

GROUP ASSIGNMENT

COMP40002

**NETWORKING CONCEPTS AND CYBER SECURITY- 2**

**CF2361COM/CF2362COM/**

HAND OUT DATE: 2nd week

HAND IN DATE: ASSIGNMENT2: 12-06-2024

WEIGHTAGE: ASSIGNMENT 1: 50%

**INSTRUCTION TO CANDIDATES:**

1. **Students are advised to underpin their answers with the use of references (cited using the Harvard Name System of Referencing).**
2. **Late submission will be awarded zero (0) unless Exceptional Circumstances (EC) are upheld.**
3. **We draw your attention to the** [**Academic Conduct**](ttps://www.staffs.ac.uk/students/course-administration/academic-policies-and-regulations/Academic-Conduct-Procedure/academic-conduct-procedure-post-sept23) **Procedure to encourage good academic practice.**
4. **Assignment presentation and modeling work should be submitted as a softcopy**

**Our group members:**

* **Dhulvin Wijewardana : CB012062**
* **Nickel Gunasekera : CB013126**
* **Senesh Maleesha :**
* **Pasindu Navodya:CB013343**

**Table of Contents**

* **Introduction** 
  + Why we choose commercial bank
  + Recent Developments and milestones
* **Critical Objectives**
* Critical Objectives in Combank
* **Critical Processes**
* Critical processes for critical objectives in commercial Bank
* **Assets** 
  + What are assets?
  + Assets for each Processes
* **Threats**
  + What are threats?
  + Threats for each assets
* **Quantitative Risk assessments for assets**
* **Disaster recovery plans focusing on threats**
* **Conclusion**

**Commercial Bank Case Study**

**Why did we decided to move on with commercial bank?**

* Banks need business continuity plans and Disaster recovery plans to make sure they can keep running smoothly even when faced with unexpected problems or disasters.
* Business continuity plans help them keep essential services going and maintain customer trust, while disaster recovery plans help them recover quickly from any disruptions, like cyber-attacks, system failures, or natural disasters.

**Recent Developments and Milestones:**

* In 2021, the bank witnessed a significant increase in its deposit base by 13.99% year on year, reaching Rs.1.443 Trillion. Moreover, the bank’s current account savings account ratio improved to 47.83%, the highest in the banking sector.
* Overseas operations contributed 12.4% of the bank’s assets and 18.6% of pre-tax profits, reflecting its global footprint and diversified revenue streams.
* Technological advancements included the adoption of digital signatures for business customers, deployments of EMV 3DS fraud prevention technology, and the launch of innovative payment solutions as LANKAQR supported android POS devices and the Q+ Payment App.

**Historical Milestones:**

* The bank has continuously evolved its digital services to better serve its customers. In 2021, it revamped its website with advanced features, ensuring a more user-friendly experience. Started internet banking in 2000. Subsequent include the establishment of the 500th ATM at maradana railway station in 2011 and the opening of the 24-hour automated banking Centre at ward Place in 2012.
* In 2018, the bank launched fully automated cheque deposit machines and became the first in srilanka to issue unionPay cards. The same year saw the introduction of the flash digital bank account.
* In 2019, the bank continued its pioneering efforts by launching WEchat Pay acceptance, ComBank Q+, and enabling Dynamic Currency conversion at ATMs for foreign Visa cards. In 2020 the bank unveiled combank digital, powered by Fiserv, a global leader in financial services technology, further enhancing its digital offerings.

**Critical objectives**

Critical objectives are the most important goals or targets that an organization aims to achieve to be successful. These objectives guide the organization’s effort and decisions, helping it stay focused on what matters most for its growth and sustainability.

**Critical objectives in commercial bank:**

1. Financial Operations Management
2. Client Relationship Administration
3. Financial Security Oversight

**Financial operations management**

* Also known as transaction Processing, making sure transactions happen smoothly and safely is really important for a bank.
* The bank has to follow the rules and make sure everything is done correctly and on time, so customers can trust that their money is being taken care of properly.

