Unit 3, Assignment 2

The Issues Related to the Use of Information

George Hotten

February 8, 2023

Legal Issues

Data Protection Act (2018)

This law specifies how businesses must safeguard and store sensitive data. Both paper and digitally stored data fall under this. The eight acts are:

- Fair and Lawful
- Purpose
- Adequate
- Accurate
- Retention
- Rights
- Security
- International Transfers

This makes sure that the organisation only collects the information that is necessary and keeps it for the duration of that need. It also ensures that all data is maintained securely. For example, the bank will collect user data and following the requirements from the Data Protection Act, all customer data will be kept secure and safe without the risk of it being seen by someone without permission.

Freedom of Information Act (2000)

This law allows individuals to request access to information held by public bodies such as government departments. Requests for information must, by law, be responded to within 20 working days. Bodies do not have to provide information if it could harm national security or expose commercially sensitive data. The act allows for transparency between the body and the public and allows the public to understand what the bodies are doing.

Computer Misuse Act (1990)

This law covers any unauthorized access to a computer system. This includes hacking into a system (i.e. via a cyber attack), brute forcing a colleague's password or using someone's computer without permission. This includes accessing and/or altering someone's data without their permission.

Ethical Issues

As within most organisations, the bank will have a code of conduct and different other policies regarding the different systems and procedures the bank follows. For example, the bank may have policies on the use of email, the internet and whistleblowing. The different policies will set the ethical standards for how staff should behave (for example, being professional within emails), the appropriate use of the internet, the confidentiality of private data and the reporting of any suspicious behaviour specifically via a whistleblowing policy.

A whistleblowing policy would include who to contact and how to contact them. This helps keep the confidentiality of the reporter and allows for the person to report people who are in a higher position than they are. Typically, companies employ a third-party company to handle the reports and contact the correct person to take appropriate action.

Opertional Issues

Backups

Within the bank, it is vital that data is backed up on a regular basis in case of a disaster. Having backups allows for minimum disruption to the bank's services as the data can be restored from the most recent backup. To have effective backups, the backup should be taken on-site and off-site. In the event of a natural disaster, the data in an off-site backup will remain unaffected and ensures data is not lost if the on-site backup is destroyed. Backups should also be taken at regular intervals, depending on the importance of the data. For example, if the data is crucial to the running of the bank, backups could be taken every 1-2 hours. Data that is less important could be backed up daily, weekly or monthly.

Contingency Plans

A good contingency plan is important to ensure that in the event of a disaster, the business is able to keep running as effectively as possible. In the event that the business is unable to use its current site, two other sites should be set up: a hot site and a cold site.

Hot Site A hot site is a different, usually nearby, location that is set up with all the required infrastructure for the employees to move into and start working almost immediately.

Cold Site A cold site is another location that required setting up before use. For example, the setting up of networking devices and servers would be required before work can continue.

Impact of Increasing Sophistication

As systems become more complex and sophisticated, it is important that the bank keeps up with the latest technology to attract customers with new features and give them a better experience with faster access times on banking services. However, having the latest technology requires large investments which can impact the organisation's resources and operations.

How the Use of Information Affects an Organisation

Electronic Information Systems

Electronic information systems allow for increased speed and productivity compared to manual paper-based information systems. For example, with electronic information systems, you can easily enter a search query and have the system find the information you are after within seconds. Compared to a manual information system, this would take a significantly longer time to find data as the operator would have to search from potentially thousands of different files.

Electronic information systems also allow for data to be backed up in case of a disaster, however, with manual systems all data could be lost in the event of a fire.

This can affect the business's use of information as it allows them to access information faster and easier allowing for increased productivity and speed when completing a task that requires access to data. Having data stored electronically can also help save, copy and replace data without the need to re-write the whole document every time an amendment needs to be made.

Complying with Legal Requirements

There are many laws businesses must follow when holding and processing data, notably the General Data Protection Regulation act. GDPR requires:

- Transparency - must be open on what data they collect and how they store it.
- Lawful Processing - must have a lawful reason for collecting and processing personal data.
- Data Minimization - collect the minimum amount of data required for their purpose.
- Data Accuracy - data collected must be as accurate and up-to-date as possible.
- Storage Limitation - data must not be stored for longer than needed.
- Security - proper security measures must be implemented to ensure personal data is protected.
- User Rights - users must be able to request a copy of their data and must be able to request its deletion.
- Data Breaches - organisations must report data breaches to the relevant authorities and the affected users within a certain time frame.
- Data Protection Officers - each organisation must appoint a DPO who oversees their data handling and protection.

This can affect the business's use of information as it adds extra complexity to getting and storing data as they must comply with the strict rules of GDPR. This can also require stricter access control to data, ensuring staff can only access what they need to complete their job. These extra layers of security help keep user information safe and helps the end-users trust in the business's handling of their data.

Vendor Lock-in

Vendor lock-in is where businesses can become trapped into using specific software or a particular operating system based on compatibility with custom integrations with other hardware devices or because of the use of proprietary software.

For example, in 2009 a company may invest a large amount of money into a system or device that integrates with the current operating system of the time: Windows 7. The company may choose to further build their whole network and systems around Windows 7 to have parity with the devices they want to integrate. However, when Windows 7 approaches end-of-life, the company may find that its software is not compatible with Windows 10 and therefore not want to spend the time and money to upgrade it, so they don't upgrade. This is an example of vendor-lock-in. This can cause in the upcoming months as the operating system stops receiving security updates leaving their systems vulnerable to attacks and malware.

This can affect the business's use of information as in the event of a cyber-attack on the business due to a lack of security updates the employees may not be able to access vital information until the issue has been resolved or the information could be outright deleted by the attackers.