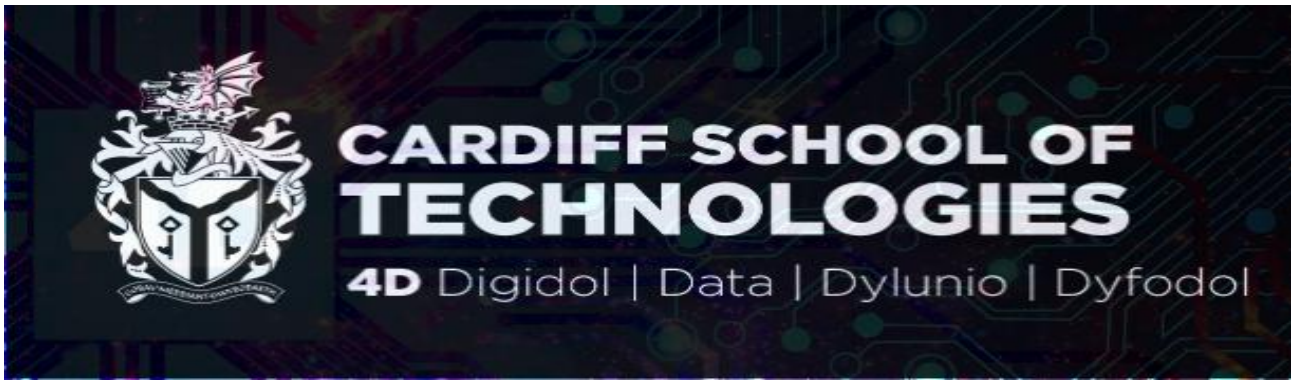

Cardiff Metropolitan University	
Cardiff School of Technologies	
Academic Year: 2024/2025	
Term: 1	
Module Name: Information Security	
Module Code: SEC7000	
Module Leader: Dr Liqaa Nawaf	
MSc Programme: Data Science	
Assignment Title: Information Security Assignment WRIT1	
Student Name: Sajina Shrestha	**Student ID: st20307767**

Table of Contents

Chapter 1 4
Section 1.1: Data Protection by Design and Default 4
Introduction 4
Integrating Data Protection by Design 4
Integrating Data Protection by Default 5
Section 1.2: Mapping Best Practices of ISO 27001, Cyber Essentials, NIST, and COBIT with GDPR 5
I. ISO 27001 and GDPR 6
II. Cyber Essentials and GDPR 7
III. NIST Cybersecurity Framework and GDPR 8
IV. COBIT and GDPR 9
Section 1.3: Mechanisms for Implementing Security and Incident Response and Reporting 10
i. Security Mechanisms 10
ii. Incident Response Mechanisms 11
iii. Incident Reporting Mechanisms 12
CHAPTER 2 13
Section 2.1. Description of the attack, exposed vulnerability, and loss to the organization. 13
Introduction 13
Overview of the Attack 13
1) Vulnerability Exploited 13
2) Loss to the Organization 14
Section 2.2: Critical Evaluation of the Attack, Tools Used by the Attackers, and Recommended Preventive Mechanisms 15
Attack Analysis: Tools and Techniques Used by Attackers 15
Evaluation of Vulnerabilities and Risks 16
Recommended Preventive Mechanisms 16
Section 3.3: Implement the Risk Management / Risk Assessment, Evaluate the impact, likelihood, and risk level associated with the incident, and propose risk mitigation strategies using risk assessment template 17
Risk Assessment Table Overview 17
Impact Evaluation 18
Likelihood Evaluation 18
Risk Mitigation Strategies: 19
Conclusion 20
Chapter 3 21

Section 3.1: Write a reflective report on your practical development of the practical activities. ... 21
Cyber Essentials Labs from Cisco: ... 21
Immersive Labs: ... 21
Conclusion: ... 21
References ... 22

Chapter 1

Section 1.1: Data Protection by Design and Default

Introduction

Data Protection by Design and Default is a key element of the UK General Data Protection Regulation (UK GDPR), which aims to include data protection safeguards throughout the lifetime of systems and services from the start (ico.org, 2024). For the organization creating surveillance technologies such as CCTV and facial recognition, as well as contact tracking apps, Data Protection by Design and Default guarantees that privacy is a top priority throughout the design, development, and deployment phases. The following are ways for integrating Data Protection by Design and Default into the systems that will be developed. (Kemper, 2024)

Integrating Data Protection by Design

i. **Privacy Impact Assessments:** Before initiating development, it is necessary to do Data Protection Impact Assessments. It assist in identifying dangers connected with processing personal data, particularly when dealing with sensitive information such as biometric data (from facial recognition) or location data (from contact tracking applications) (BritishAssessment, 2024). These evaluations should be undertaken at the beginning and updated as the project progresses to ensure ongoing compliance with privacy standards and regulations. (Delev, 2024) (Grande, 2023)

ii. **Minimization of Data Collection**: The data minimization concept states that just the data required for a specified purpose should be collected (Herath, 2023). Surveillance devices may capture photos just during the relevant fields of view and periods (GDPR-Advisor, 2023). For contact tracing, data should be restricted to the proximity information required to trace viral transmission, with identifiable personal information excluded whenever feasible. This reduces the risk of user data exposure while also ensuring compliance with privacy standards. (Sullivan, 2023)

iii. **Access Controls and Role-Based Permissions:** Only authorized individuals should have access to sensitive information, thus proper access controls are crucial (FasterCapital, 2024). Role-based access control procedures should be implemented, limiting data access to workers who have specified jobs that require it.

