Moseli Ts'oeunyane

Initial Post

Sunday, 20 March 2022, 8:56 PM

3 replies

Last Thursday, 24 March 2022, 3:04 AM

Information and communications technology are undoubtedly at the core of our modern life, impacting various aspects of modern civilization. With advent of newer technologies and digitization, the cyber threat landscape is continuously increasing and poses significant risks that, without proper mitigations, could prove catastrophic, impacting the confidentiality, integrity and availability of information systems and data.

Businesses typically build their models around trust; it is fundamental to any organization. Any cyber related incident can lead to severe reputational damage hence broken trust and loss of customers and these represents direct revenue loss. Moreover, regulatory bodies are becoming more involved and are enforcing stronger laws and regulations. In recent times, Yahoo had one of the biggest data breaches, exposing data from over 3 billion accounts. What then followed was fines against Yahoo, with Securities and Exchange handing them $35 million for failure to declare the incident, while they also had a class action settlement of $80 million (McAndrew E.J, 2018)

Whilst the attacks on data are getting more complex, they are just a component of the issues facing businesses as the skills gaps for the cyber security profession widens (Rafferty B, 2016). The highly critical Cyber Security skills gap has been widely documented and continues to be a burning topic globally. From their report, Herjavec Group (2018), provided an estimate of 3.5 million vacant positions within cyber security by the year 2021. It is has become more important than ever for institutions, organizations and governments to have solid plans around cyber security talent pools as cyber crimes become more prevalent and are a threat to modern life as we know it.

Bibliography:

McAndrew, E.J. (2018) The Hacked & the Hacker-for-Hire: Lessons from the Yahoo Data Breaches (So Far). Available from: **https://www.natlawreview.com/article/hacked-hacker-hire-lessons-yahoo-data-breaches-so-far** [Accessed on 18 March 2022].

Herjavec Group (2018). Cybersecurity Jobs Report. Available from: **https://eadn-wc01-3468285.nxedge.io/cdn/wp-content/uploads/2018/11/HG-and-CV-Cybersecurity-Jobs-Report-2018.pdf** [Accessed on 19 March 2022]

Troncoso, C. (2019) Privacy & Online Rights Knowledge Area Issue 1. The Cyber Security Body of Knowledge. Available from: **https://www.cybok.org/media/downloads/Privacy__Online_Rights_issue_1.0_FNULPel.pdf** [Accessed 19 March 2022].

Post by **Fabrice Wouche**

Re: Initial Post

Thursday, 24 March 2022, 3:04 AM

Hi Mosely,

I'm totally in agreement with your above statement regarding reputational damage and lost of customer. As reputation loss after a cyberattack can have a major impact on businesses whether small, medium, or large organisations. According to Aon's Global Risk Management Survey (2019), cyber-attack is the number one risk for reputational damage for UK businesses. The report also emphasise how a company's brand and reputation are connected; therefore, it is crucial how organisations manage and mitigate their cyber risk.

When a scandal of cybercrime happens, especially if high profile individuals are impacted, it gives the impression to the public that the organisation has of poor cybersecurity culture, consequently customers trust, and most likely revenue lost and market competitiveness. A good example is the incident on twitter 2020 by a 17-year-old who managed break into Twitter's network and took control of high-profile users such as Barack Obama, Elon Musk, and few others. The same day the company share price dropped by 4% resulting to million of revenue lost (Cybersecurity in the COVID-19 Pandemic, 2022).

CNBC (2019) pointed out that cyber-attacks cost on average $200,000 to companies. After a breach nearly 60% of small companies close within 6 months (60 Percent of Small Companies Close Within 6 Months of Being Hacked, 2022). Therefore, we can agree that the reputation damage on small and medium organisations isn't the same on large organisations which are better equipped in case of reputational damage and loss of customers, where from small and medium companies such scandal can prove devastating.

Regarding the shortage of labour in the field of cybersecurity, the University of San Diego (n.d) emphasise that, the shortage of workers isn't the main issue but skills gap in the field is, As the field is constantly evolving due to the various and innovative tactics used by the cyber criminals.

Google Books. 2022. *Cybersecurity in the COVID-19 Pandemic.* [online] Available at: **https://www.google.co.uk/books/edition/Cybersecurity_in_the_COVID_19_Pandemic/qPkWEAAAQBAJ?hl=en&gbpv=1&dq=inauthor:%22Kenneth+Okereafor%22&printsec=frontcover** [Accessed 24 March 2022].

Cybercrime Magazine. 2022. *60 Percent of Small Companies Close Within 6 Months of Being Hacked.* [online] Available at: **https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/** Accessed 24 March 2022].

n.d 2022. [online] Available at: **https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html** [Accessed 24 March 2022].

University of San Diego Online (2015) Getting a Degree in Cyber Security 8 Important Considerations. Available from: **https://34co0u35pfyt37c0y0457xcu-wpengine.netdna-ssl.com/wp-content/uploads/2015/12/USD_Cyber_eBook_Final.pdf** [Accessed 28 February 2022].