Level 1/2 Vocational

ICT

1.3.2 The impact of data loss, theft, or manipulation

Financial implications

For individuals:

- **Lost work:** Losing unsaved work due to system failure or human error.
- **Scams:** Falling victim to scams can lead to direct financial loss.
- **Bank details stolen:** This can result in significant financial loss from your accounts.

For businesses:

- **Direct financial loss:** Money stolen or diverted.
- **Downtime costs:** Loss of productivity and revenue when systems are not working.
- **Fines:** Penalties imposed by regulators for non-compliance with data protection laws.
- **Compensation:** Payments will need to be made to affected customers.
- **Staff costs:** Resources diverted to fix problems rather than perform usual tasks.

Moral and legal implications

Organisations have a moral duty to keep customer data safe and confidential. People share sensitive information (for example with banks, doctors or government bodies) expecting it to be protected.

Breaking of GDPR/DPA

Not only is there a moral obligation to keep data safe, but it is also a legal requirement. The UK GDPR and Data Protection Act 2018 (DPA 2018) mandates strict data protection.

- Organisations that fail to keep data secure face severe penalties.
- Fines can be up to £17.5 million or 4% of global annual turnover (whichever is greater).
- Failure to report a data breach can also lead to fines.

Competitor advantage

- If a company's unique software codes, product designs or secret methods are stolen, it can lose its market advantage.
- Competitors with access to this sensitive information can replicate products or services, undermining the original company's position.

Blackmail

- Stolen data can be used to blackmail organisations.
- Businesses might pay large sums of money to prevent the release of sensitive data, avoid further financial damage or protect their reputation.

Data manipulation

This involves data being changed, usually for fraudulent purposes (for example altering payment amounts or modifying records). Such changes can be difficult to detect immediately, potentially leading to significant financial losses or incorrect decisions before the manipulation is discovered.

Loss of service

When IT systems or websites go down due to data issues, services become unavailable. If a service is lost, customers cannot access accounts, purchase goods or use essential services. This leads to lost revenue, customer frustration and disruption to scheduled operations.

Loss of intellectual property (IP)

Intellectual property (IP) refers to unique ideas, inventions or designs created by an individual or company (for example game code, new product designs or logos). This is often protected by patents or copyright. If IP is lost or stolen and falls into the hands of competitors, it can be disastrous, undermining years of development and investment.

Loss of reputation

When a data breach occurs, customer trust is severely damaged. Customers expect organisations to safeguard their personal and financial data. A damaged reputation can lead to a significant loss of current and future business, as customers may choose to use more trustworthy competitors. Rebuilding a lost reputation is extremely difficult.