CAPLINE
HEALTHCARE MANAGEMENT

THE FEBRUARY 2024 CYBERATTACK ON CHANGE HEALTHCARE:

A CASE STUDY IN HEALTHCARE CYBERSECURITY VULNERABILITIES

Inc. 5000 2018 2019 2020 2022

BBB ACCREDITED BUSINESS A+

Google ★★★★★

facebook ★★★★★

Google Partner

Abstract

The impact of the February 2024 cyberattack on Change Healthcare reverberated across the healthcare industry. This case study delves deep into the depths of the attack, assessing its probable attack vectors, its multidimensional consequences, and the bigger picture it paints for healthcare cybersecurity. We will examine measures that might have been taken to avert or reduce such attacks and suggest some courses of action that are feasible for both health service providers and Change Healthcare in order to create stronger defense systems.

Change Healthcare and the Healthcare Ecosystem

Change Healthcare is a major player in the intricate system of healthcare financing. Their services extend to providers, payers, and pharmacies, covering all parts of the claims process, data analytics, and network security solutions. In this way, their core function ensures that streamlined healthcare operations can take place and help control insurance claims, allowing for the secure exchange of medical data and reliable cybersecurity solutions. This reliance on a centralized platform also leaves the operation vulnerable to a single point of failure while providing a wider surface area for cyber-criminals to attack easily.

The Rise and Fall of BlackCat

In December 2023, a glimmer of hope emerged for healthcare providers across the globe. The Department of Justice (DOJ), in a joint effort with the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), announced a major disruption of the BlackCat/ALPH-V/Noberus ransomware group. This notorious cybercrime organization had inflicted significant damage, extorting millions of dollars from its victims.

The multi-pronged attack by the DOJ and its partners crippled BlackCat's operations in several ways:

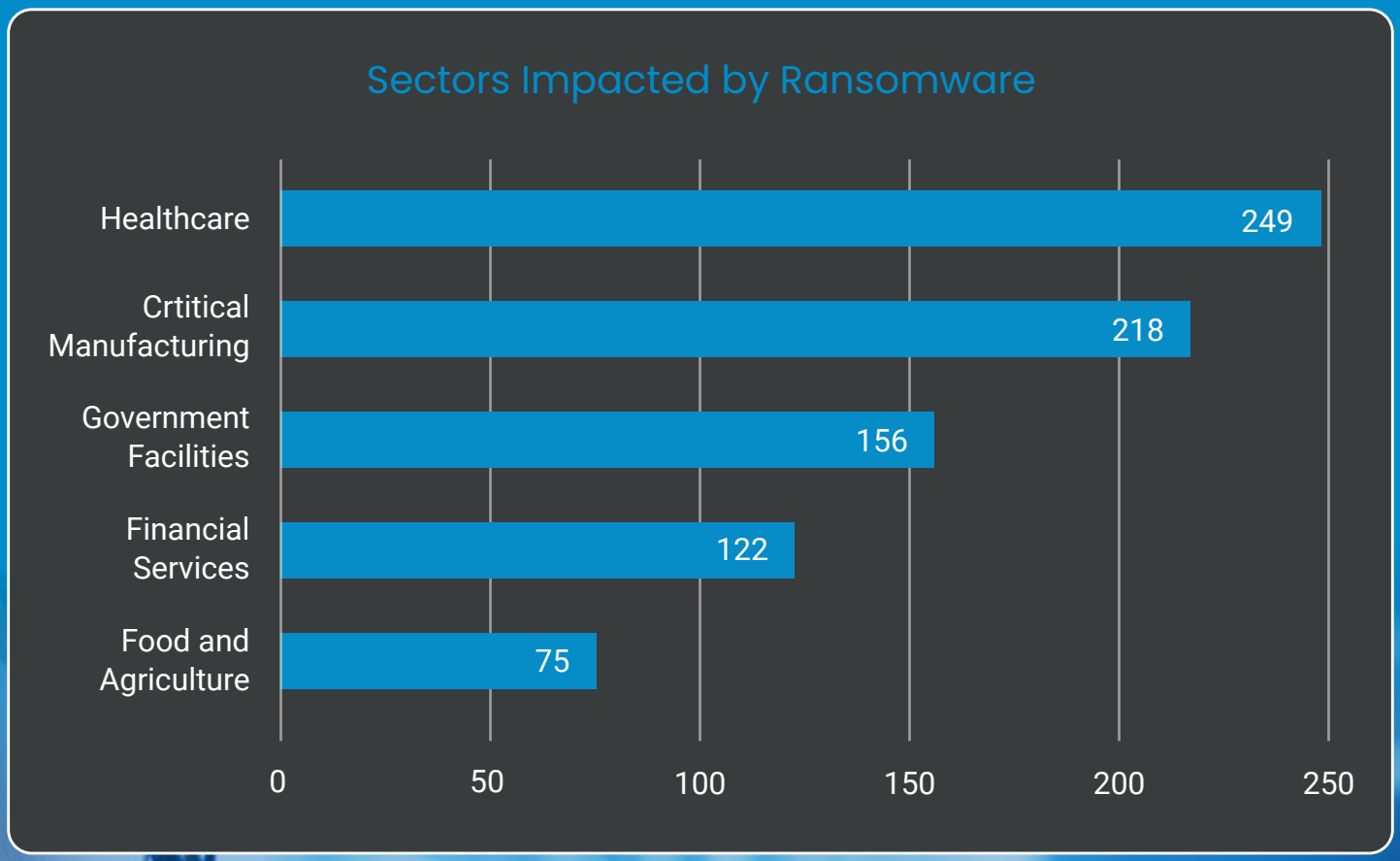
- **Disrupting BlackCat's Infrastructure:** The FBI infiltrated BlackCat's systems, seizing control of their websites and hindering their ability to function.