This strategy assures that surveillance video, contact tracing data, and other sensitive information are handled only by authorized personnel, lowering the danger of unauthorized usage or breach. (Antonenko, 2023) (frontegg, 2024)

Integrating Data Protection by Default

i. **Default Privacy Settings:** Systems must have privacy-friendly options as the default option. For example, the contact tracking software should be constructed so that it automatically opts out of unwanted data sharing. Only required data-sharing functionality should be engaged at first, with further features requiring express user permission. This guarantees that users are not subjected to unnecessary data collecting just for utilizing the system. (Secure Privacy ai, 2024)

ii. **Transparency and User Control**: Ensuring openness in data gathering processes is critical. Users must be given clear and understandable information about the data being collected, how it is processed, and for what objectives. Privacy notifications should be concise and informative, allowing consumers to make informed decisions. Furthermore, users should be able to view, amend, and delete their data using simple interfaces, giving them control over their personal information. (dataprotection.ie, 2024) (Secure Privacy ai, 2024)

iii. **Encryption and Secure Storage by Default**: To prevent unwanted access, all acquired data should be encrypted both at rest and in transit. Encrypting data, such as CCTV video or contact tracing records, is a fundamental necessity for protecting sensitive information. (gdpradvisor, 2023)

Section 1.2: Mapping Best Practices of ISO 27001, Cyber Essentials, NIST, and COBIT with GDPR

In the development of surveillance technologies and contact tracing applications for the UK government, security frameworks and standards such as ISO 27001, Cyber Essentials, NIST (National Institute of Standards and Technology), and COBIT (Control Objectives for Information and Related Technology) should be aligned with the UK GDPR principles and requirements. While GDPR focuses largely on data protection and privacy, the aforementioned standards take a holistic approach to information security management, risk reduction, and operational governance, all of

which help to achieve GDPR compliance. The following is an in-depth breakdown of various frameworks that overlap with GDPR principles and aid the company in implementing best practices. (Barrus, 2024)

I. ISO 27001 and GDPR

ISO 27001 is a widely recognized standard for managing information security. It offers enterprises a methodical approach to developing, implementing, maintaining, and constantly improving an Information Security Management System. Its strong emphasis on risk management, security measures, and accountability is completely compatible with GDPR's data protection regulations. (Mishova, 2023)

- **Risk-Based Approach**

  The risk-based approach to information security is a core ISO 27001 principle. This includes detecting, assessing, and reducing risks associated with the handling of personal data. ISO 27001 supports GDPR's emphasis on risk assessment in order to identify and apply relevant protective measures (gdpr-advisor, 2023). For example:

  - Regular risk assessments help company detect imperfections in systems and procedures that might result in unauthorized data access or breaches.
  - Set up risk treatment plans. Ensure that preventive activities are properly recorded, tracked, and implemented. (Maldoff, 2016) (gdpr-advisor, 2023)

- **Security Controls and Safeguards**

  ISO 27001 Annex A contains a comprehensive set of controls that closely correlate with the GDPR's technological and organizational safeguards (Chopra, 2024). Key controllers include:

  - **Access Control:** Access to personal data is limited to authorized employees based on their positions and responsibilities. (Chopra, 2024)
  - **Encryption:** Preventing unwanted access to personal data while it is being stored and transmitted.
  - **Audit Logs:** Recording data access events improves accountability and traceability, which is essential for showing compliance. (johansonllp, 2024)

- **Continual Improvement and Monitoring**

  ISO 27001 requires continuous monitoring and enhancement of the Information Security Management System to handle emerging threats and technological

improvements. Regular audits, evaluations, and upgrades maintain the effectiveness of security measures. This constant growth is consistent with the GDPR's need for enterprises to maintain a high level of data protection over time. (isocouncil, 2024)

- **Supplier and Third-Party Risk Management**

  Many GDPR infractions result from flaws in third-party systems. ISO 27001 sets out rules for assessing and managing risks faced by suppliers and partners. For example:

  - Contracts must include data protection terms.
  - Regular inspections guarantee third parties meet the organization's security standards. (Kosutic, 2023)

II. Cyber Essentials and GDPR

Cyber Essentials is a UK government-backed certification system that protects businesses from the most frequent cyber-attacks. Its simplicity and emphasis on core security measures make it ideal for enterprises seeking to comply with GDPR's data protection standards.

- **Secure Configuration**

  Cyber Essentials highlights the need to securely configure devices and systems to avoid unwanted access. This involves deleting unneeded accounts, turning off unwanted services, and enforcing secure password restrictions. These steps are consistent with the GDPR's require to install technological controls that protect personal data.

- **Boundary Firewalls and Gateways**

  The architecture requires enterprises to set up border firewalls to filter and manage incoming and outgoing traffic. These firewalls protect sensitive data from external threats, which helps in the GDPR's duty to secure personal data.

