Unit 6 Seminar Preparation

Security Standards

Please carry out this activity before joining the seminar this week. Your answers will be discussed during the seminar.

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

- 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.
- Evaluate the company against the appropriate standards and decide how would you check if standards were being met?
- What would your recommendations be to meet those standards?
- What assumptions have you made?

We will be discussing these articles and the wiki in this week's seminar. After the seminar, review your initial response as well as those of your colleagues. There will also be an opportunity to review your team's progress during the seminar.

---

1. The GDPR and PCI standards would apply, as these encorporate data privacy regulations for the UK/EU and payment processing privacy regulations, respectively.

2. The following is useful as a checklist for standards:

- What formal policies/procedures have been put in place?
- How do these policies address data privacy?
- Are there access controls, session management, and two-factor authentication for all internal/external users?
- How is the database protected from SQL/other database attacks?
- Are all hardware stations protected/monitored?

- Have staff undergone proper training – phishing and technical?
- Does the third party payment software comply with PCI standards?
    - Third party licensing agreement states specific compliance with proof?
    - Have the certificates been authenticated, either by in-house IT staff or externally?
- What is appropriate recourse in case of a breach?
    - Third party suppliers
    - Customers
- Are compiled data only those necessary for application use?

3. Recommendations for meeting the above standards:

- Have standard and approved policies/procedures for data breach mitigation and disaster recovery
- Have server/system penetration tested to isolate weak code areas
    - in house and independent
- Alternate: employee a Cloud server with explicit access controls, session management, and two(+)-factor authentication and regular system updates
- Employee training to address social engineering risks, personal responsibility on server
- Perform due diligence for third party payment app
- Keep unauthorized personnel from acccessing unauthorized servers
- Have a recourse plan for compensation in the event of a catestrophic breach
- Limit the amount of data kept in the database

4. Assumptions:

- Organization does not have a dedicated IT staff so will need outside assistance for compliance
- Organization will rely on third party applications for much of their server/function needs
- Organization does not have formal policies/precedures concerning data protection
- Organization has the budget for comprehensive protection/mitigation

Resources

PCI Security Standards Council. (n.d.) *Standards*. [online] Available at: https://www.pcisecuritystandards.org/standards/.

ico.org.uk. (2020) *Guide to the General Data Protection Regulation (GDPR)*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr.