Seminar 4: Security Standards

Q1: Which of the standards discussed in the sources above would apply to the website/ organisation assigned to you for the assessment?

Of the standards listed HIPAA (2020), ICO (2020) or PCI (2020), the GDPR standard and PCI standards are the most applicable to the assigned website.

GDPR is applicable because it governs security and protection of personal data which is appropriate for a human resources management (HRM) system as HR departments daily deal with personal data of their employees. Such data privacy is subject to four principles, the right to rectify, the right to be forgotten, right to object and employees' right to their personal data.

PCI Data Security Standards are applicable to HRM because these standards are designed to protect payment account data throughout its lifecycle and cover merchants, service providers, financial institutions, and secure software lifecycle. Since HRM system handle electronic employee salary payments, it is important for HRM systems to ensure end-to-end encryption, implement policies about storage of account details and importantly, for software vendors to place emphasis on development of secure software.

Q2: Evaluate your assigned website against the appropriate standards and decide how you would check if standards were being met?

To analyse the assigned HR system whether the selected standards are met I would take the following approach (in an ideal situation):

1. Read relevant documentation provided by the developers of the product, for example (https://www.orangehrm.com/assets/Documents/pdf/OrangeHRM-Data-Security.pdf).
2. Consider any public documentation provided by the website regarding GDPR (https://www.orangehrm.com/gdpr/), (https://help.orangehrm.com/hc/en-us/articles/360006543294-GDPR-Compliance-6-4-Feature).

3. Read API documentation to understand the extent of encryption used for communication. For example (https://api.orangehrm.com/) learning that their API uses industry-standard OAuth for client authentication.
4. Consider the privacy statement of the hosting provider in relation to data storage, processing, and security. For example, the assigned website uses RackSpace as a hosting provider whose privacy statement is located here (https://www.rackspace.com/information/legal/privacystatement).
5. Consider any public statements related to the hosting provider's PCI DSS compliance (https://www.rackspace.com/compliance/pci).

Considering the provided documentation, and that I can obtain a user account to the assigned website, I would access the website and look for role-based access, ability for admins to purge employee records, monitor network communications between the product and hosting provide to see if sensitive data is transferred in plain text or encrypted, look for support to view audit records (non-repudiation according to the CIA-N triad).

Q3: What would your recommendations be to meet those standards?

Since the vendor of the website have built support for GDPR and their hosting provider have support for PCI DSS standards, there is no further recommendation that can be offered to address any lack.

Q4: What assumptions have you made?

The assumptions made in relation to the above question are

- The public documentation referenced in Q2 are true (given that I am unable to sign up for a test account). Therefore, there is an element of trust in the what the statements of both the vendor and the hosting provider.

References

ICO (2020). Guide to the UK General Data Protection Regulation (UK GDPR). Available from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ [Accessed 25 Jan. 2021]

PCI (2020). PCI Security Standards Overview. Available from https://www.pcisecuritystandards.org/pci_security/standards_overview [Accessed 25 Jan. 2021]

HIPAA (2020). HIPAA For Dummies: Why was HIPAA created? Available from https://www.hipaaguide.net/hipaa-for-dummies/ [Accessed 25 Jan. 2021]