Hi Kwok, Thanks for your comments, I really appreciate it. I found the comment on multi-factor authentication very interesting. With the on-going pandemic, most organiasations have adapted to working from home for all employees. Organisation's now need to protect themselves from an extended network that is not part of their domain. Having a single password is not enough. However, it is questionable whether having multi-factor authentication is actually enough. David Harding, SVP and Chief Technical Officer of ImageWare Systems has said “Even two-factor authentication on its own has significant vulnerabilities that can be exploited.” (www.globenewswire.com, 2019)

The BBC previously reported that 2FA had been compromised for the co-founder and chief executive of Twitter, Jack Dorey; The phone number associated with his Twitter account was compromised. This technique is known as simswapping, where a sim card is reassigned to a hackers phone allowing them to take control of your number.

A slightly older attack is the RSA SecurID two-factor product, where an employee opens an email, which can lead to a virus attack on the token and impacted a number of customers using the hardware. Although 2FA is just another layer of protection, it shouldn't be limited to just a device or token but to a biometric authentication like finger print or iris.

Reference:

Chabrow, E (April 4, 2011)

Tricked' RSA Worker Opened Backdoor to APT Attack. Available from : https://www.bankinfosecurity.com/tricked-rsa-worker-opened-backdoor-to-apt-attack-a-3504 [Accessed 15 April, 2022]