SCHOOL OF COMPUTING

Diploma in Infocomm Security Management

ST2420

Data Protection for Cyber Security

DISM/FT/2B/02

Submitted By (Student ID):

Aung Kaung Chit (P2339728)

Kho Li Hao (P2341756)

Russell Chin Jun Ren (P2322357)

Hoi Damien (P2304090)

Table of Contents

1. Introduction **2**

1.1 Background **2**

1.2 Assumptions **2**

1.3 Cybersecurity Incidents **3**

1.4 Impact Analysis **4**

2. Control analysis **5**

2.1 Cybersecurity Consultant **5**

2.2 IT Manager **8**

2.3 Chief Information Security Officer (CISO) **11**

2.4 Data Protection Officer (DPO) **13**

3. Conclusion **16**

4. Task Allocations and Reflections **17**

5. References **19**

1. Introduction

1.1 Background

BrightWave Technologies, a rapidly expanding data analytics firm specializing in solutions for SMEs, faces significant cybersecurity vulnerabilities. Despite its technological innovations, the company has exhibited deficiencies in cybersecurity governance, creating potential operational and reputational risks.

The Chief Information Security Officer (CISO) possesses strong technical competencies but lacks substantial experience in data governance and policy enforcement. Additionally, BrightWave Technologies relies on third-party cloud solutions that, while cost-effective, provide insufficient security protections, thereby amplifying the company’s exposure to cyber threats.

1.2 Assumptions

1. BrightWave Technologies is only operating in Singapore. This means that all legal and compliance considerations, including data protection and cybersecurity regulations, are governed by Singaporean laws such as the Personal Data Protection Act (PDPA).
2. BrightWave Technologies hired an independent cybersecurity consultant to identify and evaluate security issues and implement solutions to address threats to the company's computer network or computer systems.
3. Employees of BrightWave Technologies have signed NDA agreements with the company due to the highly sensitive nature of the data they would handle.

1.3 Cybersecurity Incidents

1. **Heavy Reliance On Cloud Solutions**

   To save on costs, Brightwave Technologies decided to choose a cloud storage plan that has sparse security features despite storing sensitive information such as customer profiles and analytical reports on this platform. This undermines the integrity of the data protection measures that are already in place.

2. **Unencrypted Sharing of Sensitive Information**

   Employees of Brightwave Technologies often share substantial personal information like identification details, financial statements, and business strategies that was gathered when procuring new clients across unencrypted emails and defenseless cloud storage, putting it at risk of a potential breach

3. **Public Disclosure of Confidential Data**

   The CISO unknowingly shared screenshots containing proprietary methodologies and client information on social media leading to the exposure of trade secrets and confidential data and compromising contractual obligations and regulatory compliance.

4. **Former Employee Retained System Access**

   An employee was discovered to have retained unauthorised access to internal systems despite being terminated weeks ago in a scheduled security assessment by an external auditor due an oversight by the CISO.

5. **Insider Data Theft by a Current Employee**

   A disgruntled employee leveraged weak security controls to illicitly extract proprietary client data. Sensitive analytics reports were illicitly transferred to a competing firm, violating confidentiality agreements.

1.4 Impact Analysis

The organization’s failure to prevent multiple security breaches has resulted in reputational damage and loss of client trust, diminishing its competitive standing in the market.

A weak security posture also attracts malicious actors, making BrightWave Technologies a prime target for future cyberattacks. Additionally, the unauthorized exposure of proprietary methodologies and analytics models undermines the company’s competitive advantage, potentially leading to loss of business revenue and intellectual property theft.

2. Control analysis

2.1 Cyber Security Consultant

BrightWave Technologies has decided to hire a cybersecurity consultant in order to ameliorate the disastrous situation of the company's security posture. Initially, the consultant has been provided with little or no information about the company's computer networks, computer systems and their service platform. A scheduled meeting with CISO, IT manager, compliance team and cybersecurity consultant himself was held, and network topology and architecture, asset inventory, existing security policies and access control policy were provided to the consultant.

Threats and Vulnerabilities Findings

The consultant performed vulnerability assessment and penetration testing. Several major vulnerabilities and potential threats were discovered through VAPT alongside the information gathered from the team.

