# Q1 Answer

**1.Star Health Insurance:**

Star Health Insurance, One of the India’s Largest Health Insurance companies was hit by Cyber-attack in August 2024. The hacker known as “Xen Zen” has accessed and stolen Highly sensitive customer data including personal health information and insurance claims, which were leaked through telegram Chatbot and website and over 31 million of Customer’s Personal Data exposed due to Vulnerabilities like Insecure Direct Object Reference (IDOR), Credential misuse and Insider risks. (**Chheda, 2025**)

**Comprised Data:**

* Personally Identifiable Information (PII) such as Names, address, date of birth and Social Security Number (Aadhar card)
* Medical histories, diagnoses & treatment and prescriptions details.
* Policy Numbers, Policy Claim history and Coverage details.

**Impact:**

* Star Health Insurance receives ransom demand of $68000 And there is additional cost of Cybersecurity measure, Legal actions & fines from Regulatory bodies. (**Cyber Unfolded,2024**)
* The breach resulted in a loss of market value. After the breach, the stock price of the company fell by 2.5 percent (**Bing and Munsif Vengattil, 2024**)
* Company must suspend some its Service to address the breach

**Attack vector:**

* The attackers gained access to the company’s network through phishing attack part of Social Engineering. The attackers exploited vulnerabilities in Star Health’s systems to extract and exposed large volumes of sensitive data (**Cyber Unfolded,2024**)

**Timeline Diagram:**



<https://sprinto.com/wp-content/uploads/2025/01/the-hackers-MO-1024x399.jpg>

**2. Change HealthCare:**

Change healthcare is a subsidiary of UnitedHealth Group, was affected by Ransomware attack that caused problem in healthcare transactions across United Sates of America (USA). The attack was done by BlackCat/AlphV ransomware group who encrypted key system and stole sensitive healthcare data according to (**Krebsonsecurity.com,2024**)

**Compromised Data:**

According to (**Krebsonsecurity.com,2024**)

* Personally Identifiable Information (PII) such as Name, address, Social Security Number
* Medical record, Diagnoses, Medicines, test results and treatment etc.
* Records including Payment cards, financial and banking records
* Health plans, member/group ID

**Impact:**

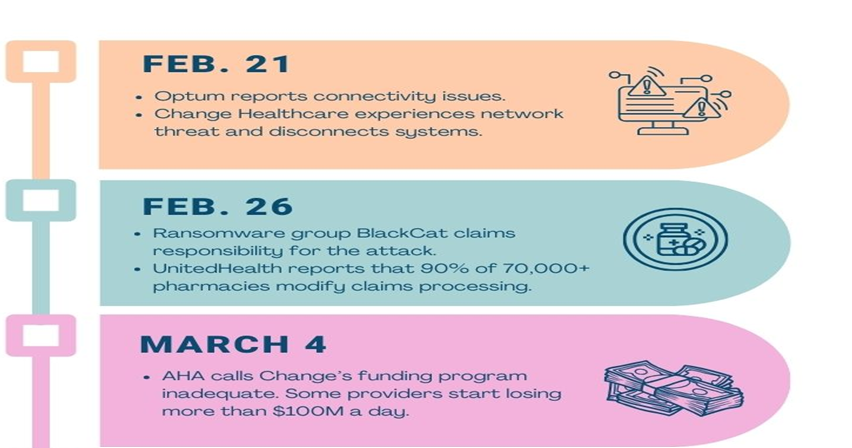
According to Team (2024) Consequences of attack delayed Hospital, Healthcare provider faced revenue loss due to

* claim payments Suspended
* having trouble not able to submit claims
* not able to obtain electronic remittance advice
* According to (**Krebsonsecurity.com,2024**) “Change’s parent firm United Health Group had incurred $1.521 billion in direct breach response costs, and $2.457 billion in total cyberattack impacts.”
* this cost also include ransomware of $22 million to BlackCat and ALPHV in exchange for to destroy the stolen healthcare data.

**Attack Vector:**

According to (**Sean Michael Kerner,2024**) Change Healthcare Network have not been Publicly Disclosed while we induce common to BlackCat/ALPHV tactics includes Gaining access through Remote desktop and brute-force attack against Active Directory (AD).

**Timeline Diagram:**





<https://www.healthleadersmedia.com/sites/hlmp/files/files/timeline.jpg>

# Q2 answer

These Incidents exposed Vulnerabilities in Health insurance sector such as compromising Sensitive data, Disrupting the operations, Causing huge financial loss and Reputational damage. To Address these Cyber-attack, we can apply CNSS Security Model also known as McCumber Cube to our PeopleInsure company.

The CNSS Security Model provides framework for Securing data evaluating the Intersection of Three core dimensions: Information, Technology and people alongside with Triad Security: Confidentiality, Integrity and Availability. Using this model, we can implement in Health insurance sector to target security controls to enhance their cyber security and mitigate future threat

## Intersection1: Information, Integrity and Storage:

**Security Control:** Cryptographic Hashing

**Description:** It Ensures the integrity of stored Health insurance data like policy details, medical records and claims history etc; this information is important for preventing unauthorized changes. Any Modification in this data will lead to major issues such as incorrect billing, altered customer information.

