In my initial post, I mentioned the growth if cybersecurity during the pandemic and exposure of the various vulnerabilities and the unpreparedness of organisations.

Thank you Shailender for your response. I agree with you that it's the employee's responsibility to ensure that their network is secure and bringing the security risks into play outside the organisation. As rightfully stated, that it's the IT administrator to ensure that the organisations network is secure however, there are some circumstances that employees would require to access the organisations via Virtual Private Network (VPN) to be able to access files. Organisations have deployed VPNs on their network to enable employees to remotely access the organisations network.

Although organisations have deployed the use if VPNs there are some security concerns and problems to deploying VPNs. There are third party vendors that may follow the practices that are not optimal. (7 Common VPN Security Risks & Issues | SecureLink, 2022). Hence the choice of VPN should be chosen wisely by the IT administrator.

Prior to the pandemic, virtual platforms for meetings were not popular as not many people were aware of this mode of communication. During the Covid-19 pandemic, businesses began to get to know about various online platforms such as Zoom, Microsoft Teams, Google Meets, etc. Zoom of the one of many online platforms for virtual discussions, the number of users expediently grew from 10 million users to 300 million users during December 2019 to April 2020. (Zoom security issues: What's gone wrong and what's been fixed, 2022).

The encryption was not end-end in which cyber-criminals too advantage of this vulnerability as Zoom were not expecting a substantial growth over a short period of time. As discussed over the 3 units so far, there are countermeasures in place to mitigate the security risk. One of them being 2-Factor-Authentication which Zoom implemented to protect the user's account. In addition, they improved the end-end encryption. (Zoom security issues: What's gone wrong and what's been fixed, 2022).

In this module so far, I learnt that it is vital to ensure that there are policies and procedures in place to mitigate the security risk of potential threats and are regularly updated continuously.

References:

- SecureLink. 2022. *7 Common VPN Security Risks & Issues | SecureLink*. [online] Available at: <https://www.securelink.com/blog/vpn-problems/> [Accessed 25 March 2022]
- Tom's Guide. 2022. *Zoom security issues: What's gone wrong and what's been fixed*. [online] Available at: <https://www.tomsguide.com/news/zoom-security-privacy-woes> [Accessed 25 March 2022].