PRACTERA FINAL PRESENTATION

TEAM 7
Raghav Khosla,
Dhruvi Rajput,
Rafid Khan,
Ali Mohamud

TABLE OF CONTENTS

Global Cyber Risk Summary

Executive Summary

In 2024, businesses face significant cyber threats, owing to the rapid technological evolution.

The major global threats predicted for 2024 are **ransomware** attacks, **supply chain** attacks and **data breaches**. Ransomware attacks are more sophisticated, and supply chain vulnerabilities are a focal point. Ensuring that data privacy regulations are met is extremely important, and the issue of human vulnerabilities remains a concern.

Emerging technologies introduce new challenges. To safeguard against these threats, businesses must adopt proactive cybersecurity strategies, including regular assessments, employee training, and investments in advanced technologies. Staying vigilant and adaptive is crucial in the dynamic cyber landscape.

Threat Vectors

Malicious Insiders

Missing or Poor Encryption

Phishing

Ransomware

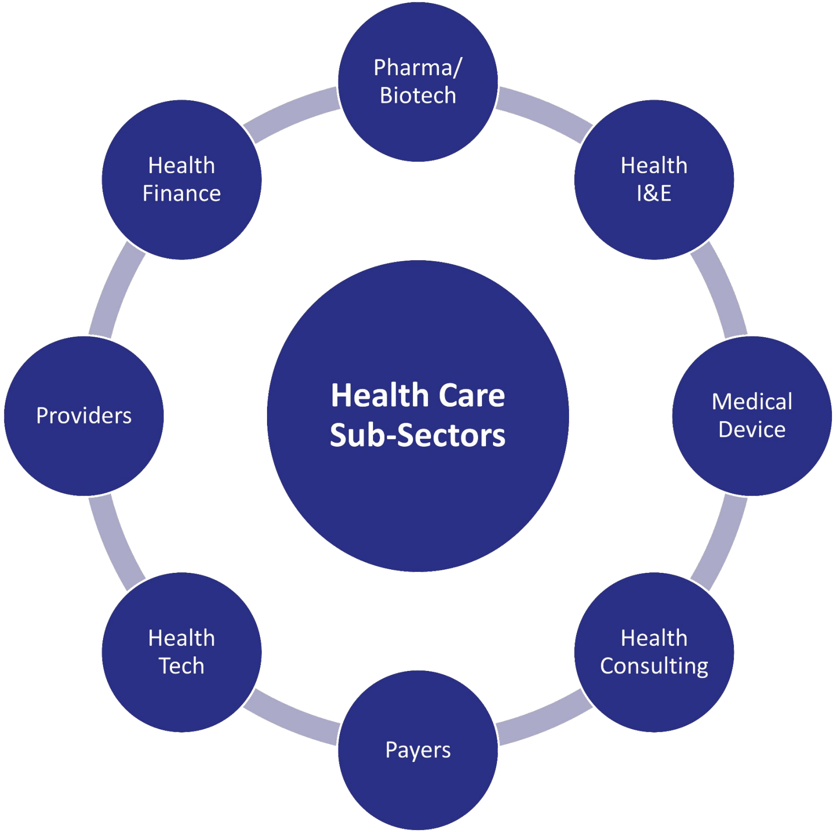
Business Environment

Supply Chain	Sales & Marketing	Legal & Compliance	Operations
Breach discloses private information, ruins supply chain partners' trust, and interrupts operations	Damage to reputation from negative publicity will deteriorate public trust and diminish customer confidence	Non-compliance may result in substantial fines and legal liability for executives	Overwhelming IT systems with traffic to disrupt (DDoS) or halt normal operations, affecting online services, websites, and network availability

Risks and Resilience in Healthcare & Insurance Tech

Key Points:

- The healthcare and insurance tech industries are rapidly evolving, driven by innovation and changing consumer demands.
- This dynamic environment also presents a unique set of risks for companies operating in these sectors.
- Understanding and mitigating these risks is crucial for long-term success and sustainability.



Health Care Sub-Sectors

Pharma/ Biotech

Health I&E

Medical Device

Health Consulting

Payers

Health Tech

Providers

Health Finance

Specific Risks to Take Into Account : Healthcare

- **Cybersecurity Breaches:** Sensitive patient data is a prime target for attackers, with potentially devastating consequences.
- **Regulatory Changes:** Frequent updates to healthcare laws and regulations can disrupt operations and compliance.
- **Technological Disruption:** Emerging technologies like AI and telemedicine could render existing business models obsolete.
- **Insider Threats:** Healthcare organizations face unique risks from malicious actors within their own workforce, who may have access to sensitive data and systems. Implementing access controls, data loss prevention tools, and strong security awareness training can mitigate these risks.
- **Supply Chain Vulnerabilities:** Healthcare relies on a complex network of vendors and suppliers, each of which poses a potential security risk. Organizations need to assess their cyber risk posture of vendors and implement security measures throughout the supply chain.

