Summary Post

Monday, 21 March 2022, 10:33 AM

3 replies

Last Sunday, 27 March 2022, 5:08 PM

International Concern for Cyber Security

The World Economy, with all of its multifaceted components, is at an existential crisis.
Hackers are threatening to destroy the world, and this is only possible, due to the interdependence of networked computers (Machin, 1998). Geopolitical states and administrative regions are now facing threats, that have never existed before the 20th Century (Jensen, 2002).

This paper explores various aspects of concern and aims to highlight the dire need for cybersecurity professionals.

Financial Systems

The Global Financial System is dependent on the inter-operational (or networked) activities of various institutions. Some important facilitators of these activities include SWIFT, as well as the Mercantile and Retail Banking sectors. Both Rachwald (2008) and Camillo (2017) agree that black-hat hackers have sufficient potential to cripple these institutions and cause devastating financial repercussions.

SWIFT itself has been compromised on multiple occasions, most notably with a 2016 case which resulted in $81 million theft from a Bangladesh Central Bank account. The perpetrator's actual goal was around $1 billion (Camillo, 2017: 197).

Data Privacy

When Data Privacy became a global concern, hefty fines and punitive measures became sanctioned. Businesses and Individuals are paying the price for not abiding by regulations, with fines leading all the way up to €50 million (Koch, 2020).

The effectiveness of these correctional measures are still somewhat disputable (Grant, 2016).

Industry

According to Chen (2010) and Hobbs (2021) the consequences of hacking firmware within nuclear power plants or gaining access to gas and petroleum pipelines can be catastrophic. Even self-operating machinery within factories are targets (Gong et al, 2020).

Since industry employs such a large number of people, then surely if hackers compromise the integrity of operational plants, livelihoods and profits would thus be at stake.

Solution

In a changing world, corporations need to safeguard their assets, by hiring competent and well educated cybersecurity staff. These professionals are trained in organizational risk mitigation strategies to address and prevent the scenarios mentioned within this paper.

References

Camillo, M. (2017) Cybersecurity: Risks and management of risks for global banks

and financial institutions. *Journal of Risk Management in Financial Institutions*, *10*(2): 196-200.

Chen, T.M. (2010) ‘Stuxnet, the real start of cyber warfare?’ [Editor's Note]. *IEEE Network*, *24*(6): 2-3.

Gong, Y., Chow, K.P., Mai, Y., Zhang, J. & Chan, C.F., (2020) Forensic investigation of a hacked industrial robot. *International Conference on Critical Infrastructure Protection*. Springer, Cham: 221-241.

Grant, H. & Crowther, H. (2016) How Effective Are Fines in Enforcing Privacy?. *Enforcing Privacy*. Springer, Cham. 287-305.

Hobbs, A. (2021) *The colonial pipeline hack: Exposing vulnerabilities in us cybersecurity*. Newbury Park: SAGE Publications.

Jensen, E. (2002) Computer attacks on critical national infrastructure: A use of force invoking the right of self-defense.

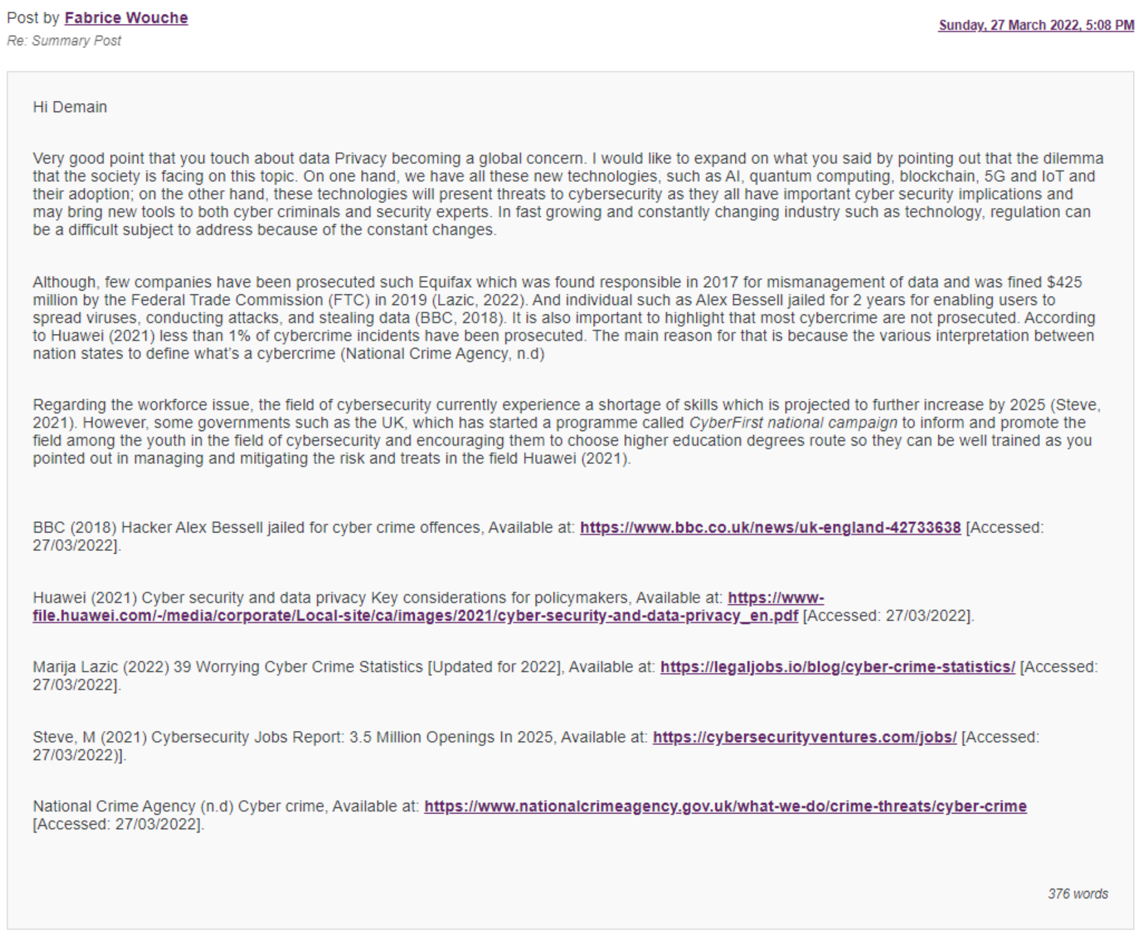
Stan. J. Int'l L., *38:* 207.