**Client Relationship administration**

* Keeping track of customer accounts is a big part of what banks do. This involves things like opening new accounts, updating customer information, keeping track of how much money is each account, and helping customers with any questions or requests they have about their accounts.
* The bank also has to make sure it follows all the rules about managing accounts to keep everything fair and legal.

**Financial Security Oversight**

* Banks have to deal with different kinds of risks, like the chance that someone might not pay back a loan, or that the value of investments might go down.
* Managing these risks is really important to make sure the banks money and its customer’s money stay safe . This involves figuring out what risks there are, how big they are, and what can be done to minimize them. It’s all about keeping things stable and secure so the bank can keep doing its job properly.

**Critical processors**

* A critical process is a really important tasks or series or tasks that a company must do to stay successful. These processes are crucial because they directly impact the company’s ability to achieve its goals and keep things running smoothly.
* If something goes wrong with critical process, it can cause big problems for the company, like losing customers or money.

**Critical processes for critical objectives in commercial Bank:**

1. **Financial Operations Management**

* Online banking
* ATMs
* Point of Sales

1. **Client Relationship Administration**

* CRM
* Data Encryption
* Data Backup

1. **Financial Security Oversight**

* Market risk management
* Operational risk management
* Credit risk management

**1. Financial Operations Management**

Online banking =>

* This is a key way for customers to manage their accounts and conduct transaction using digital platforms.
* It includes tasks like transferring funds, paying bills, and checking account balances online.

ATMs =>

* Allow customers to access basic banking services like withdrawing cash, depositing money, and checking account balances outside of traditional bank branches, providing convenience and accessibility.

Point of Sales =>

* Point of sales systems are used in retail stores to process electronic payments when customers make purchases using debit or credit cards.

**Justification:** these processes are crucial for ensuring that transactions happen smoothly and efficiently in a bank. Online banking and ATMs provide convenient ways for customers to manage their money, while POS systems enable businesses to accept payments, supporting their revenue generation.

**2. Client Relationship Administration**

CRM =>

* This involves using systems to keep track of interactions with customers, understand their preferences, and provide better service. Its helps build strong relationships with customers.

Data Encryption =>

* This is about protecting sensitive customer information, like account details, by endoing it so that only authorized people can access it. It keeps customer data safe from hackers.

Data Backup =>

* Regularly backing up data ensures that even if something goes wrong, like a computer crashing, customer account information can be recovered.

**Justification:** these process are really important for keeping customer accounts safe and secure. CRM helps banks understand and serve customers better, while data encryption and backup make sure that customer information is protected and can be recovered if needed.

**3. Financial Security Oversight**

Market risk management =>

* This means keeping an eye on things like interest rates, exchange rates, and the prices of financial stuff like stocks and bonds.
* It’s about being ready for changes in the market that could affect the bank’s money.

Operational risk management =>

* Here, the focus is on spotting and dealing with risks that come from inside the bank, like problems with systems or mistakes made by people.
* It’s about making sure everything runs smoothly so nothing disrupts business.

Credit risk management =>

* This involves looking at the risk of losing money because people or business might not pay back their loans or debuts.
* It’s about being careful when lending money to make sure the bank doesn’t lose out.

**Justification:** These process are super important for keeping the bank’s money safe and following the rules. By managing market, operational, and credit risks well, the bank can stay financially strong and products its good reputation.

**Assets for each process**

**What are assets?**

Assets are things that you own that have value. They can be tangible or intangible. Basically assets are what you own that can bring you money or provide some benefit in the future.

**1. Financial Operations Management**

Online banking (assets) =>

* **Online banking platform**: the software, applications, and hardware infrastructure that host the online banking system.
* **Authentication systems**: tools and protocols used to verify the identity of users accessing the online banking platform.