1. **Unsecured Cloud Solution**
   A cloud solution with a cost-effective plan with limited security features usually lacks encryption of data at rest and encryption of data in transit allowing the malicious actor who gained access to be able to read, modify, or steal the data easily. On top of that, the cost-effective plan might also lack data masking options which can result in allowing malicious actors to gain easy access to sensitive information like customer profiles and analytical reports since the company was storing them on the cloud platform.
2. **Ransomware & Malware Infections**
   Storing data in a cloud platform with weak security protections increases the risk of malware and ransomware attacks. Assuming the platform lacks thread detection and malware scanning, employees may download malicious files through phishing attacks that can infect the cloud storage, which can lead to ransomware attacks in which attackers encrypt critical data and demand ransom payments to restore access.

3. **Data Loss Due to Weak Backup & Disaster Recovery**
   If the cloud provider does not offer strong backup solutions, BrightWaves risks losing critical data, compromising availability. Cheap cloud plans may lack redundancy, causing data loss during outages and employees could mistakenly delete files with no recovery options, which can lead to permanent loss of valuable customer and business data.
4. **Man-in-the-Middle (MITM) Attacks**
   Common threats like data interception and data manipulation can be posed since the company employees were sharing sensitive information through unencrypted communication channels during onboarding new clients.
5. **Weak Password Practices & Credential Stuffing**
   Employees using weak or reused passwords across multiple platforms increase the risk of account takeovers. Attackers can break into accounts by brute forcing weak passwords with the use of automated tools and techniques such as John the Ripper, dictionary attacks, etc, leading to loss of control over accounts, which can escalate privileges to gain deeper access to company systems.
6. **Insider Threats**
   A failure in access control and account management also poses significant insider threats to the company. It can be denoted that key security weaknesses such as failure to implement the principle of least privilege, poor identity & access management (IAM) practices and failure to audit user accounts regularly are the contributing vulnerabilities to this threat. Consequently, failure to revoke the ex-employee's access to the company's cloud storage and internal communication systems posed significant insider threats to the company.

Recommendations

1. **Immediate Incident Response & Damage Control**
   It is strongly suggested that company's IT personnel should contain the current breaches, revoke unauthorized access, and initiate legal compliance measures. Immediate disabling access for former employees and any compromised accounts should be done.

2. **Enhancing Cloud Security Measures**

   BrightWave Technologies should adopt stringent security controls to secure its cloud environment and prevent unauthorized access. Migrating to a service plan with enhanced security features such as data encryption at rest and in transit, advanced threat detection, and activity monitoring is vital. Since the company is highly dealing with personal data, financial data and other intellectual properties, it is crucial to apply data masking techniques on data stored in compliance with PDPA. Moreover, proper identity & access management such as role-based access control (RBAC) should also be implemented for the sake of the principle of least privilege. Data warehousing services such as AWS Redshift, Snowflake and Google BigQuery can satisfy the outlined security requirements, providing high availability with ease, and threat detection services such as Amazon GuardDuty and Security Command Center(GCP) should also be considered to improve intrusion detection & prevention.

3. **Secure Internal Communication**

   Secure communication platforms for sharing sensitive data should also be adopted to prevent man-in-the-middle attacks such as email hijacking, eavesdropping, etc. Consideration of adopting end-to-end encrypted email services such as Microsoft Outlook, ProtonMail, etc should be prioritised.

4. **Password Management**

   Enforcing strong password policy and multi-factor authentication(MFA) across all access points to the company's platforms and end devices can undermine risky sharing habits among employees. Use of password managers such as Bitwarden, 1Password, etc that can generate and store strong, complex passwords, should also be promoted.

5. **Continuous Security Monitoring**

   Regular penetration testing and red teaming exercises should be conducted to identify and rectify vulnerabilities before they are exploited. Implementing Security Information and Event Management (SIEM) tools is also beneficial to detect real time anomalies such as multiple failed login attempts, access from unusual locations, or unauthorized data transfers.

