The Issues Related to the Use of Information

Unit 3, Assignment 2

Thomas Robinson
rob21005043

15th February 2023
Solihull College

Task One & Two — Issues & How They Can Affect an Organisation

Legal Issues

Data Protection Act (2018) This Act governs the use of personal information by businesses and other organisations, including the Government (Data protection, n.d.). It outlines the responsibilities of data controllers (those holding the information), data processors (those the controller exchanges and processes information with) and the rights of data subjects (those whose information is being handled).

The 2018 amendments—added after the United Kingdom voted to leave the European Union—refer to the UK's General Data Protection Regulation (2020), with stipulations identical to that of the EU Regulation of the same name (2016). It ensures that data stored and processed by organisations is done so fairly and transparently. According to the Information Commissioners Office's Guide to Data Protection (n.d.-a), there are seven principles of the act that set out that data should be handled lawfully, for specific, limited purposes, be kept accurate when required and is stored securely.

The Data Protection Act affects the bank since they are only able to use information that they require and for a legitimate purpose. They must, for example, require customers to opt-in to marketing communications. This legitimate reason must be proven, and the consent from the customer recorded. The bank must be transparent about how they use data, and it must be stored securely. Any data processors the bank deals with must be vetted to ensure they also abide by the regulation, and the bank must be careful to limit who it shares information with.

Freedom of Information Act (2000) In their guide to the Act (n.d.-b), the Information Commissioner's Office states that the Freedom of Information Act allows individuals to request information held by public organisations. The guide also explains that the Act requires that these authorities publish information, such as "policies and procedures, minutes of meetings, annual reports and financial information."

The act covers publicly-owned companies, so those in the public sector or owned by the Government (Freedom of Information Act 2000, 2000, s. 6). An example of an organisation who would have to comply with the Act is Transport for Wales, which is wholly owned by the Welsh Government (2021).

This act does not cover the bank since they are not a public-sector organisation. If they were, they would have to follow the act and the stipulations it sets out, such as publishing policies and disclosing information.

Computer Misuse Act (1990) "An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes." (1990, Introductory Text). Promotional material from the National Crime Agency's Cyber Choices campaign (n.d.) summarises each section of the act as follows:

- Section 1 of the Act covers gaining "unauthorised access to computer material", such as data or programs.
- Section 2 — "unauthorised access with intent to commit or facilitate commission of further offences"
- Section 3 — "unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer."
- Section 3ZA — "unauthorised acts causing, or creating risk of, serious damage"

- Section 3A — “making, supplying or obtaining articles for use in offence” under the other sections (exl. 2) of the Act.

Under the Act, penalties for offences can be a prison sentence, a fine of up to £5000, or both. (Computer Misuse Act 1990, 1990) (Sentencing Act 2020, 2020).

The bank must make sure that their systems are secure, however this piece of legislature prohibits unauthorised access to them. The bank should ensure that staff are trained in best security practices to prevent social engineering and phishing attacks. Staff should also be made aware of the penalties of breaking the law.

Ethical Issues & Code of Practice

Staff use of IT Ethical issues, such as the use of IT by staff, are covered by the bank’s code of conduct and other guidelines. These may include the use of social media, and the use of the bank’s IT systems for personal use. Often, they will also specify communications standards, including tone-of-voice and the use of jargon.

This impacts the working environment of the bank and the employee culture, as well as how they appear as a brand to the public.

Training the bank’s staff on relevent legislation regarding information security could assist in preventing data leakage and unethical practices. This would add extra expense to the organisation, but has the potential to have a positive impact by preventing issues before they occur.

Whistleblowing Whistleblowing is the process of raising an issue either inside or out of the organisation that is in the public interest (Public Interest Disclosure Act 1998, 1998). The UK Government (n.d.) lists the following as examples of grievances that count as whistleblowing and are protected by law:

- a criminal offence, for example fraud
- someone’s health and safety is in danger
- risk or actual damage to the environment
- a miscarriage of justice
- the company is breaking the law, for example does not have the right insurance
- you believe someone is covering up wrongdoing

Most in work are protected—you cannot be “treated unfairly or lose your job” for reporting any of these issues.

The bank must have a whistleblowing policy that outlines how complaints will be dealt with and who should be contacted.

