Addis Ababa University
አዲስ፡አበባ፡ዩኒቨርሲቲ
SEEK WISDOM, ELEVATE YOUR INTELLECT AND SERVE HUMANITY!

ADDIS ABABA INSTITUTE OF TECHNOLOGY

Fundamentals of Cybersecurity Group Assignment

Cybersecurity Risk Assessment and Mitigation

Report for the New Age Bank

Group Members: Section-1

Name	ID number
1. Biruk Amanuel	UGR-7065-14
2. Ermiyas Tesfaye	UGR-6782-14
3. Eyoab Amare	UGR-5756-14
4. Henok Eyayalem	UGR-5473-14
5. Naol Gezahegne	UGR-5473-14

Submission Date: Apr 02 – 2024

Submitted to: Senait Desalegn

Table of Contents

Introduction

The objective of this report is to conduct a cybersecurity risk assessment and propose risk mitigation strategies for the assets of the New Age Bank. The report covers the following aspects:

1. Asset description
2. Risk scenarios
3. Threats and vulnerabilities
4. Likelihood and impact analysis, and risk level determination
5. Risk mitigation strategies
6. Applicable cybersecurity controls

Brand Name

Asset Description

Brand name is the word, name, or symbol legally registered as a trademark, used by New Age Bank to identify itself distinctively from others. Customers use it to distinguish the bank from other banks. The brand name reflects the bank's various qualities like trust, reliability, innovation, or any other qualities that the bank seeks to communicate to its customers. Generally, the brand name serves as a fundamental element of the bank's identity.

Risk Scenarios

Scenario 1: Brand Impersonation Attacks

Brand impersonation is used by hackers to steal data from victims by posing as a legitimate brand.

Cyber attackers may create fake websites, social media accounts, or phishing emails that mimic the New Age Bank's branding. Imposters can mask themselves as a potential employer or legal entity to deceive customers into providing sensitive information, such as login credentials or financial details. This could result in legal and regulatory consequences. The bank may be held accountable for failing to protect customer data or for breaching consumer protection laws.

Scenario 2: Trademark Infringement

Trademark infringement is the unauthorized use of a trademark or service mark.

Competitors or malicious actors may use the New Age Bank's brand name or logo without authorization or use a trademark that is confusingly similar to the bank's trademark to deceive customers. The bank could lose customers who are confused by the infringement and may also damage the bank's reputation. And also if the New Age Bank fails to enforce its rights against infringement, it may risk losing its exclusive rights to the mark through a legal concept known as trademark abandonment.

Threats and Vulnerabilities

Threats

1. Brand Impersonation attacks since attackers may impersonate the New Age Bank's brand by creating emails, social media accounts, or fake websites.
2. Domain Spoofing since malicious actors register domain names similar to the New Age Bank's brand name with common typing mistakes or use Cyrillic characters similar to those in the New Age Bank's brand name
3. There could be unauthorized use of the New Age Bank brand name or logo by competitors or third parties may confuse customers(Trademark infringement)
4. The New Age Bank faces legal challenges related to the unauthorized use of its brand name by competitors or third parties.

Vulnerabilities

1. Insufficient monitoring tools and processes may delay the detection of brand-related cyber threats or incidents.
2. If the New Age Bank fails to register and protect its brand name as a trademark, this may expose it to infringement and unauthorized use.
3. Unable to protect the domain names associated with the New Age Bank's brand name from unauthorized access, manipulation, or exploitation.
4. Lack of awareness among employees about the importance of protecting the brand name and recognizing potential threats may increase the risk of social engineering attacks.

Likelihood and Impact Analysis, and Risk Level Determination

Scenario 1: Brand Impersonation Attacks

- **Likelihood**: high since banks hold valuable financial information and assets making them a target for this kind of attack

- **Impact**: high because the attacks can result in financial losses for both the bank and the customer and can damage the reputation and trustworthiness of the bank.
- **Risk Level**: High since high likelihood of occurrence and high potential impact.

