September 27, 2022

Security Standards

Activity

Review the following links/ websites and answer the questions below:

ICO (2020) Guide to the General Data Protection Regulation (GDPR).

PCI Security Standards.org (2020) Official PCI Security Standards Council Site - PCI Security Standards Overview.

HIPAA (2020) HIPAA For Dummies – HIPAA Guide

1) Which of the standards discussed in the sources above would apply to the organisation discussed in the assessment? For example, a company providing services to anyone living in Europe or a European-based company or public body would most likely be subject to GDPR. A company handling online payments would most likely need to meet PCI-DSS standards.
    - After the digitalization of the enterprise, Pampered Pets would have to follow the below standards:

        → General Data Protection Regulation (GDPR)

        For Privacy and Data in Europe (even if the enterprise is located outside the Europe, as soon there is business in Europe, there is a need to comply to it)

        → PCI Security Standards

        For payment on website (even if the payment gateway is outsourced, the enterprise is still liable if there are issues)

2) Evaluate the company against the appropriate standards and decide how would you check if standards were being met?

→Governance structure

→ Discern between personal and sensitive data

→ Encryption to protect data (transport and storage)

→ Access control policies and procedures

→ Role privileges and segregation of duties

→ Password policies (MFA and encryption type)

→ Patch management protocols/procedures/policies

→ System monitoring (IPS and IDS)

→ Incident management policy and plan

→ Business Continuity Plan and Recovery Plan

→ External Audit

→ Employees training and awareness

→ Physical security management

→ Information management policies

→ Data Security Standard

→ PIN Transaction Security (PTS)

→ Software Security Framework

→ Point-to-Point Encryption (P2PE)

→ Mobile Standards

→ Secure Network and System

→ Protect Account Data

→ Vulnerability Management Program

→ Monitoring and Testing Networks

→ Information Security Policies

3) What would your recommendations be to meet those standards?

→ First, establish the governance, policies, procedures, and standards

→ Follow the standards, as they are easy guides to ensure compliance

→ For the online payment gateway, out-source the solution to a trustworthy company

→ Monitor and test systems

→ Conduct external audit

4) What assumptions have you made?

→ The company is conducting business in Europe

→ The company is using online payment