George Washington University

Dr. White  
Incident Response PSCS 2304

**Incident Response Plan Project**

Written by:

Minhal Aamer   
Ahsan Ahmed  
Gertrude Bossmart  
Kanghee Kim  
Luis Ruis  
Victoria Adeniji

Due Date: April 10, 2021

# 

# **Table of Contents**

Organizations Assets (Ahsan).............................................................................3

Organizations Critical Functions (Luis) ……………………………………………...4

Maximum Tolerable Downtime (Minhal)...............................................................5

Recovery Point Objective (Kanghee)......................................................................6-7

Recovery Time Objective (Victoria)....................................................................7-8

Incident Response Management (Kanghee)…………… ………………………….8-10

Incident Response Key Personnel (Minhal)...........................................................10-11

Preparation (Kanghee)..........................................................................................11-14

Detection, Analysis, Identification (Luis).................................................................14-24

Containment (Ahsan)...............................................................................................24-28

Eradication, Recovery, Post-Incident Recovery (Trudy)............................................28-34

Disaster Recovery Plan (Victoria)............................................................................34-38

Business Continuity Plan (Minhal).............................................................................38-43

# **Organizations Assets and Functions**

Our bank is known as Rainy Days Bank and would best be described as a commercial bank and primarily serves as a financial institution that offers services in the northeastern region of the United States. Maintaining a strong and healthy relationship with our community is essential for a bank of our size so we need to make sure that our customer’s data is as secure as possible. However, we are also planning on branching out to more states so that needs to be kept in mind in the development process.

Our main office branch is in McLean, Virginia and we have 92 Branch office locations spanning from Northern Virginia to Washington D.C, Maryland, Delaware, Pennsylvania, New Jersey, and Connecticut with 1400 employees. Our revenue: We hit $320 million dollars in revenue in 2020 with a net income of $110 million and total assets of $5.6 billion.

Our bank offers financial services and handles financial matters, revolving physical money and credit. Our clients range from individuals to commercial companies, real estate companies, etc. Some of the main data that our bank deals with are those clients’ PI data which includes names, account numbers, money in their accounts, SSN, user credentials, home address, etc. This data is extremely sensitive and must be protected in order to maintain trust with our clients and in order to keep our business running. This incident response plan will help to ensure that Rainy Days Bank is prepared to deal with incidents in order to protect its data and assets.

Rainy Days Bank’s assets include the financial monetary value we receive, and handle known as our reserves. It includes the money in our vaults and credit in our systems that can include loans, investments and bonds we have established with our clients. Our assets can also include property such as real estate and automobiles that have come into our ownership due to loan defaults. All of these assets are essential to our business and the data and record of these assets must be protected in order to continue our business operations.

**Organizations Critical Functions:**

Lending is mission critical to our bank as it is how we generate profit; we need to make sure that our customers feel safe and accept us as their lending provider. When someone applies for a loan, they need to give identification, their employer and income, and their address which we must prevent from being leaked. This data leak could make our customers at high risk for identity theft and fraud. It would also make Rainy Days Bank vulnerable to fines, penalties and lawsuits creating monetary and reputational damage.

Rainy days also needs people to open and maintain checking accounts so, there needs to be additional security to ensure that their checking account information cannot be accessed by bad actors. Customers must have their money and assets available even if the bank is experiencing a breach. There also needs to be countermeasures to identify which accounts have been breached and how we can prevent further breaches. When a customer gets their checking account information breached there needs to be policies in place to prevent further theft while ensuring that they can pay their bills or purchase commodities. If their account has to be suspended for a long duration of time to be reviewed then the bank must also due their utmost make funds readily available during that period of time.

Rainy Days must make sure that our vaults are secure and cannot be accessed by external or unauthorized internal threats. There must be policies in place that identify who is authorized to access the banks financial assets (Money reserves) and how are they able they can access them. The policies in place must also ensure proper training and protocols for accessing our money storage. Those policies should also primarily include in-house safety measures such as staff accounts and passwords.

# **Maximum Tolerable Downtime (MTD)**

The company’s maximum tolerable downtime (MTD) is the span of time that the system can remain down without severe consequences. The MTD is dependent on a number of factors including the company’s assets and scope, the threat, the criticality of the functions being affected, and the downtime. If the MTD is exceeded, in that the business remains unable to conduct vital functions, the effect can be catastrophic to the business. Therefore, the time it takes for the business to recover and resume operations must be lower than the MTD, that includes the recovery time objective and the work recovery time.

Rainy Days Bank must ensure that the controls and IT infrastructure that will be set up ensure that operations will come back up before the estimated MTD of 2 hours. Due to the business’s handling of important client data and finances, and the scope of the business spanning 92 branches over the northeastern coast, this is the recommended maximum tolerable downtime before the business will be met with disastrous consequences in terms of future business. The criticality of Rainy Days Bank’s functions and operations is why the MTD is a shorter amount of time and because of this short MTD, it will be more costly to prepare for.   
  
 A short MTD, therefore a short RTO and WRT means that the cost to implement quick and efficient solutions will be higher. This is because the design for these solutions are usually more expensive and require more maintenance, such as alternate sites, backups and redundancy efforts. At the same time, a short MTD means that the business is highly critical and will experience costs and losses the longer it remains down. Outlining the costs of the results of Rainy Days Bank’s business going down and the solutions that may be implemented to bring the system back up will create a clear comparison that will allow the business to see what solutions will be most cost-effective and result in the least damage to the business.

# **Recovery Point Objective (RPO)**

In today's computer-centric economy, businesses must respond to the risks of hardware and software malfunctions, equipment failures, data loss and costly downtime associated with terrorist acts and natural disasters. As part of any business impact analysis, Rainy Days Bank management must set specific goals for disaster recovery, including recovery point objectives (RPOs). The recovery point goal is a retroactive period in which data can be restored after a disaster, allowing the Rainy Days Bank to continue its normal operation. In other words, RPO will represent the acceptable amount of data loss over an acceptable amount of time that the company can tolerate. Rainy Days Bank recovery point objectives determine how often critical business data is backed up and the skills involved in the process.

When considering the Rainy Days Bank RPO, first, we make a list of all the systems and applications our business uses to successfully complete its work. Then we clarify the functions we perform and how our loss may affect our users. Also, we calculate the potential financial losses, including lost sales or lost salaries owed to idle workers. We do this for each application. In addition, different times of the year must be considered, as they all produce results of varying degrees. After calculating these possible situations, we then decide how long we can keep functioning before these losses become unmanageable.

If Rainy Days Bank backs up information or data to the cloud or offsite backup every hour, RPO is lower than a backup once a day. The more teams read an hour without working all day, the less potential damage it has. If the Rainy Days Bank team can afford to read five hours of data without affecting the bank's customers, RPOs can do five hours. However, five hours of data is a major disruption to bank data.

A shorter recovery time for Rainy Days Bank RPO is a significant cost increase. However, if Rainy Days Bank spends longer recovery times, it loses too much data than expected. There is an efficient way to write RPO. It's planning from important applications step-by-step. For example, we will use a three-tier model to design a business continuity plan.

1 Tier 1: Mission-critical applications requiring less than 15 minutes of RTPO

2 Tier 2: Business-critical applications requiring 2 hours of RTO and 4 hours of RPO

3 Layer 3: Non-core applications requiring 4 hours of RTO and 24 hours of RPO

Importantly, mission-critical, business-critical, and non-core applications vary by industry, and Rainy Days Bank must define these layers based on its operations and requirements.

# **Recovery Time Objective (RTO)**

The Rainy Days Bank Recovery Time Objective (RTO) is measured in specific set time intervals or number of hours relating to the loss of data and service time. This could help eliminate or reduce data leak which will help protect our customers data and avoid high risk for identity theft and fraud.

The Recovery Time Objective (RTO) is the target time for how quickly you need to recover a function or resource or the amount of time you need to bring a system back online

At Rainy Days Bank, our goal is to get technical problems resolved. The ability or downtime to fulfill the Recovery Time Objective RTO depends on the severity of the disaster. An objective of one hour is attainable for a server crash while for a low or medium crash an objective of 30 minutes or less is attainable. However, it might not be realistic to expect a one-hour solution in case of a natural disaster in the area.