Scenario 2: Trademark Infringement

- **Likelihood**: low to high depending on the bank's brand visibility and industry competitiveness. If it has a highly recognizable brand the likelihood could be considered high
- **Impact**: medium to high because of its impact on the bank's reputation. It has the potential to cause confusion among customers and result in legal disputes with significant costs.
- **Risk Level**: considering the likelihood and impact factors the risk level could be categorized as medium to high.

Risk Mitigation Strategies

Scenario 1: Brand Impersonation Attacks

1. Regularly monitor and review various risks, assess the effectiveness of mitigation measures, and make adjustments as needed to stay ahead of evolving threats.
2. Customers can hand over their information to someone posing as the bank's brand. To avoid this, guiding the communication methods you use to communicate with them is essential. For example, If they know that the bank will never ask for sensitive information via an email or text message, the likelihood that they will hand over that information will decrease. Also informing employees about the partners the bank works with and the common communication patterns is important so that if an attacker attempts to impersonate the bank's brand, the employees can identify the malicious activity.
3. Working closely with domain registrars and domain name authorities to monitor and address incidents is important as the bank can report suspicious domain registrations or abuse to relevant authorities for investigation.
4. Register relevant domain names containing the bank's trademarks to prevent infringement.

Scenario 2: Trademark Infringement

1. Registering the bank's trademarks, including brand names, logos, and slogans with the appropriate authorities is important since registered trademarks provide legal protection and the ability to enforce its rights against infringers.
2. If there is any trademark infringement, the bank has to send **cease and desist** letters to the infringing parties, demanding that they stop using its trademarks.

3. **E**ntering into licensing agreements with third parties who wish to use the bank's trademarks in a controlled manner helps prevent unauthorized use and mitigate the risk of infringement.
4. If cease and desist efforts fail to resolve trademark infringement issues, the bank must take legal action against the infringing parties.

Applicable Cybersecurity Controls and Justification

Brand Impersonation Attacks

1. **Anti-Phishing:** The bank can deploy anti-phishing solutions that analyze URLs, emails, and other content

   - Justification: By using this solution the bank can detect and mitigate brand impersonation attempts such as phishing emails in real-time.

2. **Domain Name Monitoring**
   - Justification: Monitor domain registrations and variations of your organization's domain name to detect unauthorized domains used for brand impersonation. Use domain monitoring services and threat intelligence tools to identify suspicious domain registrations and take appropriate actions.
3. **Employee Training and Awareness**
   - Justification: Employees must be aware of the risks of brand impersonation attacks and how to recognize suspicious emails, websites, and social media accounts. The bank must provide regular cybersecurity training sessions to raise awareness about common phishing techniques and social engineering tactics used in brand impersonation attacks on employees.

4. **Incident Response Plan:** Develop an incident response plan designed to address brand impersonation attacks.

   - Justification: This helps in establishing clear procedures for detecting, investigating, and mitigating brand impersonation incidents, and coordination with law enforcement and third-party stakeholders.

5. **Regular Security Audits and Assessments**

   - Justification: By regularly conducting security audits and assessments the bank can identify vulnerabilities in its digital infrastructure and online presence and address any security gaps that could be exploited by attackers to conduct brand impersonation attacks.

Trademark Infringement

1. **Digital Rights Management (DRM):** It is the use of technology to control and manage access to copyrighted material.

    - Justification: The bank's digital assets such as logos and images can be protected from unauthorized use by applying digital rights management solutions. It can use encryption, watermarks, and access controls to maintain control over its brand assets.

2. **Trademark Usage Guidelines:** The bank must enforce clear guidelines for the use of trademarks in digital marketing materials and advertising campaigns

    - Justification: The bank can prevent unintended infringement by educating employees, partners, and third-party vendors about trademark policies and restrictions.

3. **Social Media Monitoring**

    - Justification: By monitoring social media platforms for unauthorized use of the bank's trademarks in usernames, profiles, and other content posted by users the bank can report trademark violations to social media companies.

4. **Cyber Investigations:** It is conducting cyber investigations and digital forensic analysis to gather evidence of trademark infringement.

    - Justification: By conducting these investigations the bank can work with law enforcement agencies, intellectual property attorneys, and cybersecurity experts to investigate and prosecute trademark infringers.