ATMs =>

* **Cash Inventory**: physical cash stored within the ATMs to facilitate withdrawals by customers.
* **ATM hardware:** physical machines installed in various locations to provide banking services.

Point of Sales =>

* **POS terminals:** physical devices installed at merchant locations to process card transactions.
* **Payment Gateway:** software and hardware facilitating secure payment processing and communication between the POS terminal and the bank’s systems.

**2. Client Relationship Administration**

CRM =>

* **CRM software:** software application used to store customer information, track interactions, and manage customer relationships.
* **Database**: centralized database containing detailed records of customer accounts, preferences, and transaction history.

Data Encryption =>

* **Encryption Algorithms**: algorithms used to encrypt sensitive data, ensuring it’s confidentially and integrity.
* **Encryption Hardware**: hardware devices such as security modules and hardware security modules (HSMs) used to perform encryption operations securely.

Data Backup =>

* **Backup servers:** dedicated servers or storage systems used for storing backup copies of customer data and transaction records.
* **Backup Media:** physical media such as tapes, disks, or cloud storage used for storing backup data.

**3. Financial Security Oversight**

Market risk management =>

* **Risk analytics Software:** advanced software tools and models for analyzing market data, assessing risk exposures, and simulating market scenarios.
* **Market risk reports:** regular reports summarizing key market risk metrics, exposures, and trends for management and regulatory purposes.

Operational risk management =>

* **Incident management system:** system for recoding, tracking, and managing operational incidents and disruptions, ensuring timely resolution and root cause analysis.
* **Workflow automation software:** automation tools that streamline incident management processes by automating tasks such as incident assignment, and notification.

Credit risk management =>

* **Credit scoring models:** statistical models and algorithms for assessing the creditworthiness of borrowers based on historical data and risk factors.
* **Loan portfolio management tools:** software applications for monitoring and managing the bank’s loan portfolio, tracking loan performance, and identifying potential credit risks.

**Threats for each critical asset**

**What are threats?**

Threats are potential dangers of risks that could harm something valuable or important.

**1. Financial Operations Management**

**Online banking (assets) =>**

* **Online banking platform**:

**Phishing attacks**: threat actors may attempt to deceive users into providing their login credential by impersonating the bank’s website or sending fraudulent emails.

**Distributed denial of service (DDoS) attacks**: attackers may flood the online banking platform with a high volume of traffic, causing service disruptions and preventing legitimate users from accessing their accounts.

* **Authentication systems**:

**Man in the middle (MITM) attacks:** cybercriminals may intercept communication between users and the online banking platform to capture authentication credentials.

**Credential stuffing**: attackers may use stolen login credentials obtained from data breaches to gain unauthorized access to user accounts.

**ATMs =>**

* **Cash Inventory**:

**ATM skimming: criminals** may install skimming devices on ATM to capture card details and PINs of unsuspecting users, enabling fraudulent cash withdrawals.

**Physical attacks:** thieves may attempt to break into ATM to steal cash directly of access the cash cassettes inside the machines.

* **ATM hardware:**

**ATM tampering:** attackers may tamper with the hardware components of ATMs, such as card readers or cash dispensers, to manipulate transaction or steal cash.

**Remote Exploitation:** vulnerabilities in the ATM’s hardware or software may be exploited by hackers to remotely compromise the machine and gain unauthorized access.

**Point of Sales =>**

* **POS terminals:**

**POS malware:** cybercriminals may infect POS terminals with malware designed to capture card information or manipulate transaction data for fraudulent purposes.

**Inside threats:** employees with access to POS terminals may misuse their privileges to steal card data or conduct unauthorized transactions.

* **Payment Gateway:**

**Payment processing errors:** software bugs or misconfiguration in the payment gateway may lead to processing errors or transaction failures, impacting customer satisfaction and revenue.

**Payment Fraud:** attackers may exploit vulnerabilities in the payment gateway’s software or infrastructure to intercept or manipulate payment transaction, resulting in financial losses for the bank and customers.