Specific Risks to Take Into Account : Insurance Tech

- **Fraud and Abuse:** The digital nature of insurance transactions creates new opportunities for fraudulent activity.
- **Algorithmic Bias:** Unfair or biased algorithms used in underwriting and claims processing can lead to discrimination.
- **Data Privacy Concerns:** Balancing the use of data for personalization and risk assessment with consumer privacy is a critical challenge.
- **Ransomware Attacks:** Insurance companies are increasingly targeted by ransomware attacks, which can cripple their operations and lead to significant financial losses. Investing in robust data backups, incident response plans, and cybersecurity training is crucial.
- **Data Breaches Exposing Financial Information:** Insurance companies manage sensitive financial data, making them targets for data breaches. Implementing layered security, encryption, and robust data governance practices can help protect this information.

SECURITY BREACH: CASE STUDY

- Health Insurance giant hit by Cyber attack
- Organization Name: Blue Shield of California
- Attack Type: Identity Theft/Data Theft
- Date of notification: November 17, 2023
- Date of attack: May 28-31, 2023
- Location: US

Organization Overview

- Blue Shield of California is an independent member of the Blue Shield Association
- Provides for a non-profit health plan dedicated to providing Californians with access to high-quality health care at an affordable price

Attack Overview

- Data hack may have compromised Blue Shield customers' confidential information
- "Confidential information of people who have Blue Shield of California vision benefits may have been compromised after hackers breached a software program used by one of its vendors"
- Last year, Health insurance giant Blue Shield joined the growing number of victims of the MOVEit data breach, which has impacted businesses worldwide
- The attack potentially exposed records of millions of patients to cybercriminals
- The attack was part of a broader wave of cybersecurity breaches by a ransomware group known as CLOP which exploited a vulnerability of an enterprise digital file-moving software known as MOVEit, which allowed hackers to steal data

Attack timeline

- Vendor discovers data breach in August 2023
- Vendor finds that an unauthorised user has tapped into information in the MOVEit server
- Unknown system vulnerability has been exploited and the insurer becomes a victim of the data breach
- Vendor immediately takes the server offline, begins investigation, and reports to FBI
- Vendor notifies Oakland-based Blue Shield on September 1
- Investigation reveals that the third-party extracted data from the server between May 28 and May 31, 2023
- A notice on the Oakland-based insurer's website dated November 17 stated that personal information was compromised
- Only the MOVEit server was compromised, with Blue Shield saying their internal emails and systems were not accessed