5. **Cyber Threat Intelligence**

    - Justification: The bank should stay informed about emerging threats and trends related to trademark infringement in cyberspace and subscribe to cyber threat intelligence feeds, industry reports, and legal updates to facilitate effective incident response and mitigation efforts.

Door Access System

Asset Description

Door Access System in the bank's head office is one of the most crucial roles. The purpose of the door access system is to control and manage physical access to several sensitive and protected areas within the building. This system aims to safeguard sensitive information, vaults, protected assets and also safety of employees.

The assets protected by the door access system includes both tangible and intangible assets which are critical to the bank's operations, security and reputation.

Tangible Assets

1. Physical Assets

Physical assets encompass building structures, data centers, server rooms, equipment and devices, cash and also office assets.

2. Human Assets

Human assets encompass employees' safety and also employee's productivity.

Intangible Assets

1. Reputation and Brand Assets

Brand image and customer trust are the main reputation and brand assets.

2. Information Assets

Customer information, financial data and regulatory and compliance documents are among the most useful information assets. These are the most important assets the bank must protect and without door access system all these assets will become highly vulnerable to threats that will ruin the bank.

Risk Scenarios

Scenario 1: Unauthorized Physical Access

Unauthorized physical access to sensitive and protected areas poses several risks to the security and operation of the bank. Mainly access to sensitive areas compromises the security of valuable assets and confidential information. This can lead to financial loss and reputational damage to the bank.

Scenario 2: Malware Attack

A malware attack targeting the Door Access System presents significant risks to the security and integrity of the bank's operations. Malicious software infecting the system could allow anyone bypass the doors which are entry to restricted areas which will jeopardize the security of sensitive information and assets stored within these areas, which will potentially lead to data breaches and theft.

Threats and Vulnerabilities

Scenario 1: Unauthorized Physical Access

Threats

1. Unauthorized individual gains access to vaults which money is stored
2. Unauthorized individual gains access to data centers and server rooms

Vulnerabilities

1. Weak Physical Security Measures
2. Lack of Surveillance Cameras
3. Insufficient Monitoring of Access Points
4. Not careful employee who has access to restricted areas

Scenario 2: Malware Attack

Threats:

1. Potentially compromising the functionality and security

Vulnerabilities

1. Lack of Proper Antivirus and Endpoint Protection Measures
2. Outdated Software
3. Insufficient Network Security
4. Lack of User Awareness and Training

Likelihood and Impact Analysis, and Risk Level Determination

Scenario 1: Unauthorized Physical Access

Likelihood: Moderate - high. It doesn’t commonly occur because to gain unauthorized physical access physical security measures have to be weak, surveillance cameras must not function and there will be insufficient monitoring.

Impact: High – Critical. If an unauthorized individual successfully bypasses the door access system, it could lead to potential theft and damage to assets which could lead to devastating results.

Risk Level: Given the combination of moderate to high likelihood and high- critical impact, the overall risk level associated with unauthorized physical access is deemed high and even critical.

Scenario 2: Malware Attack

Likelihood: Moderate – high: Due to the prevalence of malware threats and potential vulnerabilities in the system’s software and network infrastructure especially on the banking sector the likelihood of malware attack is significant.

Impact: High – critical. If a malware attack successfully done on the door system the door system won’t be able to function this could result in unauthorized access to restricted areas, vaults and compromise sensitive information leading to data breaches or theft, potential financial losses and bad reputation for the bank.

Risk Level: High – critical. Given the combination of moderate to high likelihood and high-critical impact, the overall risk level associated with unauthorized physical access is deemed high and even critical.

Risk Mitigation Strategies

Scenario 1: Unauthorized Physical Access

1. Install high quality surveillance cameras everywhere, especially in key and restricted areas to monitor every movement in the head office.
2. Installing high quality reinforced doors for restricted areas and installing access control systems.
3. Providing training for employees on security protocols and safeguarding access credentials and reporting suspicious activities.
4. Implementing biometric authentication to regulate entry to restricted and key areas within the bank.

