PRACTERA FINAL PROJECT REPORT -

Dhruvi Rajput, Raghav Khosla, Ali Mohamud, Rafid Khan

ABSTRACT

Navigating cyber threats: HealthHub Connect, a fictitious company, faces a data minefield of evolving ransomware, phishing, and industry-specific risks. A competitor's breach shows the stakes. Learn how to build a security fortress, and protect sensitive data.

1. Global Summary of Top Cyber Risks for 2023/24

1.1 Ransomware:

- Rising Popularity: According to Cybersecurity Ventures, ransomware attacks are predicted to cause $20 billion in damages globally by 2023. (Source: Cybersecurity Ventures, 2023 Ransomware Damages Report)
- Evolving Tactics: Double extortion, targeting backups, and leveraging supply chain vulnerabilities are becoming increasingly common tactics. (Source: Palo Alto Networks, 2023 Unit 42 Ransomware Threat Report)
- Broad Impact: All industries are vulnerable, with healthcare, finance, and critical infrastructure experiencing particularly high attack rates. (Source: Cisco Talos, 2023 Cybersecurity Threat Report)

1.2 Phishing and Social Engineering:

- Prevalent and Effective: Verizon's Data Breach Investigations Report 2023 found that 82% of data breaches involved phishing. (Source: Verizon, 2023 Data Breach Investigations Report)
- Remote Work Exploits: Increased reliance on email and online communication creates openings for attackers. (Source: Microsoft, 2023 Work Trends Index)
- Targeted Attacks: Employees with access to sensitive data are prime targets for social engineering attempts. (Source: IBM X-Force Threat Intelligence Index, 2023)

1.3 Cloud Security:

- Misconfiguration Risks: A 2022 Ponemon Institute study found that 79% of organizations experienced at least one cloud security incident in the past year. (Source: Ponemon Institute, 2022 Cloud Security Misconfiguration Report)
- Data Breach Target: Cloud storage holds vast amounts of valuable data, making it a lucrative target for attackers. (Source: Cloud Security Alliance, 2023 Top 13 Threats in Cloud Computing)
- Insider Threats: Cloud access for employees introduces potential vulnerabilities if proper controls are not implemented. (Source: SANS Institute, 2023 Cloud Security Survey)

1.4 Supply Chain Attacks:

- Compromised Software: Third-party software vulnerabilities can be exploited to breach multiple organizations. (Source: SolarWinds supply chain attack, 2020)

- Ransomware Targeting Supply Chains: Attacks like Kaseya VSA in 2021 can cripple entire industries through interdependent systems. (Source: REvil ransomware attack on Kaseya VSA, 2021)
- Mitigation Challenges: Complex supply chains with numerous vendors make identifying and addressing vulnerabilities difficult. (Source: MIT Technology Review, 2023 The Supply Chain Security Mess)
- One notable example of a supply chain attack is the SolarWinds cyberattack in December 2020. The attack compromised the software supply chain of SolarWinds, a company that provides IT management and monitoring software.

