Three customer update database. This has led some to believe that it was an inside job by an employee or former employee who supplied the details to the hackers.[1] This may have been possible to avoid. For example, accessing the employee system would only have been required from a retail store, company headquarters or a call centre. This would have enabled Three to filter access to their system from only permitted locations, something that would have made a remote attack harder. Limiting the data that employees can access also could have made it harder for the attackers to retrieve as many customers records as they did. Employees would rarely need to access a database of all customers due to upgrade, they would only need to access the customer they are dealing with. By limiting the database to only the customers that a specific employee is responsible for, the damage could have been greatly

---

[1] "Three Mobile cyber hack: six million customers' private information at ...." 18 Nov. 2016, http://www.telegraph.co.uk/news/2016/11/17/three-mobile-cyber-hack--six-million-customers-private-data-at-r/. Accessed 26 Feb. 2017.
[2] "Computer Misuse Act 1990 Section 1 - Legislation.gov.uk." http://www.legislation.gov.uk/ukpga/1990/18/section/1. Accessed 26 Feb. 2017.
[3] "Data protection - GOV.UK." https://www.gov.uk/data-protection/the-data-protection-act. Accessed 26 Feb. 2017.
[4] "Schwartz v. Yahoo - Santa Clara Law Digital Commons." http://digitalcommons.law.scu.edu/historical/1291/. Accessed 26 Feb. 2017.

reduced. Admittedly, some staff members would need full database access, but these would generally be more senior staff; their responsibility as part of the company combined with the fact that there are less senior staff than sales assistants means that the likelihood of them being part of an inside job is significantly lower. It would also have the additional effect of ensuring employee negligence (for example, writing down credentials on paper or keeping them unsecured on their computer) wouldn't carry as high a risk factor.

The exploitation of software permissions was highlighted in this attack but this brings up the discussion of other types of permissions as something they may need to deal with, for example physical permissions. If hackers managed to gain physical access to buildings that house data stored by Three, it may have allowed them to access the full customer database or plant malware, a situation that is thought to have caused the massive scale 2014 Sony Pictures hack. The attack is believed to have been caused by a physical intrusion which allowed an unauthorised party to install and distribute malware inside Sony Pictures' internal systems.[5] This malware created a backdoor which allowed the hackers over a long time period to secretly copy confidential files including unreleased films, internal emails and databases before erasing systems and forcing all company computers to display the hackers demands. Obviously this is an extreme example, however it highlights why companies also have to worry about unauthorised parties breaking in in ways that a firewall cannot prevent.

It has been reported that no financial data was stolen in this attack.[6] This may lead you to believe that the implications aren't as severe as they could be. While this is technically true, the people who had their data stolen are by no means safe from identity theft. This is a worldwide issue and reports of it are on the rise. The US Federal Trade Commision has shown a gradual increase in reported instances of identity theft since 1999 with almost 350,000 reports in 2014 in the US.[7] With a few basic pieces of information, experienced fraudsters can gain more information about you, which could eventually lead to a large scale fraud, such as a driver's license or even a credit card taken out in your name. Another possible route someone in possession of a person's data could take is phishing. Phishing is a type of fraud that is based around a malicious party masquerading as a genuine party (often a bank or utility provider) in order to extract sensitive data from someone. An example of this would be an email from a bank requesting that the customer confirm their account details in order to stop their account from closing; they may be taken to a page that looks like a genuine bank form, however the details are sent off to the attacker for later use, be that further fraud or sale. If an attacker holds some data on a person before attempting to phish for more, they can appear more genuine, for example by addressing the victim by name and confirming their name and address to them

---

[5] "Hackers suggest they had physical access during attack on Sony ...." 25 Nov. 2014, http://www.csoonline.com/article/2851649/physical-security/hackers-suggest-they-had-physical-access-during-attack-on-sony-pictures.html. Accessed 26 Feb. 2017.

[6] "Three Mobile hack: how to protect yourself if you've been affected." 18 Nov. 2016, http://www.telegraph.co.uk/technology/2016/11/17/three-hack-how-to-protect-yourself-if-youve-been-affected/. Accessed 26 Feb. 2017.

[7] "Consumer Sentinel Network Reports | Federal Trade Commission." https://www.ftc.gov/enforcement/consumer-sentinel-network/reports. Accessed 26 Feb. 2017.

before asking for more details. This is a technique known as “spear phishing” and it is wildly popular, an estimated 91% of attacks between February and September of 2012 were spear phishing style attacks.[8] If this style of attack becomes commonplace against Three’s customers, consumer trust in the company will fall.

If there’s one thing mobile network providers cannot afford to lose, it's the trust of their customers. With so many networks operating in the UK, most pricing their services competitively, the general population wouldn’t regret switching if it meant peace of mind surrounding the security of their data. This has been displayed recently as a result of the TalkTalk data breach of October 2015. Criminals stole the data of 157,000 customers; the data included names, addresses, phone numbers and, in 16,000 cases, bank account details. As a consequence of this, TalkTalk reported an estimated cost of around £45 million as well as lost revenue from 101,000 customers who cancelled their service with TalkTalk as a result of the breach.[9]

In conclusion, like most other data breaches, the attack on Three UK highlighted many important professional issues. From giving employees the bare minimal permissions they need to effectively do their job to limiting access to the whole system to specific locations, there may have been more the company could have done to suppress the damage an attack like this could cause. Furthermore, the leaking of sensitive data could put the company in violation of the Data Protection Act as well as putting their customers at a high risk of identity theft, something that could have a lasting effect on how the public perceive the company. As criminals become more and more advanced, companies that deal with a large amount of sensitive data must learn from the mistakes of the past and keep up in terms of security, or they face losing consumer confidence, legal battles and ultimately their business.

*Word count: **1351***

[8] "Spear Phishing: Who's Getting Caught? - The DealRoom - Firmex." 30 May. 2013, https://www.firmex.com/thedealroom/spear-phishing-whos-getting-caught/. Accessed 26 Feb. 2017.
[9] "TalkTalk loses 101,000 customers after hack - The Telegraph." 2 Feb. 2016, http://www.telegraph.co.uk/technology/2016/02/02/talktalk-loses-101000-customers-after-hack/. Accessed 26 Feb. 2017.