**Discussion Forum 3 – Summary Post**

This discussion was based on a case study of a hospital incorrectly disclosing a patient’s data to a third party. Several recommendations for controls that can be used to mitigate the risk of this type of breach were shared. It is important to note that human error is identified as the root cause of the majority of data breaches, with 95% of breaches shown to have human factors involved (Wong, 2021; Nobles, 2018). The General Data Protection Regulation (GDPR) mandates security controls across people, process, and technology in order to effectively protect personal data from being breached.

Wong (2021) suggests a personnel solution of staff training, not just on data protection, but on security too in order to embed a security culture. Building a strong security culture is a continuous process and ensures staff at all levels of an organisation take responsibility for protecting data.

To build on process controls, Wilson (2021) recommends implementing mechanisms for checking adherence to documented processes and Kufner (2021) offers the solution of completing audits to measure effectiveness. Both internal and external audits can be conducted to ensure processes meet compliance requirements (RSM, 2020). In addition, sufficient due diligence should be done on the practices of third parties that will be acting as data processors in order to ensure data is protected throughout its lifecycle (Wilson, 2021).

Furthermore, Kufner (2021) suggests utilising technical solutions to solve the challenge of human error. Using technology to automate data processing tasks can boost GDPR compliance through reducing errors (Ryan et al., 2020). However, Kufner (2021) does highlight that these solutions can be more costly.

The GDPR was introduced to create a clear central regulation to cover the protection of personal data and has incentivised businesses by administering large fines for breaches (Millward, 2021). This has been effective in getting companies to adopt holistic security measures in order to protect the confidentiality, integrity, and availability of data (RSM, 2020).

References

Kufner, J. (2021) Initial Post. Available from: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=262576> [Accessed 9 July 2021].

Millward, D. (2021) Initial Post. Available from: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=262576> [Accessed 9 July 2021].

Nobles, C. (2018) Botching Human Factors in Cybersecurity in Business Organizations. *Holistica Journal of Business and Public Administration* 9(3): 71-88.

RSM (2020) Impact of the GDPR on Cyber Security Outcomes. Available from: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/906691/Impact_of_GDPR_on_cyber_security_outcomes.pdf> [Accessed 9 July 2021].

Ryan, P., Crane, M. & Brennan, R. (2021) ‘GDPR Compliance Tools: Best Practice from RegTech’, *International Conference on Enterprise Information Systems*. Virtual, 5-7 May. Springer, Cham. 905-929.

Wilson, C. (2021) Initial Post. Available from: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=262576> [Accessed 9 July 2021].

Wong, K. (2021) Initial Post. Available from: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=262576> [Accessed 8 July 2021].