2.2 IT Manager

The role as Brightwave Technologies' IT Manager is to lead the IT department of the organisation. They are required to ensure the security, functionality and stability of the organisation's IT infrastructure like its network, data storages and computers and servers. IT Managers need to know how to evaluate the risks and vulnerabilities and implement policies to prevent them. An IT Manager must achieve these while enforcing the best practices for data protection and cybersecurity.

Key Vulnerabilities Found

1. **Insecure Cloud Storage**

Brightwave Technologies relies on storing customers' sensitive personal data and analytical reports on a relatively cheap Cloud service provider that has very limited security features. A cloud service provider having limited security features makes it very susceptible to being attacked and causing data breaches. Additionally, if the cloud provider has no encryption for data at rest or data in transit, this would result in plaintext data being easily stolen by malicious actors.

Solution:

The IT Manager needs to migrate all data stored in this current cheap cloud provider, to a more reputable and secure Cloud provider, like AWS, Google Cloud, Microsoft Azure. Such cloud providers offer end-to-end encryption using strong encryption standards, like AES-256 for data at rest. It also provides Multi-Factor Authentication (MFA) for access controls to the stored data, ensuring that only authorized employees can access the sensitive data. It is important to also have data recovery plans and policies implemented.

2. **Poor Access Controls**

An employee that is no longer part of a company should not have access to the company's data or any user credentials to authenticate itself in IT systems or computers. Ex-employees, who might even have grudges with the ex-company, may be able to steal data despite not being part of the company, or even monitor the activities that are ongoing in the company. There should also be role-based access implemented in the IT systems to give authorization to users to only access the data that is required for their job. Otherwise, employees might be able to access more data than what is necessary, and may potentially find more sensitive data that they are not supposed to access, hence compromising the confidentiality of data in the company.

Mitigations:

The IT manager will remove user credentials for the employee that was already terminated weeks ago to prevent any bad actors from doing harm through his account and the employee that has been caught committing corporate espionage to restrict him from further downloading any proprietary client data and selling them to the clients' competitors.

Solutions

Companies should disable related user accounts and revoke access immediately when an employee leaves a company. Adopting a Zero Trust Architecture (ZTA) will ensure that access to company resources is granted based on continuous verification rather than inherent trust. Role-based access control (RBAC) and privileged access management (PAM) must be enforced to prevent unauthorized access to critical systems and sensitive information. Softwares can also be integrated into computers to monitor a sudden mass download of files, which could indicate a potential unauthorized threat actor stealing data.

3. **Weak Password Policies**

The company has poor password management and policies. Employees should not be using weak passwords as they can easily be cracked through brute-forcing or dictionary attacks. Employees are also reusing their weak passwords across multiple platforms. This is not a good practice as if one of the accounts get compromised, all the others would also be at risk since they use the same passwords, which eventually means that it would lead to more data being stolen by unauthorized threat actors.

Solutions:

Conduct employee security awareness training by teaching employees good password practices. Examples include password complexity requirements, change of passwords every 90 days and enforcing password history so that employees cannot reuse the same previous password.

Mitigations:

The IT manager will implement a password change for all current employees, requiring them to change their password to one that is alphanumerical and includes special characters making it significantly harder for bad actors to gain access illegally.

4. **Insecure Data in Transit**

Employees are using insecure communication channels to share sensitive data like customer's financial statement and identification details. They are shared using unencrypted email, which makes it susceptible to eavesdropping and Man in the Middle attacks, and since the data is transmitted in plaintext, they can easily be read and stolen by attackers.

Solutions:

Enforce end-to-end Email encryption for all emails sent within the company. If the company has its own Email server, ensure it is using strong encryption standards, like using Transport Layer Security (TLS) encryption for all emails sent. Secure Email Gateways (SEG) or Data Loss Prevention Tools can also be used as a method to block all unauthorized emails that contain sensitive data. Or otherwise, employees should only be able to share sensitive documents on secure and reputable file sharing platforms, like Google Drive.