Scenario 2: Malware Attack

1. Deploying endpoint protection on systems within the network to reduce the risk of infection and unauthorized access to the door access system.
2. Using network segmentation to distinct sub-networks to enable compartmentalize to deliver unique security controls and services to the door access system. This will limit the spread of malware infections causing minimized impact on the door access system.
3. Implementing regular backup and recovery to ensure data availability and resilience against malware attacks.
4. Implementing continuous monitoring and threat intelligence capabilities to detect and respond to vulnerabilities and emerging malware attacks.
5. Implementing regular patch management to ensure known vulnerabilities are promptly addressed.

Applicable Cybersecurity Controls and Justification

Scenario 1: Unauthorized Physical Access:

1. Access Control Measures:

- Justification: Improved door access system security can be achieved by using authentication systems like keycard access control and biometric authentication. These systems will put barriers for unwanted and unauthorized access to sensitive and protected areas. Their foundation lies in unique physiological characteristics such as facial recognition or fingerprints. Additionally, they produce thorough audit trails that let security staff keep an eye on access trends and spot illegitimate attempts. This will improve the overall security resilience and lowers the probability of unauthorized access incidents. They contribute significantly to safeguarding important locations and priceless valuables, which fortifies the bank's overall security system.

2. Developing Incident Response Plan

- Justification: An incident response plan is crucial for banks to handle unauthorized access incidents and minimize their impact. It outlines clear procedures and protocols for every stage of incident response, from detection to recovery. The plan outlines protocols for detecting unauthorized access, reporting incidents to authorities, and implementing containment measures. It also assigns roles and responsibilities for key personnel, ensuring accountability and coordination. Regular training and drills are conducted to familiarize personnel with their roles. Post-incident analysis and documentation are essential for continuous improvement. This helps the bank identify root causes, lessons learned, and opportunities for enhancing security controls and procedures. By establishing clear procedures, facilitating communication, and continuously improving response capabilities, the bank can mitigate potential consequences of unauthorized access incidents and enhance its resilience to security breaches.

3. Surveillance System

- Justification: The bank has deployed surveillance cameras in key areas of its Head Office Building to enhance its physical security measures. These cameras provide continuous monitoring and recording of entry and exit points, providing valuable insights into the premises. The presence of these cameras acts as a deterrent to potential intruders, reducing the likelihood of security breaches. The recorded footage from these cameras also serves as evidence for investigating security incidents and unauthorized access attempts. This information aids in swift resolution of security incidents and strengthens the bank's ability to prosecute offenders and deter future unauthorized access attempts. The deployment of surveillance cameras is a proactive strategy for strengthening security measures.

Scenario 2: Malware Attack

1. Endpoint Protection solutions:

- Justification: Endpoint Protection Solutions, including antivirus software and comprehensive security solutions, are crucial in mitigating malware attacks on the Door Access System. These solutions monitor system activity, files, and network traffic for signs of malicious behavior, quarantine or remove malicious files, and maintain the integrity of the system. They employ advanced detection techniques, such as signature-based detection, heuristic analysis, behavioral monitoring, and machine learning algorithms, to detect and neutralize malware variants. Additional security features like firewall management, intrusion prevention systems, application control, and device control further protect against malware threats. Centralized management consoles enable security administrators to monitor and manage security policies across all network endpoints, ensuring consistent enforcement of security policies.

2. Patch Management:

- Justification: A robust patch management process is crucial for ensuring the security and resilience of a bank's door Access System. This process involves identifying, testing, and applying software and firmware updates, including security patches, to address known vulnerabilities and reduce the risk of malware exploitation. The process starts with a comprehensive vulnerability assessment and prioritization, followed by testing and validating patches in a controlled environment. Patches are then deployed to the system and other network components in a timely manner, often using automated tools. Regular and timely patching reduces exposure to known vulnerabilities and mitigates the risk of malware exploitation. Regular monitoring and verification of patch compliance ensure all systems are up-to-date, demonstrating compliance with security policies and regulatory requirements.

