SMALL REGINOAL BANK RISK MANAMGEMNT PLAN

CYS 310, 2023

Prepared by

Jaydon King and Dillon Beckerich

Prepared for

Dr. Ankur Chattopadhyay

PART 1: RISK MANAGEMENT PLAN OUTLINE

Introduction. 3

Outline 3

Scope 4

Laws 4

Key Roles and Departments. 5

Timeline 5

PART 2: RISK ASSESMENT

Introduction. 6

Scope and Boundaries. 6

Data Center Assets 6

Activities. 6

Relevant Threats and Vulnerabilities. 7

Controls for threats. 8

Key Roles and Responsibilities 8

Timeline 9

PART 3: RISK MITIGATION PLAN

Introduction 10

Threats and Countermeasures 10

Cost Benefit Analysis 12

PART 4: BIA & BCP

Introduction 15

Business Impact Analysis 15

Business Continuity Plan 17

Part 1: Risk Management Plan

Introduction:

Companies like financial institutions that hold sensitive information of customers and hold information relating to money require very high security to ensure confidentiality, integrity, and availability. The purpose of this risk management plan is to assess all the security of devices used by employees or accessed by customers that contain any customer data. This is both physical and technical security as they are both important for a bank like this. Our bank consists of 3 buildings, a headquarters and two branches not too far from the headquarters. The main goal is to protect. We are focusing on the protection of both customer and employee data, the bank's and customer's money, and to ensure physical security of our locations including servers and automated teller machines (ATMs).

These points are key, as if customer information were leaked or misused our stakeholders such as our customers and the public would lose confidence in our bank. Our reputation would be tarnished, resulting in lost profits, current customers leaving, potential new customers being lost, and losing potential future opportunities. Seeing as we are a smaller bank in a smaller area, a risk such as theft of deposited would cause economic loss to our customer as well. In a worst-case scenario, if the area was small and rural enough with a lack of other banks, it could cause economic failure in the general area.

Outline:

1. **Assessment**:
   - Identify the scope of the plan.
   - Identify assets that need protection, including customer and employee data, the banks and customer's money, and physical locations including servers and ATMs.
   - Understand the potential risks and threats to these assets and their consequences. This could include data breaches, damage to reputation, financial losses, physical theft, or natural disasters.
   - Identify the key roles and departments responsible for risk management

2. **Risk Analysis**:
   - Assess both physical and digital security risks associated with customer data, assets, and location security.
   - Evaluate the likelihood and impact of identified risks.
   - Categorize each risk as high, medium, or low.
   - Prioritize risks based on their potential impact on the bank and its stakeholders and likelihood of its occurrence.

3. **Plan Creation**:
   - Develop a comprehensive risk management plan that addresses identified risks
   - Develop strategies to mitigate, transfer, accept or avoid the identified risks.

- Assign responsibilities to people and departments:
- IT Managers: Responsible for patch management, network security, and employee security training.
- Compliance Officer: Ensure compliance with relevant laws and guidelines.
- Bank Managers and Head of Bank: Conduct cost-benefit analysis and determine acceptable risk levels.
- Physical Security Specialist: Audit physical security measures at bank branches and headquarters.
- Security Department: Implement and maintain security best practices.
- Establish risk mitigation strategies for each identified risk.

4. **Plan Implementation**:
    - Implement the risk mitigation strategies developed in the plan creation step.
    - Ensure IT managers carry out proper patch management and network security.
    - Develop security training for employees.
    - Monitor compliance with applicable laws and guidelines.
    - Implement physical security enhancements based on the specialist's audit findings.
    - Continuously maintain and update security measures.

5. **Continuous Monitoring**:
    - Regularly review and update the risk management plan to ensure it remains effective.
    - Continuously monitor and assess the effectiveness of the implemented controls.
    - Regularly review and update the plan as new threats and vulnerabilities may emerge.
    - Conduct periodic security assessments and audits, for both physical and digital, to identify any gaps or needs for improvement.
    - Stay informed about changes in applicable laws and regulations through the Compliance Officer.