2.3 Chief Information Security Officer (CISO)

The CISO oversees the overall cybersecurity strategy and governance at BrightWave Technologies. This includes establishing a cybersecurity policy framework that aligns with regulatory requirements and industry best practices. The CISO must develop and enforce Standard Operating Procedures (SOPs) to ensure consistent security protocols across all departments. Additionally, the role involves conducting simulated cyberattack drills and tabletop exercises to strengthen the organization's incident response capabilities. Regular employee training sessions should be conducted to raise awareness about emerging cybersecurity threats and best practices. This is done to improve employee security awareness and strengthen the organization's security posture and incident response capabilities.

Mitigation Strategies:

1. **Taking down social media posts**
   The CISO deactivates the account before scrubbing it and removing any social media posts that violate confidentiality agreements to contain and minimise the damage already caused by the unintentional leaks due to the posts.
2. **Termination and taking legal action**
   The CISO will terminate the employee that has committed corporate espionage and take legal action against him. In coordination with the legal team, the CISO will initiate legal proceedings based on contractual violations and Singapore's relevant cybersecurity and data protection laws. Not only will this prevent the employee from selling more proprietary client data to competitors, it will also serve as a deterrent for future internal threats and reinforce the company's commitment to safeguarding its intellectual property and client data.

Solutions:

1. **Upgrade cloud storage security**
   The CISO is required to upgrade the cloud solution to a plan that provides the highest level of security available due to the nature of sensitive information that

BrightWave Technologies is handling. This increases the difficulty for any future bad actors attempting to breach the cloud storage significantly. The choice of plan is to be researched on by the DPO and presented to CISO.

2. **Establishing Standard Operating Procedures (SOP)**

   The CISO will institutionalise a comprehensive cybersecurity training program to ensure employees understand and adhere to security best practices. Not only will establishing and enforcing cybersecurity Standard Operating Procedures (SOPs) help standardise security protocols and strengthen the level of security across departments, it will also foster a cybersecurity awareness culture as mandatory training, phishing simulations, and security drills as will significantly reduce human-related vulnerabilities that are currently prevalent in the company. Furthermore, the SOP will prevent future employees that were already terminated from retaining access to the cloud storage. Regular assessments and feedback loops are to be incorporated to measure the effectiveness of these initiatives and adapt them to emerging threats

3. **Implementation of Role Based Access Controls**

   The CISO will work together with the IT manager to implement role-based access controls (RBAC) to prevent employees from accessing information that is above their pay grade. This will stop unauthorised users from accessing sensitive data.

4. **Implementation of Identity and Access Management Solutions**

   The CISO must also oversee the implementation of identity and access management (IAM) solutions by the IT manager to prevent unauthorised access. Strict audit and logging mechanisms will be put in place to track data access and detect anomalies in real time. Furthermore, the CISO must ensure that all employees' access to critical systems is reviewed and updated periodically to prevent excessive data exposure.

2.4 Data Protection Officer (DPO)

The role of a DPO is to ensure regulations for data protection such as the PDPA are being implemented. The DPO has to conduct the Data Privacy Impact Assessments (DPIAs) regularly to evaluate potential risks involving the use of data. The collecting, storing, and disposing of data policies have to be clearly stated and enforced. By implementing a Data Loss Prevention (DLP) system, it will be able to prevent unauthorized access and leakage of sensitive information. Additionally, the DPO should lead organization-wide privacy awareness initiatives and establish a robust breach notification process to ensure timely responses to data incidents. The DPO must ensure regulatory compliance by enforcing stringent data protection measures, including regular Data Privacy Impact Assessments (DPIAs). Implementing clear data collection, storage, and disposal policies will safeguard client and corporate data. The DPO should also lead organization-wide privacy awareness initiatives.

1. **Insufficient Data Governance and implementation of policies**

Threat:

The company lacks governance over data and implementation of data protection policies. Under the PDPA, organizations have to take measures to safeguard personal data from authorized access, collection, use, and disclosure. Although the CISO has a strong technical foundation that can be effective and useful in aiding the company, it lacks the necessary experience needed in data governance and security policy implementation. This disadvantage can lead to not complying with the data protection regulations, as well as poor data protection measures and risk management.

Mitigations:

- Training employees on PDPA compliance:

The DPO should conduct updates and review policies frequently and also provide compulsory training for all employees on handling data, privacy, and the best security practices. This is to ensure that the employees are educated and aware of their legal obligations when handling personal data.