1.5 Mobile Malware:

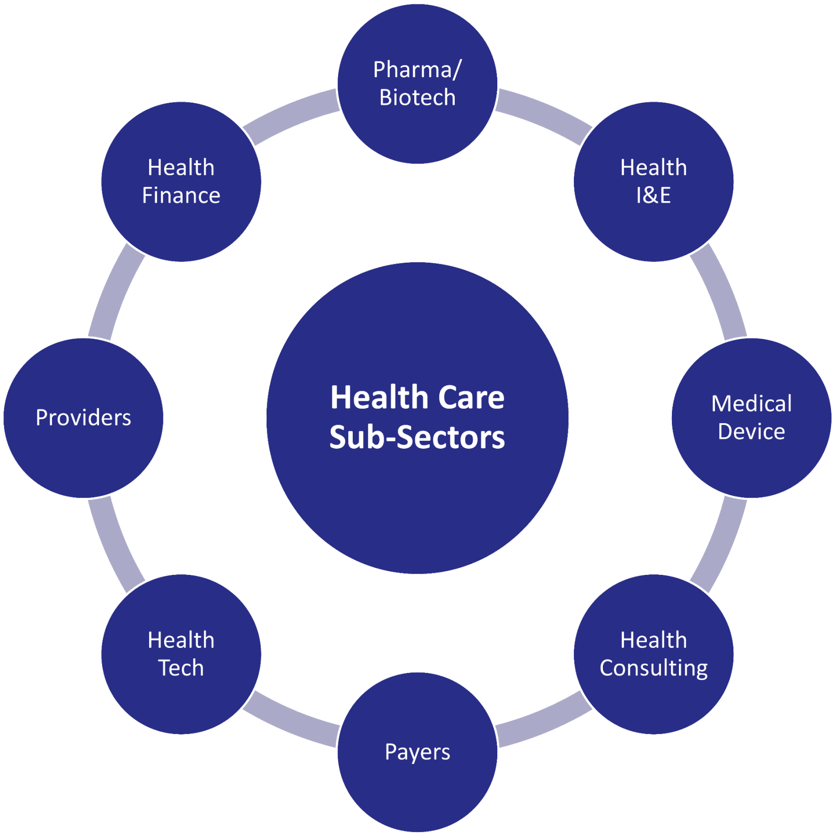
- Sophistication on the Rise: Spyware, banking trojans, and mobile ransomware are becoming increasingly sophisticated. (Source: McAfee Labs, 2023 Mobile Threat Report)
- BYOD Risks: Employee-owned devices used for work can introduce security vulnerabilities if not properly secured. (Source: Gartner, 2023 BYOD Security Best Practices)
- Lack of Awareness: Users may not be aware of mobile security threats and fall victim to malware or phishing attacks. (Source: Google, 2023 Android Security Whitepaper)

2. Industry Specific Risks (Insurance, Healthcare, and Tech)

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.



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.

3. 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 unauthorized 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.

