FACTFILE:
GCE PROFESSIONAL BUSINESS SERVICES

UNIT A2 1: SECURITY ISSUES

Rewarding Learning

Learning Outcomes

Student should be able to:

- demonstrate knowledge and understanding of the principles of keeping data safe, including: confidentiality; integrity; and availability;
- demonstrate knowledge and understanding of the types of threats associated with cyber security including: data theft; phishing; malware; and zero day attacks;
- demonstrate knowledge and understanding of the following cyber security technology: secure socket layer; hypertext transfer protocol secure (https); and two factor authentication (2FA)
- demonstrate knowledge and understanding of how cyber security technology can make the following systems more secure: email; cloud computing; and transaction processing systems;
- evaluate cyber security technology, including: secure socket layer; hypertext transfer protocol secure (https); and two factor authentication (2FA)
- Demonstrate knowledge and understanding of relevant legislation on: data protection; copyright; health and safety; computer misuse; and communications.
- demonstrate knowledge and understanding of a disaster recovery plan: files backed up; timescale for back-ups; location of back-up; storage method; and key personnel and roles identified.
- describe and justify common back-up and recovery strategies.
- analyse the main features of a disaster recovery plan.

Principles of keeping data safe

Data comes in various forms ranging from simple to complex format (University of Delaware, 2020). In a business, marketing, finance, production, and human resource departments require different types of data. In production the data may be simply a serial number for a component whilst in the marketing department data make relate to the customer's name, address, types of products purchased, volume of products purchased in the 12 months and the amount of money spent. The attributes of data include confidentiality, integrity and availability.

Confidentiality entails the management of sensitive data and ensuring that it remains secure.

Integrity relates to the management and storage of accurate, authentic and trustworthy data.

Availability refers to the timeliness and reliability of access to and use of data.

Data confidentiality

The primary focus of data confidentiality is to protect data. The threat to data can be in the form of disclosure, theft, or unauthorised access.

Data confidentiality relates to the level of privacy attributed to stored information (Rainer et al., 2013). The confidentiality is protected by limiting the number of people who are authorised to see, share and use the data. Information with low confidentiality could be viewed as carrying little threat beyond its targeted audience. Examples include the opening and closing times of a supermarket posted on its website or the titles of films on show at a cinema displayed on posters outside the venue. However, data can be highly confidential when it needs to be protected to ensure no damage to individuals or organisations e.g. a hospital patient's records or customer's bank accounts need to be secure to protect the patients' privacy and the customers' money. In addition, if there is a breach in the security of the data this can result in reputational damage to either the hospital or bank.

Data confidentiality can be effectively managed by encrypting sensitive files, managing who can access data (CPNI, 2015), providing physical (locked areas, cabinets and safes) security for data (BBC, 2020), install protocols for collecting data, manage the use of data, protect the systems, processes, hardware and software that supports the acquisition, storage, utilisation, and disposal of data.

Data integrity

Integrity relates to the accuracy, authenticity, and trustworthiness of data and ensuring the data is properly maintained or is not adversely altered (Rainer et al., 2013).

Low integrity requirements may be associated with data that has little impact on the operations of the business whereas high integrity requirements may be deemed critical to the operational activities of the business. For example, social media posts contained on a business's website may have little or no impact on operational activities whereas customer data that is corrupted or outdated can adversely affect operational activities.

Data integrity can be managed by backing up data (BBC, 2020), limiting access and restricting its use (viewing, recording, editing, and deleting), (CPNI, 2015), recording log-ins and activities, verifying that data at time of acquisition is correct and appropriate at time of use.

Data availability

Availability relates to accessibility to data and continuity of data provision.

Low availability requirements may be associated with data that has little impact on the operations of the business whereas high availability requirements may be deemed critical to the operational activities of the business e.g. the loss of a social media feed may have little impact on a business's operational activities whereas the loss of website files containing product details and price may have a negative impact on the related product sales during site downtime.

Types of threats associated with cyber security

Cyber security threats defined

'A cyber threat is an activity by a cyber-threat actor intended to compromise the security of an organisation's information system by altering the availability, integrity, or confidentiality of a system or the information it contains'. Source adapted from Government of Canada (2018, 2).

