Thank you for your informative post Austin. As you have comprehensively discussed, antivirus software has a part to play in improving security measures. Still, it needs to evolve with emerging new threats faced and is not an all end solution. Whilst antivirus has become an adopted procedure for most companies critical infrastructure systems; vulnerabilities have decreased over the years to see the future progress of antivirus is somewhat unpredictable (Eronen et al., 2009). We can assume this is due to the human factors surrounding the issues. The files generally being scanned are from the user's input which means there are prone for errors to emerge and with some many formats vulnerabilities can occur through the unpacking and decompression phases. The software itself can trust the incoming files too much, and end users can also trust the software. There is also the issue of a reduction in performance which can inhibit the end-user, and, as mentioned, the solution is not complete protection itself. It would need support from a firewall or intrusion prevention system (Roomi, 2019). The risk of becoming infected by malware leaves antivirus a practical option. Overall, antivirus software plays a role in preventative measures however can be considered not as effective unless accompanied by other technologies.

Eronen, J., Karjalainen, K., Puuperä, R., Kuusela, E., Halunen, K., Laakso, M. & Röning, J. Software Vulnerability vs. Critical Infrastructure - a Case Study of Antivirus Software. 2009.

Roomi, M. 2019. *Drawbacks & Benefits of Antivirus Software* [Online]. Available: https://www.hitechwhizz.com/2020/03/6-advantages-and-disadvantages-drawbacks-benefits-of-antivirus-software.html [Accessed 27 September 2021].