Initial Post

Using the internet has been become essential for many businesses in today’s world. It allows connectivity between the business, its customers and employees (Klaus & Elzweig, 2020). Central to this is remote access to the information stored in databases and it is here that companies have an obligation to prevent unauthorised access to this potentially sensitive data. Whilst the consequences on stock market price of a data breach for a company can vary depending on sector, (Morse et al., 2011) there is always a price to pay whether that is financial, reputational or legal. According to IBM Security (2022), the average cost of a data breach was USD 4.45 million rising to USD 4.82 million for those organisations involved in critical infrastructure.

Equifax, is one of the three major credit reference agencies in the USA. In 2017, it was allegedly hacked by the Chinese military and four individuals have subsequently been indicted for the hack (FBI, 2020). The hackers gained access by exploiting a vulnerability in Apache’s Struts 2 software (Wang & Johnson, 2018). The hackers subsequently accessed the sensitive information of 147.9 million American (Fruhlinger, 2020), 15.2 million UK (McCrank, 2017) and more than 20,000 Canadian (The Canadian Press, 2017) citizens including, names, social security numbers, birth dates, addresses, driving licence numbers and in some instances, credit card details. As of February 2020, this data breach has cost Equifax nearly USD 2 billion (Meltzer, 2020).

References:

FBI. (2020). Chinese Military Hackers Charged in Equifax Breach. Available from: https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020#:~:text=According%20to%20the%20indictment%2C%20Wu,network%20and%20back%2Dend%20databases. [Accessed 17th September 2022].

Frulinger, J. (2020) Equifax data breach FAQ: What happened, who was affected, what was the impact? Available from: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html [Accessed 27th September 2022].

IBM Security. (2022) *Cost of a Data Breach Report 2022*. New York. IBM Corporation.

Klaus, T. & Elzweig, B. (2020) The impact of data breaches on corporations and the status of potential regulation and litigation. *Law and Financial Markets Review* 14(4): 255-260. DOI: https://doi.org/10.1080/17521440.2020.1833432

McCrank, J. (2017). Equifax says 15.2 million UK records exposed in cyber breach. Available from: https://www.reuters.com/article/us-equifax-cyber/equifax-says-15-2-million-uk-records-accessed-in-cyber-breach-idUSKBN1CF2JU [Accessed 27th September 2022].

Meltzer, M. (2020). Equifax says data breach has cost it nearly $2 billion so far. Available from: https://www.bizjournals.com/atlanta/news/2020/02/13/equifax-says-data-breach-has-cost-it-nearly-2.html [Accessed 27th September 2022].

Morse, E. Raval, V. Wingender, J. (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective* 20(6): 263-273. DOI: https://doi.org/10.1080/19393555.2011.611860

The Canadian Press. (2017). Equifax says more than 19,000 Canadians affected by security breach. Available from: https://www.cbc.ca/news/business/equifax-canadians-affected-update-1.4424066 [Accessed 27th September 2022].

Wang, P. & Johnson, C. (2018). Cybersecurity incident handling: A case study of the Equifax data breach. Issues in Information Systems Volume 19(3): 150-159. DOI: https://doi.org/10.48009/3_iis_2018_150-159

Peer Responses

Dear Steve,
Based on you very interesting recent post concerning the hacking incident on the Apache strut software used by Equifax in 2017, I would like to add that the human factor played an important role to allow this attack to be successful. More specifically, on March 7,2017, the Apache software foundation announced that a few versions of its apache strut software had a vulnerability that could allow a possible remote attack on a targeted web application. It was reported that customers in Argentina tried to access their web portal using the insecure credentials (Admin/Admin). According to the article, Apache, has offered to its customers a security patch with clear instructions on how to deal with this vulnerability. Equifax, decided to ignore the warnings and to not proceed with the update of their apache software struts with the latest released patch.[1]
As a consequence, the data breach took place two months later by 4 Chinese hackers. The data breach was not easily detected because the hackers store the large data files into compressed and small size files. Afterwards, they deleted the compressed files which helped them to show minimum trails during that operation. The fact that they had managed to access the Equifax network, helped them to use the credit firm secure communication channels. Equifax has communicated this incident to its customers 6 weeks later. The impact was huge for the reputation of Equifax that suffered also huge financial losses. However, the one that were mostly affected were the 147.9 million people (almost half of the US population) whose confidential data such as their social security numbers had been exposed. The US-China relationships had also been affected. These two facts, the lack of response by Equifax personnel to the announcement of Apache and the decision to not perform the recommended updates by Apache is a indication that the human factor is an important element of the Cyber security.[2]

1. Brian Barret (2017) How 4 hackers allegedly took down Equifax. Available from: https://www.wired.com/story/equifax-hack-china/ [Accessed 29 September 2022].
2. Brian Barret (2017) Equifax officially .Available from: https://www.wired.com/story/equifax-breach-no-excuse/ [Accessed 29 September 2022].