The cyber threat actors can be states, groups or individuals whose aim is to exploit the weaknesses in an organisation's security systems, processes, policies and procedures to obtain unauthorised access to information systems. The intent of the cyber threat actors is to corrupt, destroy, infect, ransom, or steal an organisation's data. The motivation for these attacks may be geopolitical (nation states), for profit (cyber-criminal), ideological (hacktivists), or discontentment (organisational insider).

Cyber threat actors engage in cyber threat activities by exploiting technical vulnerabilities with malicious software (malware) and availing of social engineering methods (phishing and spear-phishing).

Data theft is the unauthorised transfer of data from an organisation by an individual or group within the organisation or by an individual or group outside of the organisation (CYFOR, 2020; McKinsey, 2014; Norton, 2020a).

Phishing (NCSC, 2017) is where cyber threat actors send fake emails to people asking them to reveal sensitive information (bank details).

Malware is the name for malicious software. Malware are often referred to as viruses which are: 'self-copying programs that infect legitimate software' NCSC (National Cyber Security Centre. 2017, 7). Zero day (Rouse, 2019) is a fault in the software or hardware. The software designer is not aware of this fault nor is the organisation responsible for fixing (patching) the fault.

Zero day attacks (Norton, 2020b) occur when cyber threat actors exploit the fault in the system

and gain unauthorised access to data. It is difficult for an organisation to identify when a zero day attacks is happening. This type of attack is usually aimed at high-value organisations.

Types of cyber security technology

Cyber security technology is used to offer an organisation's systems, networks and programmes a degree of protection from digital attacks (CISCO, 2020). An effective cyber security strategy uses a range of protective layers to keep computers, networks, systems or data safe and integrates employees, processes and technology.

Employees need to follow data security protocols (Smartsheet, 2020) create strong passwords, be cautious with incoming emails with attachments and back-up data regularly.

Organisations can employ processes that enable them to respond to cyber-attacks.

Protecting computers, networks, and the cloud

Secure socket layer (SSL) is 'the protocol for establishing authenticated and encrypted links between networked computers' (SSL.com, 2020). SSL was superseded by Transport Layer Security (TLS) in 1999.

Hypertext transfer protocol secure (https) is an internet communication protocol that safeguards the integrity and confidentiality of data between the user's computer and the site being visited by the user (Google, 2020).

Two factor authentication (2FA) employs two different mechanisms to verify the user's identity before the user can access their account. This may take the form of the user entering a password. To verify the user's identity, a code is then sent to their phone and this code is entered into the system so that the user can access their account (NCFC, 2017). 2FA adds additional security to website accounts that a user may possess.

How cyber security technology can make systems more secure

Email

Cyber security technology can create a secure email gateway, offer url protection, protect attachments, offer protection against impersonation, and protect internal emails.

Email gateways offer an organisation protection against spear-phishing, malware, spam and zero-day attacks. Multiple detection engines can be combined with policies and procedures to keep out threats and mitigate the risk of data being compromised.

URLs can be protected by installing multistep detection systems and systems that block malicious URLs.

Cyber security technology can use multiple anti-virus engines to detect malware, safely convert files, undertake static file analysis, and employ sandboxing (Mimecast, 2020).

Impersonation protection can be undertaken via real-time scanning of inbound emails to detect header anomalies, domain similarity, and sender spoofing.

Internal emails can be protected by scanning attachments and URLs for malware and malicious links.

Cloud computing

Niedringhaus (2020) notes that cyber technology can make cloud computing more secure in the following ways:

- adopting user access control (Kaplan et al., 2012; McKinsey, 2014);
- application of SSH keys;
- use of multi-factor authentication (MFA);
- patch management, integration with core directory.

Organisations can manage and control user access to cloud servers through:

- automated rights directory service;
- using SSH keys to ensure server connections are secure;
- using MFA to ensure only authorised staff access the cloud server.

Telemetry and system insight monitoring (DeMeyer, 2019) can be used to assess how effectively and efficiently the cloud networks and systems are being used and identify flaws.

The organisation can run a patch management programme (Keller, 2014) so updates occur regularly.

Transaction processing systems (TPS)

Khwaja (2020) notes that TPS can utilise cyber security technology in the securing payment network and payment touchpoints, within the securing operating system, network and

infrastructure, the detection of fraud on payment transactions, the securing of payment applications.

