STEVENS
INSTITUTE OF TECHNOLOGY
1870

CYBERCRIME

By

Group 8
Karthikeswar Thotakura
Lakshmi Praneetha Achanta
Shwetha Naidu
Sumaiyya Kayyum Shaikh
Swetha Suresh

05/06/2023

Problem Statement

- Advances in technology have led to an increase in the number and sophistication of cyber-attacks, which are causing significant harm to individuals, businesses, and governments.

- Cybercrime includes a wide range of illegal activities such as hacking, identity theft, phishing, ransomware, and malware, among others. These activities can result in financial losses, reputational damage, and breach of privacy, which can have a severe impact on the victims.

- Despite various measures to prevent cybercrime, cybercriminals continue to find ways to exploit vulnerabilities in systems and networks. Therefore, there is a need to develop effective strategies and technologies to prevent, detect, and respond to cybercrime in order to safeguard individuals, businesses, and governments from the increasing threat of cyber attacks

  We are discussing on the two main industries which are affected by cybercrime

- Financial Industry
- Health Industry

Factors Contributing to the Increase in Cyber Crime

Increased Connectivity

•More devices are connected to networks, creating more potential entry points for cybercriminals.

Digitization of Information

•The digitization of information has made it easier for cybercriminals to steal, manipulate, and distribute data.

•The widespread adoption of cloud computing has also made it easier for cybercriminals to gain access to sensitive information.

Exploitation of Vulnerabilities

•Cybercriminals often exploit vulnerabilities in software and hardware to gain access to systems and networks.

Use of Automation and Artificial Intelligence

•Cybercriminals are increasingly using automation and AI to carry out attacks, allowing them to scale their attacks and bypass traditional security measures.

Rise of the Dark Web

•The dark web has provided a platform for cybercriminals to buy and sell tools and services that facilitate cyber attacks.

Challenges in Preventing Cybercrime

•A typical cyber-attack involves several steps, including reconnaissance, initial access, escalation of privilege, lateral movement, data exfiltration, and command and control

•Current measures in cybersecurity may not be sufficient to prevent attacks due to evolving threats, increasing attacker sophistication, technology vulnerabilities, and human error.

•To improve cybersecurity, a comprehensive and proactive approach is necessary, including strong access controls, regular vulnerability assessments and patching, threat intelligence monitoring, employee education and training, and incident response planning.

•Multiple layers of defense can help organizations better protect their digital assets and respond effectively to cyber-attacks.

•The increasing use of connected devices and IoT creates new opportunities for cybercriminals to access and exploit sensitive information

•Comprehensive and integrated approaches to cybersecurity are needed, including proactive threat hunting, continuous monitoring, and rapid incident response, as well as increased awareness and education about the risks of cybercrime.

Comparing Cybercrime in the Financial and Healthcare Industries

•The financial and healthcare industries both deal with sensitive and valuable data, and are heavily regulated regarding data protection, privacy, and security.

•The financial industry has a stronger focus on fraud prevention and detection, while the healthcare industry focuses on protecting patient privacy and confidentiality.

•The financial industry has a more centralized and standardized approach to cybersecurity, while the healthcare industry has a more decentralized and fragmented approach.

•The financial industry has a more advanced and mature cybersecurity practice, while the healthcare industry is still catching up.

•The financial industry has a stronger tradition of sharing threat intelligence and collaborating with government agencies and other organizations, while the healthcare industry has been slower to develop such networks.

•Both industries need to prioritize cybersecurity and adopt a proactive and holistic approach to effectively protect their data and systems.

Problem Scenario-1- Financial Industry

Hackers steal critical client data from a financial organization (PNC), including credit card numbers and personal details using malware delivery. The fraudsters demand a ransom in return for keeping the data from being made public. Given the extensive nature of the stolen data which is stored in a centralized database and the possible links to other critical systems within the organization(CRM), this incident poses a severe threat to both the affected customers and the financial organization itself.

The contained system is PNC and their centralized database. On the other hand, the containing system is the broader infrastructure of the finance industry, which includes other financial organizations, regulatory bodies, and other related systems.

Malware refers to malicious software that was delivered to the financial organization's system with the intention of causing harm. It was designed to exploit vulnerabilities in the system or trick users into downloading and installing it. The attackers likely used social engineering tactics to exploit the trust that users had in the financial organization's systems or software in order to gain access to the system and steal the sensitive data.

GOALS

- To protect the affected customers' data and prevent it from being used for fraudulent purposes
- To identify the vulnerabilities that allowed the hackers to access the data and take steps to strengthen its cybersecurity defenses to prevent similar incidents in the future
- To comply with all relevant data protection laws and regulations

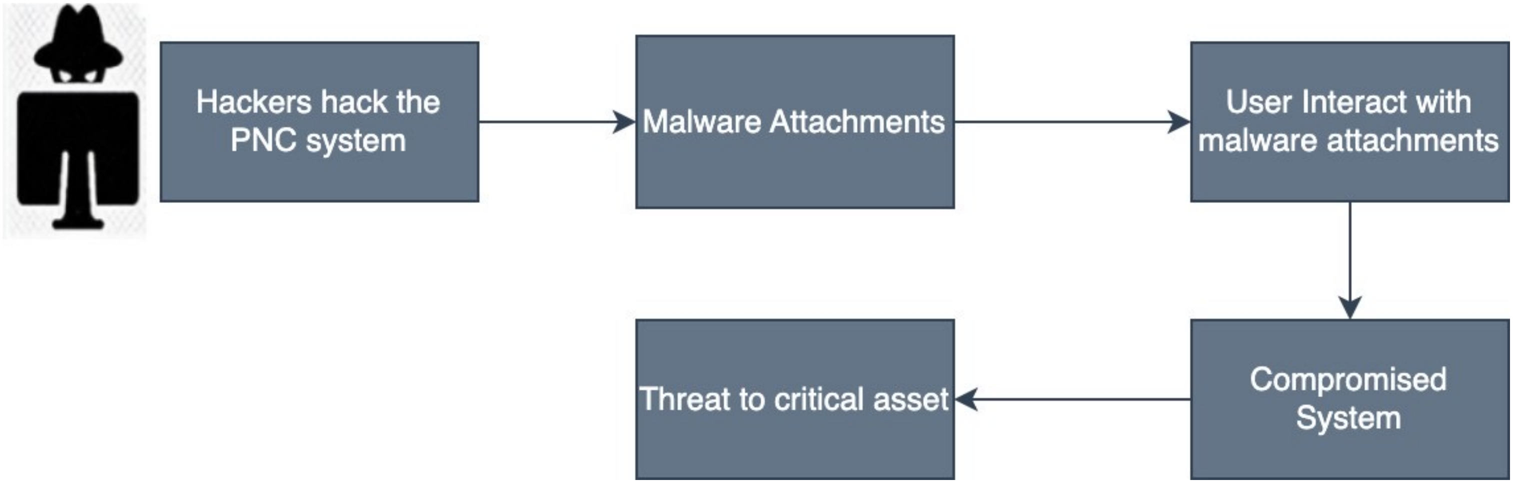
CONSTRAINTS

- Security constraint: PNC must ensure the security of its systems and data, which could limit its options for resolving the issue.
- Reputation constraint: The incident could damage PNC's reputation, which could impact its relationships with customers, partners, and other stakeholders.
- Time constraint:PNC needs to act quickly and efficiently to minimize the damage to its customers and organization.