- **User Access Control**

  Reducing access to data and systems to those who require it lowers the probability

of data breaches. Cyber Essentials supports the GDPR's data minimization principle by ensuring that personal information is only accessible for authorized and required purposes.

- **Software Updates and Patch Management**

  Cyber Essentials emphasizes the necessity of keeping software up to date. Regular updates defend against known vulnerabilities, which hackers may use to obtain unauthorized access to sensitive information. This is consistent with GDPR's duty to maintain up-to-date security measures.

III. NIST Cybersecurity Framework and GDPR

The NIST Cybersecurity Framework offers a comprehensive strategy to addressing cybersecurity concerns (NCSC, 2022). Its five primary functions Identify, Protect, Detect, Respond, and Recover provide useful direction for achieving GDPR compliance obligations.

- **Identify**

  NIST highlights the significance of understanding data flows, assets, and possible risks. Maintaining an inventory of data processing operations and maintaining transparency in data flows are consistent with the GDPR's emphasis on accountability and data mapping. (cloudflare, 2024)

- **Protect**

  NIST recommends techniques for protecting personal data from attacks. Key security measures include:

  - **Data Encryption:** Keeping data secure at idle and in transit to avoid illegal access.
  - **Access Controls:** Implementing role-based access limits guarantees that only authorized persons have access to personal information.
  - **Secure Development Practices:** Integrating security into the software development lifecycle reduces risks in programs that handle personal information. (cloudflare, 2024)

- **Respond**

  NIST points out the need for an effective incident response strategy to limit the impact of data breaches. This includes:

  - Controlling the breach.
  - Notifying impacted persons and authorities.
  - Implementing remedial measures to prevent recurrence. (cloudflare, 2024)

- **Recover**

  Recovery protocols guarantee that activities resume swiftly and effectively following a security event. This is consistent with the GDPR's focus on reducing the effect of breaches and restoring impacted persons' data access rights. (cloudflare, 2024)

IV. COBIT and GDPR

COBIT (Control Objectives for Information and Related Technologies) is a governance and management framework that defines best practices for aligning IT operations with corporate goals. Its strategy focus on accountability, transparency, and process improvement is strongly aligned with GDPR standards. (Karczewska, 2017)

- **Governance and Accountability**

  COBIT indicates the creation of explicit roles and responsibilities for data protection. It complies with GDPR's requirement for a structured governance system by guaranteeing accountability at all levels, including the appointment of Data Protection Officers (DPOs) when needed. (Kamau, 2020)

- **Risk Management Integration**

  COBIT combines IT risk management with other business operations. This enables enterprises to discover, analyze, and reduce risks to personal data, guaranteeing compliance with the GDPR's privacy by design and default principles. (Kamau, 2020)

- **Performance Monitoring**

  COBIT includes tools for assessing and monitoring the performance of IT systems and processes. This guarantees that data protection measures are not only effective but also flexible in response to new threats and compliance requirements. (Now, 2021)

- **Ethical and Privacy Considerations**

  COBIT includes ethical issues into its structure, ensuring that businesses find a balance between meeting commercial objectives and protecting human privacy. This is consistent with the GDPR's primary focus on protecting data subjects' rights and freedoms. (Kamau, 2020)

Section 1.3: Mechanisms for Implementing Security and Incident Response and Reporting

To guarantee strong data protection and regulatory compliance, the firm must adopt comprehensive security procedures as well as effective incident response and reporting protocols. These procedures are critical for minimizing the hazards associated with surveillance and contact tracking technology. (aarc-360, 2024)

i. Security Mechanisms

Implementing layered security measures is essential for protecting systems and data against unwanted access, breaches, and other threats (McCart, 2024).

- **Network Security**

  Data protection is built upon a secure network infrastructure.

  - Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS): It control and monitor network traffic, detecting and preventing harmful activity.
  - Segmentation: Isolate sensitive systems to reduce the risk of a compromise.
  - Virtual Private Networks (VPNs): Encrypt data transferred remotely to ensure secrecy and integrity. (McCart, 2024)

- **Data Encryption**

  Encryption is essential for securing personal information:

  - Encryption in Transit and at Rest: It use strong algorithms to protect data during transmission and storage.
  - Key Management: Implement centralized methods to protect and control encryption keys. (Schwikkard, 2023)

- **Access Control and Authentication**

  Restricting access guarantees that only authorized individuals can interact with sensitive systems:

  - Role-Based Access Control: This defines roles and assign access based on work duties.
  - Multi-Factor Authentication: It increases security for company by requiring several verification methods.
  - Principle of Least Privilege: Limit access to the minimum required for job functions. (Schwikkard, 2023)

- **Secure Software Development Lifecycle**

  Integrating security into software development minimizes vulnerabilities:

  - Conduct frequent vulnerability assessments and penetration tests during development.
  - Implement secure coding methods to reduce threats like SQL injection and cross-site scripting.
  - Use static and dynamic code analysis techniques to spot errors early. (Schwikkard, 2023)

ii. Incident Response Mechanisms

Incident response guarantees that security issues are detected, contained, and recovered as quickly as possible, minimizing damage and inconvenience. (Wlosinski, 2022)

- **Incident Response Team**

  An incident response team handles and resolves situations effectively.