3. Continuous monitoring and threat intelligence

- Justification: Continuous monitoring and threat intelligence are crucial for proactive detection and response to emerging malware threats. Monitoring network traffic, system logs, and security events helps identify anomalous activity. Threat intelligence feeds, security advisories, and industry reports inform security teams about malware trends, enabling proactively adjusted security controls and mitigation strategies.

4. Regular Backup and Recovery

- Justification: Regular backup and recovery procedures are crucial for a bank's infrastructure to protect against malware attacks and data loss. These procedures involve creating and storing data in secure locations, regularly testing them for integrity and effectiveness. Regular backups help minimize downtime, financial losses, and reputational damage, while demonstrating the bank's commitment to data protection and business continuity, instilling confidence among customers, stakeholders, and regulatory authorities.

Managers

Asset Description

The New Age Bank's managers play a critical role in the bank's success. These individuals hold positions of significant trust, overseeing essential functions that drive the bank's operational efficiency and strategic direction. They possess privileged access to highly sensitive data, including financial records, customer information, regulatory compliance documents, and internal systems vital for daily operations. Due to their comprehensive access and decision-making authority, these managers are prime targets for cybercriminals seeking to exploit weaknesses in the bank's security infrastructure.

Risk Scenarios

Scenario 1: Insider Threat

A manager with privileged access misuses their authority to gain unauthorized access to sensitive customer information, manipulate data, or engage in fraudulent activities. This can have severe consequences, including financial loss, reputational damage, and compromised data integrity.

Scenario 2: Data Breach

External attackers exploit vulnerabilities in the Managers' asset to gain unauthorized access to the database, resulting in the theft or compromise of sensitive managerial data. This can lead to reputational damage, legal and regulatory implications, and loss of customer trust.

Threats and Vulnerabilities

Threats

1. **Insider Threats:** Managers with privileged access may intentionally or unintentionally misuse their authority to gain unauthorized access or manipulate data for personal gain or malicious purposes.

2. **External Attacks:** Cybercriminals may target the Managers to exploit vulnerabilities and gain unauthorized access to the Managers' database, seeking financial gain or to compromise sensitive data.

Vulnerabilities

1. **Inadequate Access Controls**: Weak or misconfigured access controls increase the risk of insider threats. Insufficient segregation of duties and improper access privilege management may enable unauthorized activities.
2. **Insufficient Training**: Managers may lack awareness of cybersecurity best practices, making them more susceptible to social engineering attacks, such as phishing or pretexting.
3. **Weak Authentication**: Managers may use weak passwords or reuse passwords across multiple accounts, increasing the risk of unauthorized access. Lack of multi-factor authentication (MFA) further weakens the authentication process.
4. **Outdated Software**: Failure to regularly update and patch the system exposes it to known vulnerabilities that can be exploited by external attackers. Unpatched systems may have security weaknesses that can lead to unauthorized access or data breaches.

Likelihood and Impact Analysis, and Risk Level Determination

Scenario 1: Insider Threat

- **Likelihood:** Medium (due to the presence of privileged access and potential for insider threats)
- **Impact:** High (potential financial loss, reputational damage, compromised data integrity)
- **Risk Level:** High

Scenario 2: Data Breach

- **Likelihood:** High (as external attacks are prevalent and targeted towards valuable managerial data)
- **Impact:** Medium (potential loss of sensitive managerial data, reputational damage, legal and regulatory implications)
- **Risk Level:** High

Risk Mitigation Strategies

Scenario 1: Insider Threat

1. Implement Role-Based Access Control (RBAC) to ensure that managers only have access to the data and functionalities necessary for their roles, reducing the risk of unauthorized access.
2. Provide comprehensive cybersecurity training to managers, emphasizing the importance of strong passwords, recognizing social engineering attacks, and following best practices for data protection.
3. Enforce strong authentication mechanisms, such as multi-factor authentication (MFA), to enhance the security of manager accounts and prevent unauthorized access.
4. Regularly monitor and audit manager activities to detect any suspicious or unauthorized actions.
5. Implement data loss prevention (DLP) measures to monitor and prevent unauthorized data exfiltration or manipulation.