- **Neutralizing the Ransomware Weapon:** A critical intervention by the DOJ involved developing a decryption tool. This tool offered a lifeline to victims by allowing them to regain control of their systems without succumbing to extortion demands. Estimates suggest this intervention saved over $68 million in potential ransom payments.

- **Issuing Updated Security Guidance:** CISA released a revised ransomware advisory, equipping organizations with technical indicators of compromise and mitigation strategies to bolster their cyber defenses.

However, amidst this victory, a chilling threat arose. Cornered but not defeated, BlackCat vowed retribution, specifically targeting healthcare providers in future attacks.

If we talk about cyber attacks on healthcare organizations, it is not a rare occurrence. If we talk about 2023 alone, healthcare was the primary victim of such attacks. But what makes this attack different is the sheer size of it and the impact of this attack, that we will discuss in detail ahead.



The Attack on Change Healthcare

Timeline of Events (February 2024)

February 21, 2024

BlackCat/ALPHV launched a cyberattack against change healthcare. This attack disrupts them forcing them to go offline.

February 26, 2024

The American Hospital Association (AHA) recognizes the widespread impact of the attack and sends a public letter to the U.S. Department of Health and Human Services (HHS) expressing their concerns.

February 27, 2024

ConnectWise, a software company, responds to speculation regarding their ScreenConnect software being a potential vulnerability exploited in the attack. They deny any connection.

February 28, 2024

The Medical Group Management Association (MGMA) representing medical practices writes to HHS requesting government assistance in mitigating the attack's impact. Additionally, BlackCat/ALPHV publicly claims responsibility for the attack.

March 1, 2024

Security researchers discover a significant ransom payment of 350 bitcoins (worth roughly $22 million) made to a cryptocurrency wallet associated with BlackCat/ALPHV.

March 5, 2024

HHS finally issues a public statement regarding the attack. This statement outlines a plan to support healthcare providers in continuing to serve patients amidst the disruptions.

March 7, 2024

A critical milestone is reached as Change Healthcare restores service for prescription claim submissions and related payment systems.

March 18, 2024

This date marks the anticipated time frame for full system recovery, allowing Change Healthcare to process all medical claims again.

Attack Breakdown: Unraveling the Threads of the Change Healthcare Breach

Initial Breach:

The specific method of gaining entry into Change Healthcare's network remains under investigation. Three potential attack vectors are considered:

- **Phishing Attack:** BlackCat might have sent malicious emails containing ransomware attachments or links to Change Healthcare employees. Clicking on these emails could have inadvertently granted access to the attacker's malware.

- **Supply Chain Attack:** Change Healthcare relies on numerous third-party vendors. Gaining access to one of these vendors' systems could have allowed Black-Cat to pivot into Change Healthcare's network.

- **Unpatched Software:** Outdated software with known vulnerabilities can provide an entry point for attackers. Failure to maintain up-to-date software patches could have been a contributing factor.