**2. Client Relationship Administration**

**CRM =>**

• **CRM software:**

* **Data Breaches** => this is when unauthorized persons gain access to sensitive information stored in the CRM (customer relationship management) software.
* **Software vulnerabilities** =>these are weaknesses or flaws in the CRM software’s code that can be exploited by hackers or malicious software to gain unauthorized access or cause harm.

• **Database:**

* **SQL injections** => this is like a sneaky way for attackers to trick a database into doing something it shouldn’t .it’s kind of like someone slipping a fake ID to get into a club.
* **data corruptions** =>unintended changes or errors in stored data that can render it inaccurate, incomplete, or unusable, often caused by technical faults, software bugs, or malicious actions.

**Data Encryption =>**

• **Encryption Algorithms:**

* **insider threats** => these are risks posed by individuals within an organization who have privileged access to sensitive information.in the context of encryption algorithms, an insider threat might involve an employee intentionally or unintentionally leaking encryption keys or other critical information.
* **cryptographic attacks** => these are attempts to break through encryption by exploiting weaknesses in the encryption method itself, like trying every possible key or finding flaws in the encryption system.

• **Encryption Hardware:**

* **supply chain attacks** => this happens when bad actors tamper with hardware components during the manufacturing or distribution process, potentially compromising the security of the encryption hardware.
* **side-channel attacks** => this is when attackers use unconventional methods like monitoring power usage or electromagnetic signals to try to gather information about the encryption keys or data, by passing the encryption’s protection.

**Data Backup =>**

• **Backup servers:**

* **Ransom ware attacks** => these are malicious attempts to block access to data or systems until a ransom is paid.in the context of backup servers, ransom ware attacks can encrypt of delete backup data , rendering it unusable, and then demand payment in exchange for restoring access.
* **Unauthorized access** => this refers to individuals or entities gaining entry to backup servers without proper authorization. Unauthorized access van lead to theft, manipulation, or deletion of backup data, potentially compromising the integrity and availability of data crucial for business operations.

• **Backup Media:**

* **cloud service vulnerabilities** => this involves weaknesses in cloud storage services that can be exploited by attackers to gain unauthorized access to backup data .
* **data corruption**

**3. Financial Security Oversight**

**Market risk management =>**

• **Risk analytics Software:**

* Software vulnerabilities
* Data breaches

• **Market risk reports:**

* **Data leakage** => this refers to unauthorized or unintentional disclosure of sensitive market risk information contained in reports. Data leakage can occur through various channels, including insecure transmission methods, insider threats, or inadequate access controls.
* **Regulatory non-compliance** => this involves failing to adhere to regulatory requirements and standards governing the production and dissemination of market risk reports.

**Operational risk management =>**

• **Incident management system:**

* **System Outages** => these occur when the incident management system experiences disruptions or failures, leading to downtime and hindering its ability to effectively identify, assess, and respond to operational incidents.
* **Insider Threats**

• **Workflow automation software:**

* **Software malfunction** => this occurs when the workflow automation software experiences technical issues or errors that disrupt its normal functioning. Software malfunctions can lead to delays, inaccuracies, or failures in automated processes, impacting the efficiency and reliability of operational risk management activities.
* **Unauthorized access**

**Credit risk management =>**

• **Credit scoring models:**

* **Data quality issues** => these are problems with the accuracy, completeness, or reliability of the data used in credit scoring models. When data quality is poor, it can lead to inaccurate assessments of creditworthiness, resulting in incorrect lending decisions or increased credit risk exposure for the financial institution.
* **Model drift =>** this occurs when the predictive power of credit scoring models diminishes over time due to changes in the underlying data or economic conditions..

• **Loan portfolio management tools:**

* **Integration risks =>** these are challenges related to the seamless integration of loan portfolio management tools with existing systems and processes within the financial institution.
* **Cyber-attacks =>** these are malicious attempts to disrupt or gain unauthorized access to loan portfolio management systems and data .

