

Data Security Governance and Compliance

(ACCA7028)

Group = 1

Group member:

- | | | |
|----|------------------|-----------|
| 1. | Harsh Dhokiya | (2545109) |
| 2. | Janki Patel | (2520611) |
| 3. | Nirav Thummar | (2537379) |
| 4. | Sameer Sukhadiya | (2536690) |

Scenario 1: Data Breach at a Financial Institution

What are Legal Issues?

- **Legal issues** are problems that arise when an organization **fails to follow laws, regulations, or legal obligations**.
- In this case, the financial institution had a legal duty to protect customer information. By failing to update security software despite repeated IT warnings, it may have violated several laws.

1. Legal Issues:

A. Laws and Regulations That Apply to This Scenario

a. UK GDPR (UK General Data Protection Regulation)

Purpose:

- Protects personal data and the privacy of individuals.
- Requires organizations to keep customer information secure.

How it applies to the case:

- The financial institution failed to update security software.
- Customer personal and financial data was exposed.

- The company did not take appropriate security measures to protect data.

Key Requirement:

- Organizations must implement suitable technical and organizational security controls to protect personal information.

b. Data Protection Act 2018

Purpose:

- Supports and supplements UK GDPR in the United Kingdom.
- Sets rules for processing and protecting personal data.

How it applies to the case:

- The institution failed to adequately protect customer information.
- The breach exposed sensitive customer data.

Key Requirement:

- Organizations must handle personal data lawfully, fairly, and securely.

c. Computer Misuse Act 1990

Purpose:

- Makes unauthorized access to computer systems illegal.
- Protects organizations against hacking and cybercrime.

How it applies to the case:

- Hackers gained unauthorized access to the institution's systems.
- Although the hackers are primarily responsible for the attack, the institution's weak security contributed to the breach.

d. Financial Conduct Authority (FCA) Regulations

Financial Conduct Authority

Purpose:

- Regulates financial institutions in the UK.
- Ensures firms manage risks and protect customers.

How it applies to the case:

- The institution failed to manage cybersecurity risks effectively.
- Ignoring IT warnings demonstrates poor risk management.

Key Requirement:

- Financial institutions must maintain strong operational and information security controls.

B. Potential Legal Consequences for the Financial Institution

a. Regulatory Fines

What could happen?

- Regulators may impose substantial financial penalties.

Reason:

- Failure to protect customer information.
- Failure to follow data protection laws.

Impact:

- Significant financial loss.
- Damage to company reputation.

b. Regulatory Investigation

What could happen?

- Authorities may launch a formal investigation.

Reason:

- Determine why security warnings were ignored.
- Assess whether the organization complied with legal requirements.

Impact:

- Increased scrutiny from regulators.
- Requirement to improve security controls.

c. Customer Lawsuits

What could happen?

- Customers may sue the institution.

Reason:

- Personal information was exposed.

- Customers may suffer financial losses or identity theft.

Impact:

- Legal expenses.
- Compensation payments.

d. Compensation Claims

What could happen?

- Affected customers may request compensation.

Reason:

- Data exposure.
- Fraud or identity theft resulting from the breach.

Impact:

- Additional financial costs for the institution.

e. Enforcement Actions

What could happen?

- Regulators may require corrective actions.

Examples:

- Improve cybersecurity measures.
- Conduct security audits.
- Implement stronger risk management procedures.

Impact:

- Increased compliance costs.
- Ongoing monitoring by regulators.

f. Reputational Damage

What could happen?

- Loss of customer trust.

Reason:

- Customers expect financial institutions to protect sensitive information.

Impact:

- Customer dissatisfaction.
- Loss of existing and potential customers.
- Reduced business performance.

2. Ethical Issues:

A. Ethical Responsibilities Towards Customers

1. Protect Customer Information

Responsibility

The financial institution has an ethical duty to keep customer data safe and secure.

Why?

Customers trust the institution with sensitive information such as:

- Names
- Addresses
- Phone numbers
- Bank account details
- Financial records

Ethical Failure

The company failed to protect this information by ignoring security updates and IT warnings.

2. Act with Responsibility and Care

Responsibility

The institution should take reasonable steps to prevent harm to customers.

Why?

Customers expect their bank or financial institution to manage risks responsibly.

Ethical Failure

Management ignored known security risks, increasing the chance of a data breach.

3. Maintain Trust

Responsibility

Trust is essential in the financial sector.

Why?

Customers share confidential information because they believe it will be protected.

Ethical Failure

The breach damaged customer confidence and trust in the institution.

4. Be Honest and Transparent

Responsibility

Organizations should communicate openly when problems occur.

Why?

Customers have the right to know if their information has been compromised.