6. **Assessment**:
    - Reassess the effectiveness of the risk management plan.
    - Reevaluate the potential consequences of risks and what risk level is considered "acceptable"
    - Engage in cost-benefit analysis and review authorized decisions.
    - Make necessary adjustments based on the findings of the continuous monitoring phase.
    - Return to previous steps as needed.

Scope:

Balancing accessibility of funds for customers while also ensuring security of their data. Ensuring compliance with GLBA. Security, confidentiality, integrity, and availability of user data and access to their account. Ensuring security of the devices used by the company. Possibly use fractional reserve banking if not already implemented.

Laws:

GLBA:

- Notify customers on how their account data is being protected.
- Inform customers how their data is collected and how the company shares their data with the other branches.
- Ensure employees are trained in security of data and different security issues.
- Ensure authorization from customer to release information if needed.
- Ensure no unwanted changes are made to customers' data.

Key roles and Departments:

- IT managers:
  - Ensure proper patch management is implemented.
  - Ensure proper network security is also in place.
  - Proper security training completed by all employees of the bank.
- Compliance Officer:
  - Making sure the bank complies with applicable guidelines and laws.
  - Updates the bank on new laws that may come into effect.
  - Update bank on changes that need to be made to comply with different laws.
- Bank Managers and Head of Bank:
  - Cost-benefit analysis
  - Determine what risk is acceptable.
  - Finalize all the decisions made in terms of risk management.
- Physical Security Specialist:
  - Perform an audit of physical security of bank branches and headquarters.
- Security Department:
  - Ensuring proper security is upkept.
  - Ensure security best practices are being followed.

Timeline:

Week 1 (10/2-10/8)	Assessment/ Audit
Week 2(10/9-10/15)	Identify Risks
Week 3(10/16-10/22)	Mitigation Review
Week 4(10/23-10/29)	Cost-Benefit Analysis
Week 5(10/30-11/5)	Recommendations and final thoughts

Part 2: Risk Assessment Plan

Introduction:

Any financial institution should perform a risk assessment on a schedule to ensure that controls that were implemented are working accordingly. It is also to assess the bank's software, hardware, and practices in the company to ensure that there is proper security throughout and to handle any risks that may appear. The purpose of our risk assessment is to assess all controls and risks and mitigate them to the approved risk level. This will be done in a manner of prioritizing risks with higher likelihood and higher impact level on assets of the company as they can be the cause of loss for the institution.

Our bank is looking for risks that can target any personal information of employees and customers, such as SSID numbers, insurance information, bank account information, addresses, etc. With this, we would also be ensuring that compliance with the GLBA and other laws are being kept. We would also ensure proper physical security to prevent theft of any devices at the locations as well as securing the server room and the ATMs as this is where key assets are kept.

Scope and Boundaries:

The scope of our assessment is to assess all the company devices that have access to any personal information of both employees and customers and ensure proper security is being maintained on them. We are also looking at the software on these devices as well. Physical security is also key to this plan so we can ensure that offices and server rooms are kept secure to prevent theft of devices or unwanted access to the server room. Making sure the ATM lock is secure to prevent a thief stealing the ATM or someone from putting a credit card skimmer in the ATM. We also need to review the GLBA and any other compliance laws that apply to us to make sure things are in order. We will also check the network between the different branches and the headquarters to ensure a man in the middle attack cannot take place and to ensure the traffic of the network is filtered and secured.

Data Center Assets:

1. Customer Personal Identifiable Information: Social security numbers, phone numbers, answers to security questions, account information, financial records.
2. Employee Data: Social security numbers, phone numbers, addresses, insurance information, health records.
3. Hardware: servers, desktops, laptops, switches, firewalls, tablets, mobile phones.
4. Software: Operating systems, applications, possibly curated applications, files.

