Great points, Kwok Wai Yau and Demian. This discussion is really interesting and reminds me of an article I read regarding physical security. Cyber security is a broad range of topics but another aspect that should be taken into consideration is physical security. How do we know that people

entering an organisation are actually authorised to be there?

Once access to the organisation has been gained, the intruder could potentially steal data from a stand alone device, as long as the data is

accessible via a USB. The article I am referring to explains how important it is that physical security and cyber security teams need to work hand in hand to maintain a lockdown on the assets.

As the digital footprint grows on devices like surveillance monitoring and CCTV that connect to the internet and generate digital logs, these logs need to be reviewed regularly. The article also states that the key to safeguarding assets is to make employees aware of their environment such as access controlled areas which are only for authorised individuals and to provide education on cyber security.

Swinhoe, D.(August 4, 2021)

What is physical security? How to keep your facilities and devices safe from on-site attackers. Available from: https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html [Accessed 14 March 2022]