Thank you all for the feedback on this discussion. I have enjoyed reading this thread and found the insight valuable. I have to agree with all the points that have been mentioned. However there were one or two comments that resonated with me. Amit made a great comment on the company's ability to compete after loss of property and it reminded me of Sony security breach, which was made an example of where previous attempted attacks did not send warning signs to the management team to tighten up the security electronically or physically. A large sum of money was stolen from the firm and personal and sensitive data was leaked.

Moseli, your comment on human error being the top cause for data breaches got me curious and reminded me of the key catch phrase: you are only as strong as the weakest link. There is a great article that goes into the details where companies have had a security breach due to the attacker tricking an employee to provide a password to allow for a security breach to occur. To overcome these attacks some systems go further to provide multi-factor authentication, which is providing two factors of authentication to determine the person accessing the data is actually who they say they are compared to single factor authentication. However some can argue at what point does security stop productivity and revenue generation.

DeSot T (2015) 8 Lessons to Learn from the Sony Breach. Available from : https://www.securitymagazine.com/articles/86649-lessons-to-learn-from-the-sony-breach [Accessed 22 March 2022]

Chertoff, M and Grant. (2017) 8 Ways Governments Can Improve Their Cybersecurity. Available from : https://hbr.org/2017/04/8-ways-governments-can-improve-their-cybersecurity [Accessed 22 March 2022]