Activities:

1. Patch management
2. Human Error
3. Hardware Maintenance
4. Access Control

5. Trainings
6. Theft/Damages

Relevant Threats and Vulnerabilities:

1. Threat: Possibility of exploitation of Operating system or software in ATMs
    a. Vulnerability: Older software or operating system
2. Threat: Possibility of someone breaking into ATM
    a. Vulnerability: Locks on ATMs can be picked.
3. Threat: Possibility of someone stealing equipment
    a. Vulnerability: Poor physical security
4. Threat: Loss of company data due to social engineering
    a. Vulnerability: Lack of training for social engineering attacks
5. Threat: Loss of company data due to external threat through network
    a. Vulnerability: Misconfigured firewall
6. Threat: Robbery of one of the banks
    a. Vulnerability: Humans being threatened.

Threat-Probability Matrix

Threats and Vulnerabilities	**Probability**	**Impact Level**	**Importance Rank (1 Least important – 10 Most important)**
Possibility of exploitation of Operating system or software in ATMs due to older software operating system	20%	High	6
Possibility of someone breaking into ATM due to picking the locks of an ATM	40%	High	8
Possibility of someone stealing equipment due to poor physical security	10%	Moderate	4
Loss of company data due to social engineering due to lack of training	60%	High	9
Loss of company data due to external threat	15%	Critical	10

through network due to misconfigured firewall			
Robbery of one of the banks due to humans being threatened	5%	High	3

Controls for Threats:

1. Newer software and operating systems for ATMs to mitigate the risk of hacking.
2. More complex or obscure locks hinder a lockpicking attack.
3. Stronger doors and secure locks for server room and offices.
4. Implement security and anti-social engineering training into employee training.
5. Configure firewall to lock down any ports not being used and to implement firewall rules.
6. Silent alarm system and bullet proof glass for tellers.

Key roles and responsibilities:

IT Managers:

- Help create the training program that fits within the risk assessment
- Authorization of IT changes for security purposes
- Assisting in networking and implementation of firewall rules.
- Implementing complex password rule for user accounts

Compliance Officer:

- Ensure training is compliant with current laws and regulations
- Ensure that controls are compliant with laws and guidelines

Bank Managers and Head of Bank:

- Authorization of controls discussed in the plan
- Allocation of resources for implementing mitigations for risks listed in the assess plan

Physical Security Specialist:

- Ensure proper security of physical access to server room and offices
- Ensure proper security of any entrance
- Ensure proper surveillance of server room, lobbies, and hallways
- Ensuring the physical security of the ATM

Security Department:

- Testing controls before being implemented in the network
- Monitoring system logs and past network activities.

Timeline

Week 1 (10/2-10/8)	Assessment/ Audit
Week 2(10/9-10/15)	Identify Risks
Week 3(10/16-10/22)	Mitigation Review
Week 4(10/23-10/29)	Cost-Benefit Analysis
Week 5(10/30-11/5)	Recommendations and final thoughts

Part 3: Risk Mitigation Plan

Introduction:

This part of the plan is to take the previously mentioned risks and find controls and solutions that will mitigate them. The purpose of this is not to remove the risk completely, but rather to plan to mitigate them to an acceptable level. The previously listed risks from the last section are:

- Loss of equipment
- Misconfigured firewall
- Social engineering attack
- Older software or operating systems in ATM
- Attacker breaking into ATM
- Bank being robbed

The risks listed have threats associated with them that can cause a multitude of damage and loss to the company if exploited. The best approach to handling and dealing with these threats is to prioritize those that have a higher impact on the company's assets and have a high likelihood of occurring. The threats listed in order of prioritization are:

- Loss of company data due to stolen equipment
- Loss of company data due to misconfigured firewall
- Loss of company data due to social engineering attack
- Regulation or Compliance changes
- Loss of Operations due to older software or operating system on ATM
- Loss of Profit due to money stolen from ATM
- Loss of Profit due to bank robbery

The assets that our company uses to function are split into three categories: hardware, software, and personnel assets. The assets we found for our business are:

Hardware:

- Workstations
- Firewalls
- Routers
- Switches
- ATMs

Software:

