Week 8: Security Standards

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**.

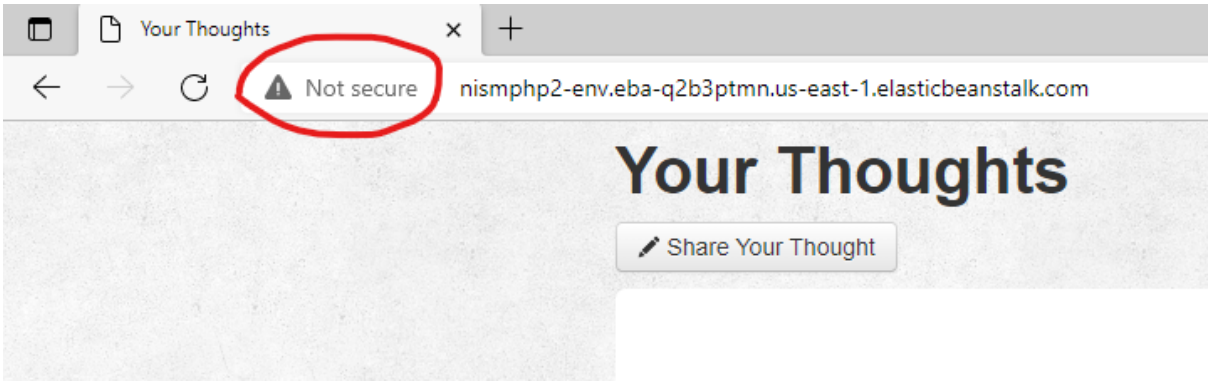
HIPAA (2020) HIPAA For Dummies – **HIPAA Guide**.

- Which of the standards discussed in the sources above would apply to the website/ organisation assigned to you for 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.

  Our client is an e-commerce company offering payment services therefore the PCI Security standards will be applicable in addition to the GDPR standards.

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

  HTTP is the protocol used for web connection on Team A's site.



  HTTP transfers data in plain text (without encryption) across a network which makes it unsecure. Team A customers are at risk of their financial information being stolen on the website. According to Brown (2017), HTTP is not PCI compliant.

- What would your recommendations be to meet those standards?

  Use HTTPS instead. It provides data encryption and protects customers from attackers who might be eavesdropping on the network.

- What assumptions have you made? None

References

Brown T. (2017). What is an SSL port? A technical guide for HTTPS. Available from: https://www.godaddy.com/garage/whats-an-ssl-port-a-technical-guide-for-https/ [Accessed 18 October 2021]