HIGH PROFILE COMPANY DATA BREACHES

Sports Direct (2016)

Cybercriminals stole personal data from over 30,000 members of staff. The company failed to report the breach until months after it happened – they claimed that since the data hadn't been 'copied' there was no need to let the employees know

http://www.bbc.co.uk/news/technology-38918498

https://www.retailgazette.co.uk/blog/2017/02/sports-direct-data-breach-hidden-from-staff-for-months/

HIGH PROFILE COMPANY DATA BREACHES

NHS Trust (2017)

WannaCry ransomware hit the NHS in October 2017, affecting more than a third of trusts in England. At least 6,900 appointments were cancelled as a result of the attack (although up to 19,000 may have been affected in total). Infected PCs had their data encrypted by the attack, which demanded payment of $300 to unlock the machine. It has been suggested that the NHS had not followed cybersecurity guidance, leaving itself vulnerable to attack.

http://www.bbc.co.uk/news/technology-41753022

https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/

http://www.wired.co.uk/article/nhs-cyberattack-ransomware-security

https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack

HIGH PROFILE COMPANY DATA BREACHES

Three (2016)

A Three employee's password was stolen and used to access personal data of over 210,000 customers.

https://www.theguardian.com/business/2016/nov/18/three-mobile-customer-data-breach-phone-upgrade

http://www.bbc.co.uk/news/business-38022309

http://www.telegraph.co.uk/technology/2017/03/14/three-mobile-hack-affected-76000-customers-thought/

Three (2017)

Customers logged into their accounts to see the bill details of another customer – name, address, telephone number, numbers called, bill amount etc.

https://www.theguardian.com/business/2017/mar/20/three-mobile-possible-data-breach-data-usage-call-history

https://www.express.co.uk/life-style/science-technology/782049/three-mobile-another-data-breach-my-3-app