[0] Hi, I'm Nicholas and today I'll be presenting to you 2 case studies about security breach.

[1] This is my matric card.

[2] So let's get started.

[3] The 2 case studies presented are the Atrium Health data breach and the British Airway Data Breach.

[4] First we will talk about the Atrium Health data breach.

[5] These are the details of the attack.

[6] Security breach was found 2 days after the end of the attack notified by AccuDoc Solutions. AccuDoc Solution is a company that provides IT and payment services for Atrium Health. According to forensics investigations, information of the patients was compromised. Fortunately, there were no signs of download or information being distributed.

[7] The breach was due to a security vulnerability at a third-party vendor. Business relationship with that vendor has already been terminated. Several information of the patients were compromised. Luckily, no sensitive financial information or medical records were affected.

[8] After the incident, AccuDoc collaborated with a forensic firm to ensure that its database is secure. Atrium has also relooked and work with forensic investigative firm to conduct an independent review of the incident. FBI were also activated to investigate this breach.

[9] It's fortunate that the information from both the AccuDoc and Atrium Health systems were unaffected.

[10] Moving on to the key findings. Firstly, Atrium health and AccuDoc failed to perform risk assessment on their third-party vendors, which may cause even more detrimental effect if the data were actually used, copied or sold. Due diligence should be heightened for those vendors with respect to the active protections they employ around Atrium's computing environments and applications.

[11] Also, there weren't any other forms of evaluation done on the third-party. Only business associate agreement was signed, which was inadequate to deter potential cyber threats from the third party's services. Regular checks should be done so as to mitigate the risks of getting its data breached again.

[12] In summary, these are the 2 contributing factors leading to the cyberattack. The security vulnerability of third-party supplier and the failure of Atrium Health and AccuDoc Solutions to do regular safety check with their third-party supplier.

[13] Next, we move on to the British Airways data breach.

[14] These are the details of the attack.

[15] Roughly 380,000 booking transactions made between 21 Aug and 5 Sep 2018 were breached. Name, addresses, email addresses and sensitive payment card details were all compromised.

[16] What's worst is that the data exfiltration breach was found by a third party and not from British Airways. By then, 2 months have already passed. The Information Commissioner's Office (ICO) was then alerted.

[17] The attack links to a criminal hacking gang that was active since 2015, named Magecart.

[18] Magecart is known for web-based credit card skimming. They will find websites that don't use secure payment data entry form or forms with details not deleted after submission.

[19] Moving on to the summary of key events. Threat detection firm RiskIQ pointed out that the payment card expiration dates and CVV were compromised, which refuted the claim from the British Airways.

[20] Thus, cross-site scripting attack was suspected by RiskIQ. Cross-site scripting is one in which bad actors identify a poorly secured webpage component and inject their own code into the webpage to alter the webpage's behaviour. No penetration to an organisation's network or servers is needed.

[21] This is the pictorial description of cross-site scripting.

[22] The script is connected to the British Airways baggage claim information page which hasn't been updated since 2012. The attacker only included 22 more lines of code and managed to grab payment data of the customers from the payment form.

[23] The attackers were so sophisticated that they even paid to set up an SSL certificate for their server. Attackers of all sorts have increasingly used these certificates to help create a sense of legitimacy, even though an encrypted site might not be necessarily safe.

[24] Part of the British Airways Android app was also affected. Malicious JavaScript component the attackers injected have also affected its mobile users. The attackers seemed to have designed the script with the mind of including touchscreen input components as well. The attack was effective as it was tailored to the specific scripting and data flow weaknesses of the British Airways site.

[25] Moving on to the key findings. First, the breach due to failing to implement access limitation. The attack could have been prevented by limiting access to applications and to do rigorous testing, in the form of simulating a cyber-attack on the business' systems.

[26] There were also no early detection from British Airways. Attack was realised after 2 months. Number of people affected, and the potential financial harm could have been more significant.

[27] There were also poor security arrangements. British Airway was not taking proper precautions when rolling out new websites and applications. They should adopt the correct security management infrastructure, knowing at all times what the risks are and being able to find the solutions before the systems are rolled out to the users.

[28] These are some of the statistics of the data breached on various customers data due to British Airways negligence.

[29] This is the timeline of the data breach incident

[30] In summary, no access limitation to the applications, data and tools, no early detection and poor security arrangements contributes to the cyberattack.

[31] With that I end of my presentation. Thank you.