Scenario 2: Data Breach

1. Regularly update and patch the system to address known security vulnerabilities and protect against external attacks.
2. Implement network security measures, such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS), to monitor and detect unauthorized access attempts and malicious activities.
3. Conduct regular vulnerability assessments and penetration testing to identify and remediate system weaknesses.
4. Implement encryption mechanisms to protect sensitive managerial data at rest and in transit.
5. Establish an incident response plan to quickly detect, respond to, and recover from potential data breaches.

Applicable Cybersecurity Controls and Justification

1. **Access Control:** Implement RBAC to ensure that managers have appropriate access privileges based on their roles and responsibilities, reducing the risk of unauthorized access.

- Justification: Access control will help restrict unauthorized access and prevent misuse of privileges, protecting sensitive data and maintaining confidentiality.

2. **Employee Training:** Conduct regular cybersecurity training sessions for managers, covering topics such as password hygiene, social engineering awareness, and data protection.

- Justification: Proper training increases managers' awareness of cybersecurity risks and equips them with knowledge and skills to identify and mitigate potential threats.

3. **Multi-Factor Authentication (MFA):** Require managers to use MFA to add an extra layer of security during the login process, reducing the risk of unauthorized access.

- Justification: MFA enhances the security of manager accounts by verifying the identity of the users through multiple factors, making it harder for attackers to gain unauthorized access.

4. **System Patching:** Regularly update and patch the People's Asset system to address known security vulnerabilities and protect against external attacks.

    - Justification: Patching ensures that the system is up to date with the latest security fixes, reducing the risk of exploiting known vulnerabilities by attackers.

5. **Monitoring and Logging:** Implement robust monitoring and logging mechanisms to track and detect any suspicious activities, allowing for timely response and investigation.

    - Justification: Monitoring and logging provide visibility into system activities, enabling the detection of unauthorized access attempts, insider threats, or abnormal behavior. This supports incident response and forensic investigations.

6. **Network Security:** Implement firewalls, IDS, IPS, and other network security measures to monitor and detect unauthorized access attempts and malicious activities.

    - Justification: Network security measures help protect against external attacks, identify potential threats, and prevent unauthorized access to the system.

7. **Encryption:** Implement encryption mechanisms to protect sensitive managerial data at rest and in transit.

    - Justification: Encryption ensures that even if the data is compromised, it remains unreadable and unusable to unauthorized individuals, maintaining data confidentiality.

8. **Incident Response Plan:** Establish an incident response plan to quickly detect, respond to, and recover from potential data breaches.

    - Justification: Having a well-defined incident response plan enables the organization to respond effectively to security incidents, minimizing the impact and facilitating a timely recovery.

Microsoft Office 365

Asset Description

Microsoft office 365 is Microsoft cloud powered productivity platforms, which includes platforms such as word, Excel, PowerPoint, Outlook, OneDrive and more.

Risk Scenarios

Scenario 1: Phishing attack

Employees might receive a message from phishing email impersonating Microsoft office 365 notification in which the email contain a fake page designed as a login page for office 365 and their credentials might be stolen.

Scenario 2: The Leakage of data

A sensitive document that contains customer information may be inadvertently shared by an employee via a public link in OneDrive for Business, potentially leading to data leakage

Threats and vulnerabilities

Threats

1. Cyber criminals might impersonate the bank to trick the employee into giving sensitive information.
2. Sensitive information being shared outside of the organization without authorization.

Vulnerabilities

1. **Misconfigured sharing settings:** Workers might unintentionally forward documents to someone they don't mean to.
2. **Lack of data loss prevention:** Office 365 may not detect and prevent unauthorized data sharing.
3. Lack of employee awareness on phishing attempts, leading to the bank's credential compromise. Lack of email filtering leads to receiving malicious emails and office 365 may not detect and block malicious phishing links.

Likelihood and Impact Analysis, and Risk Level Determination

Scenario 1: Phishing attack

Likelihood: the likelihood of phishing attacks are high, as the attacks are common and can target employees within an organization.

Impact: the impact of phishing attacks are high because, credentials that are compromised could lead to unauthorized access, data breaches, or account takeovers.