RTO includes more than just the amount of time needed to recover from a disaster. At Rainy Days Bank, we are knowledgeable enough that Recovery Time Objective RTO also includes steps to mitigate or recover from different disasters which need to contain proper testing for the measures.

The Rainy Days Bank Recovery Time Objective will help maximize the amount of time that a system resource can remain unavailable before there is an unacceptable impact on the list of system resources, supported projects or business processes, and the Maximum Tolerable Downtime (MTD). The Rainy Days Bank will utilize this time to help recover IT systems from disaster onset to resumption of businesses processes. Depending on the information system resource Recovery Time Objective (RTO) is important for selecting appropriate technologies that are best suited for meeting the Maximum Tolerable Downtime (MTD) in our bank. The goal Rainy Days Bank will attain in the Recovery Time Objective (RTO) is to calculate how quickly we need to recover and then to map out the people, processes, and budget allotment that will be needed towards business continuity. Also, it will influence the type of redundancy and backup infrastructure our bank will need to have in place. Besides time and money, Rainy Days Bank will need to consider compliance and trust reputation with the customers.

Support terms the Rainy Days Bank will effectively utilize include:

* **Availability:** This is the hours both the Rainy Days Bank staff and customers can call for support.
* **Response time:** This is how quickly the Rainy Days Bank team will contact its customers after a support request.
* **Resolution time:** This is how quickly the Rainy Days Bank team will restore the services.

**Incident Response Management**

From a security team perspective, there needs to be understanding that not all security breaches will prevented, it is inevitable that some will occur. It is important to note that with sufficient time and resources, even the most secure systems or networks can be invaded. A systematic incident response plan will not only minimize the damage caused by security breaches but will also help reduce the negative image of banks. The Incident Response Management team oversees preventing cybersecurity incidents, analyzing the cause, damage, and scale quickly in the event of an accident, and finally minimizing the damage. By analyzing and taking measures to control the entire situation from the intrusion to the mitigation, the IR plan and process can be more effectively executed.

Security incidents are events such as access, alteration, and leakage of unauthorized information assets that affect the organization's operations, unlike simple incidents that are limited to individuals who have no ripple effect on the organization or work.

Nevertheless, systematic preparation and response to security incidents are rare, and this lack of preparedness leads to greater disasters. It is proposed that the system be followed for incident response. The bank's security incident response team should be organized in advance. The security incident response team must include executive levels of IT and security professionals as well as PR, HR, and legal professionals. The management personnel will be an important factor in the security team and will be essential to completion of tasks in the IR process.

For example, management personnel will facilitate communication between members. In case the security accident paralyzes the communication infrastructure, such as the in-house LAN, management will have a plan in place for members to communicate with each other without relying on the internal communication infrastructure, such as remote connections, alternate sites, etc. In the event of an accident, the emergency communication method and responsible personnel will be set, and the internal members should be able to communicate to stop the spread of the accident quickly. Management will also be responsible for the actions to take after the incident. In the event of a hacking or other cybersecurity incident, the company's security managers will decide on an approach depending on the technique and complexity of the attack. Management will have approved specific responses to specific attacks and have already assigned duties and responsibilities for their team to execute when an incident occurs. Management will also be responsible for planning for problem/failure recovery and repair methods, as well as actual recovery tasks and subsequent reviews. When developing a recovery/repair plan, attention will be paid to the target achievement rate and carefully evaluate whether the process setup is unrealistic or difficult to implement. This will be management's decision to approve or edit mitigations, controls, and recovery tasks.

# 

# **Incident Response Key Personnel**

To develop and execute an Incident Response Plan, Rainy Days Bank will be required to develop a team of personnel that will be responsible for this project, aside from the management roles. This will include carrying out operations, outlining policies, and developing plans. Since this business has a large scope with different business functions, personnel from different departments may be required to ensure that all aspects of the business are taken into account and the IRP is well-rounded.

Aside from department heads or managers that should be involved in the process, Rainy Days Bank should also have representatives from different departments give input on how their department is run and other important information such as critical functions and devices they use. This will allow insight into the areas that will need to be focused on more when developing and executing the IRP. Representatives from the finance department and HR will also be needed. This is because there needs to be discussion about the costs when implementing solutions and analyzing the risks and loss the business is planning for. Costs may need to be adjusted as the IRP is developed, therefore a financial expert should always be present, as well as management who can approve budget changes. A representative from HR or the legal department will also be essential to discuss compliance laws, policies, fees, etc. When incidents occur, Rainy Days Bank will need to be prepared for legal fees and compliance issues because of the sensitive data and financial matters being handled. Between clients and government laws and policies, it will be important to have legal experts for important input on the matter.

There should also be key personnel assigned to different aspects of the IRP. Since the scope of Rainy Days Bank is large, to properly plan and execute the IRP different teams should be assigned to different sections of the IRP. Aside from the already established CSIRT who execute incident response actions, there will also be need for disaster recovery experts. This team will plan and execute the disaster recovery plan by identifying and planning for disasters and helping the business return to normal operations. There will also be a business continuity response team, responsible for planning and executing the business continuity plan which will include attempts to continue business operations after incidents. A crisis management team will also be important when it comes to developing and executing the IRP. A crisis management team will deal with a number of issues when in a crisis such as mitigating the loss of data, costs and life, ensuring personnel are unaffected and accounted for, and notification to high level executives and managers of the incident. All of these teams will be key personnel when dealing with Rainy Days Bank’s incident response plan.

# **Preparation**

We are constantly exposed to security accidents. Recently, as security incidents have become an issue through the media, a lot of attention has been paid to the importance of security. The rapid development of the Internet has led to the widespread use of high-speed Internet, and new network infrastructure and technology, with domestic and foreign security incidents becoming increasingly intelligent, diversified, and popular. In the face of the increasing threat of new infringement, effective and rapid measures, and procedures for responding to security accidents are required along with the security operation of the bank network. In the field of security management and operations, any electronic infringement that could affect the bank's information assets and the resulting damage are considered security incidents. Incident response means responding to an incident response quickly in the event of a security accident. The response to this breach depends on how security teams respond to this issue, how they respond to it, how they minimize damage, and when they will recover their resources.

The best way to deal with an incident is to avoid an incident response. But we cannot guarantee 100% security in the real world. Therefore, it is necessary to develop the ability to take prompt and accurate measures after an incident, and this ability is determined by how faithfully prepared Rainy Days Banks will be. If Rainy Days Bank is not prepared in advance, it will be difficult to respond to the incident and it will take more time and damage.

Therefore, preparation is perhaps the most important step in dealing with an incident. To efficiently respond to breaches, organizational strategies and countermeasures will be developed during the preparatory phase. Incident response teams will be trained to respond to their roles. In addition, Rainy Days Banks must regularly train personnel and make alternative amendments to specified plans to tailor to the changing cyberworld. In conclusion, to successfully make and execute an incident response plan, an incident response preparation plan is required.

There are five crucial steps in Rainy Days Banks preparation phase of the incident response plan. First a clear, concise and detailed contract is needed. Within this contract is the policies and plan that Rainy Days Bank have established for the team to operate within. This will establish the baseline and the culture of how a team would react to certain situations. Members can rest assured that there is written documentation for taking such action and there won’t be any unnecessary repercussions. This would in turn give the security team confidence in their abilities and the choices they make. For example, if for whatever reason, a drastic measure such as “cutting the power completely” and shutting everything down, there is a clear and defined reason of why such an action should take place.

Second, would be to encourage and practice good communication skills within the team and the public. Incidents may affect the entirety of Rainy Days Banks resulting in communication errors between personnel and the public. Without communication, response teams and management would not be able to effectively execute the Incident Response Plan resulting in time wastage and loss of data and money. In order to mitigate the damage, teams should have defined levels of seniority and understand how everyone speaks. Everyone should understand that each member has a unique set of quirks in their language and be able to accommodate each specific jargon. Team meetings should deliver policies changes, procedure changes and any other details in regard to the security framework clearly and concisely. This goes the same for the public. In order to maintain trust and reputation with clients, Rainy Days Bank will need to prepare for incidents that may cut off communication methods to the public. Methods could include emergency hotlines and alternative communication methods such as the website, email, etc.