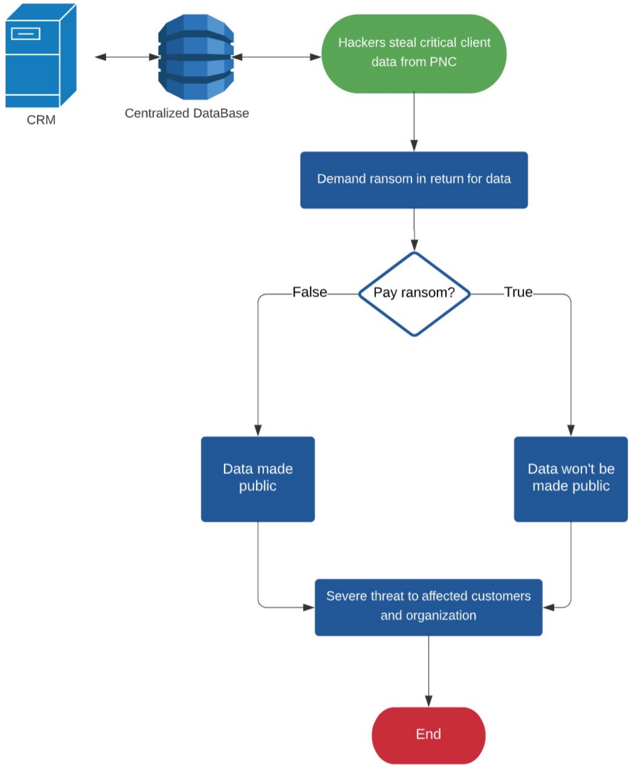
CHALLENGES

- Protecting customer data: The primary challenge faced by PNC is to protect its customers' data and prevent it from being used for fraudulent purposes
- Managing the crisis: PNC must have a crisis management plan in place and be able to execute it efficiently
- Rebuilding trust: The incident may damage PNC's reputation and erode customer trust

Structure Diagram For Problem Scenario-1


Hackers hack the PNC system
Malware Attachments
User Interact with malware attachments
Compromised System
Threat to critical asset

Process Diagram For Problem Scenario-1



CRM

Centralized DataBase

Hackers steal critical client data from PNC

Demand ransom in return for data

Pay ransom?

False

True

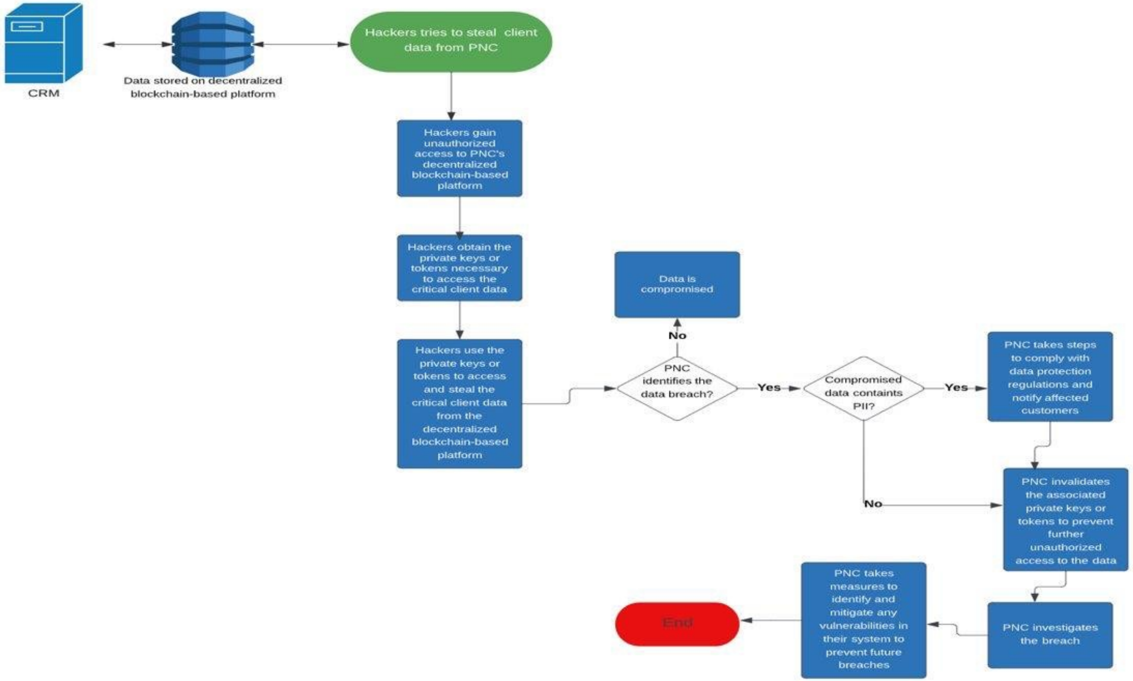
Data made public

Data won't be made public

Severe threat to affected customers and organization

End

Process Diagram for Preferred Solution –Scenario 1



CRM

Data stored on decentralized blockchain-based platform

Hackers tries to steal client data from PNC

Hackers gain unauthorized access to PNC's decentralized blockchain-based platform

Hackers obtain the private keys or tokens necessary to access the critical client data

Hackers use the private keys or tokens to access and steal the critical client data from the decentralized blockchain-based platform

PNC identifies the data breach?

No

Data is compromised

Yes

Compromised data containts PII?

Yes

PNC takes steps to comply with data protection regulations and notify affected customers

No

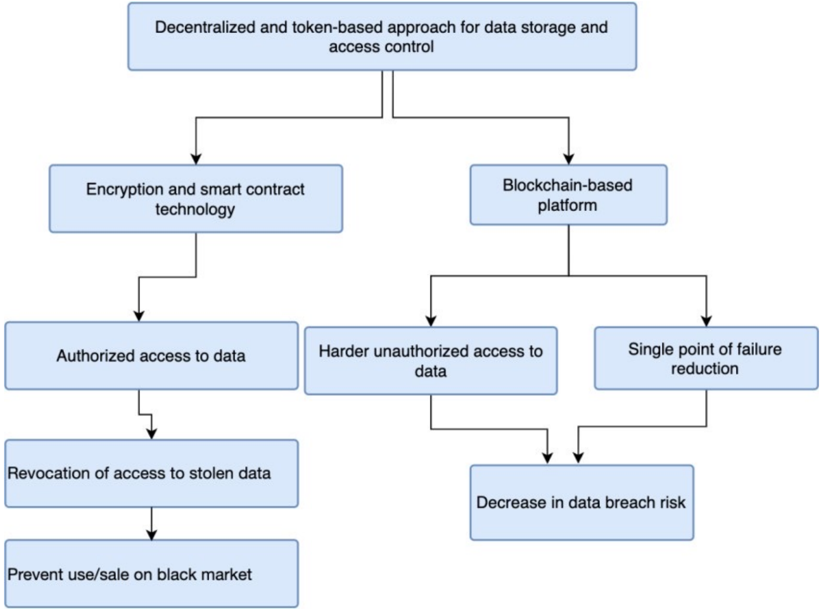
PNC invalidates the associated private keys or tokens to prevent further unauthorized access to the data

PNC investigates the breach

PNC takes measures to identify and mitigate any vulnerabilities in their system to prevent future breaches

End

Structure Diagram for Preferred Solution –Scenario 1


Decentralized and token-based approach for data storage and access control

Encryption and smart contract technology

Blockchain-based platform

Authorized access to data

Harder unauthorized access to data

Single point of failure reduction

Revocation of access to stolen data

Decrease in data breach risk

Prevent use/sale on black market

Trade-off for Preferred Solution(Scenario -1)

Strengths

- Storing data on a decentralized blockchain-based platform reduces the risk of a single point of failure and increases the difficulty for hackers to gain unauthorized access to the data.
- Tokenization provides a simple and efficient method of controlling access to the data.
- In the event of a data breach, the token-based approach enables the organization to quickly revoke access to the data by invalidating the tokens associated with the compromised data

Weakness

- The management of tokens and permissions can be complex and may require ongoing maintenance and monitoring to ensure that only authorized users have access to the data.
- Depending on the size and complexity of the data being stored, a decentralized approach may not be scalable enough to handle large volumes of data or complex queries.
- Implementing a decentralized and token- based approach for data storage and access control may require additional technical expertise and resources. This could lead to increased costs and longer implementation timelines.

