## Initial Post

The internet has vastly grown from a small network of research computers into a versatile net of devices spread across the globe (Musiani, Levinson, Cogburn and Denardis, 2020). As the world of technology evolves, the need to protect data confidentiality, integrity, and availability has become a pressing concern for organizations of all sizes. Investment in cybersecurity is crucial for organizations to maintain customers’ confidence and trust, protect against cyber-attacks and minimize potential loss (Chronopoulos, Panaousis and Grossklags, 2017).

Hennes & Mauritz (H&M) is a Swedish global retail-clothing company, popular for its fast fashion business model. In 2020, H&M faced the second largest fine of its kind in the continent of Europe of $41.4 million dollars for breach of the General Data Protection Regulation (GDPR) (Bodoni, 2020). The Data Protection Authority of Hamburg (HmbBdDI) found the company to have excessively monitored several hundred employees at their Nuremberg service centre (Page, 2020). This included private details collected by management through informal discussions about family issues and religious beliefs. Also, the company gathered and stored details about staff’s holidays and medical findings/illnesses (Bodoni, 2020).

Although the collection of staff’s personal and private information was being collected since 2014, it was discovered in 2019 when the data became accessible company-wide due to a configuration error (Page, 2020). In addition to violating GDPR, this depicts the organization’s poor access control policies. Post the incident, H&M strengthened internal auditing practices and raised awareness amongst staff and leadership to ensure compliance with applicable regulations.

It’s critical for organizations to learn from these events, review their current security policies around personally identifiable information (PII) and protected health information (PHI), and ensure sufficient controls are implemented to secure data in compliance with applicable laws and regulations. As the shift to the digital world grows, its essential organizations invest in cybersecurity, to prevent reputation and monetary loss as a result of breaching laws or regulations.

Bodoni, S., 2020. H&M German Unit Fined $41.4 Million for Snooping on Staff. [online] Bloomberg.com. Available at: <[**https://www.bloomberg.com/news/articles/2020-10-01/h-m-german-unit-fined-41-4-million-for-snooping-on-staff**](https://www.bloomberg.com/news/articles/2020-10-01/h-m-german-unit-fined-41-4-million-for-snooping-on-staff)> [Accessed 18 August 2021].

Chronopoulos, M., Panaousis, E. and Grossklags, J., 2017. An Options Approach to Cybersecurity Investment. [online] Ieeexplore.ieee.org. Available at: <[**https://ieeexplore.ieee.org/document/8110826**](https://ieeexplore.ieee.org/document/8110826)> [Accessed 18 August 2021].

Musiani, F., Levinson, N., Cogburn, D. and Denardis, L., 2020. Researching Internet Governance: Methods, Frameworks, Futures. MIT Press.

Page, C., 2020. H&M Hit With Record-Breaking GDPR Fine Over Illegal Employee Surveillance. [online] Forbes. Available at: <[**https://www.forbes.com/sites/carlypage/2020/10/02/hm-hit-with-record-breaking-gdpr-fine-over-illegal-employee-surveillance/?sh=5042f2a115ab**](https://www.forbes.com/sites/carlypage/2020/10/02/hm-hit-with-record-breaking-gdpr-fine-over-illegal-employee-surveillance/?sh=5042f2a115ab)> [Accessed 18 August 2021].

# Summary Post

As cyber threats become more prevalent, investing in cybersecurity personnel and technology is a critical driving force to protect data confidentiality, integrity, and availability. In addition to the threats posed by external attackers in the digital realm, organizations must also consider internal threats, like employee negligence, intent to sabotage, or non-compliance, when developing a security program. As articulated in Kingsley Onyeemeosi’s peer response, risk management practices and regulations around data governance must be examined to improve cyber risk management (Onyeemeosi, 2021). To maintain customers’ confidence and trust, protect against cyber-attacks and minimize potential loss, it’s critical that organizations invest in cybersecurity and bring it to the forefront (Chronopoulos, Panaousis and Grossklags, 2017).

The importance of data governance has been consolidated into the General Data Protection Regulation (GDPR). GDPR was designed to unify data privacy laws across Europe, protect EU citizens’ data, change the way organizations using EU citizens’ data approach privacy, and to allow regulatory bodies to enforce, audit and penalize organizations that aren’t compliant (Garber, 2018).

Hennes & Mauritz (H&M), a Swedish global retail-clothing company, was hit with a $41.4 million dollar fine for collecting their staff’s personal and private information without their knowledge (Bodoni, 2020). This included details obtained from informal conversations, like family and religious beliefs. As outlined in Zihaad Khan’s peer response, to ensure GDPR compliance organizations must be transparent about data collection and usage, and retention periods. If H&M created their security policies around personally identifiable information (PII) and protected health information (PHI) in accordance with GDPR requirements, they would have been spared of the monetary loss and reputational damage.

As attacks become more complex, organizations must design security policies and architecture with defense in depth in mind – a layered security approach designed to prevent, deter, detect, and correct attacks (Coole, Corkill and Woodward, 2012) with the appropriate technical and administrative controls. Organizations investing and implementing strategies with broader compliance in mind, essentially baking the different compliance requirements into the business processes to streamline efforts, will save costs and lower risk levels (Garber, 2018).

**Reference List**

Bodoni, S., 2020. H&M German Unit Fined $41.4 Million for Snooping on Staff. [online] Bloomberg.com. Available at: <https://www.bloomberg.com/news/articles/2020-10-01/h-m-german-unit-fined-41-4-million-for-snooping-on-staff> [Accessed 30 August 2021].

Chronopoulos, M., Panaousis, E. and Grossklags, J., 2017. An Options Approach to Cybersecurity Investment. [online] Ieeexplore.ieee.org. Available at: <https://ieeexplore.ieee.org/document/8110826> [Accessed 30 August 2021].

Coole, M., Corkill, J. and Woodward, A., 2012. *Defence in Depth, Protection in Depth and Security in Depth: A Comparative Analysis Towards a Common Usage Language*. [online] Edith Cowan University. Available at: <https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1023&context=asi> [Accessed 30 August 2021].

Garber, J., 2018. GDPR – compliance nightmare or business opportunity?. *Computer Fraud & Security*, 2018(6).

Khan, Z., 2021. *Collaborative Learning Discussion 1*. [online] Available at: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=270911> [Accessed 30 August 2021].

Onyeemeosi, K., 2021. *Collaborative Learning Discussion 1*. [online] Available at: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=270911> [Accessed 30 August 2021].