Table of Contents

[What is the specific aspect of GDPR that your case study addresses? 1](#_Toc144368142)

[How was it resolved? 1](#_Toc144368143)

[If this was your organisation, what steps would you take as an Information Security Manager to mitigate the issue? 1](#_Toc144368144)

[Learning Outcomes 2](#_Toc144368145)

[References 2](#_Toc144368146)

GDPR Case Studies

**Case Study: Data Breach in Healthcare Industry (Data Protection Commission, 2020)**

# What is the specific aspect of GDPR that your case study addresses?

The chosen case study addresses the unauthorized access and disclosure of sensitive patient data, a direct infringement of Article 32 of GDPR, which mandates the implementation of appropriate technical and organizational measures to ensure a level of security appropriate to the risk [1].

# How was it resolved?

The issue was resolved by imposing a fine on the healthcare organisation and mandating it to revise and implement stronger security protocols. An external audit was also conducted to ensure compliance with GDPR regulations [1].

# If this was your organisation, what steps would you take as an Information Security Manager to mitigate the issue?

As an Information Security Manager, the following steps would be taken to mitigate the issue:

**Immediate Investigation:**

Launch an immediate investigation to understand the scope of the breach.

**Risk Assessment:**

Use tools like ISO 31000-based integrated risk management process assessment models to assess the impact and risks [2].

**Employee Training:**

Educate employees about GDPR compliance and the importance of securing sensitive data, as outlined in "Threat modelling: designing for security"[3].

**Enhanced Security Measures:**

Implement multi-factor authentication, data encryption, and regular audits as recommended in the top 10 IT security frameworks [4].

**DR Plans:**

Adopt robust Disaster Recovery (DR) plans as discussed in various evaluation strategies by Alhazmi & Malaiya [7].

**Legal Counsel:**

Consult legal advisors to ensure compliance with laws and regulations.

By these measures, I would aim to significantly lower the security risks and vulnerabilities in information systems and ensure GDPR compliance.

# Learning Outcomes

* The case study provides valuable insights into identifying and analysing security risks in information systems.
* Methodologies and tools like ISO 31000-based integrated risk management have been utilized to manage the issues [2].
* Legal and ethical considerations, integral to GDPR, were also considered.

# References

[1] Data Protection Commission. (2020). Case Studies: Data Protection Commission.

[2] Barafort, B., Mesquida, A.-L. & Mas, A. (2019). ISO 31000-based integrated risk management process assessment model for IT organizations. Journal of Software: Evolution and Process 31(1): e1984. DOI: 10.1002/smr.1984

[3] Shostack, A. (2014). Threat modeling: designing for security. 1st ed. Wiley & sons ltd. Chapters 3-6.

[4] Kirvan, P. (2021). Top 10 IT security frameworks and standards explained.

[5] Andrade, E., Nogueira, B., Matos, R., Callou, G. & Maciel, P. (2017). Availability modeling and analysis of a disaster-recovery-as-a-service solution. Computing 99(10): 929–954.

[6] Alhazmi, O. & Malaiya, Y. (2013). Evaluating Disaster Recovery Plans using the Cloud. 2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS) 1(1): 1-6.