**Quantitative Risk assessments for assets**

We as group have done the risk assessment by identifying the Asset Value (AV), Exposure Factor (EF), single loss Expectancy (SLE), Annual Rate of Occurrence (ARO) and Annual Loss Expectancy (ALE) for each asset based on a threat.

* Asset value: - the estimated worth or value of an asset to the organization.
* Exposure Factor: - the percentage of loss that would occur if a specific threat materializes and impacts the asset.
* Single loss expectancy: - the expected monetary loss for a single occurrence of a threat exploiting the vulnerability of an asset.
* Annual rate of Occurrence: - the frequency at which a specific threat is expected to occur annually.
* Annual loss expectancy: - the expected monetary loss per year due to a specific threat affecting the asset.

**1. Financial Operations Management**

**Online banking (assets) =>**

* **Online banking platform**:

**Distributed denial of service (DDoS) attacks**:

**Asset Value**: the online banking platform is worth $500,000 to the organization.

**Exposure Factor**: when a DDOS attack happens, it could cause a 70% loss of service availability.

**Single loss expectancy:** for one DDoS attack, the expected loss is $350,000 is (500,000 \* 70/100)

**Annual rate occurrence**: attacks happen once every two years. (1/2 = 0.5)

**Annual loss expectancy:** the expected yearly loss due to DDos attack is $175000

* **Authentication systems**:

**Man in the middle (MITM) attacks:**

**Asset value**: $20,000 (customer data, transaction data)

**Exposure factor:** Assume that if a MITM attack occurs, it could lead to 70% exposure of authentication credentials.

**Single loss expectancy:** $20,000 \* 70/100 = $14000

**Annual rate or Occurrence:** MITM attacks targeting authentication systems occur once a year. (ARO =1)

**Annual loss expectancy:** $20 000 \* 1 = $20 000

**ATMs =>**

* **Cash Inventory**:

**ATM skimming:**

**Asset value**: $8,000 (cash, ATM cash cassettes, cash loading processes)

**Exposure factor:** Assume that if ATM skimming occurs, it can result in a 50% exposure of the cash inventory.

**Single loss expectancy:** $8,000 \* 50/100 = $4000

**Annual rate or Occurrence:** assume that ATM skimming incidents occur four times a year (ARO =4)

**Annual loss expectancy:** $4000 \* 4 = $16 000

**ATM hardware:**

**ATM tampering:**

**Asset value**: $6000(card reader, cash dispenser, PIN pad)

**Exposure factor:** Assume that if ATM tampering occurs, it can lead to 85% exposure of the ATM hardware.

**Single loss expectancy:** $6,000 \* 85/100 = $5100

**Annual rate or Occurrence:** assume that ATM tampering incidents occur two times a year (ARO =2)

**Annual loss expectancy:** $5100 \*2 = $10 200

**Point of Sales =>**

* **POS terminals:**

**POS malware:**

**Asset value**: $2000(display screen, PIN pad)

**Exposure factor:** assume that if POS malware infects POS terminals, it can result in a 68% exposure of the POS terminals.