Organisations can circulate EMV cards (EMV Connection, 2020) and implement EMV Acquiring at card-based locations. Where a card is not presented, 3D Secure (Littler, 2020) should be used for added security.

They can secure the operating system, network and infrastructure with Enterprise grade antivirus (Sophos, 2020) and anti- malware software.

An AI based fraud detection system can be used to detect fraudulent payment transactions and TPS payment applications can be made secure through via an IRIS transaction processing system (TPS, 2020).

Evaluation of cyber security technology

SSL, https, and 2FA offer different security features to an organisation's website.

Secure socket layer (SSL) protects an organisation's website and their customers who use the site from cyber threat actors. The value of SSL can be assessed Cade (2019) via the reputation of the SSL certification authority, the pricing of the SSL certificate, if a refund is guaranteed if a digital certificate is cancelled, the specifications of the SSL contract, and the level of technical support offered by the SSL provider.

Hypertext transfer protocol secure (https) enables an organisation's website to be less vulnerable to cybercrimes Schumann (2020). Https provides an organisation's website three layers of protection consisting of encryption, data integrity, and authentication (Kelsey, 2020). For example, https offers an organisation website payment page security whereby cyber threat actors cannot intercept this website content and create the same payments page. This protects the organisation from loss of revenue, ensures the customers' financial details and payment are secure, and the reputation of the business is protected. In addition, https may also help to move an organisation up the search engine rankings. The negatives with https are the cost of the certificate and the need to check that the certificate has not expired.

2FA is regarded as a simple and cost-effective means to ensure users are who they say they are. The value of 2FA can be assessed (Duo Security, 2014; Duo Security, 2018) via the security impact offered against cyber threat actors, its degree of integration with strategic business initiatives, its reliability, cost of ownership, the speed at which it can be implemented and activated, resources required to operate it, ease of use (usability, convenience, and flexibility), ease of administration (detection, reporting, and maintenance) and the scalability of the system.

Legislation

'The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government'. Gov.uk (2020)

Copyright, Designs and Patents Act 1988

Extract on databases

'(1) In this Part "database" means a collection of independent works, data or other materials which:
(a) are arranged in a systematic or methodical way; and
(b) are individually accessible by electronic or other means.

(2) For the purposes of this Part a literary work consisting of a database is original if, and only if, by reason of the selection or arrangement of the contents of the database the database constitutes the author's own intellectual creation.' UK IPO (1988, 27)

Health and Safety at Work etc. Act 1974

Extract on Health and Safety at Work

2. General duties of employers to their employees.

(1) 'It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees'. Legislation.gov.uk (1974)

Computer Misuse Act 1990

Extract on Computer Misuse

'Unauthorised access to computer material'.

(1) A person is guilty of an offence if:

(a) they cause a computer to perform any function with intent to secure access to any program or data held in any computer [F1, or to enable any such access to be secured];

(b) the access they intend to secure [F2, or to enable to be secured,] is unauthorised; and

(c) they know at the time when they cause the computer to perform the function that that is the case'. Legislation.gov.uk (1990)

Communications Act 2003

Extract on Communications

'Application of the electronic communications code

(1) This act regulates the supply of electronic communication networks.

(3) The electronic communications code shall have effect:

(a) In the case of a person to whom it is applied by a direction given by OFCOM; and

(b) In the case of the Secretary of State or any Northern Ireland department where the Secretary of State or that department is providing or proposing to provide an electronic communications network'. Legislation.gov.uk (2003)

This act addresses issues such as:
Piggy Backing: the use of someone's internet connection without their knowledge.

Threating Behaviour Online: Commonly known as 'trolling'. This behaviour is illegal and the act protects receipt of online threats.

Offensive and indecent Images: Sending and/or deliberately sharing these types of images is an offence under this act.

Disaster Recovery Plan (DRP)

Files backed up: data back-up and recovery should be a key element in the continuity plan. Key data should be backed up and in line with agreed back-up and storage protocols (Ready, 2018).

Timescale for back-ups: a schedule relating to the backup of data should take account of the date, frequency, timing, and time taken to back-up data.

Location of back-up: Is this site accessible to designated staff? How sustainable is this location in terms of resources, operations and time? Will key stakeholders (customers and suppliers) be able to attend this venue?