Security teams do not want to be always reacting to a situation, rather it would be preferable to be more proactive in their security approach. However, security teams across the world know that it is one of the most unspoken rules of cyber security is that no matter how well you plan and prepare, a cyber-attack is a matter of when and how. Therefore, a security team will be constantly updating and analyzing their database of logs and threat intelligence feeds. If traffic is monitored, companies can blacklist certain IP’s that are irregular traffic or potentially malicious. A common occurrence of this will be a private user that is using a VPN shared by hundreds of people, and the user tries to access a website. Only to find that the IP is blocked because it detected unusual activity from the IP address from a previous user. This was most likely implemented by the website's security team after it was monitoring its systems traffic.

The fourth step in the preparation phase, would be to implement a cyber hunting team or member. According to studies of the recent attacks of major corporations, we know that once a hacker has gained access to a system, they move even more cautiously in order to breach further into the system. Small amounts of data are slowly moved around, in the meantime hackers stay in the system waiting for that one crucial credential to be used so they can keep moving up the hierarchy of the company. In order to ensure that this is not the case, a specialized team or member should be deployed as if they were watching the inside of the fort.

Fifth, just like history has shown, cyber-attacks are always evolving and coming up with more sophisticated ways to breach a network. With that in mind, cyber security teams should constantly be auditing their systems to make sure that they are deploying the correct software with the proper tools for their company. Risk assessment for certain parts of their framework should be conducted frequently. And lastly taking on the mentality that the plan they established is vulnerable no matter how well thought out it is. Practice and vigilance is always necessary so everyone on the team can improve little by little.

Another big factor of the preparation phase is money. In order to prepare for an incident, costs should always be evaluated. Analyzing the assets, inventory and functions of Rainy Days Bank as well as the multiple tasks laid out in the incident response plan, will give a picture as to how much money Rainy Days Bank will need to prepare for our IRP. Rainy Days Bank has This can be done through cost-analyses and assessments. Rainy Days Bank has a net value of $110 million and assets that are valued more than $5 billion. Some of the main functions of the bank are accepting deposits and issuing loans. If an incident impacts these functions, it is expected to result in millions of dollars including data loss of client and company information. The preparation phase will emphasize these functions and assets to prioritize them because of the high impact they have on Rainy Days Bank. Preparation will be done by preparing security controls and threat detection methods, evaluating costs, auditing, and issuing policies for employees and security teams.

# **Detection, Analysis, and Identification**

The purpose of the detection phase of the incident response life cycle is to be able to identify adverse events and analyze whether it poses a significant threat to Rainy Days Bank. Not all adverse events pose a significant enough threat to our systems but, when the threat level is authentic and poses a genuine risk then it will be categorized as an incident. To better identify these incidents so that they can be handled using the proper methods, they will be classified as either incident candidates or an actual incident. The difference between these two classifications is that an incident candidate that gives the possibility of an incident occurring and an actual incident, which is actively harmful to the system. This step is necessary because not each incident will be handled by the CSIRT, in fact they will only handle the actual incidents that were reported depending on the threat severity of the actual incident.

The reason why not every possible incident will be handled by the CSIRT is due to how possible threats are identified. These threats are identified by incident indicators or through a precursor. An incident indicator will signal the team when an adverse event such as unusual network traffic, denied requests or new user accounts. Whenever an event that is out of the normal occurs, an indication of it will be flagged however, this can also cause false positives or noise that will alert the team to out of the ordinary behavior while it is a nonevent. These nonevents can derive suspicious activities such as altered system logs will be definite indicators of an incident, these types of indicators will flag an ongoing incident that will need to be immediately tackled by the Incident Response Plan.

Threat Classification:

Not all incidents can be planned for or handled in the same way and to be able to use the best strategy against them then we must classify and categorize them in ways that we can later respond to them. Following the most recent publication of NIST Special Publication 800-61, Rev 2 will allow us to categorize incidents through their attack vector. These attack vectors can include but are not limited to the following: Impersonation, Loss or Theft of Equipment, Attrition, or Web attacks. By understanding the attack vector and the “Kill Chain” then the CSIRT will be able to angle their perspective to that of the attacker and plan accordingly.

Furthermore, because there are many potential signs of an incident, Rainy Days Bank will also be classifying the incident indicators so that the team can best identify, which adverse events are most likely to cause an actual incident. The categorization of incident indicators that Rainy Days Bank will use will be composed of possible incident candidates, probable incident candidates and definite incident candidates. Possible incident candidates will be the least likely to occur and suggest the prospect of an incident occurring. This will also be categorized into four types of events which occur with unfamiliar files being registered, unknown programs, spikes in memory consumption or system crashes. These do not guarantee that the system is being targeted by an attacker and the causes can vary. Possible Incident Indicators will also be categorized into four types, which are unfamiliar accounts being found, attacks being reported, notifications from an Intrusion Detection and Prevention System or unexpected network traffic. Lastly, the definite indicator, which suggests that an attack is underway, will be categorized into five types. These five types of definite incident candidates are system logs undergoing unauthorized edits, the hacker tools being found in the system, inactive accounts becoming active, and finally being notified by another partner/organization or the attacker themselves of the incident.

Kill Chains:

The CSIRT team will also have to study and understand the structure of a kill chain because this will give them valuable insight as to how attackers conduct their attacks. Without knowledge to back up an attack pattern or methodology then incident response plans will not be able protect the system. This knowledge will allow the team to find which aspects of the system are vulnerable, how an attack or exploit would be conducted and how they plan to gain access to the systems in place. There are seven stages to the kill chain, and they are the reconnaissance stage, weaponization stage, delivery stage, exploitation stage, installation stage, command & control stage and finally the actions on the objective. Before the implementation of any plan, the team should walk through these seven stages and how they interact with the incident or plan.

False Positives:

A false positive is a are wrongly flagged adverse events that are identified by the collection system as an incident. Occasionally, a bug or glitch in the system can cause it to be flagged by the collection system resulting in it being reported as an incident. These represent normal behaviors in Rainy Day’s computer systems and frequent false flags may create noise that allows actual incidents to remain unnoticed. To reduce the noise from false positives, it would be beneficial to provide increased training to the data collection team or by providing a feedback system to improve the collection system. However, a feedback system has the potential to result in false negatives which have the potential to compromise the system.

False Negatives:

A false negative are actual incidents that are not detected by the system and were not caught. incidents can be highly sophisticated and designed to elude monitoring technology but can also occur due to noise from false positives. Regardless of how they eluded the system or team there exists the very real and likely scenario that they can cause a data leak. One way that these false negatives can be prevented is by tuning the collection or feedback system after every change, this way it can stay up to date and can combat ever changing technology. However, no system is perfect and false negatives, while unlikely to occur, will occur. In that case, there should always be some additional and semi-regular internal monitoring or assessment to look for possible false negatives that penetrated the system.

Detection Strategies:

Attacks on the system will usually show a deviation of normal behaviors, so the classification of adverse events into attack vectors and incident candidates will allow the employees to be able to detect these changes and respond in the appropriate fashion. There are a multitude of possible detection strategies, which change based on an attack vector or incident however, the general strategies that Rainy Days Bank must employ are as follows.

* Monitoring the network and system for signs of intrusion or abnormal behavior.
* Monitoring files for any possible and unauthorized changes
* Checking for equipment that could be tapping into hardware functions
* Ensuring that physical devices have not been accessed by unauthorized sources.
* Reviewing adverse events for a deviation of normal behaviors.
* Ensuring that employees understand and have been trained to follow the correct plans.

The general detection strategies mentioned will provide coverage for the most common incidents but are not as reliable when dealing with more sophisticated or advanced incidents. Those incidents occur less frequently and require specialized approaches; these will cover the incidents that happen more frequently but can prove equally detrimental when not addressed.