  - The roles and responsibilities include technical analysts, legal consultants, and communication professionals.
  - Regular training and tabletop exercises enhance preparation for many circumstances. (Appleby, 2018)

- **Incident Detection and Monitoring**

  Proactive monitoring detects possible breaches early:

- Security Information and Event Management: This analyzes logs to identify abnormalities and prioritize problems.
- Threat Intelligence: Utilize real-time information to identify and address developing threats.
- Automated Alerts: Set up automated alerts to detect suspicious activity.
- systems and mitigate vulnerabilities before restarting operations. (Appleby, 2018)

- **Post-Incident Review**

  A detailed analysis improves future incident handling:
  - Document the incident's cause, timeframe, and actions.
  - Improve response procedures by identifying gaps and making recommendations.
  - Improve incident response strategies based on lessons learned. (Appleby, 2018)

iii. Incident Reporting Mechanisms

Incidents should be reported in a timely and transparent manner to guarantee regulatory compliance and stakeholder confidence.

- **Internal Reporting**

  Create explicit mechanisms for reporting issues within.
  - Employees should be trained to identify and report suspicious activity as soon as possible.
  - Establish escalation channels to ensure the IRT responds quickly to major issues. (Appleby, 2018)
- **Communication with Affected Parties**

  Transparency with affected persons is essential.
  - Provide clear and practical details about the compromise.
  - Provide advice on precautions, such as monitoring accounts or upgrading credentials. (Appleby, 2018)

CHAPTER 2

Section 2.1. Description of the attack, exposed vulnerability, and loss to the organization.

Introduction

One of the biggest impactful and well-known security breaches of 2024 was when Dropbox Sign (formerly known as HelloSign) got hit by cyber criminals back in April. Basically, this attack took a shot at Dropbox's working systems, spilling the beans on customers' login details and private account info. Dropbox is like this top-notch giant in storing stuff online and helping people work together easily, so this incident really kind of hurt their image and shook-up users' faith. (Spencer, 2024)

Overview of the Attack

unauthorized access to Dropbox's to the production environment for Dropbox's Sign, exfiltrated sensitive customer account information. The stolen data consists of email addresses, usernames, hashed passwords, and sensitive authentication credentials, including OAuth tokens, API keys, and multi-factor authentication (MFA) bypass tokens. This gave attackers access to many customer accounts and applications that rely on Dropbox's services. The compromise was accomplished by using improperly secured systems coupled with phishing attacks against employees. (Spencer, 2024)

The breach had ripple effects throughout Dropbox's customer base. To date, Dropbox Sign is used by more than 50K companies ranging from a small seller to big enterprises that manage sensitive agreements. Consequently, if user credentials were compromised, that translated directly into a risk to these organizations, potentially widening the breach beyond Dropbox alone. (marom, 2024)

1) Vulnerability Exploited

The attackers took use of an unpatched vulnerability in a third-party integration utilized within the Dropbox environment. Insufficient monitoring of the API key's usage and an inadequate implementation of an MFA enabled the attackers bypass multiple defensive layers. The incident illustrated how the weaknesses in supply chains and weak third-party security practices can cascade to have wide-ranging effects on mission-critical systems. (Abrams, 2024)

The other significant issue leading to the compromise was insufficient separation of production and development environments, enabling attackers to move laterally from initial entry to access sensitive systems. In addition, it was observed that the authentication management of Dropbox failed to detect anomalies in token activity in a timely manner, having given to the attackers more extended time to exfiltrate customer data. (fournet, 2024)

2) Loss to the Organization

The Dropbox breach resulted in major financial, operational, and reputational consequences:

a. Financial impact:

Dropbox incurred millions of dollars in costs related to incident response, customer notification, forensic investigations, and improvements in its cybersecurity framework during the period of the breach incurring thousands for Dropbox. Furthermore, the breach put Dropbox in the possible future risk of regulatory fines under GDPR and other global privacy laws for failing to secure sensitive customer data adequately. (Mascellino, 2024)

b. Operational Impact:

Dropbox clarified that in the current situation, they are pausing services related to Dropbox Sign to prevent any further exploitation immediately after the attacks. It would affect business operations for a large number of these customers, whom the company depends on for critical document handling, causing lost productivity and income for all these companies. (Sharwood, 2024)

c. Reputational Damage:

Only the breach harmed consumer trust and damaged much of the strong customer confidence among business clients who had embraced Dropbox as their go-to for all secure operations. Estimate that many consumers will voice their concerns about this company's ability to keep sensitive information private, which will, to some extent, force them to migrate to some of its competitors with better practices. Investors reacted to the situation, and with little opportunity for further dropping, Dropbox's share price fell dramatically. (Mascellino, 2024)

Section 2.2: Critical Evaluation of the Attack, Tools Used by the Attackers, and Recommended Preventive Mechanisms

The Dropbox Sign breach, which contained significant customer details vulnerable, provides an important case study for analyzing contemporary ways of breaking into computer systems. It reveals the ability of malicious players to exploit several vulnerabilities on cloud-based platforms, which makes it an outstanding example of the risks related to hygiene and poor security in production environments. (Kapko, 2024)