Storage method: is the data digitally stored or is a mixed storage model employed where hard copies are also kept? Is the storage method susceptible to threats such as fire, human error, power failure or irregular power outages?

Key personnel and roles identified: Ensure that key personnel know what is required of them. Allocate clear roles to staff with designated reporting lines which are noted on an organisational chart (Kirvan and Lelii, 2019). Keep staff informed of developments via a communication plan.

Back-up and Recovery strategies

Kirvan (2018) provides an account of the features regarding back-up and recovery strategies (Brush et al., 2020). The back-up and recovery strategies are an essential feature of business resilience. If there is nothing backed up then nothing can be recovered. Growth in cloud based storage means that organisations have more choice regarding storage of data. Factors to consider include:

Multiple vendors handling different activities: If the organisation employs more than one vendor to handle backups and recovery it needs to ensure there is an agreed coordination of activities.

Cloud v bricks and mortar: Is all data to be located in the cloud or will some be stored on site?

Testing: How often are tests conducted to confirm if the organisation can recover effectively?

Frequency of backups: What is the agreed schedule for backup of data?

Non-electronic backups: Where will hard copies of documents be stored? Are the storage premises secure (fire-retardant)?

Back-up technology: (e.g. mirroring, replication, disk, cloud and tape). Have the backup systems kept pace with standard storage processes?

Speed of back-up: If data is needed in an emergency can it be accessed quickly?

Speed of recovery: Can vendor(s) have critical systems operational when required?

What needs to be backed up? Are you backing up essential data?

Recovery Time objective (RTOs): how soon after a 'disaster' hits must a business return to 'normal i.e. how long can it survive in its damaged state – hours, days, weeks or longer?

Recovery Point Objective (RPOs): this is expressed in time (seconds or days) and refers to a business's 'loss tolerance' i.e. how much data can they lose before significant harm is noticeable. This time period is measured from the loss event to the most recent preceding back-up.

Business changes: Have these affected the type of data and the way it's stored and retrieved?

Data security: Ensure the data is secure during backup and recovery.

Disaster Recovery Plan features

There is no all-embracing template in relation to an IT disaster recovery plan (DRP). Each organisation is unique in terms of scale and scope of IT operations. The DRP for a small business will be markedly different to that of an organisation with numerous outlets or divisions that span the globe. The quality,

content and structure of the DRP will be influenced by the competence of the stakeholders involved in its construction and the resources and time allocated to its development and execution. Clearly the main features of a DRP will be dependent on the perspectives of its authors and the objectives set in relation to the plan.

The listed features are taken from various authors (Brush et al., 2020; Pritchard, 2019) and consulting firms (Bacula Systems, 2020; Entechus, 2018) that have studied the constructs of DRPs. These features include: business risk analysis; break down IT risks; setting recovery objectives; command and control; test the response plan; communication plan and role assignments; plan for your equipment; data continuity system; backup check; detailed asset inventory; pictures of the office and equipment (before and after prep); vendor communication and service restoration plan; authorisation; facility plan; electricity plan. Rather than analyse each feature, the features in general will be analysed from the perspective of Fayol's Functions of management and a strategic perspective.

Clearly this is a plan, so are the other elements of Fayol's functions of management evident within the features? Command and control are present and relate to the need for leadership and the deployment of management information systems. Interestingly coordination is missing from the list although it could be argued that the plan combined with leadership direction that everyone should be allocated to undertake activities as and when required.

From a strategic perspective, the starting point is to undertake an environmental analysis so that one can clarify where we are and then where do we want to get to. Business risk analysis and IT analysis are evident within the features and this fits with the strategic approach. Strategic objectives flow from an environmental analysis and this is also reflected in 'the setting of recovery objectives'. A key aspect of strategic planning is the formulation of options, the screening of options, and the decision to choose an option. This formulation – screening process seems to be missing from the features list. Perhaps some consideration could be given to this process in relation to the IT DRP. The next stage in the strategy process is implementation of the DRP. This is a challenge for those leading the DRP as it is essentially a contingency plan. However, there is a reference to 'test the response plan' which in part, meets the implementation requirement although the timing and frequency of this testing needs to be considered.

