**Unit 8 - Seminar 4 – Prep**

**Security Standards**

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

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

PCI Security Standards.org (2020) Official PCI Security Standards Council Site - [**PCI Security Standards Overview**](https://www.pcisecuritystandards.org/pci_security/standards_overview).

HIPAA (2020) HIPAA For Dummies – [**HIPAA Guide**](https://www.hipaaguide.net/hipaa-for-dummies/).

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.

A company known as ‘Loaded Commerce Store’ operates an e-commerce website called "https://loadedwithstuff.co.uk/". The company’s product catalogue includes digital accessories, laptops, mobile phones and more. Customers visiting the website would browse for a product and proceed to perform a purchase. Customers can also create accounts by entering their personally identifiable information (PII) such as names, e-mail addresses, contact details and address information for shipping purposes. The company operates from the United Kingdom and is therefore subjected to the following governing bodies and associated regulations:

* UK GDPR (General Data Protection Regulation of the European Union)
* PCI DSS (Payment Card Industry Data Security Standard)
* ICO (Information Commissioners Office)

The Information Commissioners Office (ICO) is responsible for upholding information rights for the UK public as well as to provide guidance in adherence and compliance to the UK GDPR (ICO, 2021). Since the e-commerce website accepts credit cards for payments, it will need to comply with the PCI DSS.

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

For GDPR – Use a GDPR Scanner:

<https://2gdpr.com/395321740>

On 25 May 2018, the DPA was replaced by the General Data Protection Regulation (GDPR) according to

<https://www.privacycompliancehub.com/gdpr-resources/data-protection-act-vs-gdpr-getting-to-grips-with-the-changes/>

FOR PCI DSS:

According to: <https://itstillworks.com/do-tell-website-pci-compliant-5968912.html>

“There is only one way for a consumer to tell if a website is PCI compliant. If the website accepts credit card payments, it is compliant. If the site sells merchandise and does not accept payment, it is not compliant. According to the Council, because of the standards set, "Compliance with the PCI set of standards is mandatory for their respective stakeholders, and is enforced by the major payment card brands who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. For example, any site that sends a person to another site, like PayPal, or other card processing site, they are non-compliant. They send the customer to the third-party sites because they have a contract with the third party to take the card payments for them. This is usually because the site itself is non-compliant.”

What would your recommendations be to meet those standards?

According to: <https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security>

If you accept or process payment cards, the PCI Data Security Standards apply to you.

These standards cover technical and operational system components included in or connected to cardholder data.

**Build and Maintain a Secure Network**

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

**Protect Cardholder Data**

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

**Maintain a Vulnerability Management Program**

5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

**Regularly Monitor and Test Networks**

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

**Maintain an Information Security Policy**

12. Maintain a policy that addresses information security for employees and contractors

============================

According to: <https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security>

A model framework for security, the PCI Data Security Standard integrates best practices forged from the years of experience of security experts around the world.

The standard works for some of the world’s largest corporations. And it can work for you.

* Buy and use only approved PIN entry devices at your points-of-sale.
* Buy and use only validated payment software at your POS or website shopping cart.
* Do not store any sensitive cardholder data in computers or on paper.
* Use a firewall on your network and PCs.
* Make sure your wireless router is password-protected and uses encryption.
* Use strong passwords. Be sure to change default passwords on hardware and software – most are unsafe.
* Regularly check PIN entry devices and PCs to make sure no one has installed rogue software or “skimming” devices.
* Teach your employees about security and protecting cardholder data.
* Follow the PCI Data Security Standard.

What assumptions have you made?

* Payments are made directly on the website and does not integrate with a 3rd for payment processing.

**References**

ICO (2021). Information Commissioners Office – Guide to the General Data Protection Regulation – Security. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security [Accessed 09 December 2021].