Hi Haseeb,

Thanks for your great post with a lot of reference data. According to the organizations move online remote work due to the COVID-19 pandemic, organizations should be aware of the new challenges in the security breaches. With the exploded online conference providers, Zoom, Microsoft Teams, and Slack, the business customers and revenue have been increased dramatically since 2019. The fastest-growing apps, Zoom, compared with the Q3 FY 2020 (97 billion meeting minutes), annual Zoom meeting minutes have (3.3 trillion meeting minutes) increased by 3300%, in Q3 FY 2021 (Brian, 2021).

Great reward often comes great risk, the security issue in the software came to the surface in a year like end-to-end encryption controversies, unauthorized meeting disruptions, data handling issues and privacy concerns, software vulnerability… etc. In August of 2021, Zoom has agreed to pay $85 million and bolster its security practice to settle the lawsuit alleging that it shared users' personal information without permission with Facebook, Google, and LinkedIn, as well as allow hackers to break into virtual meetings in the platform during the pandemic. (Alison, 2021).

This is an example that shows the costs of playing cybersecurity catchup. An organization without a good security plan start from the beginning, even they have hired and buy a security company to fix and enhance the security, they still must settle a large amount of cost for security breaches on the information protection.

Brian, D. (Mar 10, 2021) Zoom User Stats: How Many People Use Zoom in 2021?. *Backlinko*. Available from: https://backlinko.com/zoom-users [Accessed 20 Aug 2021].

Alison, R. (Aug 5, 2021) Zoom has to pay $85 million to people for privacy issues. Here's how to claim your money. *Cnet*. Available from: https://www.cnet.com/tech/services-and-software/zoom-has-to-pay-85-million-to-people-for-privacy-issues-heres-how-to-claim-your-money/

[Accessed 20 Aug 2021].