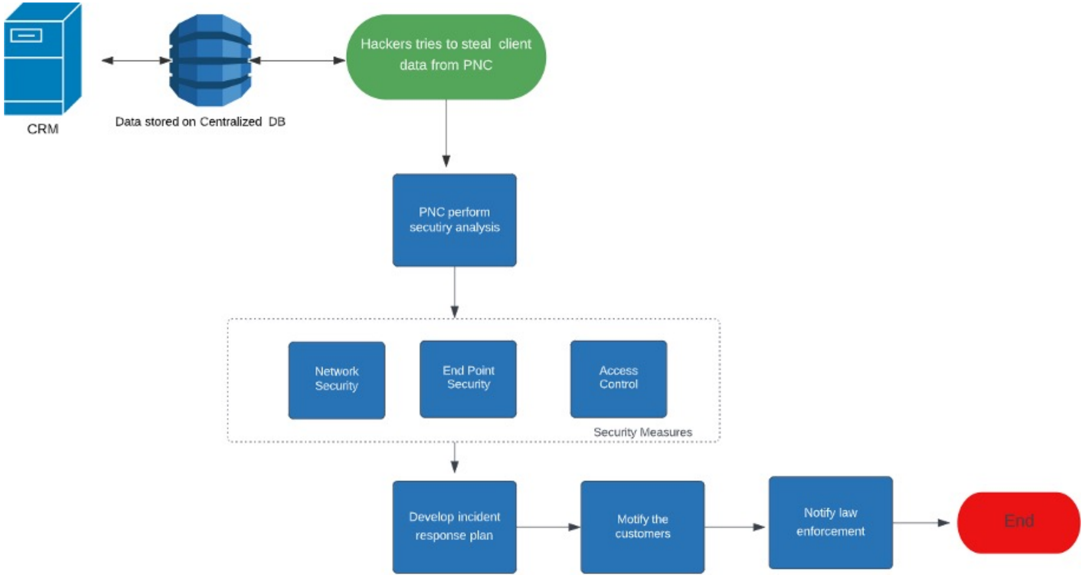
Cost Analysis-Preferred Solution

Assumptions:

- 10,000 users

Cost Item	Estimated Cost
Infrastructure	$100,000
Development	$450,000
Tokenization (creation and distribution)	$50,000
Operational (maintenance, security, auditing)	$100,000
Training	$25,000
Total	$725,000

Process Diagram for Alternate Solution –Scenario 1



CRM

Data stored on Centralized DB

Hackers tries to steal client data from PNC

PNC perform secutiry analysis

Network Security

End Point Security

Access Control

Security Measures

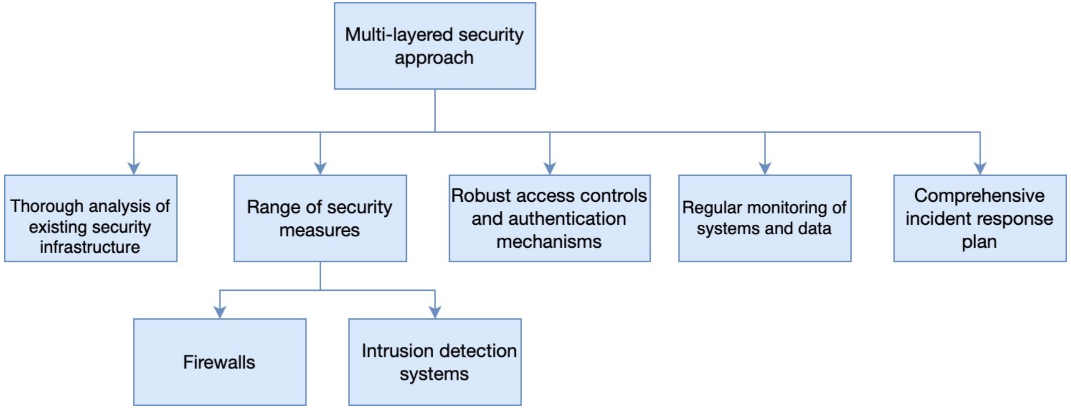
Develop incident response plan

Motify the customers

Notify law enforcement

End

Structure Diagram for Alternate Solution –Scenario 1



Multi-layered security approach
Thorough analysis of existing security infrastructure
Range of security measures
Robust access controls and authentication mechanisms
Regular monitoring of systems and data
Comprehensive incident response plan
Firewalls
Intrusion detection systems

Trade-off for Alternate Solution(Scenario -1)

Strengths

- By implementing multiple layers of security measures, PNC can significantly reduce the risk of a successful cyberattack.
- Having a comprehensive incident response plan can help PNC minimize the impact of a security incident.
- Regularly monitoring systems and data for unusual activity can help PNC detect security incidents early and take action.

Weakness

- Managing a multi-layered security infrastructure can be complex.
- The implementation of multiple layers of security measures can potentially impact the performance resulting in slower response times and reduced efficiency.
- Robust access controls and authentication mechanisms resulting in a poorer user experience.

Cost Analysis-Alternate Solution(Scenario –1)

Assumptions:

- 10,000 users

Cost Item	Estimated Cost
Security analysis and planning	$100,000
Implementation of security measures (firewalls, IDS, etc.)	$200,000
Access control and authentication mechanisms	$150,000
Ongoing monitoring for unusual activity	$50,000
Incident response planning	$50,000
Training	$25,000
Total	$575,000

Mechanism of Integration-Preferred Solution(Scenario-1)

- Design and develop a decentralized blockchain-based platform that can store and manage data securely.
- Develop a token-based system that grants authorized users access to the data stored on the platform.
- Integrate the token-based system with the access control policies of the blockchain-based platform to ensure that only authorized users can access the data.
- Train employees and other authorized users on how to use the system effectively.
- Regularly monitor the system for any anomalies or potential security breaches.
- Continuously improve the system's security by implementing best practices and adopting new technologies as they become available.

Why? Preferred solution over alternative solution (Scenario-1)

- The use of a blockchain-based platform and encryption in Solution 1 makes it more difficult for hackers to gain unauthorized access to the data.
- Solution 1's token-based approach allows for quick revocation of access to the data if it is compromised, which prevents the stolen data from being used or sold on the black market.
- Solution 1 addresses the problem of a single point of failure by using a decentralized approach for data storage, which significantly reduces the risk of a data breach.

While the cost of implementing Solution 1 may be higher than that of Solution 2, the benefits it offers in terms of security, data integrity, and regulatory compliance make it a better choice for PNC.

Problem Scenario-2-Health Industry

A healthcare organization experiences a ransomware attack that shuts down its systems, preventing doctors and nurses from accessing patient records and providing care. The cybercriminals demand a ransom payment in exchange for restoring access. Design a system to prevent such future incidents and a responsive plan.

Their containing system is Health Organization.

GOALS

1-Restore system functionality:-Prioritize recovery of critical systems and data to ensure patient access.
2-Protect patient data:- Healthcare organizations should take steps to protect patient data during and after an attack.
3- Investigate the attack:- Investigate ransomware attack to identify cause and prevent future attacks.
4- Develop a response plan:- Healthcare organizations should develop a comprehensive response plan for future ransomware attacks to contain and mitigate damage.

