Unit 6: The Practical Implications of Security and Risk Standards

Title: Security Standards

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr

https://www.pcisecuritystandards.org/standards/

https://www.hipaaguide.net/hipaa-for-dummies

Pampered pets are a bricks-and-mortar business, based in a leafy suburb of Hashington-on-the-Water. It employs 4 staff; Alice the owner/ manager; Cathy the shop manager; Andrea the store assistant and Harry the warehouse manager. 90% of their business is carried out face to face, with people coming into the store to buy items. A small percentage of clients will email their orders – once these are ready the staff email the clients who then travel to the store to pick up goods and pay. Recently Harry has started to use an old, networked computer (with a spreadsheet package) to keep track of warehouse deliveries and item locations. The front desk uses a computer for all sales and purchases so that transactions are recorded digitally – this makes VAT and Tax submissions easier. The main shop has a wireless gateway and hub that both computers are connected to. In addition, all the staff use the wireless connection for various apps on their smart phones.

The business is most famous for the quality of its pet foods – using the highest quality ingredients from local suppliers, with many items being prepared and packed in-house. This has a number of advantages including easy and regular quality checks of ingredients and a guaranteed supply chain – if necessary, employees could get into their cars and drive 10 minutes to the suppliers (mostly local farms) to pick up the ingredients by hand.

- Which of the standards discussed in the sources above would apply to the organisation discussed in the assessment

  Pampered Pets would have to follow the seven principles of the UK GDPR which are as follows -

  - Obtaining the data Lawfully,
  - Processing the data fairly
  - Ensure Transparency to the individually
  - Data is used for Purpose and not beyond the limitation as agreed
  - Ensuring the data is correct fit for purpose and limited to what is necessary.
  - Storage limitation

    Data is not kept for longer than required

- Integrity and confidentiality

  Ensure data is kept with appropriate security measures
- Accountability

If an online presence was required, which would result in online payments the PCI Security Standards Council (PCI SSC) PCI Data Seruity standards would need to be followed.

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

  All data stored by Pampered Pets, which was related to customers or vendors would have to be reviewed. A consent would be required informing them that we hold data on the user outlining what the data is, for what reason and for how long we will retain the information.

  A review of how the data is kept ensuring appropriate security measures are place and access is restricted to only individuals who need the data

  Ensure a policy is in place on how information would be used and what to do in a compromise.

- What would your recommendations be to meet those standards?

  The recommendation would be ensuring the policy and data is reviewed over a periodical period like the PCI DSS to ensure credit card transactions are secure.

- What assumptions have you made?

  Pamper Pets is located within the UK or Europe.

  Pamper Pet will go digital