Collaborative Learning Discussion 1

Initial Post

Cybersecurity is vital because it defends against the theft and loss of all forms of data. This category includes sensitive personal data, personally identifiable information (PII), protected health information (PHI), intellectual property, data, and public and private sector information systems. Without a cybersecurity programme, a firm is powerless to protect from data breach efforts, an unavoidable target for cyber attacks. As a result of global connectivity and the expanding usage of cloud services and e-commerce, both inherent and residual hazards are increasing.

E-commerce has advanced at a rapid rate during the previous decade. Following the internet's global expansion, e-commerce became the next major revolution. Numerous businesses have pushed the boundaries of e-commerce but have fallen short of security standards. A significant data breach involving Australia occurred at eBay, where a computer hacking attempt revealed up to 145 million consumers' personal information. According to eBay, the breach occurred in 2014 as a result of a small number of employee credentials being compromised. These credentials were used to obtain access to personally identifiable information (PII) about customers. Financial institutions also suffered losses as a result of the hack, as evidenced by the need to reissue cards and update payment systems. These losses were estimated to be in the neighbourhood of $200 million.

According to VanSyckel (2018), for every action to store, secure, and use data, there is an equal or greater reaction to stealing data. Another instance, LinkedIn allegedly suffered a catastrophic data breach in 2021, with over 700 million users' personal information being sold on the dark web. LinkedIn was the victim of many cyber breaches, with over 500 million users' data being sold on the dark web, according to Privacy Sharks. Whether the latest intrusion and the previous cyber-attack are connected is unknown at the moment. According to the most recent disclosure, the breach affected 92% of LinkedIn's 756 million users.

For instance, “ According to a 2020 research report by IBM (NYSE:IBM), a single data breach event could cost an organization US$3.86 million” (Pistilli, M). To summarise, the key reasons an organisation should invest in cyber security are to maximise profit, retain customers and the company, and mitigate the hazards connected with remote working.

References:

"The significance of mandatory data breach warnings to identity crime" Eric Holm Bond University and Geraldine Mackenzie Bond University dated on 1-1-2014

"Attacks on Ebay" By: Jaspuneet Sidhu, Rohit Sakhuja & David Zhou; https://www.eecs.yorku.ca/course_archive/2015-16/W/3482/Team12_eBayHacks.pdf

"HOW CYBER SECURITIES PLAY AN IMPORTANT ROLE FOR ANY ORGANIZATION" International Journal of Engineering Applied Sciences and Technology, 2020 Vol. 5, Issue 3, ISSN No. 2455-2143, Pages 280-282. Published Online July 2020 in IJEAST (http://www.ijeast.com) by Rahul Kumar Chawda Department Of Computer Science, Kalinga University

Pistilli, M. (2021, June 24). Why is Cyber Security Important? Investing News. https://investingnews.com/daily/tech-investing/cybersecurity-investing/why-is-cybersecurity-important/.

Initial post-Unit-1-Discuss why Cyber Security is now a global issue and why it is important for companies to invest in Cyber Security.pdf