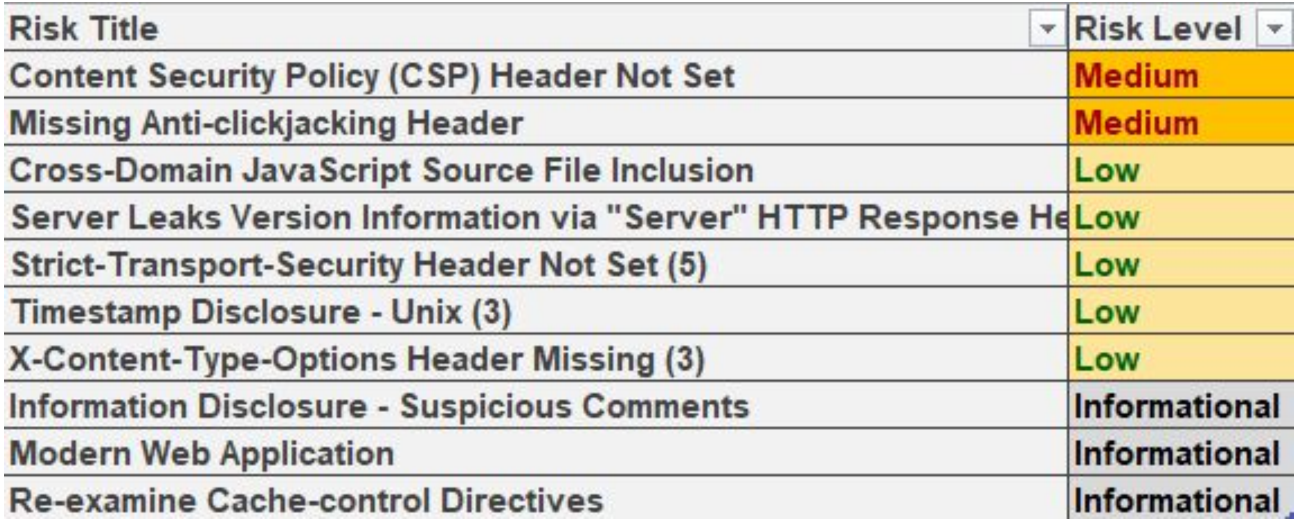
Impact of the Breach

- Server breach puts 4.5M patient records at risk
- Blue Shield has not disclosed how many of its 4.5 million customers have vision plans and may have had their data taken
- Blue Shield determined that the information affected may have included: member name, member date of birth, address, subscriber ID number, subscriber name, subscriber date of birth, subscriber Social Security number, group ID number, vision provider’s name, patient ID number, vision claims number, vision related treatment and diagnosis information and vision related treatment cost information

What could have been done to prevent such an attack?

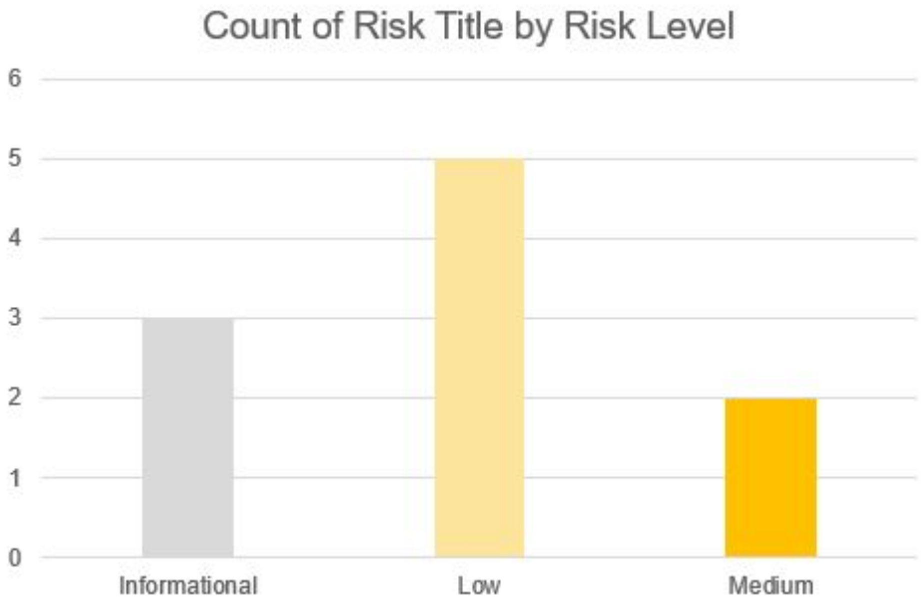
- Best Practice - Carefully review your credit reports regularly and account statements & notify law enforcement of suspicious activity.
- You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months.
- Fraud Alert - You may want to consider placing a fraud alert on your credit file.
- Security Freeze – You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze.

Risks and Recommendations



Risk Title	Risk Level
Content Security Policy (CSP) Header Not Set	Medium
Missing Anti-clickjacking Header	Medium
Cross-Domain JavaScript Source File Inclusion	Low
Server Leaks Version Information via "Server" HTTP Response He	Low
Strict-Transport-Security Header Not Set (5)	Low
Timestamp Disclosure - Unix (3)	Low
X-Content-Type-Options Header Missing (3)	Low
Information Disclosure - Suspicious Comments	Informational
Modern Web Application	Informational
Re-examine Cache-control Directives	Informational

Risks and Recommendations



Risks and Recommendations

Medium level threats

1) Content Security Policy (CSP) Header Not Set: Within the HTTPS response, if the content security policy header isn't set, this leaves the website vulnerable to various attacks such as cross-site scripting, clickjacking, and data injection.
   a) Our recommendation is to increase security defense by adding the Content security policy and configuring it so that there are a set of rules on allowed content sources.

2) Missing Anti-clickjacking Header: Without clickjacking headers, users are not protected from Clickjacking attacks which is when users are tricked into clicking something they didn't intend to click. If successful, attackers could potentially carry out unauthorized actions, install malware, and take over user accounts.
   a) What we recommend is to add an anti-clickjacking header to your HTTP responses.

Risks and Recommendations

a) For the low and information level threats, it depends on many factors such as tolerance for potential consequences, the resources required for mitigation, and whether existing controls are effective. We recommend consulting with security experts to receive personalized insights and guidance on risk management tailored to the company’s specific context, considering the unique priorities, risk tolerance, and operational characteristics.

Thank you