**Implementation:** Cryptographic hashing is a way to verify data integrity by using cryptographic hashing algorithms to generate a unique hash for each data entry. the hash is calculated and stored alongside with data. Regular check can be made by recalculating the hash and it can compare with original hash to identify any difference in hash number.

## Intersection 2: Technology, Confidentiality and Transmission

**Security control:** End to End Encryption

**Description:** This Ensures the Confidentiality of sensitive information protected during Transmission of Sensitive health insurance, also ensures data is not Intercepted during transmission it’s important to prevent data breach.

**Implementation:** End to End Encryption(E2EE) should be encrypted before data has been sent and should be only decrypted after reaching destination. this prevent data being decrypted during transmission and it will be unreadable to unauthorized user.

## Intersection 3: People, Availability and Operations

**Security Control:** Training and Awareness

**Description:**  From two incident we can learn that Threat actor most common way to breach is phishing. By Ensuring Availability of health insurance services need a well-trained people who can manage cybersecurity threat effectively. Human mistake is huge contributor for Security breaches and server down time. So, it’s crucial to invest in training and awareness program E.g. Social Engineering attack and best practice to respond promptly to incident.

**Implementation**: Security Awareness program should be conducted regularly for all employee from customer service to IT team to Our PeopleInsure Employee. This program should cover the topic which includes such as phishing, password management and Incident response.

## Intersection 4: People, Availability and Operations

**Security Control:** Redundancy and Failover Systems

**Explanation**: In Our PeopleInsure, Maintaining Availability during downtime is critical operational especially during Cyberattack, Hardware failure and System crash. Downtime will lead to financial loss, Customer Dissatisfaction etc E.g. Change Healthcare Suffered Huge Financial loss due to Unavailability during Cyber-attack.

**Implementation:**  Establish Redundant Infrastructure in Key areas like Application and Database Servers, If One System fails another can Take over and it will minimize the downtime. Establish Backup and Recovery process quickly to Restore Service after Incident

# Q3 answer

In Address Cyber Attack and prevent our organization from attack like Star Health Insurance and Change Healthcare Ransomware attack we must Establish key Security role with Defined Responsibilities to ensure strong Cybersecurity Posture

**Chief Information Security Officer (CISO):**

* Develop and Implement Cybersecurity Strategies which is aligned with Framework such as GDPR and HIPAA
* Ensure Risk Management and Compliance

**Data Protection Officer (DPO):**

* Oversees Data Protection, privacy and Encryption policies to prevent from data breaches
* Implement access control to secure sensitive health data

**Identity and Access Management (IAM) Specialist:**

* Create and Manage Role-Based Access Control (RBAC) a Multi-Factor Authentication (MFA)
* Prevent from unauthorized access and reduce insider threat

**Security Operation Centre (SOC) team:**

* Monitor Real time network traffic and respond to unusual cyber incident or activities
* Conduct forensic investigation to detect and neutralize threat

**Incident Response (IR) Team:**

* Develop a Incident Response plan(IRP) and Minimize Operation disruption during attack like ransomware incident

**Conclusion:**

By Establishing Roles, Our Organization ensure Security, Prevention and Disaster Recovery while increasing Confidentiality , Integrity and Availability (CIA) complying with Industry Regulations

# References

Bing, C. and Munsif Vengattil (2024). *Exclusive: Hacker Uses Telegram Chatbots to Leak Data of Top Indian Insurer Star Health*. [online] Reuters. Available at: <https://www.reuters.com/technology/cybersecurity/hacker-uses-telegram-chatbots-leak-data-top-indian-insurer-star-health-2024-09-20/>.

Chheda, H. (2025). *Star Health Insurance Data Breach: Lessons in Cybersecurity*. [online] Sprinto. Available at: <https://sprinto.com/blog/star-health-insurance/>.

Cyber Unfolded. (2024). *Star Health Cyberattack: a Detailed Analysis of the $68,000 Ransom Demand and Data Leak*. [online] Available at: [https://cyberunfolded.in/blog/star-health-cyberattack-a-detailed-analysis-of-the-68-000-ransom-demand-and-data-leak](https://cyberunfolded.in/blog/star-health-cyberattack-a-detailed-analysis-of-the-68-000-ransom-demand-and-data-leak?utm_source=chatgpt.co) [Accessed 20 Feb. 2025].

Krebsonsecurity.com. (2024). *Change Healthcare Breach Hits 100M Americans – Krebs on Security*. [online] Available at: <https://krebsonsecurity.com/2024/10/change-healthcare-breach-hits-100m-americans/>.

Sean Michael Kerner (2024). *The Change Healthcare attack: Explaining How It Happened*. [online] WhatIs. Available at: <https://www.techtarget.com/whatis/feature/The-Change-Healthcare-attack-Explaining-how-it-happened>.

Team, H. (2024). *Understanding the Change Healthcare Breach and Its Impact on Security Compliance*. [online] Hyperproof. Available at: <https://hyperproof.io/resource/understanding-the-change-healthcare-breach/>.