- Developing PDPA data protection policies:

  To establish clear guidelines on the collecting, using, storing, and retention of sensitive data. Thus, this outlines the responsibilities of the employees in preventing mishandling of personal data.

2. **Insufficient Cloud Security and data management measures**

Threat:

Brightwave chose a cost-effective cloud service that offered very limited security features from a third-party provider. Under the PDPA, organizations are required to ensure personal data in the cloud are safe and secured from data breaches and unauthorized access. When boarding new clients, the company collects extensive data such as identification details and often shared among employees through unencrypted emails and unprotected cloud storage. This makes the client's data exposed to vulnerabilities such as inadequate encryption, exposing sensitive data, and insufficient monitoring of the system, which can lead to unauthorized access and potential security breaches.

Mitigations:

- Upgrading of Cloud Security:

  Upgrade the cloud service plan that includes enhanced security features. This would ensure security and minimize the chances of a security breach.

- Frequent audits and implementation of encryption

Implement and conduct regular cloud security checks with third-party security experts to address any potential vulnerabilities in the cloud infrastructure. Encrypting data at rest and in transit to prevent any unauthorized access or enabling multi-factor authentication (MFA) to prevent unauthorized logins. This would allow sensitive information to be shared among the employees safely as it will be encrypted in a safe environment.

3. **Disclosure of sensitive data on social media platforms**

Threat:

BrightWave makes an effort to showcase their projects on their professional social media channel. However, the posts reveal their clients' sensitive information, such as proprietary methodologies and analytical models. Thus, this breaches the confidentiality agreement between the company and the client. Companies are to obtain consent from the other party before using or disclosing personal data. Moreover, they can only collect, use, or disclose for legitimate business purposes.

Mitigations:

- Implement social media policy:

  Employees are not allowed to share confidential and private information of the client without having approval. Companies can also incorporate stricter confidentiality measures when wanting to post clients' sensitive data online.

3. Conclusion

BrightWave Technologies faces significant cybersecurity risks due to weak cloud security measures, improper data governance, and insufficient access controls. The security incidents identified—including unauthorized access by former employees, insider threats, and data breaches—highlight the need for immediate corrective actions.

To address these vulnerabilities, we have proposed strategic risk mitigation measures, such as enhancing cloud security, enforcing robust access control policies, implementing encrypted communication channels, and improving employee cybersecurity awareness. The adoption of stronger compliance frameworks will ensure that the company strengthens its security posture and regulatory compliance under Singapore’s laws.

By implementing the recommended security improvements and fostering a culture of cybersecurity awareness, BrightWave Technologies can mitigate threats, safeguard its clients' data, and maintain its reputation as a trusted data analytics firm. Ongoing security assessments, regular penetration testing, and continuous employee training will be essential to maintaining long-term cybersecurity resilience.

4. Task Allocations and Reflections

Name	Task(s) allocated
Aung Kaung Chit	Assumptions,Impact Analysis, Control Analysis (Cyber Security Consultant)
Damien Hoi	Control Analysis (DPO)
Kho Li Hao	Background, Cybersecurity Incidents, Control Analysis (CISO), Conclusion
Russell Chin	Control Analysis (IT Manager)

Aung Kaung Chit:

Performing as a cyber security consultant for a disaster recovery role play exercise has provided deeper understanding of how a cyber security consultant plays a crucial role in securing an organisation's infrastructure. It reinforced the importance of cybersecurity frameworks, proactive risk mitigation, and collaboration with key stakeholder

Hoi Damien:

This project allowed me to know and understand the importance of PDPA in protecting personal data. The role of a DPO is really important to companies to ensure that personal data are well protected. Companies should properly safeguard their data with encryption and with that are able to keep their data safe and secured.

Kho Li Hao:

This project has provided valuable insights into the intersection of cybersecurity and legal compliance, particularly in the context of Singapore’s Personal Data Protection Act (PDPA) and other regulatory frameworks. Through the analysis of BrightWave Technologies' security vulnerabilities, I have come to appreciate the critical role that legal requirements play in shaping an organization’s cybersecurity policies and practices.