**Single loss expectancy:** $2000 \* 68/100 = $1360

**Annual rate or Occurrence:** assume that POS malware incidents occur 5 times a year. So the ARO is 5.

**Annual loss expectancy:** $1360 \*5 = $6800

* **Payment Gateway:**

**Payment Fraud:**

**Asset value**: $15000 (software, transaction data)

**Exposure factor:** assume that if payment fraud occurs, it could lead to an 80% exposure of the payment gateway

**Single loss expectancy:** $15000 \* 80/100 = $ 12000

**Annual rate or Occurrence:** assume that payments fraud incidents occur 3 times a year.

**Annual loss expectancy:** $12000 \*3 = $36 000

**2. Client Relationship Administration**

**CRM =>**

• **CRM software:**

* Data Breaches

**Asset value**: $30000 (customer data, contact management tools)

**Exposure factor:** assume that if a data breach occurs, it could lead to 70% exposure of the CRM software.

**Single loss expectancy:** $30000 \* 70/100 = $ 21000

**Annual rate or Occurrence:** assume that data breach incidents targeting the CRM software occur 4 times a year.

**Annual loss expectancy:** $21000 \*4 = $84 000

• **Database:**

* SQL injections

**Asset value**: $300,000(security credentials, account information)

**Exposure factor:** assume that if a SQL injection occurs, it could lead to a 75% exposure of the database.

**Single loss expectancy:** $300000 \* 75/100 = $ 225 000

**Annual rate or Occurrence:** assume that SQL injection targeting the database attacks happen once every five years. (1/5 = 0.2)

**Annual loss expectancy:** $225 000 \*0.2 = $45 000

**Data Encryption =>**

• **Encryption Algorithms:**

* insider threats

**Asset value**: $700,000 (data encryption algorithms, key management systems, secure hardware modules)

**Exposure factor:** assume that if an insider threat occurs, it could lead to a 60% exposure of Encryption algorithms.

**Single loss expectancy:** $700 000 \* 60/100 = $ 420 000

**Annual rate or Occurrence:** assume that insider threat incidents targeting encryption algorithms occur three times a year. ARO = 3

**Annual loss expectancy:** $420 000 \*3 = $1,280,000

• **Encryption Hardware:**

* supply chain attacks

**Asset value**: $100,000 (network encryption devices, key management appliances)

**Exposure factor:** assume that if a supply chain attack occurs, it could lead to an 80% exposure of encryption hardware.

**Single loss expectancy:** $800 000 \* 80/100 = $ 640 000

**Annual rate or Occurrence:** assume that supply chain attack incidents targeting encryption hardware occur twice a year. ARO = 2

**Annual loss expectancy:** $640 000 \*2 = $1,280,000

**Data Backup =>**

• **Backup servers:**

* Ransom-ware attacks

**Asset value**: $50,000

**Exposure factor:** assume that if a ransom-ware attack occurs, it could lead to a 70% exposure of Backup servers.

**Single loss expectancy:** $50 000\* 80/100 = $40 000

**Annual rate or Occurrence:** assume that ransom-ware attack incidents targeting backup servers occur four times a year. So ARO=4

**Annual loss expectancy:** $ 40000 \* 4 = $120 000

• **Backup Media:**

* data corruption

**Asset value**: $45,000

**Exposure factor:** assume that if data corruption occurs, it could lead to 50% exposure of Backup media.

**Single loss expectancy:** $45000\* 80/100 = $36 000

**Annual rate or Occurrence:** assume that data corruption incidents targeting Backup media occur three times a year.

**Annual loss expectancy:** $ 36 000 \* 3 = $108 000

**Disaster recovery plans focusing on threats**

**What is DRP?**

It’s a structured approach that outlines how an organization can recover and restore its critical business functions and IT infrastructure after a natural or man-made disaster.

The plan typically includes procedures work arrangements, and strategies for minimizing downtime and ensuring business continuity in the face of unexpected events.

**1. DDoS attack (distributed denial of service):**

When we detect a DDoS attack, we quickly bring together a team to with it, we start taking actions to stop the attack and make sure our online banking banking keeps working as much as possible.

**Fault tolerance and redundancy:**

Implement fault-tolerant architecture for critical systems, ensuring redundancy in network infrastructure, servers, and services to withstand DDoS attacks.

Utilize redundant internet connections and load balancers to distribute incoming traffic and mitigate the impact of DDoS attacks on the online banking platform.

**RAID 1 and RAID 5 for Hard Drive Protection:**

* Employ RAID 1 (mirroring) and RAID 5 (striping with distributed parity) configurations for hard drives in servers hosting critical banking applications and databases.
* RAID 1 ensures data redundancy by mirroring data across multiple drives, while RAID 5 provides both redundancy and performance benefits through distributed parity.