- ATM Operating system
- ATM software

Data/info:

- Compliance
- Customer information
- Employee information

Threats and Countermeasures:

Loss of company data due to stolen equipment:

The threat that should be handled first is the loss of company data due to stolen equipment as the data stored on these is confidential and could affect the business operations. The first control recommended is to implement the use of Kensington locks to lock the equipment to the desks. This would help ensure that the equipment could only be moved by those authorized in the company to do so. Another control is to ensure offices or rooms with equipment with sensitive data on them are locked with doors using some sort of advanced lock like biometrics, card reader, number pad, etc. The ability to lock accounts on computers in the case of equipment being stolen can also help in mitigating this threat as well.

Loss of company data due to misconfigured firewall:

The second threat to mitigate is misconfigured firewalls at the headquarters of the company. The best control for this threat would be to implement a standardized firewall application to help enhance the firewall. Another control that would help with mitigation would be to configure the rulesets of the firewall to better protect the network from any suspicious traffic coming in and out of the router.

Loss of company data due to social engineering attack:

The next threat to mitigate is the loss of company data due to social engineering. This can occur at any of the branches and the headquarters. The best control for this attack would be to ensure that proper training of employees is occurring that covers social engineering attacks and what to do in these situations. Another control would be to ensure there are cameras in proper areas such as the server room, work area where tellers are, and any other areas an attacker might target. Testing employees against a phishing attack would also be beneficial as if any employees fail the test, then proper instructional action should take place. If in any case, an employee fails the phishing test more than once, then proper disciplinary action should take place.

Regulation or compliance changes:

Every company must make sure that they follow any rules and regulations that apply to their industry. These can vary from industry to industry. The key control would be to hire a regulation officer to ensure that we are compliant with all regulations, mainly the GLBA.

Loss of operations due to older software or operating system on ATM:

Most of all ATMs in use run an older operating system or software that is outdated. This means there are most likely vulnerabilities that are associated with these operating systems and software. The main control for this would be to upgrade to the newer version of the operating system if the software is able to. Another control would be to test a different software in a sandbox on the operating system running in the ATM and see if it would mitigate the vulnerabilities before implementing the control. Another control would be to use a Linux operating system and configure an application for the bank's ATMs. This control is only if there is someone who would be able to program the application.

Loss of Profit due to money stolen from ATM:

ATMs are very prone to being broken into as there is money inside that thieves will try and steal, which can lead to a loss of profit. A control for this would be to improve the physical security of the ATM itself. An example would be to use a digital keypad to unlock the ATM, which would mitigate lockpicking and simply breaking into the ATM. Another control would be to ensure the ATM is properly secured to the ground or locked in place so that no one can steal the ATM itself.

Loss of Profit due to Bank Robbery:

Bank robberies can occur at any time in this day and age, which can result in a loss of profit as well. To mitigate this, the control to use would be to come up with a contingency plan. This plan would include what actions to take in the instance of a robber being present. Another control would be to improve the physical security of the bank as well. Hiring a guard is a good example of this, as well as ensuring there is a silent alarm to notify authorities in reach of any of the tellers.

Cost Benefit Analysis:

Purpose:

The Cost Benefit Analysis is used to give an idea as to how beneficial the mitigation or counter measure will be if implemented. It is essentially a way for the business to evaluate whether or not it Is profitable to implement the abovementioned countermeasures. It uses the loss before and after implementation of a countermeasure to estimate the projected benefits in the equation:

Loss Before Countermeasure – Loss After Countermeasure = Projected Benefits

The next value is the value the countermeasure value after benefits, which uses the following equation:

Projected Benefits – Cost of Countermeasure = Countermeasure Value

Below is a CBA for each of the suggested controls listed above.

