Risk of the digital transformation in the health care sector

The more digital our world becomes, the more vulnerable it is. The fact of how fast the volume of data is increasing is frightening. Big Data has not only advantages but also potential risks. Since Big Data plays a role in almost all areas of our society, I will focus on just one area (AlMadahkah, 2016). The health care sector is suffering from an increase in cyber security risk. Data was manipulated for 81% of 223 organisations surveyed and more than 110 million patients in the US in 2015 alone. The causes of the big data cyber-attacks in the health care sector are more than just attractive. Here are a few aspects of why hacker attacks the health care sector:

- Data theft for financial gain: Stealing personal data to make money.

- Data theft with consequences: Stealing sensitive medical information from celebrities, politicians or other high-ranking persons.

- Ransomware: Blocking access of user accounts in order to earn money to reopen it.

- Data falsification: Deliberate falsification to manipulate test results for political or personal reasons. (Based on my observation, the covid pandemic has boosted this argument. People manipulate their vaccination status to obtain freedom for a political reason).

- Disruption of Services: Network or system interruption by overloading it with millions of requests for revenge, extortion or activism.

- Business email compromise: fake personal communication for a financial reason like obtaining funds.

- Uncertainty: Employees deleting sensitive data unintentionally by using an updated and risky system (Martin et al., 2017).

"Some say that people are the biggest risk of cyber security". Of course, if there were no people who attacked the health care system, no risks would occur. However, these arguments above give the people reasons for attacking the health care sector. Since digitalisation will constantly increase, cybersecurity is increasingly in demand. Organisations like the International Organisation for Standards (ISO) and International Electrotechnical Commission (IEC) need it all the more in the future to update the information security standards.

References:

AlMadahkah, A., M. (2016) Big Data In computer Cyber Security Systems. *IJCSNS International Journal of Computer Science and Network Security* 16(4): 1-10.

Martin, G. et al. (2017) Cybersecurity and healthcare: how safe are we?. *BMJ* 358: 1-4. DOI: https://doi.org/10.1136/bmj.j3179