Hi Steve,
Your post and information are both well researched and fairly shocking, it made me think about the sheer amount of money spent on cybersecurity in companies. It’s interesting to see that even within the UK the south and the north businesses have varied opinions on the importance of cybersecurity. 51 % of businesses in London are more likely to see cybersecurity as a very high priority than others. 71% of businesses in the north of England are less likely to view cybersecurity as a high priority. It seems it’s not just the size of the company that affects the outlook of security. If we look at the cybersecurity survey (UK) in 2019 businesses on average lost £4,180 annually due to data loss from breaches, and charities lost £9,470 annually. It seems that from at least 2017-2019 there has been a decrease in breaches reported by businesses (46%-32%). This can be due to companies becoming more cyber aware and secure; however, it could also be a change in the attacker's aims and them narrowing in on certain types of businesses and certain types of “rewards” (Vaidya, 2019).

It's interesting to see from your post how companies can be struck by one event and must pay billions to fix/clean up the situation, it’s important for us as emerging experts in this field to remember not all companies that are affected are huge international businesses, but rather every company that uses any kind of online interaction needs to implement security in their businesses. The best way to stop or reduce cyber-attacks is to increase awareness of the severity and how they can be prevented.

Thank you!

Works Cited

Vaidya, R. (2019). *Cyber Security Breaches Survey 2019.* London: Department for Digital, Culture, Media & Sport.

Dear Steve,
This is an illuminating piece Steve.
Emenike (2021) also pointed out that organizations are been affected to data loss due to breaches that occur due to increase remote working by employees during the COVID-19 pandemic. Emenike (2021) further elaborated that most of these organizations normally have a poor security posture, threat and incident management and risk management. Snyder (2022) concurred by indicating that organizations should have clear strategic plans for ransomware attacks. This will ensure that they are able to prevent or quickly recovery from such an attack and hence protect their reputation (Snyder, 2022). Shrivastava, Hazarika and Rea (2021) along similar lines also indicated a cyber-attack does not only lead to disruption of operations, but also to loss of capital, data and reputation.

References

Emenike, S.U., 2021. Data loss prevention in a remote work environment. Masters dissertation, University of Skovde.
Snyder, D.L., 2022. A Qualitative Meta-synthesis on the Benefits of Planning for

Ransomware Attacks at a Strategic Organizational Level. Doctoral dissertation, Colorado Technical University.
Shrivastava, U., Hazarika, B. and Rea, A., 2021. Restoring clinical information system operations post data disaster: the role of IT investment, integration and interoperability. Industrial Management & Data Systems

Discussion 1: Summary Post

My original post focussed on the 2017 Equifax hack and its consequences.

As Antonios points out in his post, the human factor played a huge role in the hack and subsequent consequences of this security breach.

Threat actors exploited a known vulnerability in the Apache Struts software which was used by Equifax to build a client resolution portal (GAO, 2018). The vulnerability was identified, and a patch released on 7/3/2017 (Ullrich, 2017). From this point on, a litany of failures resulted in the initial hack and the subsequent exfiltration of data. These include not applying a patch to the Struts software when instructed to by the vendor and not renewing a public key certificate which meant that encrypted data being exfiltrated by the threat actors was not being inspected by network monitoring tools. Equifax management then chose not to disclose the hack until 6 weeks later (it was later alleged that company executives sold stock during this period to limit their financial losses once the breach was announced; one executive was charged in this respect (Moyer, 2018) Even then, the company's official communication channels kept directing customers to an incorrect web address where clients could see if they had been affected and when clients did eventually get to the correct site, Equifax tried to limit its legal liability by advising customers that just by using the site they forfeited their rights to sue over the breach. The result has been a USD 2billion cost in court settlements and upgrades and huge reputational damage (Meltzer, 2022).

Whilst interesting in themselves, Daniel's comments regarding working from home and protection against ransomware attacks were not relevant to this case, but his point about the consequence of a security breach is well made as demonstrated above.

I enjoyed reading Stella's input regarding the attitudes of different companies to the risk of cyber threats, the trend in related costs and possible reasons for these trends. In this case, Equifax had spent a great deal of money on cyber security since 2005 (Riley et al.) but a system is only as strong as its weakest link. In this case the human factor was by far the weakest link and coupled with poor management oversight, a failure to segregate different parts of its network and a general lack of system resilience, resulted in one of the largest data breaches in history.

References.

GAO. (2018) *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach,* GAO-18-559. Washington, D.C.

Meltzer, M. (2020). Equifax says data breach has cost it nearly $2 billion so far. Available from: https://www.bizjournals.com/atlanta/news/2020/02/13/equifax-says-data-breach-has-cost-it-nearly-2.html [Accessed 27th September 2022].

Moyer, L. Former Equifax executive charged with insider trading for dumping nearly $1 million in stock ahead of data breach. Available at: https://www.cnbc.com/2018/03/14/former-equifax-executive-charged-with-insider-trading-ahead-of-data-breach.html [Accessed 10th October 2022].

Riley, M. Robertson, J. Sharpe, A. (2017) The Equifax Hack Has the Hallmarks of State-Sponsored Pros. Available from: https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros [Accessed 10th October 2022].

Ullrich, J. (2017) Critical Apache Struts 2 Vulnerability (Patch Now!) Available from: https://isc.sans.edu/diary/22169 [Accessed 10th October 2022].