Risk level: the risk level of phishing attacks are High

Scenario 2: The Leakage of data

Likelihood: Moderate, accidental mishaps and human error may not happen frequently, but they can happen.

Impact: High, Data leaks may result in lost customer trust, reputational harm, and regulatory noncompliance.

Risk level: Medium

Risk mitigation strategies

Scenario 1: Phishing attack

1. **Security awareness training**: Educate employees about phishing techniques, how to recognize suspicious emails, and the importance of verifying sender identities.
2. **Email Filtering and anti-phishing solutions**: Implement advanced email filtering in Office 365 to detect and block phishing emails before they reach users.
3. **Multi-factor Authentication (MFA):** Enable MFA for Office 365 accounts to add an extra layer of security, even if credentials are compromised.
4. **Incident response plan:** Develop and implement an incident response plan specific to phishing attacks, outlining steps for detection, containment, and recovery.

Scenario 2: The Leakage of data

1. **Data Loss Prevention (DLP):** Use office 365 DLP policies to detect and stop unwanted data sharing based on pre-established guidelines.
2. **Access control permission:** To make sure that only those with the appropriate authority

can access sensitive data, make sure to check and modify permissions and access restrictions

3. **User training awareness:**
4. Give staff members through instruction on appropriate document sharing procedures and stress the need of data protection.
5. **Regular Audits and Monitoring**;
6. To find and fix any vulnerabilities, do routine checks and keep an eye on Office 365 data sharing activities.

Applicable Cybersecurity Controls and Justification

Scenario 1: Phishing attack

1. **MFA**
   - Justification - MFA mitigates the risk of unauthorized access even if credentials are compromised in a phishing attack.
2. **Email filtering**
   - Justification - Advanced email filtering prevents phishing emails from reaching users, reducing the likelihood of successful attacks.

Scenario 2: The Leakage of data

1. **DLP policies**:
   - Justification - DLP policies prevent unauthorized data sharing, reducing the risk of data leakage.
2. **Access controls:**
   - Justification - Proper access controls and permissions ensure that sensitive data is only accessed by authorized personnel, mitigating the risk of accidental sharing.

Personnel Data

Asset Description

Personnel data is an essential resource that forms the basis of many internal processes and communications. This includes data about workers, including their roles, employment history, and relevant personal information. It is, in essence, the information we retain about each and every one of our workers, including their names, positions, work histories, and other pertinent details.

New Age Bank prioritizes protecting the security and privacy of employee data. To make sure it is treating this information appropriately, there are a few guidelines that it must adhere to. Inappropriate access to or improper handling of personnel data could have major repercussions, including invasions of privacy, legal problems, and reputational harm.

Risk Scenarios

Scenario 1: Unauthorized Access by Employees

Employees within bank may attempt to gain unauthorized access to personnel data for various reasons, including curiosity, personal gain, or malicious intent. This unauthorized access could involve viewing, modifying, or disseminating sensitive employee information without proper authorization. This scenario poses a significant risk to the confidentiality, integrity, and privacy of personnel data, potentially leading to legal liabilities, breaches of trust, and reputational damage to the organization.

Scenario 2: Insider Threats

Disgruntled or former employees may pose a threat to personnel data by intentionally or unintentionally compromising the security and confidentiality of this information. Such individuals may engage in malicious activities such as unauthorized data access, data exfiltration, or sabotage, aiming to disrupt operations, tarnish the company's reputation, or seek revenge. Insider threats represent a complex and challenging risk scenario that requires proactive measures to mitigate.

Threats and Vulnerabilities

Threats

1. **Unauthorized Access by Employees**: Employees attempting to access sensitive banking data without proper authorization, potentially for personal gain or malicious purposes.

2. **Insider Threats**: Malicious activities or negligence by current or former bank employees that compromise the security and confidentiality of sensitive financial information.
3. **Data Exfiltration**: Unauthorized extraction or transfer of banking data from the bank's systems, posing risks of data breaches and financial fraud.
4. **Sabotage**: Intentional actions aimed at disrupting banking operations or damaging the reputation of the financial institution.
5. **Negligence**: Unintentional mishandling or exposure of sensitive banking data due to carelessness or lack of awareness among bank staff.