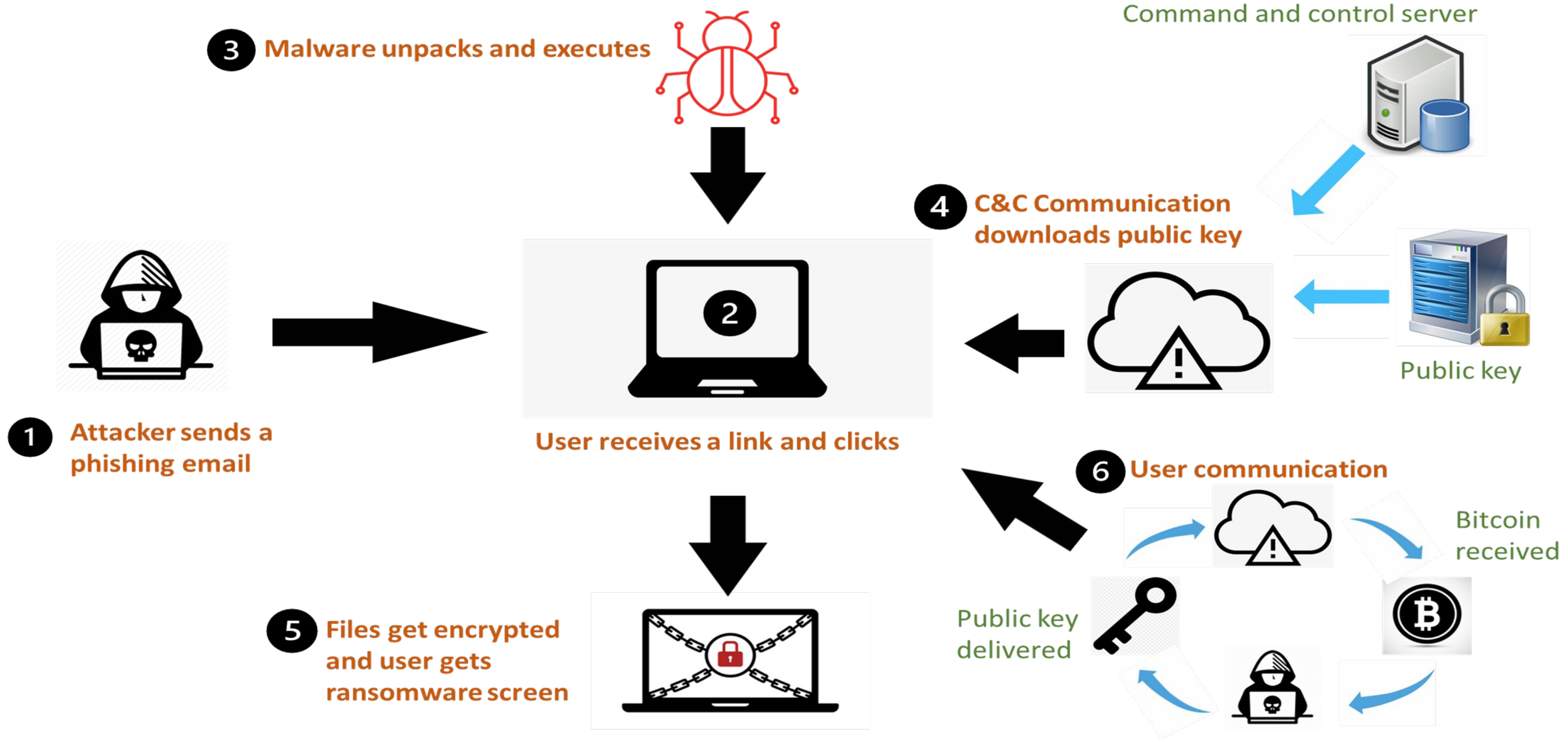
CONSTRAINTS

1-Time Constraints:- Healthcare organizations must act quickly to limit damage, but recovery can be time-consuming.
2- Resource Constraints:- Healthcare organizations may not have the resources to implement cybersecurity measures.
3- Regulatory Constraints:- Healthcare organizations face regulatory requirements that limit their ability to respond to ransomware attacks.
4- Staff Constraints:- Healthcare organizations rely on staff to provide patient care, but staff may not be trained.

CHALLENGES

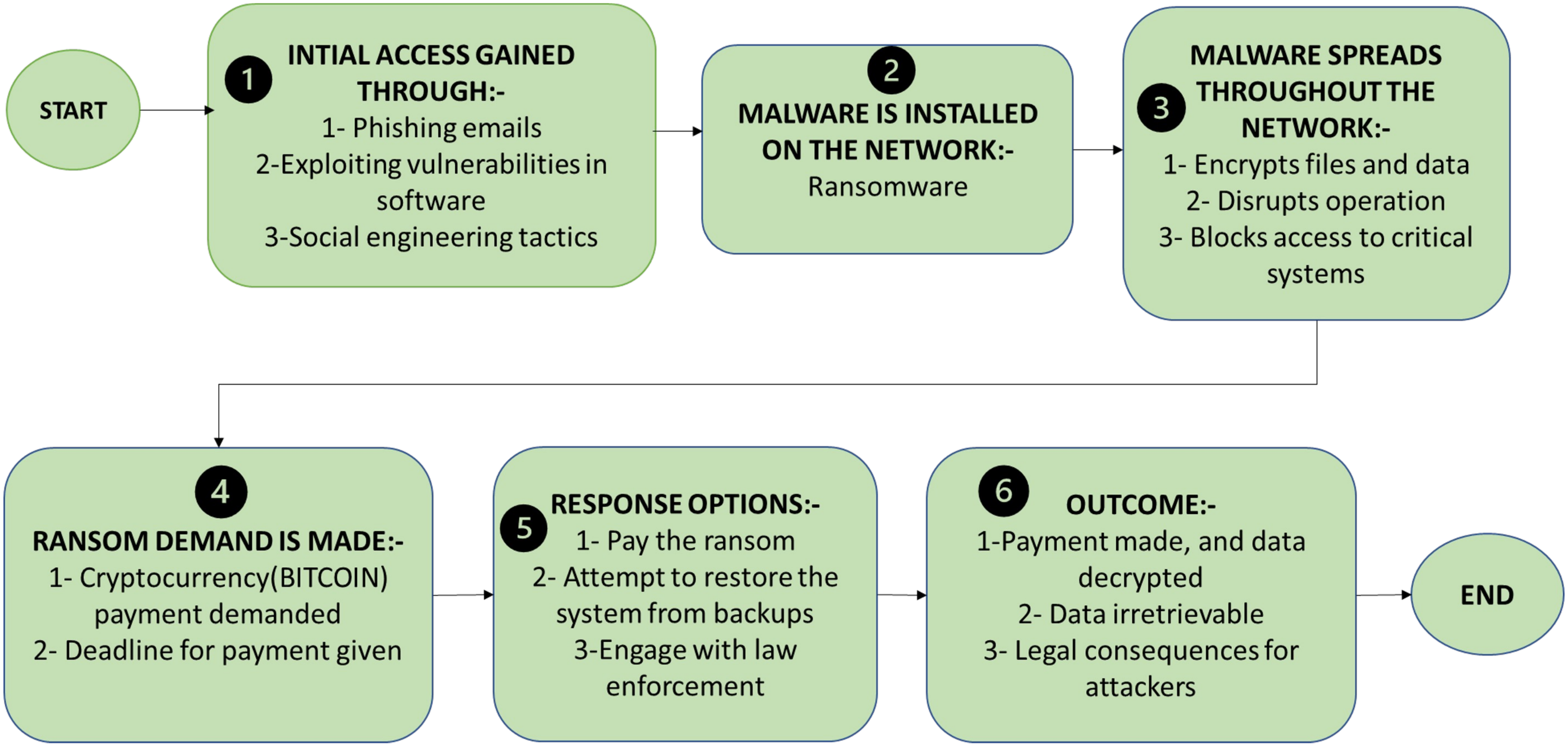
1- Patient Care:- Ransomware attacks can disrupt healthcare organizations' ability to provide patient care.
2- Data Loss:- Data loss from ransomware attacks can have catastrophic consequences for healthcare organizations.
3- Regulatory Compliance:- Ransomware attacks can lead to violations of patient data protection regulations.
4- Reputation Damage:- Ransomware attacks can damage a healthcare organization's reputation, leading to a loss of business.