Lateral Movement and Data Exfiltration:

Once inside the network, the attackers likely moved laterally, exploring the system and identifying critical infrastructure and valuable data. BlackCat's claims suggest they may have exfil-trated a staggering 6 terabytes of data, though this has not been independently verified. Potentially leaked data could include patient information, financial records, and internal doc-uments.

Ransomware Deployment and System Shutdown:

BlackCat deployed their ransomware, likely employing encryption techniques to render vital data inaccessible and cripple Change Healthcare's operations. Upon discovering the attack, Change Healthcare took decisive action by disconnecting the affected system and taking additional systems offline to contain the spread of the ransomware.

Aftermath:

The attack caused significant disruptions across the healthcare ecosystem, impacting pharmacies, healthcare providers, and potentially patients seeking essential medications.

Attack Response: Mitigating the Damage from the Change Healthcare Breach

The cyberattack on Change Healthcare sent shockwaves through the U.S. healthcare system, prompting a multi-pronged response effort from various stakeholders. Here's a breakdown of the key actions taken:

Change Healthcare's Response:

- **Manual Processes and Workarounds:** Recognizing the critical role they play in healthcare operations, Change Healthcare immediately transitioned to manual processes and alternative solutions to keep essential services functioning.

- This likely involved tasks like paper-based claims processing and manual verification procedures.

UnitedHealth's Involvement:

- **Cybersecurity Experts:** UnitedHealth, Change Healthcare's parent company, promptly engaged cybersecurity firms to investigate the attack. These specialists would be responsible for analyzing the breach, identifying the attackers' methods, and assessing the scope of the damage.

- **Collaboration with Authorities:** UnitedHealth collaborated with the U.S. government, sharing critical information about the attack. This would assist law enforcement agencies in their investigation and potentially lead to the identification and prosecution of the perpetrators.

Ransomware Payment:

- **Unconfirmed Reports:** There are unconfirmed reports that a ransom of roughly $22 million in Bitcoin was paid. While some companies resort to ransom payments to expedite recovery, this approach can incentivize future attacks and doesn't guarantee the complete restoration of data or systems.

Federal Response:

Initial Concerns:

The healthcare sector initially expressed concerns regarding the federal response. They called for stronger action from the Department of Health and Human Services (HHS) to address the disruption, particularly its impact on the pharmaceutical supply chain.

HHS Measures:

In response to these concerns, HHS implemented several measures to aid healthcare providers:

- **Clearinghouses Switch:** To provide flexibility, HHS facilitated switching clearinghouses for processing claims within Medicaid and Medicare programs. This allowed healthcare providers to bypass the compromised Change Healthcare systems.

- **Policy Relaxation:** HHS encouraged healthcare bodies to relax policies related to "prior authorization." This refers to the process where healthcare providers require approval from insurance companies before certain procedures can be performed. Easing this process aimed to streamline care delivery during the disruption.

- **Accelerated Payments:** HHS implemented measures to allow for accelerated payments to healthcare providers. This would provide them with much-needed financial assistance during a period of potentially reduced revenue due to processing delays.

- **HIPAA Investigation:** Recognizing potential HIPAA (Health Insurance Portability and Accountability Act) violations, HHS opened an investigation on March 13th, 2024. This investigation would assess whether Change Healthcare complied with federal regulations regarding patient data privacy, security, and breach notification.

While the full picture of the response may not be entirely clear due to the sensitive nature of cyberattacks, these actions demonstrate a coordinated effort between Change Healthcare, UnitedHealth, cybersecurity firms, and the U.S. government to mitigate the attack's impact and restore normalcy to the healthcare system.

Exposed Vulnerabilities

The cyberattack on Change Healthcare serves as a stark reminder of the vulnerabilities within the U.S. healthcare sector. Here's a closer look at the problems exposed by this incident:

Legacy Infrastructure and Manual Workarounds:

The forced shift to manual processes by Change Healthcare underlines potential shortcomings in the healthcare industry's infrastructure. Outdated systems and a lack of robust digital alternatives can significantly hinder operations during cyberattacks.

Data Security Concerns:

The very nature of the attack, targeting a company processing sensitive medical information, raises concerns about data security practices within the healthcare sector. The potential for patient data breaches and the disruption of critical services like claims processing highlight the need for robust cybersecurity measures.