1. Kensington Locks (Countermeasure type: NIST 800-53 PE-3):
   - Loss Before Countermeasure: $100,000
   - Loss After Countermeasure: $50, 000
   - Projected Benefits: $50, 000
   - Cost of Countermeasure: $1,500
   - Countermeasure Value: $48,500

2. Advanced Locks for doors (Countermeasure type: NIST 800-53 PE-3):
   - Loss Before Countermeasure: $100,000
   - Loss After Countermeasure: $50,000
   - Projected Benefits: $50,000
   - Cost of Countermeasure: $15,000
   - Countermeasure Value: $35,000

3. Configuring Firewall (Countermeasure type: NIST 800-53 AC-4):
   - Loss Before Countermeasure: $75,000
   - Loss After Countermeasure: $25,000
   - Projected Benefits: $50,000
   - Cost of Countermeasure: $5,000

- Countermeasure Value: $45,000

4. Social Engineering Training (Countermeasure type: NIST 800-53 AT-2):
   - Loss before Countermeasure: $125,000
   - Loss After Countermeasure: $50,000
   - Projected Benefits: $75,000
   - Cost of Countermeasure: $15,000
   - Countermeasure Value: $60,000

5. Camera System (Countermeasure type: NIST 800-53 PE-6):
   - Loss Before Countermeasure: $125,000
   - Loss After Countermeasure: $40,000
   - Projected Benefits: $85,000
   - Cost of Countermeasure: $25,000
   - Countermeasure Value: $60,000

6. Complying with Standards (Countermeasure type: Procedural; NIST 800-53 CA-2):
   - Loss Before Countermeasure: $150,000
   - Loss After Countermeasure: $50, 000
   - Projected Benefits: $100,000
   - Cost of Countermeasure: $50,000
   - Countermeasure Value: $50,000

7. Upgraded ATM Software (Countermeasure type: NIST 800-53 SI-2):
   - Loss Before Countermeasure: $50,000
   - Loss After Countermeasure: $20,000
   - Projected Benefits: $30,000
   - Cost of Countermeasure: $10,000
   - Countermeasure Value: $20,000

8. Advanced Locks for ATMs (Countermeasure type: NIST 800-53 PE-3):
   - Loss Before Countermeasure: $80,000
   - Loss After Countermeasure: $50,000
   - Projected Benefits: $30,000
   - Cost of Countermeasure: $10,000
   - Countermeasure Value: $20,000

9. Physical Security Guards (Countermeasure type: NIST 800-53 PE-3):
    - Loss Before Countermeasure: $90,000
    - Loss After Countermeasure: $30,000
    - Projected Benefits: $60,000
    - Cost of Countermeasure: $30,000
    - Countermeasure Value: $30,000

Part 4: Business Impact Analysis and Business Continuity Plan

Introduction:

The Purpose of the Business Impact Analysis is to evaluate possible impacts disasters and interruptions may have on our company. The analysis takes into consideration the business functions and processes that are required for the business to function properly. The Business Continuity Plan is meant to act as a planned reaction to different possible incidents and disasters that could happen. Impacts and disasters are ones that can most commonly occur with the location of the business as well as possible scenarios like robberies and fires that can occur anywhere.

Business Impact Analysis:

This part of the BIA lists the Critical Business Functions (CBFs). These are functions or processes that are needed for the company to be able to work and be able to make a profit. The critical business functions we found for our company are:

- Employees accessing servers
- Network traffic through routers
- Switches connecting devices
- Firewalls filtering traffic
- ATM application usage

Critical Resources:

The BIA also lists the Critical Resources that are used in the business for the Critical Business Functions and processes. These resources are used by employees and customers in the workplace and are what keep the business going. The critical business resources for our business are:

- **Internet**
- **Backups**
- **Internal network connection**
- **Workstations**

Maximum Acceptable Outage and Impact:

The next part of the BIA is determining the Maximum Acceptable Outage and the Impact of the functions listed above. The MAO is the maximum amount of time that the function can be down where the total loss is acceptable for the business. The MAOs for the above Critical Business Functions are listed in the table below:

Maximum Acceptable Outage and Impact

CBFs	MAO	Impact Level (Low, Medium, High)
Employees accessing servers	2 Hours	High
Network traffic through routers	4 Hours	High
Switches connecting devices	4 Hours	High
Firewalls filtering traffic	6 Hours	Medium
ATM application usage	10 Hours	Low

The table also lists the impact level of the function, which is the importance of the function for the business. The functions with the higher impact level should be prioritized first since they are the most important for the business to function. All of the functions are critical for the business, but the higher impact ones should be recovered first.