The following are the day-to-day instances that Rainy Days Bank can expect to see phishing attempts, malware, ransomware, attacks on the web system, intrusions, and compromised software.

Phishing attempts: This type of incident is the most common because it costs the least to for the attacker to exercise. With basic information, phishing attempts can target regular employees for Rainy Days Bank however, as more information is gathered even middle management to C-level executives will be targeted. These attempts are masquerades that pose as other employees, partners, or federal organizations and management personnel to exploit any communication vulnerability in Rainy Days Bank and download malicious content or extort a payment. These attempts are also the ones most easily avoided if employees are properly trained on internal communications, the chain of command and suspicious links in emails sent from public domains or from misspelt domains.

Malware: Malware incorporates a vast resource of malicious code most commonly including viruses and worms. The damage that these malicious codes can have on the computer systems may vary from stealing information to damaging or infecting critical software. Most malware will be detected by using antivirus protection and it is recommended that Rainy Days Bank uses a multiple anti-virus software to protect the gaps where malware can be undetected.

Ransomware: This is a difficult incident to detect in time and can quickly spread throughout a workstation, or the entire computer system to infect and change code to lock access to their desired target. Once the system has been locked, the attacker will notify the users with a demand on the condition of restoring access. The best ways to detect these intrusions are to monitor files for suspicious activity and create honeypots to distract and isolate the attacker.

Attacks on the web system: Rainy Days Bank will have a web server and an ecommerce server to conduct business on the web. These attacks are detected as soon as they are commenced and will be spotted by any changes or suspicious behavior on the web site. Definite incident candidates will alert the team to these types of incident and should an attack be identified; it should be reported to the CSIRT so that they can further monitor and access the situation.

Intrusions: This is another challenge that Rainy Days Bank will face since intrusions can occur from internal or external points of attack to target the internal system. These can be detected using IDPS systems, or through system logs. If there is a high amount of network traffic during off hours, then this may suggest that data is being exfiltrated from the system. These types of incidents should be frequently monitored due to the confidential customer data being held by Rainy Days Banks.

Compromised Software: This occurs when the detection tools employed by Rainy Days Bank become infected by malicious code or else. In this situation, the only form of detection is by testing and verifying that the software is working as needed and removing it from production for patches and updates to provide software integrity, as needed.

Detecting incidents is an ongoing routine, and the number of incidents increase day to day and attack patterns will become more sophisticated as to mislead users or employed software. To stay up to date with all the new exploits and attacks, Rainy Days Bank should routinely collect data to monitor and analyze. This will allow the user and software to better detect current and future incidents before they can exploit the system’s vulnerabilities. In consideration to attacks from the web and ransomware, data collection, analyzation, and monitoring may be the best practical defense and detection strategy.

Intrusion Detection and Prevention:

Once the incidents have been identified and detection strategies have been planned out for the anticipated incidents then it becomes the time for the installation of an Intrusion and Detection System. There are many types of IDPS for many different required roles, but they all serve one goal: to monitor, detect and prevent an intrusion on the network. The uses of IDPS technology are vast with them being able to identify violations of the security policy as well as kill chains and possible incidents they can also be used to record information of the threat frequency. When an IDPS is deployed, it will alert the team of any adverse events when they are detected, respond to stop, or modify the attack if possible and create a log summarizing the event that occurred for further analysis.

There are two types of methodologies that an IDPS will utilize to detect threats: Signature-Based Detection and Anomaly-Based Detection. A signature-based detection methodology will compare the signature or pattern of a known threat with the possible incident candidates and will act according to its configurations upon a match. The issue with this methodology is that it needs to be consistently updated because if a known threat is marginally changing its pattern, it can evade this detection method all together, until its new pattern gets recorded into a database. The anomaly-based detection method is its contrary, it can identify unknown threats. This is possible because it creates a profile of what normal behavior is on the system and creates alerts based on those deviations. These deviations can also possibly include infrequent patches and updates to the system, and this can create issues with detecting false negatives and positives. This is because it is possible to trick the detection method into thinking that an adverse event is considered normal activity when it is in fact malicious but follows the behavior profile which could have been influenced over time by an attacker. If a signature-based detection method is being implemented, then there needs to be routine maintenance and if an anomaly-based detection method is being implemented then the behavior profiles need to be occasionally tested and re-trained.

Before deploying an IDPS, the Rainy Days Bank must decide which types of IDPS will be implemented. The detection methodologies are only configurations and the types of IDPS technology is vast and changing depending on organizational needs. The ones that are applicable to Rainy Days Bank are Network-Based, Wireless, Application-Based and Host-Based IDPS technology. The Network-Based IDPS is typically deployed with firewalls, VPNs, and other security measures to provide an in-depth security standard. This will allow the entire network to be monitored but presents a challenge such that the volume of traffic through the network overwhelms it. The Wireless IDPS will monitor suspect wireless protocols but will only monitor and detect intrusions on the data link and physical layers of TCP/IP and will not monitor and detect intrusions from the transport or application layers. The application based IDPS will be able to monitor specific applications with the ability to read encrypted files, it is also more susceptible to tampering and attacks than the others. Finally, the host based IDPS will provide a monitor and detect intrusions on a single host such as a server or workstation, but it is only monitoring that host and many host-based detection systems may be required to be deployed to multiple servers or workstations.

Understanding those key differences from those IDPS will allow for a better deployment strategy. Rainy Days Bank will deploy a Network based IDPS for general detection, a wireless IDPS to monitor wireless protocols and host and application based IDPS to critical servers or applications. These IDPS will become an integral part of the Rainy Day’s defense in depth strategy so it is crucial to understand each one. Without this knowledge, the misconfiguration, and misuse of the IDPS becomes a real threat that could lull the Rainy Days Bank into false security. Each IDPS has its own strengths and weaknesses as well as configuration and maintenance requirements and it falls upon the CSIRT team to make sure that selection, integrity, design, controls, and implementation of each IDPS are carefully examined before their deployment onto the network.

Security Information and Event Management:

Security and event management software are used to primarily collect and analyze the data obtained from sources such as firewalls or intrusion and detection systems. These security systems use a seeded ruleset to create alerts based on the category of the incidents. In the case of login information, it can differentiate between a user forgetting their information and the conduction of a brute force attack. The IDPS Rainy Days Bank has in place will be monitoring the system for suspicious activity or adverse events and will then alert the SIEM to the possible incident, which also includes brute force attacks. The SIEM will then collect the alerts from the IDPS systems and will analyze the data collected and create a timeline to be able to determine if there is a definite incident and what impact it will have on the technology infrastructure of Rainy Days Bank. In the case of a brute force attack, it will analyze whether the login attempts occur sparsely within a longer timeframe or if the attempts are occurring at a high frequency in a shorter amount of time. In the former case, it will be reported as a possible incident with the possibility of user error but in the latter case it will determine the activity as a definite incident and categorize it as a brute force attack. The SIEM software that Rainy Days Bank uses will be capable of real-time monitoring, incident response, threat intelligence, user activity monitoring and compliance reporting. The threat monitoring, incident response and threat intelligence capabilities form a vital and core feature for the SIEM software and will be explained in further detail.

Threat Monitoring:

The threat monitoring capability of the SIEM software will reduce the amount of time it takes for a system intrusion to be detected so that Rainy Days Bank can reduce their losses due to data exfiltration. Without this capability, attackers will be able to operate within the technology infrastructure for a longer time gathering information to form a more sophisticated, complex, and devastating attack. One example of these could be an attacker remaining on the system for months and finding a zero-day exploit before it is patched so that they can conduct a zero-day attack. However, by being able to monitor the system and correlate previous attack and activity patterns, the SIEM software will be able to identify ongoing attacks or intrusions so that they can be contained as to minimize company losses.

Incident Response:

The SIEM software should also be capable of assisting in the incident response investigations by utilizing automatic responses in conjunction with alerting the CSIRT team so that they can coordinate a defensive reaction based on the information and notifications gathered. The SIEM that Rainy Days Bank will be using will have the capacity to identify certain incidents and guide the staff on how to respond to them. This is only possible due to the tracking and documentation features included in the SIEM and its ability to interact and collect data from other systems such as the firewalls and IDPS.