Structure Diagram For Problem Scenario-2



Command and control server
3 Malware unpacks and executes
4 C&C Communication downloads public key
Public key
2
1 Attacker sends a phishing email
User receives a link and clicks
6 User communication
Bitcoin received
Public key delivered
5 Files get encrypted and user gets ransomware screen

Process Diagram For Problem Scenario-2



START

1 **INTIAL ACCESS GAINED THROUGH:-**

1- Phishing emails

2-Exploiting vulnerabilities in software

3-Social engineering tactics

2 **MALWARE IS INSTALLED ON THE NETWORK:-**

Ransomware

3 **MALWARE SPREADS THROUGHOUT THE NETWORK:-**

1- Encrypts files and data

2- Disrupts operation

3- Blocks access to critical systems

4 **RANSOM DEMAND IS MADE:-**

1- Cryptocurrency(BITCOIN) payment demanded

2- Deadline for payment given

5 **RESPONSE OPTIONS:-**

1- Pay the ransom

2- Attempt to restore the system from backups

3-Engage with law enforcement

6 **OUTCOME:-**

1-Payment made, and data decrypted

2- Data irretrievable

3- Legal consequences for attackers

END

Process diagram for preferred solution- Scenario 2

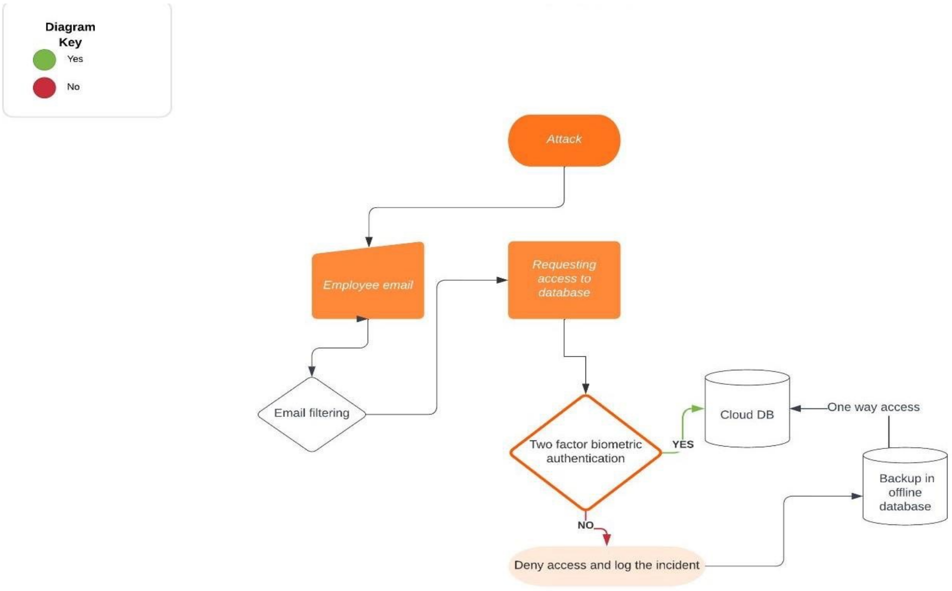


Diagram Key

🟢 Yes

🔴 No

Attack

Employee email

Email filtering

Requesting access to database

Two factor biometric authentication

YES

Cloud DB

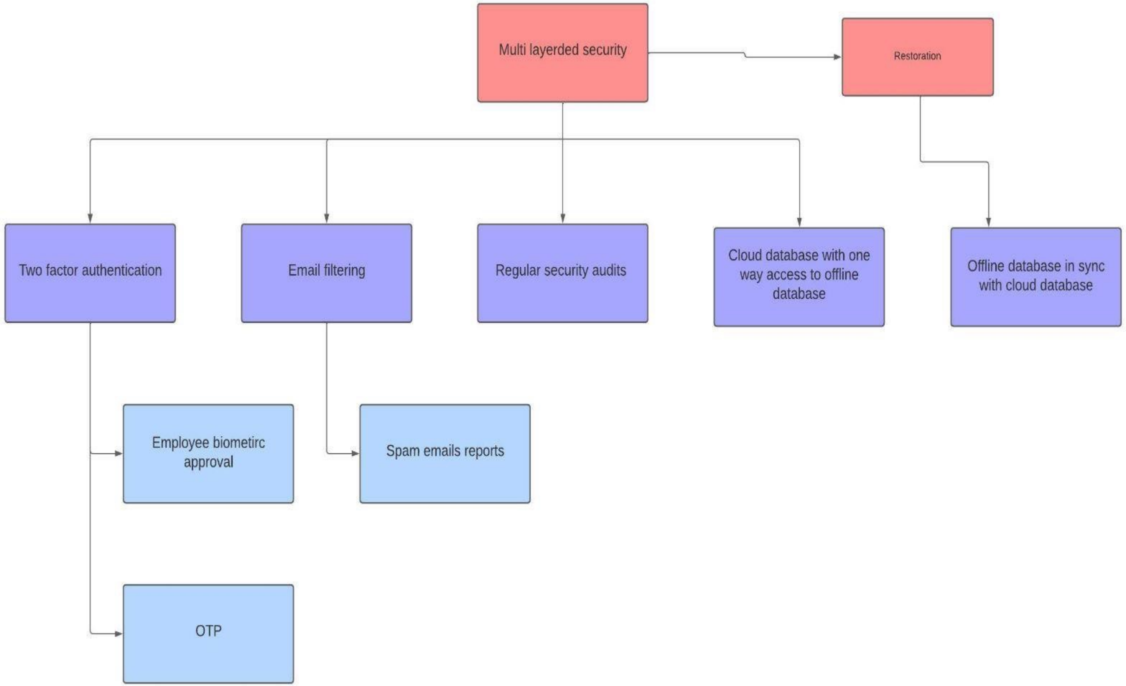
One way access

Backup in offline database

NO

Deny access and log the incident

Structure diagram for preferred solution(scenario2)


Multi layerded security
Restoration
Two factor authentication
Email filtering
Regular security audits
Cloud database with one way access to offline database
Offline database in sync with cloud database
Employee biometirc approval
Spam emails reports
OTP

Trade-off mechanism Preferred Solution(Scenario -2)

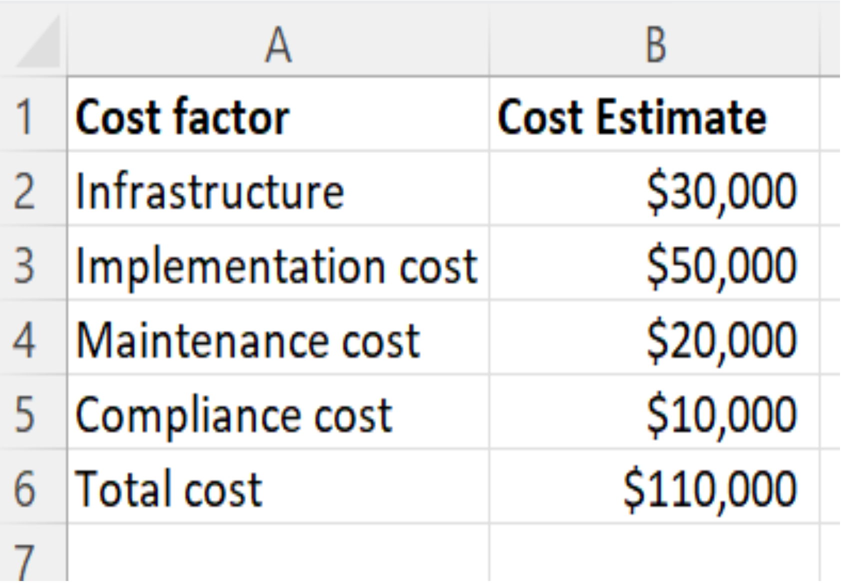
Strengths

- There are three security measures for deployed model.
- There is a scope for restoring data in the event of data breach or ransomware.
- Backup offline database connected to the cloud database, is used to restore the data and helps continuing the support for patients if the cloud data base is compromised.