Attack Analysis: Tools and Techniques Used by Attackers

The Dropbox Sign (previously called HelloSign) attack was accomplished by abusing a range of weaknesses in the IT infrastructure of the organization. Attackers used phishing, API key theft, and improper authentication protocols to penetrate the Dropbox systems. (Zorz, 2024)

a) Phishing Campaign:

One of the major channels exploited by the attackers was phishing emails aimed at Dropbox employees. These emails contained malicious links or attachments intended to collect login information (Baran, 2024). This first penetration enabled the attackers to obtain access to internal systems and move laterally throughout the business.

b) Exploitation of API Key Vulnerabilities:

After gaining initial access to the compromised system through the phishing attack, the attackers then sought to exploit unprotected API keys and OAuth tokens. These credentials were the gateway to some of Dropbox's most important systems, including user account information and authentication systems. Their stolen keys were then used to access and exfiltrate sensitive data. (Zorz, 2024)

c) **Inadequate Multi-Factor Authentication (MFA) Controls**:

Dropbox has adopted multi-factor authentication (MFA) however attackers were able to circumvent it, most likely by exploiting weaknesses in the MFA configuration or using stolen tokens that overcame the second stage of authentication. Multi- factor authentication bypass methods, such as SIM swapping or using stolen session tokens, were most likely employed in this case. (Baran, 2024)

Evaluation of Vulnerabilities and Risks

The incident exposed many critical flaws in Dropbox's security posture:

a) **Lack of Segmentation**:

Once the attackers gained access via phishing, they were able to pivot inside the environment and compromise other portions of the network. The lack of network segmentation allows attackers to gain deeper access to vital systems without meeting substantial restrictions. (Dropbox dign team, 2024)

b) **API and Key Management Weaknesses**:

This caused a problem with dependency wherein Dropbox overly relied on APIs for authentication and managing user access. Poor API key management practices made it easier for attackers to illicitly extract sensitive data. API keys that were broadly scoped, insecurely stored within the environment became a critical vulnerability in the organization (Baran, 2024).

Recommended Preventive Mechanisms

Avoid similar dangers and solve the vulnerabilities discovered during the Dropbox Sign breach, consider the following preventive mechanisms:

a) **Enhanced User Training and Awareness:**

Employee awareness training should be the first step in preventing phishing assaults. Companies may dramatically limit the chance of gaining early access through social engineering by training their staff on phishing strategies, particularly those targeting high-value targets such as senior executives. Regular phishing simulation exercises may help reinforce these concepts (Zorz, 2024).

b) **Stronger API Security and Management**:

Organizations must use a zero-trust security strategy for API access. This includes stringent access restrictions, such as restricting API key rights to the absolute minimum required for operations (Baran, 2024). Additionally, API keys should be

rotated on a regular basis and securely maintained, preferably in an encrypted vault. This prevents illegal access if a key is compromised.

c) **Multi-Factor Authentication (MFA) Improvements**:
Multi-Factor Authentication must be installed taking into account advanced attack strategies. This involves the use of hardware tokens or biometric authentication to provide greater security than typical SMS- or app-based MFA. Organizations dealing with sensitive information should prioritize the implementation of phishing-resistant MFA systems that cannot be avoided using stolen credentials. (Dropbox dign team, 2024)

d) **Continuous Monitoring and Incident Detection:**
To identify suspicious activity early, real-time monitoring and anomaly detection systems should be implemented to detect abnormal behaviors in user accounts, such as abrupt access to several systems or the use of aberrant API credentials. Security Information and Event Management (SIEM) solutions might be used to condense logs and spot anomalous patterns, resulting in faster response times during an attack. (O'Flaherty, 2024)

Section 3.3: Implement the Risk Management / Risk Assessment, Evaluate the impact, likelihood, and risk level associated with the incident, and propose risk mitigation strategies using risk assessment template

In this section, we use a Risk Management Framework to assess the effect, likelihood, and risk level connected with the Dropbox Sign data breach. The given risk assessment form will be used to conduct the analysis, which will include the identified vulnerabilities, threats, and assets. We will also offer effective risk mitigation techniques to help the firm reduce future threats and improve its security posture. (AragonResearch, 2024)

Risk Assessment Table Overview

The Dropbox Sign breach is assessed based on the primary assets affected, the vulnerabilities used by the attackers, and the probable ramifications to the enterprise

(CheckRed, 2024). We will use the risk assessment table to identify and examine the vulnerabilities associated with each asset.