Recovery Point Objective:

The RPO is the amount of data loss the company is willing to accept before there is substantial loss or damage to the company. This is mainly focused on how far the company is willing to revert back to for the functions if that is necessary. This is usually used to help decide how often to back up systems and servers and how to pick which backup to pick if backing up is necessary.

Recovery Point Objectives for CBFs

CBFs	RPO
Employees accessing servers	6 Hours
Network traffic through routers	24 Hours
Switches connecting devices	24 Hours
Firewalls filtering traffic	12 Hours
ATM application usage	8 Hours

The table lists the amount of time that the company is willing to revert back to in the case of something going wrong that would result in a determined acceptable data loss. This is prioritized based on the functions that contain key data as well as processes that are key to the business that need to be working first.

Recovery Time Objective:

The Recovery Time Objective is the set time that the recovery team must aim to recover the resources and functions of the resources. These times are based on how long the business can go without these resources before functions are impacted by the outages. The RTO for the resources of our business listed above are:

Recovery Time Objective

Resources/Functions	Recovery Time Objective (RTO)

Internet	6 Hours
Server	2 Hours
Routers and Switches	4 Hours
Workstations	1 Hour
Firewalls	8 Hours
ATM	12 Hours

Business Continuity Plan:

Purpose:

The purposed of this Business Continuity Plan is to help employees of the business know what to do in the event that an incident occurs. Below there are three main incidents that we felt affected the business the most and how they should be handled. Other incidents would have a similar plan and would be activate by the Business Continuity Plan officer.

Incidents:

- Business goes through power outage
- Business catches on fire
- Business is robbed.

Strategies:

In the case of the business losing power:

1. Ensure all employees save any data to the server from workstations before UPS runs out of power after 15 minutes.
2. IT manager ensures breaker is switched on to ensure it is not internal power outage.
3. Power company is contacted to report outage and acquire time frame.
4. Ensure building is locked and closed signs are up and signs directing customers to other locations.
5. If power is not on within two hours, then employees are to leave for the day.

In the case of the business catching on fire:

1. Ensure employees are evacuated following the fire exits.
2. Contact local fire department and proper emergency services.
3. Wait for fire department to arrive.
4. Depending on severity of fire, employees may work at other locations until their location is recovered.

In the case of the business being robbed:

1. Press silent alarm under tellers desk to alert authorities.
2. Employee complying with robber and giving money if asked to prevent any liabilities
3. Police would arrive and recover any physical evidence left at scene
4. Manager will go over video footage and provide footage to police.
5. Business will return to normal after police have finished investigating scene

Notifications/Activation: The BCP coordinator is alerted of any disruption or impact to any function covered in the strategies.

Recovery Phase: This is when strategies for the recovery of business due to a disaster or disruption starts, following the specified strategy listed in the BCP.

Reconstruction phase: This is when business can start working and functioning like normal. Proper relocation or accommodation may occur according to BCP for incident.

Testing and Training: Phase where BCP is tested and revised to ensure it works as accordingly. This phase can include:

Training employees about the BCP and its procedures.

Testing to ensure the BCP will work as planned in the scenarios.

Exercises to show how the BCP will work. This can include fake scenarios to ensure employees follow BCP to ensure quick recovery.

BCP need to be updated as things change, which can lead to retraining and retesting employees.

Works Cited

Darril Gibson and Andy Igonor. 2022. *Managing risk in information systems*, Burlington, MA: Jones et Bartlett Learning.

Joint Task Force. 2020. Security and Privacy Controls for Information Systems and organizations. (December 2020). Retrieved December 13, 2023 from https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final