The final three parts of the strategy jigsaw are control, evaluation, and feedback. Control is in place but features relating to evaluation and feedback are not evident. However, it could be argued that feedback is encapsulated within communication. While there appears to be gaps in the features' list regarding Fayol and the strategy process, it is possible that there are other IT DRP lists with features that would bridge these perceived gaps.

References - Security

Bacula Systems (2020) Disaster Recovery Software Solution. Sample Disaster Recovery Plan Template from Bacula Systems. Available at: https://www.baculasystems.com/best-enterprise-data-backup-solutions/it-disaster-recovery-plan-template-software-solutions?gclid=EAIaIQobChMI2IHcvOT06QIVCbLtCh0Y-QlYEAMYAyAAEgJszPD_BwE [Accessed on 01 May 2020].

CPNI (2015) Passport to good security- for senior executives. Centre for the Protection of national Infrastructure. Available at: https://www.cpni.gov.uk/system/files/documents/b0/69/CPNI_Passport_to_Good_Security.pdf [Accessed on 23 April 2020].

BBC (2020) Data security. British Broadcasting Corporation. Available at: https://www.bbc.co.uk/bitesize/guides/zw3cwmn/revision/2 [Accessed on 21 April 2020].

Cade, V. (2019) Top 6 Factors to Consider While Evaluating SSL Certificate Companies. Available at: https://digipromarketers.com/top-6-factors-to-consider-while-evaluating-ssl-certificate-companies/ [Accessed on 23 May 2020].

CISCO (2020) What Is Cybersecurity? Available at: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html [Accessed on 23 May 2020].

CPNI (2015) Passport to good security- for senior executives. Centre for the Protection of national Infrastructure. Available at: https://www.cpni.gov.uk/system/files/documents/b0/69/CPNI_Passport_to_Good_Security.pdf [Accessed on 23 April 2020].

DeMeyer, Z. (2019) What is System Insights?Available at: https://jumpcloud.com/blog/system-insights [Accessed on 23 May 2020]

Duo Security (2014) Two-Factor Authentication Evaluation Guide. Available at: https://www.ciosummits.com/Online_Assets_Duo_Security_Two-Factor_Evaluation_Guide.pdf[Accessed on 06 May 2020].

Duo Security (2018) Two-Factor Authentication Evaluation Guide. Available at: https://duo.com/assets/ebooks/Duo-Security-Two-Factor-Evaluation-Guide.pdf [Accessed on 06 May 2020].

EMV Connection (2020) Acquirers/Processors. Available at: https://www.emv-connection.com/acquirersprocessors/ [Accessed on 22 May 2020].

Entechus (2018) 7 Key Elements of a Business Disaster Recovery Plan. Available at: https://entechus.com/7-key-elements-of-a-business-disaster-recovery-plan/ [Accessed on 13 May 2019].

Forcepoint (2020) Cloud security: A Buyer's Guide. Available at: https://www.forcepoint.com/form/thank-you-cloud-security-buyers-guide-ebook?form_id=1363&file=48976&resource=36221&category=ebooks [Accessed on 06 May 2020].

Google (2020) Secure your site with HTTPS. Available at: https://support.google.com/webmasters/answer/6073543?hl=en [Accessed on 21 May 2020].

Gov.uk (2020) Data protection. Available at: https://www.gov.uk/data-protection [Accessed on 04 June 2020].

Government of Canada (2018) An introduction to the cyber threat environment. Canadian Centre for Cyber security. Available at: https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf [Accessed on 03 April 2020].

Kaplan, J., Rezek, C., and Sprague, K. (2012) Protecting information in the cloud. McKinsey & Company. Available at: mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Protecting%20information%20in%20the%20cloud/Protecting%20information%20in%20the%20cloud.ashx [Accessed on 23 May 2020].

Keller, G. (2014) Patching Servers Easily and Quickly with JumpCloud. Available at: https://jumpcloud.com/blog/patching-server-easily-quickly-jumpcloud [Accessed on 22 January 2018].

Kelsey, T. (2020) How Increasing Website Security with HTTPS Boosts SEO. Available at: https://www.prontomarketing.com/blog/how-increasing-website-security-with-https-boosts-seo/ [Accessed on 04 May 2020].