Threat Intelligence:

Information about threats that allow for better understanding of threats and threat actors so that mitigation techniques can be developed or successfully conducted is called threat intelligence. This is a crucial capability that the Rainy Days Bank SIEM software is capable of and it will be used to recognize and assess suspicious activities and adverse events to process the impact of the attack and the threat to Rainy Days assets. This core feature will allow the SIEM software to be able to monitor, analyze, and respond to these threats accordingly.

A SIEM software that fits the criteria and needs to protect the information and record of Rainy Days Bank’s customers and infrastructure will be expensive, difficult to configure and will take a long time to implement but, when used in tandem with IDPS it will reduce losses by a considerable amount. To ensure that Rainy Days Bank can maximize the value that the SIEM software can produce there should also be additional training should only be maintained by senior staff members that are trained to maintain this software. That will allow for better data to be collected and to reduce the number of lower-level threats the staff faces daily. All the data the SIEM software collects from the IDPS and firewalls will also be further filtered allowing a better acquisition of data, records, and logs that the staff can use in the future to contain the threats and incidents. The ability to analyze threats and coordinate the staff’s response to those threats will also reduce the amount of time it takes to address definite and ongoing incidents and limit major security breaches.

# **Containment**

Containment is the method or techniques used to minimize the damage caused by the incident while ensuring the business continuity. In Short, to contain the incident and to ensure the damage is as minimum as possible. It provides the time to come up with the remediation plan.

During the containment phase, the incident response team begins interacting with affected systems and attempts to keep further damage from occurring because of the incident. Containment might include taking a system off the network, isolating traffic, powering off the system, or other items to control both the scope and severity of the incident. This phase is also typically where a binary (bit-by-bit) forensic backup is made of systems involved in the incident. An important trend to understand is that most organizations will now capture volatile data before pulling the power plug on a system.

Containment phase requires the decision making which at the time of incident can be very challenging, so it is very important to have a strategy in place for the containment phase of Incident response as well.

Possible cyberattacks against the RainyDays Bank could be Brute force attacks, credential stuffing, phishing emails attacks, Malware attacks and many others. To be able to minimize the damage against the assets of RainyDays Bank it is important to understand what type of incident our resources are facing. Once the attack has been identified then the incident response team can quickly focus towards containing the attack so they can focus towards the mitigation plan.

Containment During a DDOS attack:

During a DDOS attack against the bank’s web application; the incident response team will redirect the traffic to the sandbox platform of the web application to secure the production domain. After the redirect, the team can look into the logs/traffic of the sandbox environment and determine the Ips that are sending the enormous amount of traffic per min. once the Ips have been identified; the team can blacklist those Ips and review the logs again to ensure if there’s any IP that is still sending a huge number of requests to the web application. Once things are under control the team can focus towards creating custom rate rules to help detect and block such requests in future to avoid facing the scenario in future and put the production web application back online.

Containment During a Ransomware attack:

After the identification of a ransomware attack the infected systems or applications should be immediately removed from the network and reroute the clients towards the backup system or application. This will help to contain and minimize the damage caused by the ransomware attack. The incident response team should work with the internal forensics team to investigate the root cause of what led to the ransomware attack. It is important to determine the severity of the problem. For example, Failure to quickly isolate the system from the network may contribute to the incident by allowing the malware to continue to encrypt files on the local system and/or network shares, ultimately causing greater damage to the bank.

The incident response team needs to ensure that access to the file servers is restricted only to the allowed personnel and access is restricted for the rest of the people. The team should not restrict the access through the network or host-based firewall ACL but change permissions on the files within a share to restrict access since depending on the number of files, permission propagation could take hours and would allow the encryption process to continue during this time.

Also, if the bank file servers are running on operating systems like UNIX or Linux etc. The team should ensure to protect those OS as well. This will greatly reduce the chance of these shares being encrypted because to the ransomware they will appear to be Windows shares.

Containment Policy of Rainy Days Bank:

Containment phase policy of Rainy Days Bank requires to follow the sequence mentioned below:

Short-term containment:

Under this category, the goal of the incident response team should be to limit the damage as soon as possible. The team should be quickly able to isolate the affected or infected systems or applications from the network and the traffic should be routed from the production servers down to the failover or back up servers. It is our incident response team's responsibility to ensure that if the incident level is high or P1 then the category should fall under short-term containment because this will quickly work towards limiting the damage before things get worse.

System backup:

To investigate the incident and find the root cause the team should take necessary steps to take proper forensic images of the affected systems or applications with the tools used by the internal forensics team. (Currently, our forensic team currently uses Forensic tool kit (FTK), EnCase, et al). The goal should be to identify the root cause that lead to the incident and to understand if the incident was the result of a criminal act or be used for the learning lessons phase.

Long term Containment:

Under the Long-term containment primarily the affected systems or applications should be fixed temporarily to continue to be used in Production environment; depending on the criticality of the system or application that is targeted to ensure the business continuity. Although, that’s not the end of it; the incident response team should work with the application team or required IT professionals to work towards fixing the problem. Ensure all the backdoors or unwanted user accounts have been removed, security patches have been applied, perform a set of testing to ensure the system or application has been cleaned from the damage and is ready to continue business operations as expected.

Documentation:

The incident response team has an important responsibility towards documenting every single step that was taken to contain the incident. This should include steps that helped to identify the type of incident, steps that indicated the infected systems and applications, steps that helped to isolate those systems or applications from the network, steps that were taken to perform the fix and last but not least include the detailed report that is shared by the internal forensics team. The goal is to document these steps to not only for lessons learned but to also share with the cybersecurity professionals of our bank during the all hands cyber conference to share the knowledge and also help them understand so they can be self-prepared as well to report any anomaly within the network.

Conclusively,

A good example of containment is disconnecting affected systems by either disconnecting the affected system’s network cable or powering down switches and/or routers to entire portions of the network to isolate compromised systems from those that have not been compromised. This in turn will isolate the problem from the rest of the production network and limit the spread of any malware or reduce the risk of further systems being compromised.

# **Eradication, Recovery, Post-Incident Recovery**

Eradication

Eradication and Recovery: Once the incident is contained, the goal is to eliminate the entry point(s) that the hacker used to gain access to the network. This might include patching the hardware, reconfiguring systems and application architecture and rebuilding the systems for production. The first most important thing is to disconnect the infected systems from the network, disconnect the remote access, change the settings on the firewall, prompt employees to change their password accounts and all credentials should also be updated to prevent future attacks. Eliminate the affected components of the *incident* by deleting malware and disable breached user accounts. Quarantine, disinfect and delete infected files immediately.

The IR team will take the necessary measures to address the root cause of the incident and restore systems to normal operation. The incident response team identifies the steps required to clean up the incident that is to remove the malware.

Advanced and Successful hackers intentionally leave a malware behind to continue damaging the system even after they have gone, and they also leave a backdoor that can allow them for a second attack, assess and identify any presence of malware , assess the files, user accounts, the data and the system logs-because hackers can modify the system logs so all affected and unaffected assets , the system log should be monitored continuously to prevent concurrent recurrence- that is when the attackers use the same method to attack for the second time, destroy any compromised computer if it’s possible, and track them until completed. All affected components should be replaced as it were before the incident occurred.

Recovery

Full recovery is when the Rainy Days Bank has Implemented a backup and recovery plan before the incident happened, this helps to carry out the steps effectively to mitigate the incident. Network systems should successfully monitor, track, and delete from the system before any damaged data can be recovered. This includes all data recovery or restoration efforts that need to take place as well.

The incident response team will decide the time and the date operations will be restored, verify and test that infected components that are not re-infected or compromised because this is the main task associated with this step of incident response. Test, verify, and monitor for any abnormal behaviors, and use tools to validate.

The goal of Rainy Day Bank is to recover all damage devices so at the recovery stage, any production systems affected by an incident should be brought back and continued to be monitored for malicious activity.

The next step is damage data recovery. Systems should be upgraded, Policies and procedures should be modified, verify backups and restores service as expected. The system should be monitored to alert if any unusual activity is going on.

