Initial Post

Cybersecurity is one of the fastest growing industries globally, as supported by Plachkinova and Pittz (2021). The demand for cybersecurity is due to the increase in cyber-attacks and data breaches to companies around the world. Cyber-attacks pose a threat to companies as they migrate to the digital online world. Furthermore, the risk of cyber-attacks is intensified through the use of IoT (Internet of Things) devices connected to the internet (Danso, 2021). According to the Global Risks Report 2021 approximately 40% of the World Economic Forum (WEF) respondents forecasted that cybersecurity will become a critical threat to the world within the next two years affecting the global economy (Mclennan, 2021).

In November 2018 Marriott International (a US-based hospitality company) announced a data breach in their network affecting approximately 500 million guests. Marriot acquired Starwood in the year 2016 however according to Marriott’s investigation led by cyber security experts’; hackers gained unauthorized access to the Starwood network in 2014 (Starwood hotels, 2018). This is a typical example of an Advance Persistent Threat (APT) attack where hackers gain access to the network and remain hidden for a long period of time to gather information (Danso, 2021). According to VanSyckel (2018) APT attacks tend to be the most dangerous form of cyber-attacks. Personal Identifiable Information (PII) such as credit card details, travel itineraries, passport numbers, etc. of Starwood’s client base were exposed. As a result of the data breach, a fine amounting $122 million was imposed on Marriott by the General Data Protection Regulation (GDPR) authority (Daigle & Khan, 2020).

Cyber-attacks are constantly evolving and becoming more sophisticated in the present day affecting the global economy. The acts of cyber criminals’ results in companies losing millions in revenue every year (Lewis & Crumpler, 2019) as confirmed in the Marriott case study. This warrants companies and organizations the demand to invest in cybersecurity practices to predict, prevent, detect, and respond to possible cyber-attacks efficiently and successfully. Fines imposed by the GDPR authority are hefty and the reputational damage, financial loss and customer confidence to any organization can be detrimental to its success.

**LIST OF REFERENCES**

Daigle, B. & Khan, M. (2020). The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities. *Journal of International Commerce and Economics* 332(1): 13-14. Available from: <https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf> [Accessed 13 August 2021]

Danso, S. (2021) *Launching into cyber security* [Lecturecast].LCYS\_PCOM7E August 2021 Launching into Cyber Security. University of Essex Online.

Lewis, A J, & Crumpler, W., Center for Strategic and International Studies. (2019) *The cybersecurity workforce gap*. Available from: <https://apo.org.au/node/219801> [Accessed 12 August 2021].

Mclennan, M. (2021). *The Global Risks Report 2021 16th Edition Insight Report.* Geneva: World Economic Forum. Available from: <http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf> [Accessed 13 August 2021].

Plachkinova, M, & Pittz, T. (2021) Assessing the Awareness of Cybersecurity Within Entrepreneurship Students: The Cyberpreneurship Project, *Entrepreneurship Education and Pedagogy* 4(3): 564–582. Available from:

<https://journals.sagepub.com/doi/abs/10.1177/2515127420913056> [Accessed 12 August 2021].

Starwood hotels. (2018). *Original notice from November 30, 2018*. Available from: <http://starwoodstag.wpengine.com/wp-content/uploads/2019/05/us-en_First-Response.pdf> [Accessed 13 August 2021]

VanSyckel, L (2018) *Sealevel Systems White Paper - Introducing Cybersecurity*. Available from <https://www.sealevel.com/support/white-paper-introducing-cybersecurity/> [Accessed 13 August 2021]