Organisational Policies In general, the policies of the bank can affect the culture of the company and its employees, impacting the way they work and interact with customers. Organisational Policies can provide consistency in communication and decision making by setting out expectations and standards for the company.

Operational Issues

Operational issues can affect the bank in a multitude of ways. Loss of productivity, information and data can be safeguarded against.

Backups Backups are the process of keeping multiple copies of information in the event of a hardware failure, software issue or human error. A common rule to follow regarding backups is the '3-2-1 rule,' where there three overall copies of a piece of data. Two should be on different storage mediums, for example a Hard Disk Drive and a Tape Drive, and one should be offsite and air-gapped. Version control systems—for example, using a Git repository for software development—can provide the facility to rollback to a previous version of a file. This feature is also supported by modern filesystems and operating systems, such as ZFS snapshots and Windows File History.

Continuance Plans Continuance plans refer to the process of addressing issues and major events affecting the company. In the context of IT and information, this includes contingency plans and disaster recovery plans, which can help the bank recover in the event of a failure or disaster. These may outline a process of having multiple sites available if one is unusable or the process of restoring from appropriate backups.

Increasing Sophistication & Use of Technology A significant issue with the increasing use of technology is vendor-lock in. This is the process by which a company becomes reliant on a specific piece of hardware or software and is unable to migrate to a different solution without significant time or expense. For example, the bank may rely on a propriety piece of software provided by a different company for certain aspects of business. If this program does not provide any data export functionality or stores data in an unusual way unlike other programs, it may not be possible to easily move to a different platform. This problem is especially apparent if the maintainers of the software were to go out of business, discontinue the product or introduce significant changes or price rises. It is not uncommon for companies to buy the rights to a legacy program they rely on and begin maintaining it themselves rather than moving to a different solution.

Another problem with increasing technological reliance, especially for information access, is availability and information access. Information only available by technological means may be out of reach for those who are not technically literate. This can disproportionately affect those who are most vulnerable, including homeless people, the elderly and the disabled. It is particularly important in this case, since most everyone requires access to banking services. The bank must make important information available in alternate formats for this purpose.

Conclusion

In closing, there are many restrictions and regulations governing the use of information. It could be argued that this level of regulation could hinder the productivity of the bank by adding complexity to doing business. This argument, however, is overshadowed by the importance of keeping information safe, accessible, and transparent.

References

Computer Misuse Act 1990 (1990). Retrieved February 1, 2023, from https://www.legislation.gov.uk/ukpga/1990/18/

Data protection. (n.d.). Retrieved February 1, 2023, from https://www.gov.uk/data-protection

Freedom of Information Act 2000 (2000). Retrieved February 1, 2023, from https://www.legislation.gov.uk/ukpga/2000/36

Information Commissioner's Office. (n.d.-a). *Guide to Data Protection*. Retrieved February 1, 2023, from https://ico.org.uk/for-organisations/guide-to-data-protection/

Information Commissioner's Office. (n.d.-b). *Guide to freedom of information*. Retrieved February 1, 2023, from https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

National Crime Agency Cyber Choices. (n.d.). *HACKING IT LEGAL - The Computer Misuse Act*. Retrieved February 1, 2023, from https://nationalcrimeagency.gov.uk/who-we-are/publications/523-cyber-choices-hacking-it-legal-computer-misuse-act-1990/file

Public Interest Disclosure Act 1998 (1998). Retrieved February 8, 2023, from https://www.legislation.gov.uk/ukpga/1998/23

Regulation (EU) 2016/679 of the European Parliament and of the Council (2016). Retrieved February 1, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504

Regulation (EU) 2016/679 of the European Parliament and of the Council…United Kingdom General Data Protection Regulation (2020). Retrieved February 1, 2023, from https://www.legislation.gov.uk/eur/2016/679

Sentencing Act 2020 (2020). Retrieved February 1, 2023, from https://www.legislation.gov.uk/ukpga/2020/17

Welsh Government. (2021, February 8). *Welsh rail franchise now in public ownership*. Retrieved February 1, 2023, from https://www.gov.wales/welsh-rail-franchise-now-public-ownership

Whistleblowing for employees. (n.d.). Retrieved February 8, 2023, from https://www.gov.uk/whistleblowing