The incident response team will regularly review the past incidents to identify the vulnerability areas where correction is needed. It also includes intermittent tabletop exercises which are representatives from each group that will be provided information to communicate with other participants in their break room for each of them to discuss their roles and responsibilities for each step during an incident.

System Upgrades, patch vulnerabilities. Improve and secure configuration of systems, improve the architecture systems and newer versions of software tools should also be discussed.

Post Incident Activity of Rainy Days Bank’s

Post-incident reviews a detailed retrospective that allows Rainy Days Bank’s to carefully understand each part of an incident occurred from the beginning of the incident to the end. Post incident activity is a phase where sometimes we disregard, but we must make sure that we do not neglect this phase. In the post incident activity phase, we determine what happened, why did it happen, and what we can do to prevent it from happening again.

The purpose of this phase is not to blame anybody but rather come together as a team to work and lessen the impact of future incidents. By completing a post-incident review, security teams are able to detect the network vulnerabilities and weaknesses that have been compromised by a hacker. Any internal issues associated with and manipulated by the hacker to gain access to the system must be identified and addressed. The outcome of a good post-incident review will reveal steps and actions the hacker used and will teach the security team what tools can be used to detect, deter, and respond to minimize the impact of any attack.

Lessons Learned

Lessons learned is a critical phase of incident response because it helps to educate the employees at Rainy Days Bank and improve future incident response efforts. This is the step that gives Rainy Days Bank’s the opportunity to update their incident response plans with information that may have been missed out during the incident. Investigation of this phase is to identify the root cause of the incident , and determine the priority and the scope. Remediation is the post-incident repair of affected systems, communication, and instruction to affected parties, and analysis that confirms that the incident has been contained as well as the determination of whether there are regulatory requirements for reporting the incident to outside parties.

This section also provides guidelines for addressing some issues. The Incident Response Team (CSIRT), Director of Information Security should be notified for this post incident activity meeting. The primary purpose and the goal for this meeting is to limit the impact of an information security incident to customers, partners, employees, and Rainy Days Bank itself. This requires timely action and a coordinated approach with the stakeholders involved to budget the resources required to implement the strategy.

Users should be educated on guidelines for the Incident Response process when there is an attack and a response to the incident. Problems encountered during the incident; may have different responses.

Business survival depends on how well the organization is prepared for the unexpected. The Responsibilities relies on the managerial team, the administrative personnel, the information security office (The CSIRT) and all stakeholders to restore service in a short possible time. The Bank must work to rebuild damaged reputations, market share, and regulations. It is important to keep an eye on the affected system and make sure that it does not continue spreading/

Assess to know of each server location in the building, the computing system environment, physical plant security, installed security devices, access control system, software, personal, backup, and operating procedures. Implement rules of unauthorized access for both external and internal to access certain information. Prevent the administration from gaining unauthorized access to servers on the network, to view or copy information without the approved permission, using the organization’s network resources to share pirated content, such as music, and using unassigned workstations should be prohibited.

Common logs should be centralized and placed at protected locations of the network area. Strong authentication of passwords should be required to get access to the system and implement documented policies and enforce it. Plans should be developed to evaluate the lessons, report the findings, the type and severity of the incident conducted should follow-up, what technical actions and strategies were used, the effectiveness of the strategy, what actions slowed the recovery and what could be done differently.

How to recognize an attack trains a user to know what is expected of the team, how to recognize an attack, update antivirus, antimalware software.

Communications Plan

The necessary information to share about the incident will be determined by the chief owner of the organization and the following personals( Administrative authorities),the Incident Response Coordinators(CSIRT) and the director of Information Security .

Do not provide information over the phone or through email, do not install unauthorized software. All incident response procedures will follow the current privacy requirements as in the Policy.

Documentation

The purpose of this documentation is to learn from the attack and increase the security team’s expertise. Incidents sometimes are an opportunity to learn and improve our skills. The need to keep up with the latest techniques and procedures.

Documentation is very important in this phase as it provides information for future incidents. A thorough analysis of how the incident was detected, notified, handled, contained, eradicated and recovered is very necessary because the reports give a clear view of how the incident happened and it may be used during meetings as training materials for new employees. Documentation: Tracking and reporting all incident response activities will be included, the methods used with consistent chain of custody and confidentiality requirements. Incidents will be prioritized and ranked according to their potential to disclose restricted data. As an investigation progresses, that ranking may change, resulting in a greater or lesser prioritization of resources. Incidents will be reviewed post-mortem to assess whether the investigational process was successful and effective. Subsequent adjustments may be made to methods and procedures used by other participants to improve the incident response process. The facts obtained during an investigation may be deleted after the conclusion of the investigation and post-mortem analysis unless otherwise directed.

The incident plan should be updated according to the results of the analysis to improve alert analysis, response times, and to improve the efficiency of the incident response procedures. Document important points made during the meeting, send emails with the results of the meeting, and follow up with those who could not attend the meeting. The results of these meetings can be used as a training tool for new hires, and it can also be used to update policies and procedures and can be useful during future incidents. Awareness programs about malware attacks should be distributed to users.

Recommendation

Suggest and develop recommendations, and all collected evidence should be documented.

The team should learn how to detect, respond, and improve to any future attacks. The team should learn how to implement preventative measures. Evaluate the cost-effectiveness of the current defense given its performance in this incident. Assess the impact and the damage the incident has caused. The system must be thoroughly assessed in the area that must be checked which includes the vulnerabilities, system configurations, the network operations, and weaknesses.

If there are issues that cannot be addressed immediately, try to work around it; for example, if a server cannot be patched right away, make sure the detection system covers that server and its connections are limited and secured.

Things to avoid during the incident: Do not use the internal systems to communicate about the incident to outside parties because the hackers can still read those communications unless the malware has been detected and removed. Consider using your mobile phone to make calls and to receive emails using accounts that are not associated with your organization.

Avoidable Delays: avoid long delays in detecting intrusions, taking too much time to restore service can be very costly, User authentication controls; each user should have a unique identifier. The system should have automatic log off when users are idle for a period. User’s accounts should be locked out after several logins failed attempts. Users should change their password every 3 months and the minimum recommended should include upper and lower case, special character and numbers. User access should be revised periodically.

Separation of duties should be addressed: There should be a time frame to remove terminated employee accounts from the system. Do not allow personal devices to share data be used to share data or be connected to the organization network.

Assess Role

Identify everyone affected by the incident, either they are involved or should have been involved. Assign each task to appropriate stakeholders and anyone that can accomplish the full task. There is an adage that says, “That which does not kill us makes us stronger”. Train all the employees to have the knowledge and the skill needed to respond to future incidents.

In conclusion. Encourage the use of automation to provide senior leaders and the CSIRT the necessary information to make cost-effective. The Bank must work to restore and rebuild the damaged reputation. It is important to monitor and keep an eye on the affected system. The Information Security organization is responsible for staying current on any industry developments around incidents.

# **Disaster Recovery Plan**

It is important to know that the rate at which data and information technology infrastructure has been lost to disasters appears to be increasing in today’s world that is why it is important for Rainy Days Bank to plan, implement and utilize a Disaster Recovery Plan if a disaster occurs. A disaster recovery plan is part of contingency planning and allows organizations to create a plan of action in case a disaster occurs. Disasters can be defined by a number of things such as the impact of the incident, what is affected and how the incident occurred. A disaster recovery plan is included in the IRP because often incidents that occur may be elevated to a disaster although first noticed by the incident response team. A disaster recovery plan may be implemented when natural disasters such as tornadoes, floods, earthquakes occur, or when man-made disasters occur such as critical cyberattacks, fires, physical attacks.

Rainy Days Bank will make use of a disaster recovery plan checklist which includes identifying critical IT systems and networks, prioritizing the RTO which has been explained in the IRP, and outlining the steps needed to restart, reconfigure, and recover systems and networks. This plan will minimize and mitigate any negative effects on business operations if a disaster occurs. The goal of Rainy Days Bank is to ensure that our financial institution has a structured plan to recover business operations in the event of a man-made or natural disaster or critical cyberattack.

