Unit 4

Optional Activity – Danske Bank GDPR Related Case Studies

Introduction

Danske Bank, one of the largest financial institutions in Denmark, has faced significant scrutiny regarding its compliance with the General Data Protection Regulation (GDPR). GDPR, enforced since May 25, 2018, aims to protect the personal data and privacy of EU citizens. The regulation mandates strict protocols for data handling, requiring organizations to implement robust security measures to safeguard personal data. This case study examines a specific GDPR breach at Danske Bank, explores how it was resolved, and outlines steps an Information Security Manager could take to prevent such issues in the future.

GDPR Breach at Danske Bank

Danske Bank experienced a notable GDPR breach involving unauthorized access to sensitive customer information. This breach specifically contravened Article 32 of the GDPR, which requires data controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (GDPRhub, 2024).

Incident Overview

In this incident, it was discovered that unauthorized individuals gained access to sensitive customer data due to inadequate encryption and insufficient access control mechanisms. The breach exposed personal information, leading to potential risks for the affected individuals and significant reputational damage to the bank (Bjerregaard & Kirchmaier, 2019).

Resolution of the Issue

Notification and Transparency

Danske Bank adhered to GDPR Article 33 by promptly notifying the relevant Data Protection Authority (DPA) about the breach. Additionally, they informed the affected customers as required by Article 34, ensuring transparency and compliance with regulatory obligations (GDPR, 2016).

Investigation and Rectification

An internal investigation was initiated to understand the breach's root cause. The bank collaborated with cybersecurity experts to analyze the breach and prevent future occurrences. This comprehensive investigation was crucial in identifying the weaknesses in their security systems (Data Privacy Manager, 2022).

Enhancing Security Measures

Post-breach, Danske Bank implemented several key enhancements:

- Encryption: The bank upgraded its encryption standards, ensuring that sensitive data is securely encrypted both in transit and at rest (Danske Bank, 2018).
- Access Controls: Strengthened access control mechanisms were put in place, including multi-factor authentication (MFA) and role-based access control (RBAC), to restrict data access to authorized personnel only (O'Dwyer, 2019).
- Monitoring and Response: Danske Bank enhanced its monitoring systems, enabling real-time detection and response to suspicious activities. This included deploying advanced threat detection tools and increasing the frequency of security audits and penetration testing (Guo & Guo, 2023).

Mitigation Steps for Information Security Managers

If this breach occurred in my organization, as an Information Security Manager, I would take the following steps:

Comprehensive Risk Assessment

Conducting a thorough risk assessment is vital. This includes identifying potential vulnerabilities in data handling and storage processes. Risk mitigation strategies should be developed based on the assessment findings (Thurmond, 2024).

Enhance Technical Measures

- Encryption: Ensure all personal data is encrypted both in transit and at rest, utilizing advanced encryption standards (Jena, 2024).
- Access Controls: Implement strict access control policies, such as MFA and RBAC, to limit data access to authorized individuals only.
- Regular Security Audits: Conduct regular security audits and penetration testing to promptly identify and address vulnerabilities.

Organizational Measures

Training and Awareness: Develop a comprehensive training program to educate employees about GDPR requirements and data protection best practices (Skillcast Group, N.D.).

Incident Response Plan: Establish and regularly update an incident response plan, outlining steps to be taken in the event of a data breach, including notification procedures and remediation efforts.

Continuous Monitoring and Improvement

Implement continuous monitoring systems to detect and respond to suspicious activities or potential breaches in real-time. Regularly review and update security policies and procedures to adapt to evolving threats and regulatory changes (Sundararajan & Dietz, 2023).

Vendor and Third-Party Management

Conduct due diligence and regular assessments of third-party vendors to ensure they comply with GDPR requirements and maintain adequate security measures (RskXchange, 2022).

Conclusion

Danske Bank's GDPR breach underscores the critical need for robust data protection measures. By promptly addressing the breach and enhancing their security protocols, the bank demonstrated a commitment to safeguarding customer data. For any organization, implementing comprehensive risk assessments, enhancing technical measures, fostering organizational awareness, and continuously monitoring security systems are crucial steps in ensuring GDPR compliance and protecting personal data.

References

Bjerregaard, E. & Kirchmaier, T. (2019) 'The Danske Bank Money Laundering Scandal: A case study', *SSRN Electronic Journal* [Preprint]. doi:10.2139/ssrn.3446636.

Danske Bank (2018) *Findings of the investigations relating to Danske Bank's branch in Estonia*, *Danske Bank*. Available at: https://danskebank.com/news-and-insights/news-archive/press-releases/2018/pr19092018 (Accessed: 13 July 2024).

Data Privacy Manager (2022) *GDPR fine: Danske Bank fined €1.3 million over non-compliant data deletion processes*, *Data Privacy Manager*. Available at: https://dataprivacymanager.net/gdpr-fine-danske-bank-fined-e1-3-million-for-non-compliant-data-deletion/ [Accessed: 10 July 2024].

GDPR (2016) *Art. 34 GDPR – Communication of a personal data breach to the data subject*, *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/art-34-gdpr/ (Accessed: 08 July 2024).

GDPRhub (2024) *Article 32 GDPR*, *GDPRhub*. Available at: https://gdprhub.eu/Article_32_GDPR [Accessed: 12 July 2024].

Guo, J. and Guo, H. (2023) 'Real-time risk detection method and protection strategy for Intelligent Ship Network Security based on cloud computing', *Symmetry*, 15(5), p. 988. doi:10.3390/sym15050988.

Jena, B.K. (2024) *AES encryption: Secure Data with Advanced Encryption Standard*, *Simplilearn.com*. Available at: https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption [Accessed: 10 July 2024].

O'Dwyer, G. (2019) *Danske Bank Launches Initiative to help SME customers with Cyber Security: Computer Weekly*, *ComputerWeekly.com*. Available at: https://www.computerweekly.com/news/252463629/Danske-Bank-launches-initiative-to-help-SME-customers-with-cyber-security [Accessed: 11 July 2024].

RskXchange (2022) *Third Party GDPR compliance: RiskXchange*, *riskxchange.co*. Available at: https://riskxchange.co/278/thrid-party-risk-management-gdpr-compliance/#:~:text=Third%2Dparty%20compliance%20GDPR%20requirements,authorised%20to%20process%20personal%20data. (Accessed: 10 July 2024).

Skillcast Group (N.D.) *GDPR compliance: GDPR Compliance Courses*, *Skillcast*. Available at: https://www.skillcast.com/gdpr-compliance-training-courses [Accessed: 09 July 2024].

Sundararajan, V. & Dietz, E. (2023) *Centralized hierarchical cybersecurity monitoring towards securing the Defense Industrial Base Supply Chain* [Preprint]. doi:10.2139/ssrn.4603578.

Thurmond, T. (2024) *5 risk management best practices for organizational management*, *KirkpatrickPrice*. Available at: https://kirkpatrickprice.com/blog/5-important-risk-management-best-practices/ [Accessed: 08 July 2024].