Thank you, Jitesh some very insightful points made.

As mentioned in the British Airways case, Advanced Persistent Threats are grave concerns for companies and are considered highly severe for cybercrime. (VanSyckel, 2018) indicates such attacks usually form from a network probe by finding a vulnerability or used an employee access gateway. Very much unscrupulously, the infiltrator would be undetected whilst storing information and performing malicious measures.

The notion that attackers go undetected with malicious activities is highlighted by (Williams, 2019) by using the Pone Institute report that the average time for detecting a breach was 197 days. Further, to fix a vulnerability, a patch could take, on average, 67 days to be implemented.

Thereby, the importance of investment by companies is weighted further so that responses to cyberattacks can be swift and decisive, so the company does not incur any further negative financial implications to their business.

Vansyckel, L. 2018. *Sealevel Systems White Paper - Introducing Cybersecurity.* [Online]. Available: https://www.sealevel.com/support/white-paper-introducing-cybersecurity/ [Accessed 12 August 2021].

Williams, L. 2019. Secure Software Life Cycle, Knowledge Area Issue 1. *The Cyber Security Body of Knowledge.*