Weakness

- In some scenarios email filtering protocol may not be sufficient to detect all kinds of junk malicious emails or phishing attacks, which leads to compromise of the system.
- Though there is a backup database, it is connected to one way access protocol, which may not provide full protection against data breaches.
- All employees may not be able to handle sensitive information and prevent security breaches without proper training.

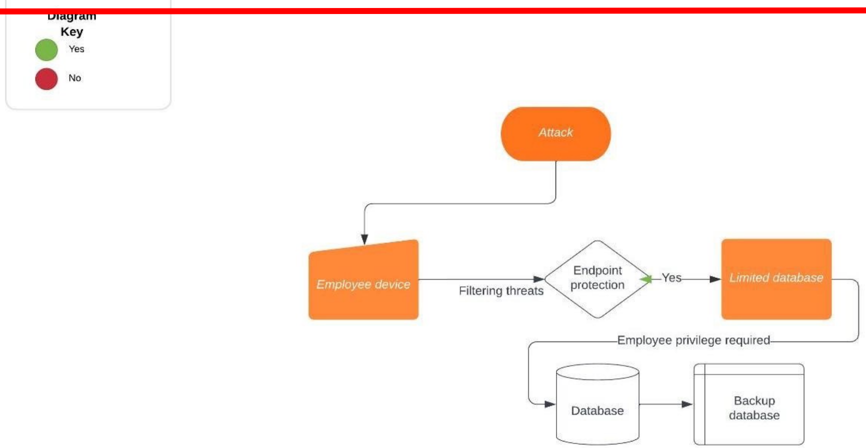
Estimated Cost analysis for preferred solution(Scenario -2)



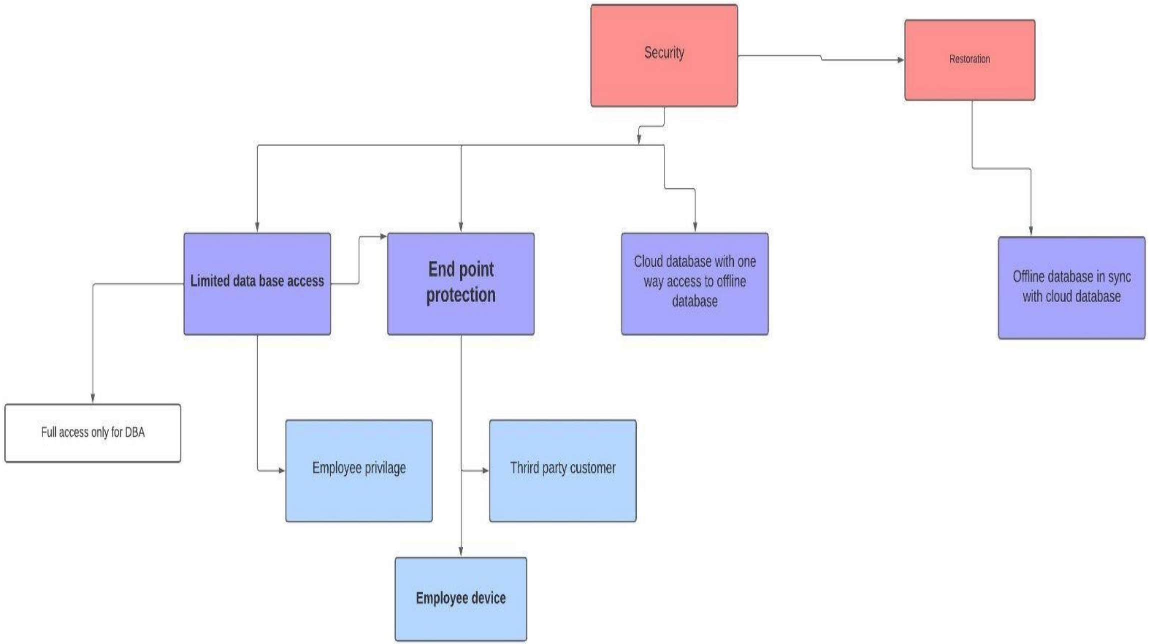
	A	B
1	**Cost factor**	**Cost Estimate**
2	Infrastructure	$30,000
3	Implementation cost	$50,000
4	Maintenance cost	$20,000
5	Compliance cost	$10,000
6	Total cost	$110,000
7		

- Assumed that there are 10k users.

Process diagram for alternative solution(Scenario -2)



Structure diagram for alternative solution (scenario2)



Tradeoffs for Alternative solution (Scenario -2)

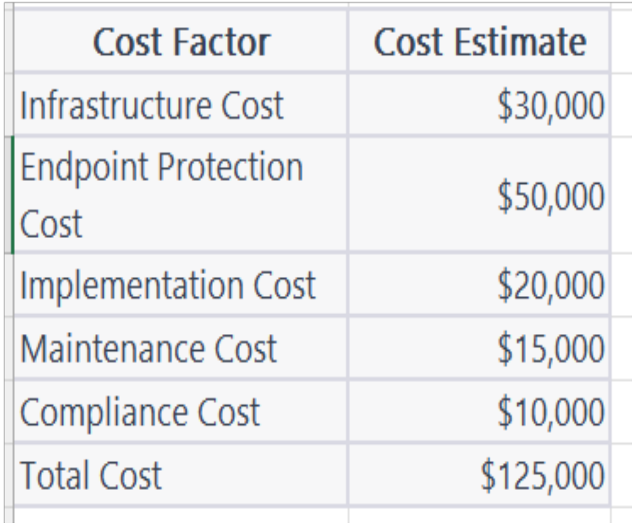
Pros

- End protection software acts as like an antivirus and eliminates the identifies threats.
- In the event of malware compromised device , the hacker cannot have access to the entire database, instead only part of the database is granted for the employee is compromised.
- A backup database is connected to the cloud database, even if the cloud database is compromised.

Cons

- The limited access database may not provide sufficient protection against targeted attacks, where the attacker gains access to multiple employee devices and combines the stolen information to access the entire database.
- Due to lack of specific measures for monitoring and auditing the system, which is difficult to identify security breaches and take appropriate actions.

Estimated cost analysis for alternative solution(scenario 2)



Cost Factor	Cost Estimate
Infrastructure Cost	$30,000
Endpoint Protection Cost	$50,000
Implementation Cost	$20,000
Maintenance Cost	$15,000
Compliance Cost	$10,000
Total Cost	$125,000

- Assumed that there are 10k users
- Maintenance cost include maintaining endpoint protection software and limited access data base
- Compliance cost includes regulatory requirements like HIPAA and GDPR.

Why? Preferred solution over alternative solution(scenario 2)

- **Multi layered security strategy:** alternative solution depends on security measures(Endpoint protection software and limited access database), preferred solution employs a multi layered security strategy with three security measures(Email filtering, two factor authentication and one way access backup database). This makes preferred solution is more secure and less prone to cyberattacks.
- **Comprehensive Protection:** preferred solution addresses a larger spectrum of security concerns. For instance, it uses email filtering to defend against phishing attempts, whereas's alternative solution depends on end point protection software which may not be as effective against phishing attacks.

Contd..