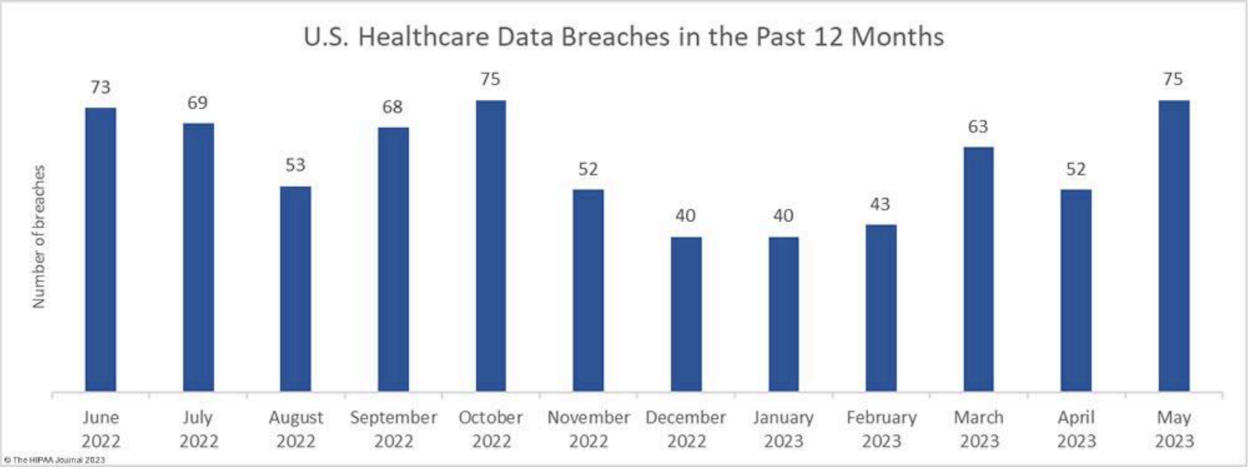
Impact of the Breach

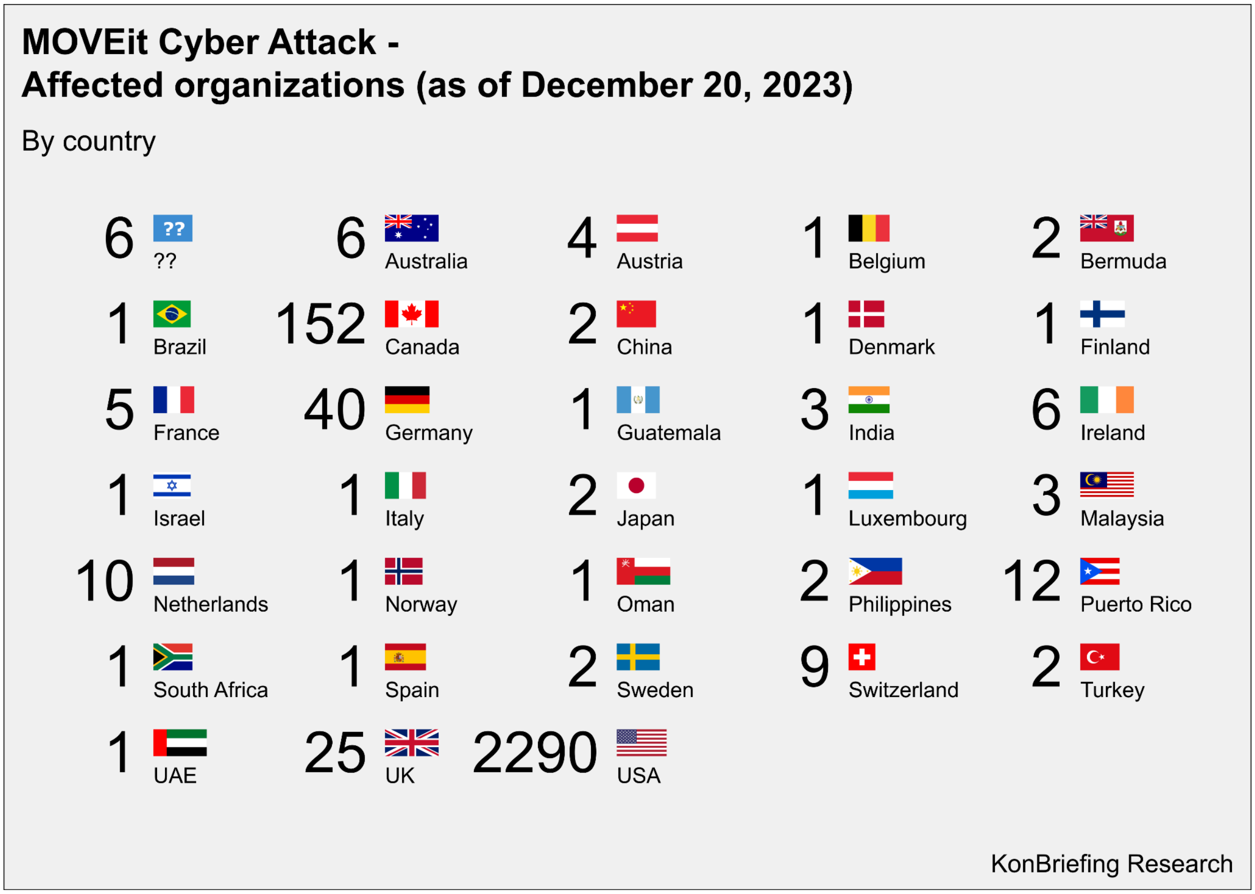
- Server breach puts 4.5M patient records at risk.
- Blue Shield has not disclosed how many of its 4.5 million customers have vision plans and may have had their data taken.
- Blue Shield determined that the information affected may have included: member name,

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.