One key takeaway from this assessment is that compliance is not just about avoiding penalties but also about maintaining trust and integrity. BrightWave Technologies' failure to secure sensitive client data and prevent unauthorized access could lead to severe legal repercussions under the PDPA, which mandates that organizations implement reasonable security measures to protect personal data from unauthorized access, use, or disclosure. The unintentional data leaks and insider threats identified in this case highlight the importance of strict access controls, data encryption, and audit mechanisms to align with legal obligations.

Additionally, this project has emphasized the necessity of data governance policies that comply with PDPA guidelines. The lack of proper data protection policies within the company could expose it to legal liabilities, including potential fines and enforcement actions by the Personal Data Protection Commission (PDPC). Organizations must not only adopt technical safeguards but also establish clear internal policies, employee training programs, and incident response protocols to ensure compliance with data protection laws.

Another significant learning point is the role of corporate accountability. The CISO's failure to revoke access for former employees and the IT Manager's weak password enforcement demonstrate lapses in duty that could be considered negligent under cybersecurity regulations. By enforcing best practices such as Zero Trust Architecture (ZTA), Role-Based Access Control (RBAC), and Multi-Factor Authentication (MFA), companies can significantly reduce the risk of regulatory non-compliance and data breaches.

In conclusion, this project has reinforced my understanding that cybersecurity is not solely a technical field but also a legal and ethical responsibility. As organizations continue to navigate evolving cyber threats and regulatory landscapes, it is crucial to adopt a security-first approach that aligns with legal mandates. Moving forward, I aim to deepen my expertise in cybersecurity law and compliance to contribute effectively to

securing digital ecosystems while ensuring adherence to legal and regulatory standards.

Russell Chin:

This project has allowed me to learn importance of cybersecurity and data protection in modern organizations. Analyzing the given scenario allowed me to understand how security vulnerabilities, such as the lack of role-based access control and unencrypted data in transit, can increase the risk of data breaches and insider threats. Poor access management and weak security policies not only expose a company to data breaches but also lead to regulatory non-compliance, which can have serious legal and financial consequences. Through this project, I gained a deeper appreciation of the role of an IT Manager in implementing robust security measures, enforcing policies, and ensuring compliance with data protection regulations. I learnt how to identify vulnerabilities and proposing solutions and mitigations which required lots of research and a structured approach. I learnt about many ways organisation can protect personal data and ensures it complies with the PDPA. For example, not using cost-saving cloud solutions that compromise security features for data at rest and data in transit, implementing role-based access controls to ensure that only authorized employees are able to access confidential personal data.Overall, through this project and analyzing its scenario, I was able to learn how to enforce the Confidentiality, Integrity, and Availability of data within an organisation, which has allowed me to enhance my understanding of Data Protection for Cybersecurity and their real-world applications.

5. References

Amazon Web Services, [ND]. *Amazon Redshift* [online]. Available from: https://aws.amazon.com/redshift/ [Accessed: 6 Feb 2025]

Amazon Web Services, [ND]. *What is Data Masking?* [online]. Available from: https://aws.amazon.com/what-is/data-masking/ [Accessed: 6 Feb 2025]

Amazon Web Services, [ND]. *What is GuardDuty?* [online]. Available from: https://aws.amazon.com/guardduty/ [Accessed: 6 Feb 2025]

Amazon Web Services, [ND]. *Amazon Redshift backups* [online]. Available from: https://docs.aws.amazon.com/aws-backup/latest/devguide/redshift-backups.html [Accessed: 6 Feb 2025]

Tobin D., 2024. *AWS Redshift vs. The Rest — What's the Best Data Warehouse?* [online]. Available from: https://www.integrate.io/blog/amazon-redshift-how-aws-redshift-compares-to-other-warehouse-data-solutions/ [Accessed: 6 Feb 2025]

https://singaporelegaladvice.com/law-articles/essential-pdpa-compliance-guide-singapore-businesses/

https://www.microsoft.com/en-us/security/blog/2023/07/05/11-best-practices-for-securing-data-in-cloud-services/

https://cloud.google.com/blog/products/storage-data-transfer/google-cloud-storage-best-practices-to-help-ensure-data-privacy-and-security