Vulnerabilities

1. **Weak Access Controls**: Inadequate enforcement of access controls, such as weak passwords or insufficient authentication mechanisms, leaving banking systems vulnerable to unauthorized access.
2. **Lack of Monitoring:** Inadequate monitoring and auditing of employee activities and data access, allowing malicious or unauthorized actions to occur unnoticed.
3. **Insider Collusion**: Collaborative efforts among bank employees to bypass security measures and access sensitive financial data for unauthorized purposes.
4. **Inadequate Training:** Lack of comprehensive security awareness training for bank employees, increasing susceptibility to social engineering attacks and compromising data protection measures.
5. **Ineffective Termination Procedures**: Failure to promptly revoke access privileges and credentials for terminated or departing bank employees, risking unauthorized access to sensitive banking data.

Likelihood and Impact Analysis, and Risk Level Determination

Scenario 1: Unauthorized Access by Bank Employees

- **Likelihood:** Medium (potential for unauthorized access exists due to insider knowledge and access privileges within the banking systems)
- **Impact:** High (unauthorized access can lead to breaches of privacy, loss of trust, and legal consequences)
- **Risk Level:** High

Scenario 2: Insider Threats within Banking institutions

- **Likelihood:** Low to Medium (incidents may occur but are less frequent compared to external threats, incidents of insider threats within banking institutions can still occur)

- **Impact:** High (insider threats can result in significant damage to personnel data and the organization's reputation of the bank)
- **Risk Level:** Medium to High

Risk Mitigation Strategies

Scenario 1: Unauthorized Access by Employees

1. **Implement Robust Access Controls:** Utilize role-based access permissions and conduct regular access reviews to restrict employees' access to sensitive banking data beyond their job roles.
2. **Conduct Comprehensive Security Awareness Training:** Educate all bank employees on the importance of data confidentiality, integrity, and compliance with banking policies and regulations to prevent unauthorized access.
3. **Deploy Monitoring and Auditing Mechanisms:** Utilize advanced monitoring and auditing tools to track employee activities within banking systems, detecting any unauthorized access attempts or suspicious behavior promptly.
4. **Establish Clear Incident Reporting Procedures:** Implement clear policies and procedures for reporting and investigating incidents of unauthorized access. Swift action and appropriate disciplinary measures should be taken to deter future occurrences.

Scenario 2: Insider Threats

1. **Foster a Culture of Trust and Accountability:** Promote a culture of trust, transparency, and accountability within the banking organization. Encourage open communication and address employee grievances promptly to mitigate potential insider threats.

2. **Implement Stringent Access Controls:** Enforce stringent access controls and segregation of duties within banking systems to prevent collusion among employees and limit the impact of insider threats on sensitive financial data.

3. **Conduct Regular Security Assessments and Audits:** Perform regular security assessments and audits to identify and address vulnerabilities in banking data protection mechanisms, ensuring continuous improvement in security measures.

4. **Establish Clear Termination Procedures:** Develop clear policies and procedures for employee termination, including the prompt revocation of access privileges and conducting exit interviews to collect company-owned assets and ensure data security.

Applicable Cybersecurity Controls and Justification

1. **Access Control:** Enforcing robust access controls, such as role-based permissions and user authentication mechanisms, helps prevent unauthorized access to sensitive financial data within banking systems, maintaining data confidentiality and integrity.
2. **Security Awareness and Training:** Providing comprehensive security awareness training to bank employees ensures they understand the risks associated with insider threats and adhere to best practices for data protection and compliance, thereby reducing the likelihood of successful insider-related incidents.
3. **Monitoring and Auditing:** Implementing advanced monitoring and auditing mechanisms enables banks to detect and investigate suspicious activities or unauthorized access attempts promptly, facilitating timely response and mitigation actions to safeguard banking data.
4. **Incident Response:** Establishing a comprehensive incident response plan enables banks to effectively respond to and mitigate insider threats and unauthorized access incidents, minimizing the impact on data security and banking operations.