MOVEit Cyber Attack -
Affected organizations (as of December 20, 2023)

By country

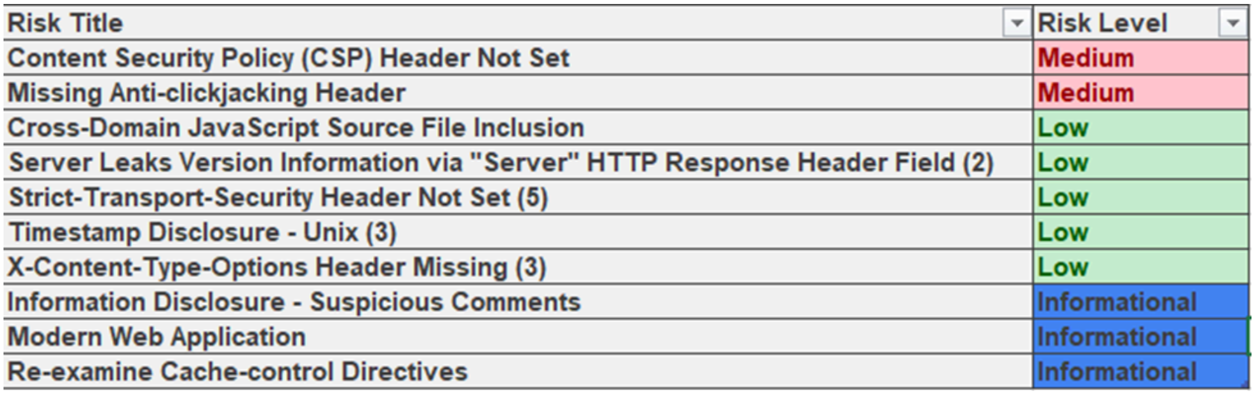
6	??
6	Australia
4	Austria
1	Belgium
2	Bermuda
1	Brazil
152	Canada
2	China
1	Denmark
1	Finland
5	France
40	Germany
1	Guatemala
3	India
6	Ireland
1	Israel
1	Italy
2	Japan
1	Luxembourg
3	Malaysia
10	Netherlands
1	Norway
1	Oman
2	Philippines
12	Puerto Rico
1	South Africa
1	Spain
2	Sweden
9	Switzerland
2	Turkey
1	UAE
25	UK
2290	USA

KonBriefing Research

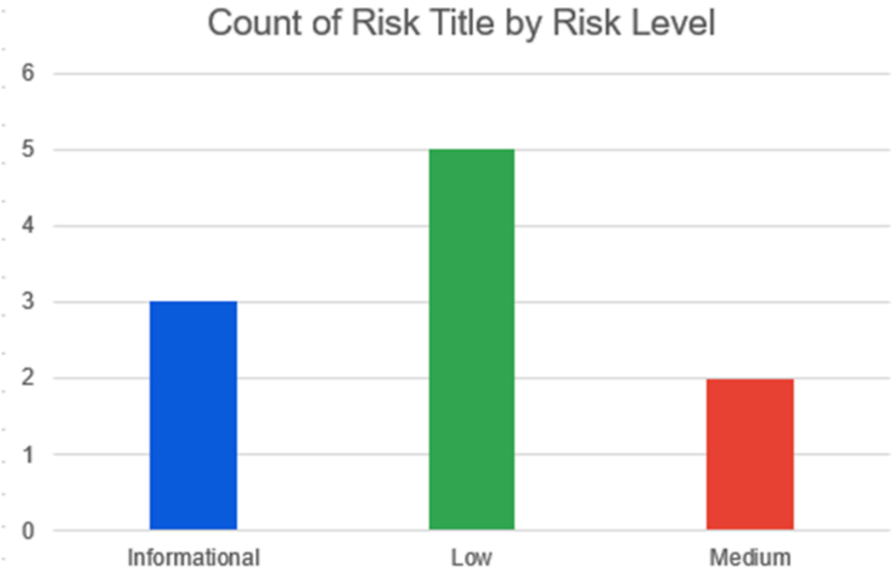
Conclusion from Sections 2 and 3:

Cybersecurity threats pose a significant challenge for all businesses, especially those handling sensitive data like HealthHub Connect. By understanding the top cyber risks, implementing proactive security measures, and maintaining a vigilant posture, HealthHub Connect can protect its business, its clients, and their employees from potential cybersecurity attacks. By learning from competitor incidents and adopting best practices, HealthHub Connect can build a robust and resilient security posture that safeguards its valuable data and ensures the trust of its stakeholders.

