Digital Transversal Skills

Group Assessment CA3

Student Full Name: Xiu(Janet) Shi

Student Number: sba23167

We self-formed a team of five members: Ronan Broderick, Daniella Kooh, Breege Murray, Jade Sheridan, Xiu (Janet) Shi. We have created a Whatsapp group to maintain contact and discussions. We each share a part of the assessment task. We have a shared google doc to collaborate each task, adding objective feedback of each other’s work and poster higher quality output. When team member have query or suggestions, we respond and reach to a conclusion promptly.

My contribution of this project is Data security and GDPR Compliance

Data security and GDPR Compliance [0-10%]

* Explain the potential consequences of non-compliance with GDPR.

1. Significant Financial Fines: GDPR non-compliance can result in significant financial fines, reaching up to ten million or two percent of a company’s annual global turnover for the most serious violations.
2. Legal Risks: TechSolutions Inc. could face potential legal disputes. It can be a time consuming and costly process and disrupt the company’s activities and lead to revenue loss.
3. Reputation Damage: A security data breach at TechSolutions Inc. lead to loss customer trust and negative public perception, impacting the brand value and existing customer loyalty, worst existing customer revenue loss, new prospect loss.
4. Business disruptions: To address non-compliance issues can demand human and hardware resources, which can disrupt normal business operation, leading to postpone or cancel business services.

* Propose measures to improve data security and ensure GDPR compliance.

Based on 7 Data Protection Principles and TechSolutions Inc. Data Security Breach, the follow measures should be implemented as soon as possible, ranked by urgency and priority

Report Breach:

1. Report Security Breach to The Data Protection Commissioner with seventy-two hours of first becoming aware of the breach.
2. Obtain incident logs and isolate server contains effected customer accounts, compile breach report. Carry out forensic analysis.
3. Initial notification of effected customers with Breach Report. Consider the potential adverse consequences for individuals and finance risk and impact. Follow with prompt updates.
4. Stakeholder communication

Implement corrective actions:

1. Appoint Data Protection Officers, Data Processor, Data Controller in TechSolutions Inc.
2. Ensure Database audit post breach and implement industry up-to-date encryption standard. Implement all employees with multi-factor authentication access, internal and external communication encryption. Role-based access of data, only relevant stakeholders can obtain database read and write permission.
3. Ensure regular security audits and training are carried out.
4. Implement data validity and the right to forget policy and process.
5. Implement real time monitoring and reporting of data breach and cyber attack.
6. Long-term data protection strategy

Wolford, Ben. "What Are the GDPR Fines?" GDPR.EU, GDPR.EU, 11 July 2018, gdpr.eu/fines/. Accessed 11 Nov. 2023.

The Data Protection Commission. “Breach Notification | Data Protection Commission.” *Breach Notification | Data Protection Commission*, The Data Protection Commission, 2018, www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification. Accessed 11 Nov. 2023.