Khwaja, S. (2020) Securing Payment Systems. Available at: https://www.tpsworldwide.com/securing-payment-systems-to-prevent-cyber-attacks/ [Accessed on 04 May 2020].

Kirvan, P. (2018) Converged backup and recovery strategies offer efficiency, reliability. Available at: https://searchdisasterrecovery.techtarget.com/tip/Converged-backup-and-recovery-strategies-offer-efficiency-reliability [Accessed on 12 February 2020]

Kirvan, P. and Lelii, S. (2019) Free IT disaster recovery plan template and guide. Available at: https://searchdisasterrecovery.techtarget.com/feature/IT-disaster-recovery-DR-plan-template-A-free-download-and-guide [Accessed on 23 February 2020].

Legislation.gov.uk (2003) Communications Act 2003. Available at: http://www.legislation.gov.uk/ukpga/2003/21/section/106[Accessed on 05 June 2020].

Legislation.gov.uk (1990) Computer Misuse Act 1990. Available at: http://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences [Accessed on 05 June 2020].

Legislation.gov.uk (1974) Health and Safety at Work etc. Act 1974. Available at: http://www.legislation.gov.uk/ukpga/1974/37/section/2 [Accessed on 07 June 2020].

McKinsey (2014) Perspectives on transforming cybersecurity. McKinsey & Company. Available at: https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx [Accessed on 23 June 2019].

Mimecast (2020) Email Security With Targeted Threat Protection. Available at: https://www.mimecast.com/products/email-security-with-targeted-threat-protection/ [Accessed on 14 February 2020].

Micro Focus (2017) IT Disaster Recovery Planning: A Template. Available at: https://www.microfocus.com/media/unspecified/disaster_recovery_planning_template_revised.pdf [Accessed on 04 May 2020].

Niedringhaus, C. (2020) Cybersecurity with Cloud Computing. Available at:https://securityboulevard.com/2020/01/cybersecurity-with-cloud-computing/ [Accessed on 05 May 2020].

Norton (2020a) What is a data breach? Available at: https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html [Accessed on 01 April 2020]

Norton (2020b) Zero-day vulnerability: What it is, and how it works. Available at:

https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html [Accessed on 14 May 2020].

NCSC (2017) Cyber security: Small Business Guide. National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/files/cyber_security_small_business_guide_1.3..pdf [Accessed on 01 May 2020].

Pritchard, S. (2019) Five essential steps to a sound disaster recovery plan. Available at: https://www.computerweekly.com/feature/Five-essential-steps-to-a-sound-disaster-recovery-plan [Accessed on 03 June 2020].

Rainer, K., Prince, B., Watson, H. (2013) Management Information Systems. Third edition, John Wiley & Sons, Inc.

Ready (2018) IT Disaster Recovery Plan. US Government. Department of Homeland Security. Available at: https://www.ready.gov/business/implementation/IT [Accessed on 12 May 2019].

Rouse, M. (2019) zero-day (computer) Available at: https://searchsecurity.techtarget.com/definition/zero-day-vulnerability [Accessed on 08 May 2020].

Schuhmann, A. (2020) Website Security with HTTPS, SSL and TLS: What Exactly are the Differences Between the Trio. Available at: https://www.prontomarketing.com/blog/website-security/ [Accessed on 05 May 2020].

Sophos (2020) Powerful, Enterprise-Grade Antivirus. Available at: https://www.sophos.com/en-us/content/enterprise-antivirus.aspx [Accessed on 11 May 2020].

Smartsheet (2020) Cyber Security: How You Can Protect Your Company's Assets with a Few Simple Steps. Available at: https://www.smartsheet.com/cyber-security-tips-and-policies [Accessed on 21 May 2020].

SSL.com (2020) What is SSL? Available at: https://www.ssl.com/faqs/faq-what-is-ssl/ [Accessed on 20 April 2020].

TPS (2020) IRIS Payment Platform. Available at: https://www.tpsworldwide.com/iris-payments-platform/ [Accessed on 22 May 2020].

UK IPO (1988) Copyright, Designs and Patents Act 1988. Available at:)https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/772818/copyright-designs-and-patents-act-1988.pdf[Accessed on 22 April 2020].

University of Delaware (2020) Data Management. Available at: https://www1.udel.edu/security/data/ [Accessed on 22 April 2020].