Rainy Days Bank will have a disaster recovery team that will beresponsible for developing, implementing, and maintaining the disaster recovery plan. They will help identify the team members and each of the members of the team’s responsibilities and provide their contact information. Every personnel will have a copy of the disaster recovery plan at home and in their office in case an emergency occurs, and they need to execute the plan. The disaster recovery plan will also identify various non-personnel entities that will be contacted in the event of a disaster or emergency which will include third party vendors, alternate site hosts, and clients. Management will be responsible for ensuring that the disaster recovery plan is being executed as planned and the employees that are responsible for their specified tasks are doing what they need to. It will be the chief operations officer who will be responsible for overlooking the disaster recovery plan though it will be essential for them to contact other department managers and executives. This is because in an emergency a disaster will affect the entirety of Rainy Days Bank, which will mean that all business departments will have specific disaster recovery tasks to execute with their personnel and management.

Rainy Days Bank will identify and assess disaster risks, which will enable our disaster recovery team to identify and assess the risks to our bank. Since Rainy Days Bank is in the Northeastern region of the country, there is a low probability of certain natural disasters, however our financial institution is still susceptible to fires, physical and cyber incidents. For example, Rainy Days Bank may be hit with a virus that is unable to be contained with the containment methods leading to system administrators unable to access the system. These types of incidents will need to be identified and prioritized based on probability and impact. This will enable the Rainy Days Bank team to better understand natural disasters, emergencies, and technology related incidents and assist the team in identifying the recovery strategies and resources required to recover from disasters within a predetermined and acceptable timeframe. The disaster recovery team will be briefed and remain up to date on the security controls and mitigation methods that will be put in place for the disaster risks identified.

Rainy Days Bank’s teams will then determine critical applications, documents, and resources. Many of this information will be in the inventory and asset assessments established in the IRP already. The team will evaluate its business processes to determine which are critical to the operations of the organization. The Rainy Days Bank plan will focus on short-term survivability, such as generating cash flows and revenues, rather than on a long-term solution of restoring the organization’s full functioning capacity. However, the team will then recognize that there are some processes that should not be delayed if possible. Like the processing of payroll, client contacting and major business functions such as lending and accepting payments. These processes will need to be a high priority in case of disaster, meaning that the team will work to bring back these functions first in order to make sure that the damage will decrease and the business will be able to continue.

One of the main elements of a successful disaster recovery plan lies in our team’s ability to back up our IT environment and recover data. Rainy Days Bank’s team will specify backup and off-site storage procedures. The team’s procedures should identify what to back up, by whom, how to perform the backup, location of backup and how frequently backups should occur. All critical applications, equipment, and documents will be backed up as well. Documents that the Rainy Days Bank team will consider backing up are the latest financial statements, tax returns, a current list of employees and their contact information, inventory records, customer listings. Having backups will make it faster and easier to recover data and equipment function at the main site.

The Rainy Days Bank team must test and maintain the disaster recovery plan frequently. It is important to know that disaster recovery planning is a continual process as risks of disasters and emergencies are always changing. The team will routinely test the Disaster recovery plan to evaluate the procedures documented in the plan for effectiveness and appropriateness. The recovery team will regularly update the Disaster recovery plan to accommodate for changes in business processes, technology, and evolving disaster risks.

There will be different tiers of the disaster recovery service that Rainy Days Bank will utilize. This will make the process of DR more secure and organized.The Rainy Days Bank will have different teams in charge of these different tiers, which will be assigned and monitored by management.

**Tier 0 -** No off-site data. In this tier, Rainy Days Bank team understand that the recovery is only possible using an on-site system

**Tier 1 -** Physical backup with a cold site. The Rainy Days Bank team responsible for this tier will understand that data is likely on tape, which is transported to an off-site facility that does not have the necessary hardware installed.

**Tier 2 -** Physical backup with a hot site. The Rainy Days Bank team responsible for this tier will understand that data is likely on tape, and it is transported to an off-site facility that has the necessary hardware installed to support key systems of the primary site

**Tier 3 -** Electronic vaulting. The Rainy Days Bank team responsible for this tier will understand that data is electronically transmitted to a hot site.

**Tier 4 -** Point-in-time copies/active secondary site. The Rainy Days Bank team responsible for this tier will understand that vital data is copied across the primary and secondary sites, each site backing up the other. Also, disk is often used in this tier.

**Tier 5 -** Two-site commit/transaction integrity. The Rainy Days Bank team responsible for this tier will understand that data is continuously transmitted across sites

**Tier 6 -** Minimal to zero data loss. The Rainy Days Bank team responsible for this tier will understand that recovery is instantaneous, and it often involves disk mirroring or replication.

It is important to know that while the ability to recover improves with the next highest tier, costs also increase. The purpose of a disaster recovery plan is to ensure that our bank can respond to a disaster or other emergency that affects information systems which in turns minimize the effect on our bank operations.

# **Business Continuity Plan**

The Business Continuity Plan (BCP) is one of the last sections of an IRP. When an incident occurs the BCP helps outline how the business will continue operations. The main goal of a BCP is to have enough critical functions back online to continue the business while simultaneously reducing loss and costs. A business continuity plan is usually more extensive than a disaster recovery plan as it addresses many aspects such as identification of assets and functions, reduction and mitigation of disruptions, business partners and clients, etc. A disaster recovery plan, like mentioned in this IRP, usually aims to resume operations at the main site and to return to normal operations. Whereas, a business continuity plan will aim to resume business functions, usually at a secondary or alternate site as it is not necessary for the business to return to normalcy in order to continue its operations.

Rainy Days Bank’s IRP will include both a comprehensive disaster recovery plan (DRP) and business continuity plan. When these plans are combined it is known as a business resumption plan. For a financial institution like Rainy Days Bank that handles important personal and financial data and assets, a comprehensive business resumption plan works best. When an incident occurs the BCP will be executed for the business to continue until the DRP can be completed and the business can return to its main site allowing minimal loss. Rainy Days Bank’s BCP will include the following elements: an analysis of the Business Impact Analysis, establishment of a business continuity response team, identification of controls and solutions, and an overview of the phases that will be executed when an incident occurs.

An important task that must be fulfilled is the Business Impact Analysis of Rainy Days Bank. A BIA will identify critical functions and assets of the business making it easier for the CSIRT team to identify which aspects of the business must be protected and prioritized. The critical functions of Rainy Days Bank include:

Lending:

This critical function allows the borrowing of funds between Rainy Days Bank and it’s clients. Important data is exchanged in this process including routing and checking information, personal information, and money, occurring at all of our branches and being done through phones, online services and in-person services.

Accepting and Safeguarding Deposits:

Rainy Days Bank is responsible for the acceptance, transferring and protecting of monetary deposits. This is a main function that occurs at all our branches. Both credit and physical money are accepted and stored online or in our vaults. It is also our responsibility to manage checking and savings accounts of clientele and to issue fees, charge or pay interest and do credit evaluations.

If these critical functions are directly impacted by an incident then Rainy Days Bank may experience loss of data, costs and trust. Therefore, these functions are critical and must hold priority over any other business function. What also must be defined is our essential assets or equipment that will be needed to continue operations. Computers, phones, cables, software, licenses, etc. and their versions, model numbers, vendors, and frequency of usage will all be included in Rainy Days Bank’s essential assets. Our business impact analysis will define and outline this, as well as risks that are posed to these functions and assets which can include DDos attacks, ransomware and physical threats.

Once the important assets and functions of Rainy Days Bank have been identified and the BIA is analyzed, the BCP must establish the business continuity response team. This will outline the personnel who will be responsible for relocating critical functions, personnel and equipment to alternate sites in order to continue operations. Rainy Days Banks’s business continuity response team includes:

BCP Management Team:

This includes managers and personnel with high-level authority, who are responsible for planning and managing the BCP. This team will coordinate and assign outlined responsibilities to personnel in order to efficiently execute the business continuity plan. They will also conduct communications between different departments, stakeholders, and third-party vendors or contractors.