Notes

Risk Assessment sheet

Asset Name	Confidentiality	Integrity	Availability	Asset Value	Known threats	Threat Value	Vulnerability Description	Vulnerability Value	Possibility of occurrence	Current Control	Risk Score	Risk Treatment	Possibility of occurance after traetment	Residual risk
Database Server	high	high	high	high	Unauthorized Data Access	high	Exploitation of misconfigured API	high	high	Firewall and limited access	high	Accept	medium	N/A
Cloud Storage	high	high	high	high	Third-party API Misuse	high	Insufficient API traffic monitoring	high	medium	Basic encryption applied	high	Reduce	low	N/A
File Transfer	high	medium	high	high	Credential Hijacking	high	Weak authentication on shared system	medium	high	Password-protected transfers	high	Reduce	medium	N/A
Endpoint Devices	medium	medium	medium	medium	Malware Delivery	medium	Lack of robust endpoint protection	medium	high	Antivirus implemented	medium	Reduce	low	N/A
Third-party Integrations	high	medium	medium	high	Supply Chain Attack	high	Poor vetting of third-party tools	high	medium	Basic vendor contracts	high	Reduce	medium	N/A

Figure 1: Risk Assessment Table

Impact Evaluation

According to the Dropbox Sign breach, it concerned their API server-an asset that high-value thieves broke into at access points made available by exploitation of weaknesses in managing API keys. Through these exploitations, the attacker has access to sensitive personally identifiable information and other confidential documents. (Dropbox dign team, 2024)

- **Confidentiality Impact**: The intrusion compromised the confidentiality of user data since sensitive files and customer information were accessed. The attackers might steal personal information and contract information, affecting user confidence. (Spencer, 2024)
- **Integrity Impact**: The attackers may possibly have altered or modified data in the system, however there is no clear evidence of data manipulation. The attackers had full access to the backend, therefore the intrusion may have impacted data integrity. (Spencer, 2024)
- **Availability Impact**: The breach had no substantial impact on the availability of Dropbox's services, but affected systems may have been pulled offline, interrupting corporate operations. (brief news, 2024)

Likelihood Evaluation

Based on the possibilities of occurrence and the present safeguards in place, the probability of similar occurrences occurring is graded as medium. Misconfigured permissions and inadequate API management were key vulnerabilities that were exploited

(Zorz, 2024). Dropbox has built firewalls and Multi factor authentication, however these were inadequate to thwart the assault. A medium likelihood indicates that the intrusion may have been avoided with stronger API security and more staff awareness training**.** (Baran, 2024)

Risk Mitigation Strategies:

Using the risk assessment framework, we suggest the following risk treatment strategies:

- **Mitigating API Vulnerabilities**
  - API Management: API key management should be subject to stricter constraints, such as token expiration and frequent audits. Implementing OAuth 2.0 and JWTs (JSON Web Tokens) would boost API security. (Spencer, 2024)
- **Enhanced Employee Awareness Training:**
  - Phishing Prevention: Conduct frequent phishing simulation exercises to teach staff how to identify fraudulent emails. Making sure that all workers are aware of phishing strategies will lower the danger of gaining initial access through social engineering assaults (Spencer, 2024).
- **MFA Implementation:**
  - Stronger Multi-Factor Authentication (MFA)**:** While Multi-Factor Authentication was established, it is critical to ensure that it is phishing-resistant and to update MFA systems on a regular basis to avoid the exploitation of weak tokens or bypass techniques (Baran, 2024).
- **Vulnerability Management**:
  - Patching and Regular Audits: Adopting an agile patching approach is crucial for quickly addressing vulnerabilities in API servers, databases, and other key systems. Regular penetration testing and vulnerability assessments will also help to detect and resolve problems ahead of time. (Software ag, 2024)

- **Data Encryption and Backup**:
  - Encryption of confidential information: Encrypting both data at rest and data in transit ensures that attackers cannot read or change the data. Additionally, improving backup processes and frequency will prevent data loss in the case of an attack (Dropbox dign team, 2024).

Conclusion

The Dropbox Sign breach shows serious flaws in API security, multi-factor authentication (MFA), and staff knowledge that attackers used to gain unauthorized access and compromise sensitive customer data. This event resulted in considerable financial, operational, and reputational loss, underscoring the importance of a strong cybersecurity architecture. Proactive measures like phishing-resistant multi factor authentication, zero-trust API management, frequent penetration testing, and improved staff training may dramatically decrease the likelihood of such attacks. Strengthening these defenses is critical for safeguarding sensitive data, preserving customer confidence, and guaranteeing organizational resilience to potential attacks. (Abrams, 2024)

Chapter 3

Section 3.1: Write a reflective report on your practical development of the practical activities.

Finishing the 8 Cyber essentials Labs and immersive labs of Cisco helped me increase my knowledge and skills regarding cybersecurity. Each activity integrated theoretical principles with practical applications, providing a full learning experience.

Cyber Essentials Labs from Cisco:

Cisco labs were associated with network security, cryptography, risk management, incident response, etc. Tasks included configuring firewall, implementing access control and conducting risk assessment that reinforced class room lessons. The labs stressed on setting up security systems and spotting threats before they impact. After finishing all eight modules, I gained more confidence in applying best practices to protect the system and data.

Immersive Labs:

Immersive Labs offered training where one gets to experience and describe a real-life cyber-attack. Through these activities, one could think critically, solve problems, and work with others. I was allowed to practice incident response and develop a systematic way on how to handle threats. The changing nature of the labs show the importance of learning how to adapt to changes to the threat.

Conclusion:

Both of these experiences made the theories we learned in class become real-time experiences. My ability to recognize, eliminate, and act against threats was enhanced in accordance with industry and government standards.