- **Fast recovery time:** In the case of data breach or ransomware attack, preferred solution offers a faster recovery time. This is due to fact that it contains an offline backup database that can be utilized to swiftly restore the data, but alternative solution does not, which may lead to longer recovery times.
- **Better auditing:** preferred solution logs all refused requests for access to the cloud database, it offers better auditing capabilities. This aids in identifying prospective security risks and enhancing current security procedures. This degree of auditing is not provided by alternative solution.

Mechanism of integration for preferred solution (scenario 2)

- Email filtering is the initial security precaution, which identifies and removes phishing emails using established email filtering techniques. This may be done by employing software that checks incoming emails for questionable links, attachments and content before allowing them to reach users inbox
- The two-factor authorization increases security layer of defense. Users are required to supply two pieces of information a password or a unique code deliver to their device, as a part of this security process to validate their identity. As a result, even if the user's login information is stolen, illegal access to the database is prevented.
- Backup database with one-way access is linked to the cloud database. This permits data to flow from the cloud database to the backup database but prohibits any data from returning to the cloud. The backup database can be utilized to recover the data and continue patient assistance in case of data breach or ransomware attack.

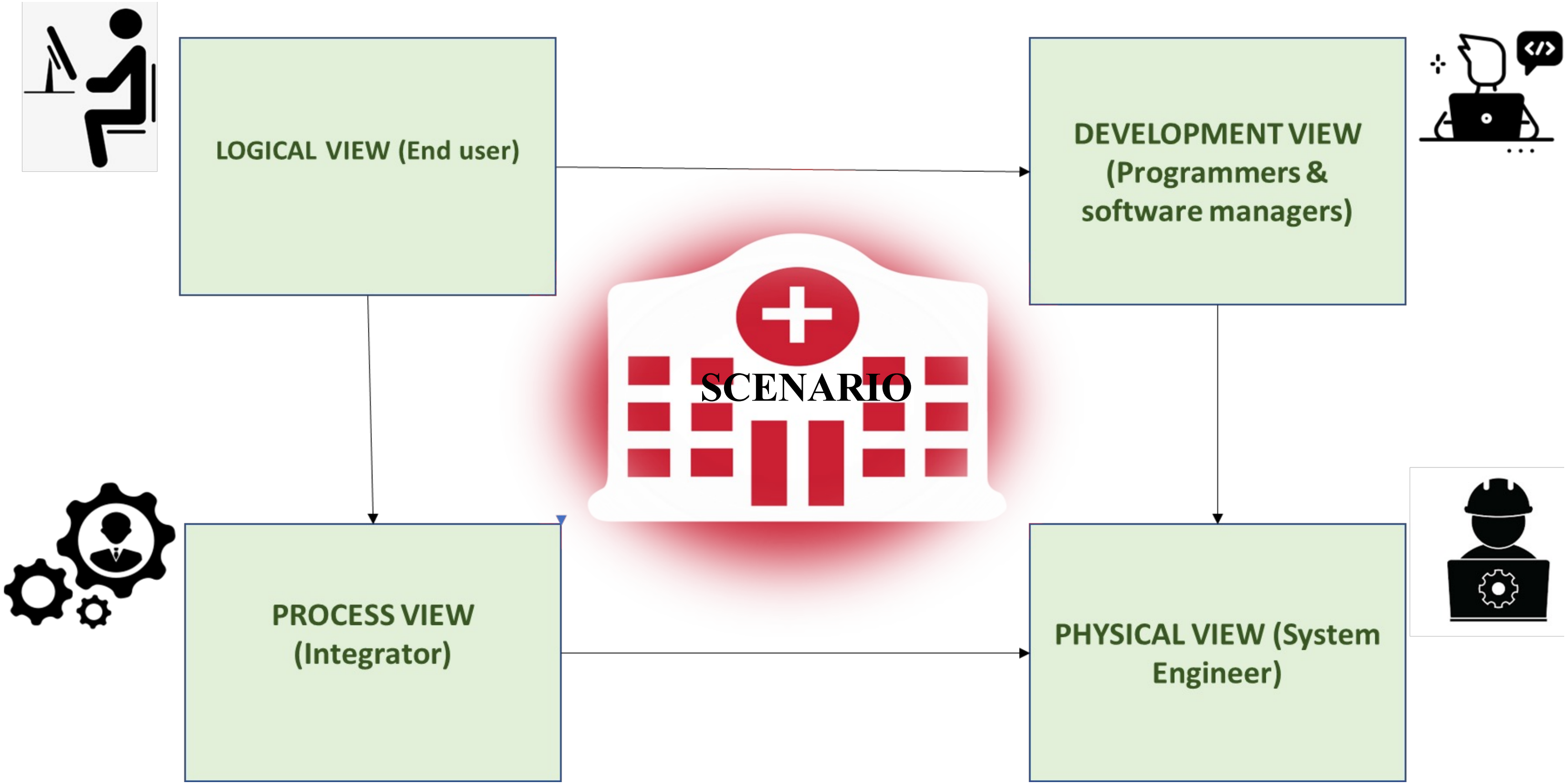
4 + 1 View Model of Architecture based on solution Scenario 2

- The 4+1 architecture model of healthcare organizations is a software architecture model that includes four views - logical, development, process, and physical - plus one scenario view. Here's how this model might be applied to a healthcare organization that experiences a ransomware attack:

  - **Logical View:** The logical view describes the functional requirements and the key software components of the
  - healthcare system.
  - **Development View:** The development view describes the software development process and tools used to build and maintain the healthcare system
  - **Process View:** The process view describes the workflows and business processes that are supported by the
  - healthcare system.
  - **Physical View:** The physical view describes the hardware and infrastructure components that support the healthcare system.
  - **Scenario View:** The scenario view describes how the healthcare system functions in a specific use case or scenario. In the case of a ransomware attack, this view would include a detailed description of the attack vector, the impact on the organization, and the steps taken to contain the attack and restore critical services.

- **Overall, the 4+1 architecture model can help healthcare organizations to better understand their IT systems, identify security vulnerabilities, and develop effective security controls and incident response plans to protect patient data and critical services in the event of a ransomware attack.**

4 + 1 View Model of Architecture



LOGICAL VIEW (End user)

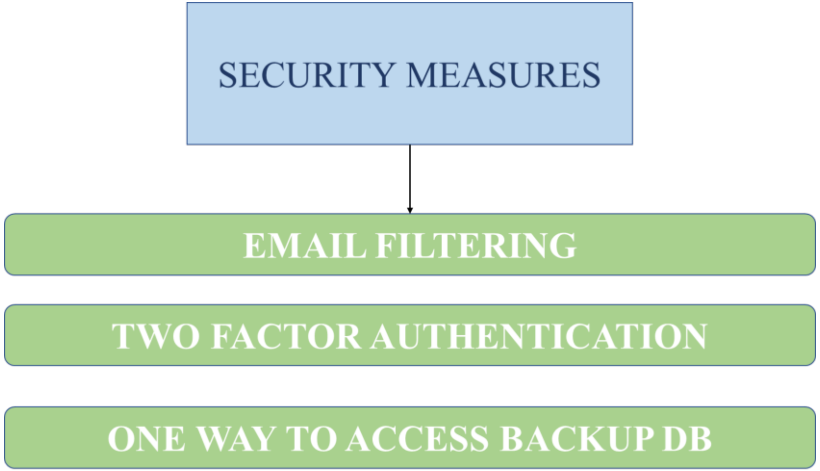
DEVELOPMENT VIEW (Programmers & software managers)

SCENARIO

PROCESS VIEW (Integrator)

PHYSICAL VIEW (System Engineer)