4. Vulnerability Scan Assessment:



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 Header Field (2)	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



Recommendations:

Medium level threats :

- 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. Our recommendation is to increase security defense by adding the Content security policy and configuring it so that there are set of rules on allowed content sources.

For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

- 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. What we recommend is to add an anti-clickjacking header to your HTTP responses.

Steps on adding an anti-clicker on your HTTP responses:

1. Identify what server you are using (Apache, Nginx, Microsoft IIS, etc.)

2. Add the X frame options header to your HTTP responses

   a. This header has three possible values: Deny, SAMEORIGIN and ALLOW FROM uri

   Example of how to add the X frame options header to an Apache. access file:

   Header always append X-Frame-Options SAMEORIGIN

3. Test your website.

   a. OWASP ZAP, BURP Suite, Clicking test

Low level threats

- Cross-Domain JavaScript Source File Inclusion
- Server Leaks Version Information via "Server" HTTP Response Header Field (2)
- Strict-Transport-Security Header Not Set (5)
- Timestamp Disclosure - Unix (3)
- X-Content-Type-Options Header Missing (3)

Informational Level Threats

- Information Disclosure - Suspicious Comments
- Modern Web Application
- Re-examine Cache-control Directives

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 recommended 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.

Conclusion

Cybersecurity threats pose a significant challenge for all businesses, especially those handling sensitive data like HealthHub Connect. By understanding the top cyber risks, implementing proactive security measures, and maintaining a vigilant posture, HealthHub Connect can protect its business, its clients, and their employees from potential cybersecurity attacks. By learning from competitor incidents and adopting best practices, HealthHub Connect can build a robust and resilient security posture that safeguards its valuable data and ensures the trust of its stakeholders.

Sources

- Cybersecurity Ventures (2023). Ransomware Damages Report. https://cybersecurityventures.com/ransomware-will-strike-every-2-seconds-by-2031/
- Palo Alto Networks (2023). Unit 42 Ransomware Threat Report. https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html
- Cisco Talos (2023). Cybersecurity Threat Report. https://blog.talosintelligence.com/recent-cyber-attack/
- Verizon (2023). Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
- Microsoft (2023). Work Trends Index. https://www.microsoft.com/en-us/worklab/work-trend-index
- IBM (2023). X-Force Threat Intelligence Index. https://www.ibm.com/reports/threat-intelligence
- Ponemon Institute (2022). Cloud Security Misconfiguration Report. https://www.upguard.com/blog/cloud-misconfiguration
- Cloud Security Alliance (2023). Top 13 Threats in Cloud Computing. https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/

- SANS Institute (2023). Cloud Security Survey. https://www.sans.org/webcasts/sans-2022-cloud-security-survey/

- SolarWinds supply chain attack (2020) https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
- REvil ransomware attack on Kaseya VSA (2021) https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/
- MIT Technology Review (2023). The Supply Chain Security Mess. https://micromasters.mit.edu/scm/
- McAfee Labs (2023). Mobile Threat Report. https://www.mcafee.com/en-us/resources/cybersecurity-reports-and-guides.html
- Gartner (2023). BYOD Security Best Practices. https://www.gartner.com/en/documents/3992495
- Google (2023). Android Security Whitepaper. https://cloud.google.com/docs/security
- The 10 Biggest Cyber Security Trends In 2024 Everyone Must Be Ready For Now:https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now/
- https://www.blueshieldca.com/en/home/about-blue-shield
- BlueShield Cyber Attack (2023)https://www.latimes.com/business/story/2023-12-01/blue-shield-cyberattack-data-breach
- https://www.sfchronicle.com/health/article/hackers-stole-confidential-data-california-blue-18527505.php
- https://news.blueshieldca.com/cybersecurity-attack-on-vendors-files-may-have-impacted-blue-shield-of-california-member-data
- https://www.acunetix.com/vulnerabilities/web/content-security-policy-csp-not-implemented/
- https://www.iothreat.com/blog/missing-anti-clickjacking-header
- WHAT IS A SUPPLY CHAIN ATTACK?(2023): https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/