References

aarc-360, 2024. *AAR360.* [Online]
Available at: https://www.aarc-360.com/ensuring-data-security-compliance-best-practices-and-strategies/
[Accessed 02 12 2024].

Abrams, L., 2024. *Bleepingcomputer.* [Online]
Available at: https://www.bleepingcomputer.com/news/security/dropbox-says-hackers-stole-customer-data-auth-secrets-from-esignature-service/
[Accessed 04 12 2024].

Abrams, L., 2024. *BleepingComputer.* [Online]
Available at: https://www.bleepingcomputer.com/news/security/dropbox-says-hackers-stole-customer-data-auth-secrets-from-esignature-service/
[Accessed 7 12 2024].

Antonenko, D., 2023. *Business tech weekly.* [Online]
Available at: https://www.businesstechweekly.com/cybersecurity/data-security/role-based-access-control-rbac/
[Accessed 24 11 2024].

Appleby, T., 2018. *INFOSEC.* [Online]
Available at: https://www.infosecinstitute.com/resources/incident-response-resources/10-step-post-breach-incident-response-checklist/
[Accessed 04 12 2024].

AragonResearch, 2024. *AragonResearch.* [Online]
Available at: https://aragonresearch.com/dropbox-reassures-customers-after-being-hacked/
[Accessed 6 12 2024].

Baran, G., 2024. *Cyber Scurity News.* [Online]
Available at: https://cybersecuritynews.com/dropbox-sign-hacked/
[Accessed 5 12 2024].

Barrus, R., 2024. *PivotPoint.* [Online]
Available at: https://www.pivotpointsecurity.com/how-iso-27001-supports-gdpr-compliance/
[Accessed 29 11 2024].

brief news, 2024. *Dropbox Sign Hit by Security Breach: Customer Data Exposed.* [Online]
Available at: https://www.brief.news/cybersecurity/2024/05/02/dropbox-security-breach
[Accessed 6 12 2024].

BritishAssessment, 2024. *British Assessment Bureau.* [Online]
Available at: https://www.british-assessment.co.uk/services/iso-27001/?&utm_source=bing&utm_medium=paid&utm_campaign=Bing%20Ads%20-%20ISO%2027001%20Certification%20(Search)&utm_term=data%20protection%20management&hsa_acc=6188181041&hsa_mt=p&hsa_src=o&hsa_cam=Bing%20Ads
[Accessed 21 11 2024].

CheckRed, 2024. *CheckRed Security.* [Online]
Available at: https://checkred.com/resources/blog/the-dropbox-breach-understanding-the-need-for-

robust-cloud-security-measures/
[Accessed 5 12 2024].

Chopra, S., 2024. *Impanix.* [Online]
Available at: https://impanix.com/security/annex-a-controls/
[Accessed 30 11 2024].

cloudflare, 2024. *Cyber Essentials.* [Online]
Available at: https://www.cloudflare.com/trust-hub/compliance-resources/cyber-essentials/
[Accessed 01 12 2024].

dataprotection.ie, 2024. *Data Protection Commission.* [Online]
Available at: https://www.dataprotection.ie/en/individuals/know-your-rights/right-be-informed-transparency-article-13-14-gdpr
[Accessed 26 11 2024].

Delev, Z., 2024. *GDPR Local.* [Online]
Available at: https://gdprlocal.com/the-data-protection-impact-assessment-dpia-evaluating-privacy-risks/
[Accessed 21 11 2024].

Dropbox dign team, 2024. *dropboxsign.* [Online]
Available at: https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign
[Accessed 6 12 2024].

FasterCapital, 2024. *fastercapital.* [Online]
Available at: https://fastercapital.com/keyword/file-access.html
[Accessed 03 12 2024].

fournet, 2024. *FourNet.* [Online]
Available at: https://fournet.co.uk/news-events/2024/05/08/dropbox-sign-security-incident/
[Accessed 4 12 2024].

frontegg, 2024. *Frontegg.* [Online]
Available at: https://frontegg.com/guides/access-control-in-security
[Accessed 25 11 2024].

gdpr-advisor, 2023. *GDPR ADVISOR.* [Online]
Available at: https://www.gdpr-advisor.com/gdpr-and-iso-27001-building-a-robust-data-security-and-compliance-plan/
[Accessed 29 11 2024].

GDPR-Advisor, 2023. *GDPR ADVISOR.* [Online]
Available at: https://www.gdpr-advisor.com/data-minimization/#:~:text=At%20its%20core%2C%20data%20minimisation%20under%20GDPR%20requires,the%20purposes%20for%20which%20it%20is%20being%20processed.
[Accessed 23 11 2024].

gdpradvisor, 2023. *GDPR Compliance and Encryption.* [Online]
Available at: https://www.gdpr-advisor.com/gdpr-compliance-and-encryption-integrating-security-measures-in-policies/
[Accessed 28 11 2024].

Grande, D., 2023. *The Privacy Group.* [Online]
Available at: https://theprivacygroup.com/articles/what-is-data-minimization/
[Accessed 21 11 2024].