Koch, R. (2020) GDPR fines. Available from: https://gdpr.eu/gdpr-requirements-data-breach-reporting/ [Accessed 11 Mar 2022]

Machin, S. & Van Reenen, J. (1998) Technology and changes in skill structure:

evidence from seven OECD countries. *The quarterly journal of economics*, *113*(4): 1215-1244.

Rachwald, R. (2008) Is banking online safer than banking on the corner?. *Computer Fraud & Security*, *2008*(3): 11-12.



Post by **Fabrice Wouche**

Re: Summary Post

Sunday, 27 March 2022, 5:08 PM

Hi Demain

Very good point that you touch about data Privacy becoming a global concern. I would like to expand on what you said by pointing out that the dilemma that the society is facing on this topic. On one hand, we have all these new technologies, such as AI, quantum computing, blockchain, 5G and IoT and their adoption; on the other hand, these technologies will present threats to cybersecurity as they all have important cyber security implications and may bring new tools to both cyber criminals and security experts. In fast growing and constantly changing industry such as technology, regulation can be a difficult subject to address because of the constant changes.

Although, few companies have been prosecuted such Equifax which was found responsible in 2017 for mismanagement of data and was fined $425 million by the Federal Trade Commission (FTC) in 2019 (Lazic, 2022). And individual such as Alex Bessell jailed for 2 years for enabling users to spread viruses, conducting attacks, and stealing data (BBC, 2018). It is also important to highlight that most cybercrime are not prosecuted. According to Huawei (2021) less than 1% of cybercrime incidents have been prosecuted. The main reason for that is because the various interpretation between nation states to define what's a cybercrime (National Crime Agency, n.d)

Regarding the workforce issue, the field of cybersecurity currently experience a shortage of skills which is projected to further increase by 2025 (Steve, 2021). However, some governments such as the UK, which has started a programme called *CyberFirst national campaign* to inform and promote the field among the youth in the field of cybersecurity and encouraging them to choose higher education degrees route so they can be well trained as you pointed out in managing and mitigating the risk and treats in the field Huawei (2021).

BBC (2018) Hacker Alex Bessell jailed for cyber crime offences, Available at: **https://www.bbc.co.uk/news/uk-england-42733638** [Accessed: 27/03/2022].

Huawei (2021) Cyber security and data privacy Key considerations for policymakers, Available at: **https://www-file.huawei.com/-/media/corporate/Local-site/ca/images/2021/cyber-security-and-data-privacy_en.pdf** [Accessed: 27/03/2022].

Marija Lazic (2022) 39 Worrying Cyber Crime Statistics [Updated for 2022], Available at: **https://legaljobs.io/blog/cyber-crime-statistics/** [Accessed: 27/03/2022].

Steve, M (2021) Cybersecurity Jobs Report: 3.5 Million Openings In 2025, Available at: **https://cybersecurityventures.com/jobs/** [Accessed: 27/03/2022)].

National Crime Agency (n.d) Cyber crime, Available at: **https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime** [Accessed: 27/03/2022].

376 words