Logical view design on scenario 2



SECURITY MEASURES

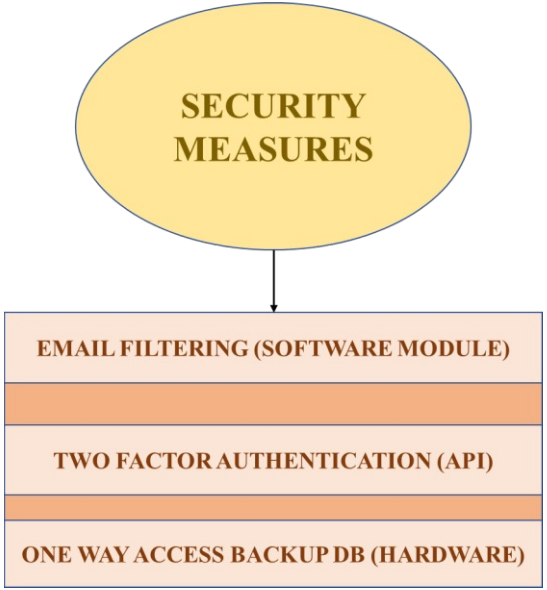
EMAIL FILTERING

TWO FACTOR AUTHENTICATION

ONE WAY TO ACCESS BACKUP DB

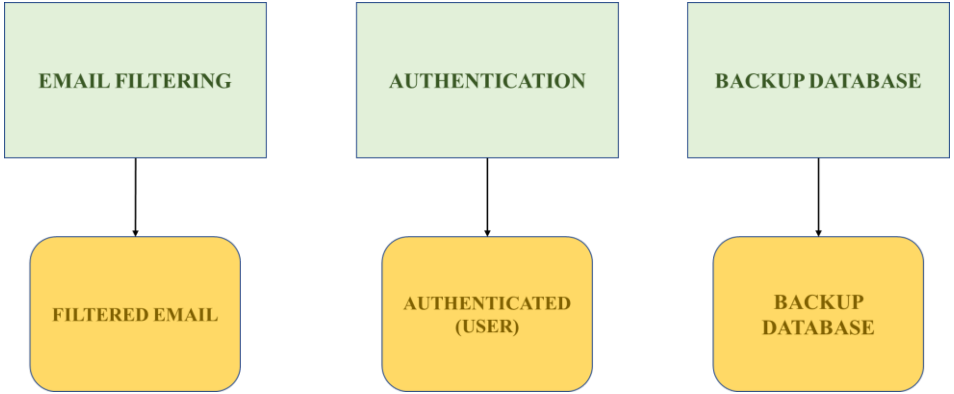
In the case of a ransomware attack, this view would include the security controls that are in place to protect patient data and IT systems, such as access controls, encryption, intrusion detection and prevention, and backup and recovery mechanisms.

Development view design on scenario 2


SECURITY MEASURES
EMAIL FILTERING (SOFTWARE MODULE)
TWO FACTOR AUTHENTICATION (API)
ONE WAY ACCESS BACKUP DB (HARDWARE)

In the case of a ransomware attack, this view would include the software testing and security review processes that are in place to ensure that security vulnerabilities are identified and addressed before deployment.

Process view design on scenario 2



In the case of a ransomware attack, this view would include incident response and business continuity plans that outline how the organization will respond to a security incident and recover critical services.

Final cost estimation-Scenario 1

Cost Item	Estimated Cost
Infrastructure	$100,000
Development	$450,000
Tokenization (creation and distribution)	$50,000
Operational (maintenance, security, auditing)	$100,000
Training	$25,000
Total	$725,000

Factors of cost estimation-Scenario 1

- **Security analysis and planning:** This includes hiring security experts and conducting audits to identify potential threats and vulnerabilities in the system.

- **Implementation of security measures**: The estimated cost for implementing various security measures, including firewalls, intrusion detection systems (IDS), and other security software, is $200,000. This includes the purchase, configuration, and maintenance of these tools.

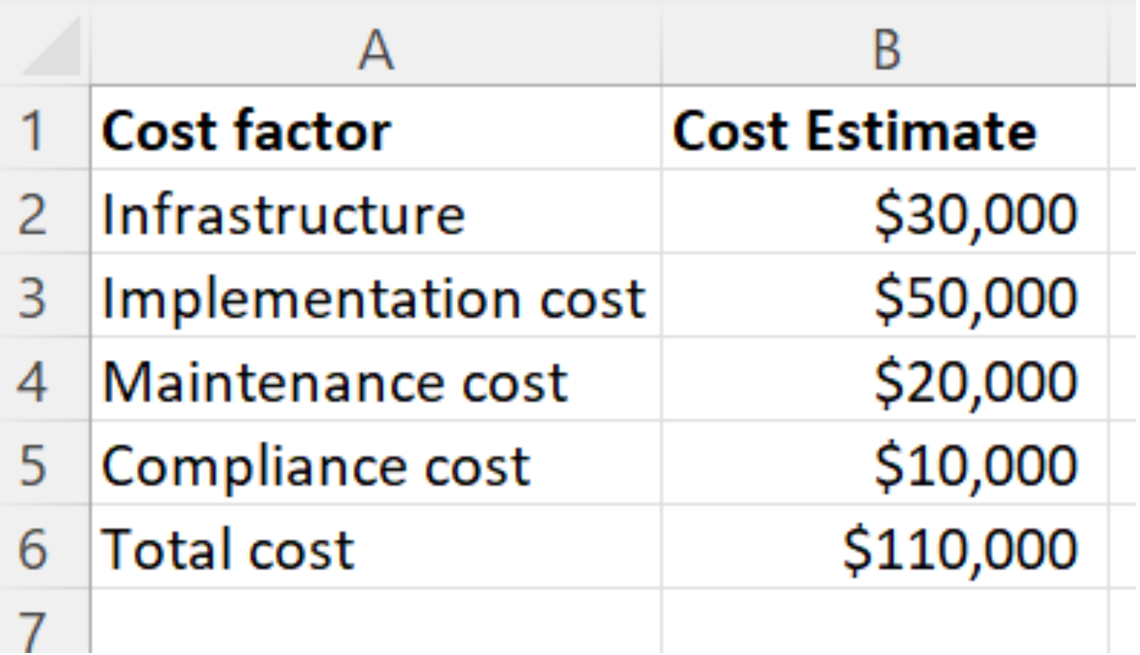
- **Access control and authentication mechanisms**: This includes developing and implementing these measures to ensure that only authorized individuals can access the system.

- **Ongoing monitoring for unusual activity**: This includes hiring security analysts and purchasing monitoring tools to detect and respond to any suspicious activity.

- **Incident response planning**: This includes hiring incident response specialists and conducting drills to test the effectiveness of the plan.

- **Training**: This includes developing and delivering training programs to ensure that all employees are aware of their role in maintaining the security of the system.

Final cost estimation-Scenario 2



Cost factor	Cost Estimate
Infrastructure	$30,000
Implementation cost	$50,000
Maintenance cost	$20,000
Compliance cost	$10,000
Total cost	$110,000

Factors of cost estimation -Scenario 2

- **Infrastructure Cost:** This includes the cost of servers, networking equipment, and storage devices required to deploy the security measures.
- **Implementation Cost:** This includes the cost of implementing the security measures, such as hiring a team of security experts, configuring the email filtering protocols, setting up two-factor authentication, and establishing one-way access to the backup database.
- **Maintenance Cost:** This includes the cost of maintaining the security measures over time, such as updating the email filtering protocols, monitoring the two-factor authentication system, and periodically testing the backup database.
- **Compliance Cost:** This includes the cost of complying with regulatory requirements related to data security, such as HIPAA, GDPR, or PCI DSS.

The three security measures deployed in this scenario are Email Filtering, Two-Factor Authentication, and One-Way Access Backup Database. Each of these measures plays a crucial role in protecting sensitive data from cyber threats. Email Filtering protects against phishing attacks, Two-Factor Authentication secures access to the cloud database, and the One-Way Access Backup Database provides a way to restore data in the event of a breach.

Overall, the cost of deploying these security measures is significant but necessary to protect patient data and comply with regulatory requirements.

THANK YOU