The WannaCry attack is a particularly shocking example for the NHS. None of the hospitals affected had properly patched systems, and mostly used legacy equipment (Ghafur, 2019). The attack would most likely have been preventable, had a more rigorous approach to cyber security and risk management been in place. As you rightfully pointed out in your conclusion, staff training and awareness of the correct use of the network are absolute musts.

Another area where the NHS has had issue in the past is data protection. Data from the Hospital Episodes Statistics (HES) database became available on Google Cloud in 2014, via a third party. More recently, in 2018, Public Health England gave all records of patients who underwent lung cancer treatment in England to a tobacco company. (Anderson, 2020).

Handing over data without patient consent is unforgiveable and a less lacklustre approach to cyber security could have prevented the WannaCry attack (or at least mitigated the outcomes). Overall, I think the NHS and the UK government need to do more to protect the privacy of patients. Would you agree with this assessment or is the “Data Security Centre” proving sufficient?

References

Anderson, R. (2020) *Security engineering: A guide to building dependable distributed systems.* Indianapolis, Indiana: John Wiley & Sons, Inc. DOI: 10.1002/9781119644682

Ghafur, S., et al. (2019) A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digital Medicine* 2(98): 5-6. DOI: 10.1038/s41746-019-0161-6

I enjoyed this post, and agree that cyber security is now a global imperative. The UK government seem to agree with this. In 2021, they launched the “Integrated Review”, which outlines the government’s security policy. A new approach to cyber security was outlined in the review, and the UK government are going to be investing heavily in the area (Miller, 2023).

We’ve already seen cyberweapons in use. The USA have used “Stuxnet” to attack Iran’s nuclear facilities; Russia have also used “NotPetya” to inflict millions of dollars worth of damage to firms in Ukraine (Anderson, 2020).

An argument can be made that after the Snowden leaks, the US government have suffered a blow to their reputation, and their use of technology should be more regulated. This would naturally prevent the development of any “cyberweapons”. Furthermore, cyberattacks are based around deception. This calls into questions the ethics of cyberwarfare, especially if civilian infrastructure is harmed. With that in mind, will the use of such weapons become more prolific?

References

Anderson, R. (2020) *Security engineering: A guide to building dependable distributed systems.* Indianapolis, Indiana: John Wiley & Sons, Inc. DOI: 10.1002/9781119644682

Miller, C. (2023) *Emerging and Disruptive Defence Technologies.* Available from: <https://commonslibrary.parliament.uk/research-briefings/cbp-9184/> [Accessed 10 May 2024].

I have been amazed at the recent growth in McDonald’s use of technology. It seemed not long ago, the only way to get anything from the restaurant was to drive to your closest franchise and pay at the counter. Now McDonald’s has self-service touch screens, their own app and make extensive use of online delivery systems. McDonalds deliveries is estimated to be worth $3 billion USD globally (Adams, 2019).

Recently, the restaurant was hit by outages in the UK and other countries. A computer system failure caused issues with their mobile ordering and self-service kiosks (Sky News, 2024). While it is claimed this was not a cyberattack, it does highlight the importance of sound network design, with availability being an important tenet of cyber security.

It would be interesting to know what sort of cyber security measures McDonald’s has in place, and how high they rank its importance compared to other business outputs. Md also raises an interesting point. Seen as McDonald’s has such global reach, how can it implement measures to ensure they are complying with different regulations in each country?

References

Adams, E. (2019) McDonald’s Operators are Worried by the Chain’s Huge Delivery Success. Available from: <https://table.skift.com/2019/02/04/mcdonald-operators-are-worried-by-the-chains-huge-delivery-success/> [Accessed 10 May 2024].

Sky News. (2024) McDonald’s apologises after IT outage shuts restaurants worldwide but rules out cybersecurity attack. Available from: <https://news.sky.com/story/mcdonalds-customers-in-uk-say-restaurants-are-closed-after-it-outage-reported-in-countries-across-the-world-13094645> [Accessed 10 May 2024].