Hardware/Software or OS Team:   
  
 This will include two teams in which one team will be responsible for setting up and maintaining equipment such as desktops, phones, servers, etc and the other team will be responsible for installing software such as the operating systems, user accounts, and applications on the hardware.

Network Team:

This team will be responsible for managing and setting up the network for the alternate sites, including wired and wireless connectivity. Devices such as routers, hubs, modems, firewalls, and cables.

Data Management Team:

This includes a team of personnel solely responsible for the data restoration and recovery after the incident. This can be done either on-site or off-site and they may work closely with the disaster recovery team in order to better preserve and restore the data.

These are the main teams that are established for Rainy Days Banks business continuity plan. There may be a need for more teams or individuals that need to carry out smaller tasks such as ensuring that personnel have the supplies they need at the alternate site so that the relocation and continuation of operations runs smoothly.

The BCA and the business continuity response team must be made aware of the security controls in place as outlined in the preparation phase of this IRP. It’s important to have knowledge about the pre-existing protection measures that were in place in case of incidents. Simultaneously, the BCA and the response team should have proper recovery strategies in place in case of these incidents which is also covered in this IRP. Two strategies that are essential, however, to also outline in the BCA are alternate sites and backup methods. Rainy Days Bank’s BCA will include how to mitigate losses when an incident occurs while simultaneously maintaining business functions which will be done through data backup and establishment of alternate sites.

In case of an incident occurring, one of the best practices a business can undergo is backing up their data. This is especially important in a BCA because having a backup of essential data is important to continue business operations. In Rainy Days Bank’s BCA, it will ensure that data such as personal and monetary information, transaction, and auditing functions, etc., will be backed up multiple times a day through an automatic process requiring little supervision. This data will be stored in different physical alternate sites to ensure that if one site or server location is affected, the data will still be preserved at another location. These locations will be routinely tested, assessed and maintained to ensure the storage of data is being conducted properly and there is no data loss, corruption or damage to the backups.

The other recovery strategy is essential to BCPs as the main purpose of this plan is to begin business functions as soon as possible, usually at a different location than the affected main site. Establishment of alternate sites or off-sites where the main functions of the business can be carried out while the incident that occurred can be contained and dealt with is one of the most important aspects of BCPs. An alternate site is only essential when the incident cannot be contained at the main site within the maximum tolerable downtime or recovery time objective. Otherwise, the disaster recovery plan is executed, and the business is able to resume operations at the main site with normalcy.

Rainy Days Bank will include an alternate site located near the main site, which will include installed hardware, software and connectivity which will be continuously maintained by the business continuity response team. This hot site will be established because of the short maximum tolerable downtime that was established in the IRP meaning that in case of incidents, the business will need to continue operations in a short time requiring readily available equipment and software. This site will be located in McLean, VA, not far from our main office, allowing easy relocation of employees to and from the sites. Only personnel that are essential to the critical business functions will be relocated to the hot site. This site will include backups of essential data and software available for personnel to access to continue the only essential business functions.

The remaining personnel will be sent home and allowed to telework. This will require the business continuity response team to plan for remote connectivity between those personnel and the business software and applications. This will also require personnel to have access to proper equipment at home. All personnel will be required to submit or request a working desktop computer for business use. Once this is established the business continuity response team will need to grant remote access to personnel and establish user accounts. The proper management personnel will also need to establish communications with personnel. Once alternate sites and teleworking personnel are established roles and responsibilities of personnel will need to be assigned to continue business operations. A communication channel such as e-mail or telephone will be essential to contact and coordinate with employees.

Now that the essential strategies have been established for Rainy Days Banks BCP including data recovery and backups and alternate sites, it is important to outline the phases that will occur according to the BCA when an incident occurs that will require moving to an alternate site to continue business operations. The first step for Rainy Days Banks will be for the business continuity management team to be notified and have them deploy the designated business continuity response personnel to their specific duties. This will include data recovery processes, preparing and ensuring the hot site is ready, and helping other personnel with relocation. The next step would be for managers to convey a message to the public and clients. This will be done with a message on our customer service line or on the online website, notifying clients of the incident and the best way to conduct their business with us.

The business continuity team will ensure that the hot site is running properly and that the critical functions of the business will be supported at the site. The next step will be to establish and relocate personnel to either work at the alternate site or telework. This will be done in an established schedule in which essential job duties will be prioritized. These personnel will continue business functions at the alternate site while the threat will be contained and eradicated and the recovery will begin including the disaster recovery plan. Once Rainy Days Banks’ main site returns to normal it will be the business continuity response teams’ responsibility to move employees back to the main site and return the alternate site back to its normal condition. The team will then undergo auditing and documentation of the events to create a record of the incident allowing for improvements and updates in the future.

### Works Cited

Whitman, M. E., & Mattord, H. J. (2021). *Principles of incident response & disaster recovery*.

*6 Phases in the Incident Response Plan*. (2021). SecurityMetrics. https://www.securitymetrics.com/blog/6-phases-incident-response-plan

*Ransomware response guide*. (n.d.). IBM Incident Response Services. https://cdn2.hubspot.net/hubfs/233484/Open%20Systems%20Specialists/Content/Ransomware%20Response%20Guide.pdf?t=1507156230392

SANS Institute. (2011). Incident Handler’s Handbook. *Incident Handler’s Handbook*, <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

Bandos, T. (2019, June 26). *The Five Steps of Incident Response*. Digital Guardian. <https://digitalguardian.com/blog/five-steps-incident-response>

Barracuda.(2021). Disaster Recovery. https://www.barracuda.com/glossary/disaster-recovery

Chai, W., Beaver, K., & Rosencrance, L. (2020, October 27). *incident response*. SearchSecurity. https://searchsecurity.techtarget.com/definition/incident-response

MKS&H CPAs and Business Consultants. (2021, June 8). 5 ELEMENTS OF A DISASTER RECOVERY PLAN-IS YOUR BUSINESS PREPARED. https://mksh.com/5-elements-of-a-disaster-recovery-plan-is-your-business-prepared/

Puricica, C. (2021, March 25). *RPO and RTO definitions, values and common practices*. Veeam Software Official Blog. https://www.veeam.com/blog/rto-rpo-definitions-values-common-practice.html

Sanders, S. (2021, January 13). *Incident Response Plan Is Key to Surviving Cyberattack*. CSI. https://www.csiweb.com/what-to-know/content-hub/blog/incident-response-plan-is-key-to-surviving-cyberattack/

Security, R. (2020, January 14). *What Is Security Incident Management?* RSI Security. https://blog.rsisecurity.com/what-is-security-incident-management/

Singh, J. (2021, January 27). *Understanding RPO and RTO*. Druva. https://www.druva.com/blog/understanding-rpo-and-rto/

Team, T. H. (2021, March 15). *The 6 Phases of an Incident Response Plan*. Hartman Executive Advisors. <https://hartmanadvisors.com/the-6-phases-of-an-incident-response-plan/>

DeVoe, Charles & Rahman, Syed. (2015). Incident Response Plan for a Small to Medium Sized Hospital. International Journal of Network Security & Its Applications. 5. 10.5121/ijnsa.2013.5201.

Be prepared: Why you need an incident response policy. (2021) [https://www.techrepublic.com/article/be-prepared-why-you-need-an-incident-response-policy](https://www.techrepublic.com/article/be-prepared-why-you-need-an-incident-response-policy/)

How to create a business impact Analysis (BIA). (n.d.). Retrieved April 10, 2021, from <https://www.cubcyber.com/how-to-create-a-business-impact-analysis>

Rosencrance, L. (2020, February 07). What is siem and why is it important? Retrieved April 10, 2021, from <https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM#:~:text=Security%20information%20and%20event%20management%20(SIEM)%20is%20an%20approach%20to,sim%22%20with%20a%20silent%20e>.

Pratt, M. (2017, November 28). What is siem software? How it works and how to choose the right tool. Retrieved April 10, 2021, from <https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html>

Cichonski, P., Millar, T., Grance, T., &amp; Scarfone, K. (2012, August 06). Computer security incident handling guide. Retrieved April 17, 2021, from https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final