Herath, S., 2023. *Privacy Harm.* [Online]
Available at: https://files.eric.ed.gov/fulltext/EJ1415199.pdf
[Accessed 01 12 2024].

ico.org, 2024. *ICO..* [Online]
Available at: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/accountability-and-governance/data-protection-by-design-and-by-default/
[Accessed 20 11 2024].

isocouncil, 2024. *The iso council.* [Online]
Available at: https://isocouncil.com.au/maintaining-iso-27001-compliance-2/
[Accessed 30 11 2024].

johansonllp, 2024. *johanson group.* [Online]
Available at: https://www.johansonllp.com/blog/iso-27001-annex-a-controls
[Accessed 30 11 2024].

Kamau, O., 2020. *ISACA.* [Online]
Available at: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/building-a-privacy-focus-area-using-cobit-and-the-nist-privacy-framework
[Accessed 01 12 2024].

Kapko, M., 2024. *CyberSecurity dive.* [Online]
Available at: https://www.cybersecuritydive.com/news/dropbox-sign-cyberattack/714999/
[Accessed 05 12 2024].

Karczewska, J., 2017. *ISACA.* [Online]
Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2017/cobit-5-and-the-gdpr
[Accessed 01 12 2024].

Kemper, B., 2024. *SAE international.* [Online]
Available at: https://connect.sae.org/cybersecurity?gad_source=1&gclid=CjwKCAiAjeW6BhBAEiwAdKltMnf_V944J5dIneDQKAGqmgF-kR5zIZwMbmfSROlb_eckSNndS8MmtxoCIwYQAvD_BwE&gclsrc=aw.ds
[Accessed 20 11 2024].

Kosutic, D., 2023. *Advisera.* [Online]
Available at: https://advisera.com/27001academy/blog/2014/06/30/6-step-process-for-handling-supplier-security-according-to-iso-27001/
[Accessed 30 11 2024].

Lamba, S., 2024. *Legalvision.* [Online]
Available at: https://legalvision.co.uk/regulatory-compliance/gdpr-storage-limitation-explained/
[Accessed 29 11 2023].

Maldoff, G., 2016. *iapp.* [Online]
Available at: https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf
[Accessed 30 11 2024].

marom, O., 2024. *Varonis.* [Online]
Available at: https://www.varonis.com/blog/dropbox-sign-data-breach
[Accessed 04 12 2024].

Mascellino, A., 2024. *Infosecurity Magazine.* [Online]
Available at: https://www.infosecurity-magazine.com/news/security-breach-dropbox-sign/
[Accessed 4 12 2024].

McCart, C., 2024. *comparitech.* [Online]
Available at: https://www.comparitech.com/antivirus/what-is-layered-security/
[Accessed 03 12 2024].

Mishova, A., 2023. *GDPR LOCAL.* [Online]
Available at: https://gdprlocal.com/gdpr-iso27001-other-iso-standards-similarities-differences-intersections/
[Accessed 29 11 2024].

NCSC, 2022. *National Cyber Security Center.* [Online]
Available at: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-0-January-2022.pdf
[Accessed 01 12 2024].

Now, I., 2021. *ISACA.* [Online]
Available at: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-19/3-things-cobit-is-3-things-it-isnt
[Accessed 02 12 2024].

O'Flaherty, K., 2024. *assured intelligence.* [Online]
Available at: https://assured.co.uk/2024/dropbox-hack-5-lessons-from-the-dropbox-sign-breach/
[Accessed 7 12 2024].

Schwikkard, C., 2023. *Scopic.* [Online]
Available at: https://scopicsoftware.com/blog/secure-software-development-life-cycle-ssdlc-guide/
[Accessed 03 12 2024].

Secure Privacy ai, 2024. *Secure Privacy.* [Online]
Available at: https://secureprivacy.ai/blog/mastering-privacy-by-design-guide
[Accessed 26 11 2024].

Sharwood, S., 2024. *TheRegister.* [Online]
Available at: https://www.theregister.com/2024/05/02/dropbox_sign_attack/
[Accessed 4 12 2024].

Software ag, 2024. *Softwareag.* [Online]
Available at: https://www.softwareag.com/en_corporate/resources/api/wp/api-security-strategy.html?utm_source=google&utm_medium=cpc&utm_campaign=aim_api-intg&utm_region=hq&utm_subcampaign=stg-1&utm_content=stg-1_whitepaper_build-an-effective-enterprise-api-strategy&gad_
[Accessed 6 12 2024].

Spencer, P., 2024. *Kitework.* [Online]
Available at: https://www.kiteworks.com/cybersecurity-risk-management/dropbox-sign-breach/
[Accessed 6 12 2024].

Spencer, P., 2024. *Kiteworks.* [Online]
Available at: https://www.kiteworks.com/cybersecurity-risk-management/dropbox-sign-breach/
[Accessed 04 12 2024].

Sullivan, M., 2023. *Transcend.* [Online]
Available at: https://transcend.io/blog/data-minimization
[Accessed 24 11 2024].

Wlosinski, L. G., 2022. *ISACA.* [Online]
Available at: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
[Accessed 04 12 2024].

Zorz, Z., 2024. *Help Net Security.* [Online]
Available at: https://www.helpnetsecurity.com/2024/05/02/dropbox-sign-breached/
[Accessed 5 12 2024].