**Failover Cluster and Redundant Power Sources:**

* Deploy failover clusters for critical servers to automatically switch to backup servers in the event of hardware or software failures caused by DDoS attacks.
* Ensure redundant power sources, such as uninterruptible power supplies (UPS) and backup generators, to maintain server uptime and availability during power outages or disruptions caused by DDoS attacks.

**Alternate Processing Sites:**

* Establish alternate processing sites or data centers geographically separated from the primary site to ensure business continuity and service availability in the event of a DDoS attack or site-wide outage.
* Implement real-time data replication and failover mechanisms to facilitate seamless failover to alternate processing sites in case of a DDoS-related disruption.

**Backup and Offsite Storage:**

* Perform regular backups of critical data and systems using a combination of full, incremental, and differential backup strategies.
* Store backup data on secure storage media, including magnetic tape, and ensure offsite storage at geographically distant locations to protect against data loss due to DDoS attacks or other disasters.

**Incident Response and Recovery:**

* Conduct post-incident analysis and root cause investigation to identify vulnerabilities exploited during the DDoS attack.
* Implement remediation measures and security enhancements to strengthen the organization's resilience against future DDoS attacks.
* Update the DRP based on lessons learned from the incident to improve preparedness and response capabilities for mitigating DDoS threats in the future.

**Disaster Recovery Plan (DRP) for Ransom ware Attacks:**

* Activate the Incident Response Team (IRT) immediately upon detection of a ransom ware attack.
* Isolate infected systems to prevent further spread of ransom ware.
* Disconnect affected backup servers from the network to prevent encryption of backup data.
* Communicate with relevant stakeholders, including IT personnel and management, to provide updates on the situation and expected resolution timeframes.

**Data Backup and Recovery:**

* Ensure regular backups of critical data and systems using a combination of full, incremental, and differential backup strategies.
* Store backup data on secure storage media, including offsite locations and cloud-based storage services, to protect against ransom ware encryption and data loss.
* Implement robust authentication and access controls to prevent unauthorized access to backup systems and data.

**Network Segmentation and Access Controls:**

* Implement network segmentation to isolate critical systems and data from potentially compromised network segments.
* Enforce strict access controls and least privilege principles to limit access to sensitive systems and data, reducing the risk of ransom ware infiltration and lateral movement within the network.

**User Education and Security Awareness:**

* Provide regular cyber security training and awareness programs to educate employees about the risks of ransom ware attacks and best practices for identifying and reporting suspicious activities.
* Encourage employees to exercise caution when opening email attachments, downloading files, or clicking on links from unknown or suspicious sources to mitigate the risk of ransom ware infection.

**Incident Response and Recovery:**

* Conduct post-incident analysis and root cause investigation to identify vulnerabilities exploited during the ransom ware attack.
* Implement remediation measures and security enhancements to strengthen the organization's resilience against future ransom ware attacks.
* Update the DRP based on lessons learned from the incident to improve preparedness and response capabilities for mitigating ransom ware threats in the future.

**Disaster Recovery Plan (DRP) for Insider Threats:**

* Activate the Incident Response Team (IRT) immediately upon detection of an insider threat.
* Investigate the incident to determine the scope and extent of the insider's actions.
* Implement measures to contain and mitigate the impact of the insider threat, including revoking access privileges and securing compromised systems and data.

**Access Control and Privileged Account Management:**

* Implement robust access controls and least privilege principles to limit access to sensitive systems and data.
* Monitor and audit user activities, particularly those with privileged access, to detect and prevent unauthorized or suspicious behavior.
* Implement multi-factor authentication (MFA) and strong authentication mechanisms to verify the identity of users accessing critical systems and data.