Ethical Failure

If the company delays or hides information about the breach, it would be acting unethically.

5. Respect Customer Privacy

Responsibility

Personal information should be treated with respect and confidentiality.

Why?

Customers have a right to privacy.

Ethical Failure

The breach exposed private information that should have been protected.

B. How Should the Company Address the Breach Ethically?

1. Inform Customers Immediately

Action

Notify all affected customers as soon as possible.

Purpose

- Allow customers to protect their accounts.
- Reduce the risk of fraud and identity theft.

Ethical Benefit

Demonstrates honesty and transparency.

2. Take Responsibility

Action

Acknowledge the mistake and accept accountability.

Purpose

Avoid blaming others or hiding the problem.

Ethical Benefit

Shows integrity and professionalism.

3. Provide Support to Affected Customers

Action

Offer assistance such as:

- Credit monitoring services
- Fraud protection
- Customer support helplines

Purpose

Help customers reduce potential harm.

Ethical Benefit

Demonstrates care and responsibility.

4. Conduct a Full Investigation

Action

Identify how and why the breach occurred.

Purpose

Prevent similar incidents in the future.

Ethical Benefit

Shows commitment to improvement.

5. Improve Security Measures

Action

Implement stronger cybersecurity controls:

- Regular software updates
- Security audits
- Employee training
- Multi-Factor Authentication (MFA)

Purpose

Protect customers from future breaches.

Ethical Benefit

Demonstrates responsibility and commitment to customer safety.

6. Be Transparent About Improvements

Action

Inform customers about the steps being taken to strengthen security.

Purpose

Rebuild trust and confidence.

Ethical Benefit

Shows openness and accountability.

3. Professional Issues:

A. What Professional Standards and Practices Were Neglected?

1. Patch Management

Definition: Keeping software and security systems updated with the latest patches and fixes.

Neglected Practice:

- The institution failed to update its security software.
- Known vulnerabilities remained unpatched despite warnings from the IT department.

Impact:

- Attackers exploited these vulnerabilities, leading to the data breach.

2. Risk Management

Definition: Identifying, assessing, and mitigating security risks before they cause harm.

Neglected Practice:

- IT staff identified the security risk and issued multiple warnings.
- Management failed to assess and address the risk appropriately.

Impact:

- The known risk developed into a major security incident.

3. Security Governance

Definition: The framework through which management directs and controls cybersecurity activities.

Neglected Practice:

- Senior management ignored security recommendations.
- Security concerns were not treated as a priority.

Impact:

- Weak decision-making contributed to the breach.

4. Continuous Monitoring

Definition: Regularly monitoring systems for vulnerabilities and security threats.

Neglected Practice:

- The institution did not effectively monitor or respond to security weaknesses.
- Vulnerabilities remained unresolved.

Impact:

- Threats were not detected or addressed in time.

5. Due Diligence and Professional Responsibility

Definition: Taking reasonable precautions to protect organizational and customer data.

Neglected Practice:

- The institution failed to act on clear warnings from cybersecurity professionals.
- Preventive measures were not implemented.

Impact:

- Customer data was exposed, resulting in legal and reputational consequences.

B. How Can the Institution Improve Its Information Security Practices to Prevent Future Breaches?

1. Implement Regular Software Updates

Action:

- Install security patches immediately after release.
- Maintain an effective patch management schedule.

Benefit:

- Reduces vulnerabilities that attackers can exploit.

2. Conduct Regular Risk Assessments

Action:

- Identify potential threats and weaknesses.
- Evaluate the impact and likelihood of security risks.

Benefit:

- Helps prioritize security improvements.

3. Strengthen Security Governance

Action:

- Ensure management takes cybersecurity risks seriously.
- Establish clear security policies and responsibilities.

Benefit:

- Improves decision-making and accountability.

4. Provide Cybersecurity Training

Action:

- Train employees and managers on security awareness.
- Educate staff about current cyber threats and best practices.

Benefit:

- Creates a stronger security culture throughout the organization.

5. Use Multi-Factor Authentication (MFA)

Action:

- Require users to verify their identity using multiple authentication methods.

Benefit:

- Provides an additional layer of security against unauthorized access.

6. Perform Security Audits and Penetration Testing

Action:

- Regularly test systems for vulnerabilities.
- Review security controls and compliance.

Benefit:

- Identifies weaknesses before attackers can exploit them.

7. Develop an Incident Response Plan

Action:

- Create procedures for detecting, responding to, and recovering from cyber incidents.

Benefit:

- Minimizes damage and improves recovery time during future attacks.

8. Implement Continuous Monitoring

Action:

- Monitor networks, systems, and user activities in real time.
- Use security tools to detect suspicious behaviour.

Benefit:

- Enables faster detection and response to threats.