# Review 1 - 1866016921 and Review 2 – 1864805875

## Review 1 – 1866016921

GDPR is only apparent if Queens Medical Centre is based in, or has patient data from the EU. It may be subject to other regulations such as HIPAA (U.S. Department of Health and Human Services, N.D.), for example if it is based in the US.

An encouraging observation of the Langlois (2020) report is the reduction in malware exploits, indicating success in organisations implementing technological tools such as anti-malware. However, this further highlights the gap in addressing human factors in cybersecurity including human error, social action, and hacking, which as the author correctly mentions, often requires pretexting in order to be successful.

The essay makes a good case for banning social networking sites from being accessible from company devices or networks. This is a good example of removing opportunity for human error or misuse. However, gleaning employee information is also achievable from other open-source intelligence (OSINT) on the web, especially for those in senior roles. This is an easy way to build user profiles from their digital footprints, which can be later used for spear phishing, whaling, or other social engineering attacks (Mindpoint Group, N.D.). User awareness campaigns can be especially useful here, to highlight to users what information is available to the public and to make them aware of the possible ways they could be exploited.

## Review 2 – 1864805875

Two factor authentication (2FA) is an effective security practice, however it does not always have to be something humans know and have. Biometrics is an alternative factor, being something you are and is extremely usable for authentication as it does not require users to enter additional information.

Systems should be configured to remove human intervention where possible. By automating security controls, it minimises human error. However, when this is not possible, follow the principle of least privilege.

Security training addresses users’ capability through knowledge, however it falls short if they are not empowered to respond effectively. It is important users enjoy fruitful relationships with security staff so they feel comfortable reporting incidents (ENISA, 2018), and that top management are invested in security for them to feel supported, developing subjective norms which are important for changing cybersecurity behaviour (Cox, 2012). Users need to feel they can contribute to security through self-efficacy and empowerment.

Regulations improve organisations’ reputation, and requires them to implement effective security tools. However, they create a sense of complacency if seen as box ticking exercises employed simply to make themselves compliant (Haney & Lutters, 2020). Organisations must look at their security holistically and intervene where they can leverage cybersecurity most effectively. These regulations rarely incorporate the human factors in security, nor how to influence them.

## References

Cox, J. (2012) Information systems user security: A structured model of the knowing–doing gap. Available from: <https://www.sciencedirect.com/science/article/abs/pii/S0747563212001318> [Accessed 09 July 2022].

ENISA. (2018) Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. Available from: <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/@@download/fullReport> [Accessed 09 July 2022].

Haney, J & Lutters, W. (2020) Security Awareness Training for the Workforce: Moving Beyond "Check-the-Box" Compliance. Available from: <https://0-ieeexplore-ieee-org.serlib0.essex.ac.uk/stamp/stamp.jsp?tp=&arnumber=9206408> [Accessed 09 July 2022].

Langlois, P. (2020) 2020 Data Breach Investigations Report. Available from: <https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf> [Accessed 09 July 2022].

Mindpoint Group. (N.D.) Social Engineering Part 2: Open-Source Intelligence (OSINT). Available from: <https://www.mindpointgroup.com/blog/social-engineering-part-2-open-source-intelligence-osint#:~:text=Open%E2%80%90Source%20Intelligence%20(OSINT),craft%20realistic%20social%20engineering%20campaigns>. [Accessed 09 July 2022].

U.S Department of Health and Human Services. (N.D.) [Health Information Privacy](https://www.hhs.gov/hipaa/index.html). Available from: <https://www.hhs.gov/hipaa/index.html> [Accessed 09 July 2022].