**User Education and Awareness:**

* Provide regular training and awareness programs to educate employees about the risks of insider threats and the importance of safeguarding sensitive information.
* Encourage employees to report any suspicious activities or concerns to the appropriate authorities for investigation and remediation.

**Data Encryption and Key Management:**

* Implement strong encryption algorithms and key management systems to protect sensitive data from unauthorized access and disclosure.
* Ensure that encryption keys are securely stored and managed to prevent unauthorized use or compromise by insiders.
* Regularly review and update encryption policies and procedures to address emerging threats and vulnerabilities.

**Incident Response and Recovery:**

* Conduct thorough post-incident analysis and forensic investigation to identify the root causes and motives behind insider threats.
* Implement remediation measures and security enhancements to prevent similar incidents from occurring in the future.
* Update the DRP based on lessons learned from insider threat incidents to improve detection, response, and recovery capabilities.

**Conclusion:**

* Our comprehensive analysis of the critical objectives, processes, assets, and associated threats within our commercial bank has provided invaluable insights into our organization's risk landscape. Through diligent research and meticulous assessment, we have identified key vulnerabilities and quantified the potential impact of various threats on our operations.
* By prioritizing the protection of critical assets and processes, we aim to bolster the resilience of our bank against potential disruptions and ensure the continuity of essential services. Our commitment to proactive risk management strategies, informed by quantitative risk assessment, underscores our dedication to safeguarding the integrity, confidentiality, and availability of our resources.
* The development of a robust Disaster Recovery Plan (DRP) tailored to address critical threats serves as a cornerstone of our risk management framework. By implementing measures such as incident response protocols, access controls, encryption technologies, and employee training, we strengthen our ability to detect, respond to, and recover from adverse events.
* Looking forward, we recognize the importance of sustained vigilance and adaptability in the face of evolving threats and regulatory requirements. By fostering a culture of continual improvement and collaboration, we can effectively navigate emerging challenges and maintain the trust and confidence of our customers, stakeholders, and partners in our bank's resilience and preparedness.

**Reference list**

*Cisco Learning Network* n.d., learningnetwork.cisco.com, viewed 17 May 2024, <https://learningnetwork.cisco.com/s/article/ccna-security-risk-quantitative-assessment>.

CLOUDIAN n.d., *4 Disaster Recovery Plan Examples and 10 Essential Plan Items*, Cloudian.

*Commercial Bank of Ceylon PLC | Annual Report 2019* n.d., combank2019.annualreports.lk, viewed 17 May 2024, <https://combank2019.annualreports.lk/>.

*Commercial Bank of Ceylon PLC | Annual Report 2021* n.d., combank2021.annualreports.lk.

*Commercial Bank of Ceylon PLC | Annual Report 2022* n.d., combank2022.annualreports.lk.

*Commercial Bank of Ceylon PLC | Colombo* n.d., www.combank.lk.

*Commercial Bank of Ceylon PLC Annual Report 2023 |* n.d., combank2023.annualreports.lk.

*Cybersecurity Risk Assessment* n.d., www.itgovernance.asia.

*Cybersecurity Risk Assessment | IT Governance USA* 2016, Itgovernanceusa.com.

Imperva 2022, *Cyber Security Threats | Types & Sources | Imperva*, Learning Center.

Skillset 2016, *DRP - Disaster Recovery Plan Testing (CISSP Free by Skillset.com)*, YouTube, viewed 17 May 2024, <https://www.youtube.com/watch?v=lLbK5Twv6GM>.

Tunggal, AT 2022, *What is a Cyber Threat?*, www.upguard.com.

ULFinance 2020, *Quantitative Risk Management - Lecture 1*, YouTube, viewed 17 May 2024, <https://www.youtube.com/watch?v=KUdZFqY4sxs&list=PL4i4aZbplv9KLOA0T4Vw\_6PW\_eYEYGSXR>.

*What is a Disaster Recovery Plan? Definition and Related FAQs | Druva* n.d., www.druva.com.