Supply Chain Risks:

The attack's impact on the pharmaceutical supply chain underscores the interconnectedness of the healthcare system and the potential risks associated with disruptions at any point in the chain. Cyberattacks can create bottlenecks and delays in medication deliveries, potentially impacting patient treatment plans.

Limited Federal Oversight:

The initial concerns regarding the federal response point towards a potential gap in oversight and preparedness for large-scale cyber attacks within the healthcare sector. Stronger federal involvement and collaboration with industry stakeholders can be crucial in developing robust cybersecurity frameworks and response protocols.

The Change Healthcare attack serves as a wake-up call for the U.S. healthcare industry. It emphasizes the need for:

- **Investment in Modernized Infrastructure:** Upgrading healthcare infrastructure with more secure and resilient technologies is essential.

- **Enhanced Cybersecurity Measures:** Implementing robust cybersecurity protocols, including data encryption, access controls, and regular system audits, is crucial for safeguarding sensitive patient data.

- **Diversification of Vendors:** Reducing reliance on single vendors for critical services can help mitigate the impact of disruptions at any one point in the system.

- **Stronger Collaboration:** Improved communication and collaboration between healthcare providers, vendors, and government agencies are essential for a coordinated response to cyberattacks.

By addressing these vulnerabilities, the healthcare sector can build a more resilient and secure system prepared to withstand future cyber threats.

What Needs To Be Changed

The cyberattack on Change Healthcare, while a common tactic (ransomware attacks), highlighted critical vulnerabilities within the healthcare system due to its interconnected nature and nationwide reach. This section explores policy considerations to mitigate the impact of similar attacks in the future.

Challenges of a Cyber Incident Response

- **Traditional Response Limitations:** Existing response structures designed for physical disasters may not be sufficient for cyber incidents due to their complex, evolving nature and potential for delayed downstream effects.

- **Fragmented Federal Response:** The current two-pronged approach with the FBI investigating attackers and DHS assisting victims lacks a unified federal response.

Existing Frameworks and their Shortcomings

- **National Cybersecurity Strategy and National Cyber Incident Response Plan (NCIRP):** These decade-old policies are due for updates, particularly the NCIRP which CISA is currently revising. Uncertainties exist around whether the NCIRP is being used and how potential changes are being tested.effects.

- **Cyber Unified Coordination Group (UCG):** Established to coordinate interagency resources, it's unclear if a UCG was formed for the Change Healthcare attack, as mandated by policy.

Potential Policy Improvements

- **Infrastructure Investment and Jobs Act (IIJA):** While the IIJA authorizes declarations for significant cyber incidents and a cyber response and recovery fund, these currently don't address real-world consequences of attacks.

Information Parity: Sharing Critical Information

- **Coordination of Offensive and Defensive Actions:** Improved information sharing between CISA, SRMAs (Sector Risk Management Agencies), and the private sector is crucial. This would allow for a better understanding of attacker capabilities and potential retaliatory actions.

- **Knowledge for Decision-Making:** CISA might require additional access to information to effectively declare incidents "significant." Policymakers could explore improved reporting, industry partnerships, or enhanced interagency collaboration for a more complete picture.

- **Information Sharing Reach:** While CISA and FBI share information on ransomware threats to hospitals, expanding reach to the broader healthcare sector (physicians, pharmacies) is essential. HHS, as the SRMA for healthcare, might be better positioned to ensure

An Action Plan For Healthcare Providers

The Change Healthcare attack serves as a wake-up call for healthcare providers to prioritize cybersecurity measures. Here's what you can do to protect your organization:

Security Awareness Training:

Invest in regular cybersecurity awareness training for all staff members. This training should educate employees on identifying phishing attempts, password security best practices, and the importance of reporting suspicious activity.

Endpoint Security Measures:

Implement robust endpoint security solutions on all devices used within your network, including computers, laptops, and mobile devices. These solutions should include antivirus, anti-malware, and firewall protection.

Data Encryption:

Encrypt sensitive patient data both at rest and in transit. This additional layer of security makes it significantly harder for attackers to access information even if they breach your systems.

Regular Backups:

Maintain regular backups of your data and store them securely offsite. This ensures you can recover critical information quickly in the event of a cyberattack or system failure.

Incident Response Plan:

Develop a clear and documented incident response plan that outlines the steps to take in case of a cyberattack. This plan should include procedures for identifying, containing, eradicating, and recovering from an attack.

Regular Risk Assessments:

Conduct regular risk assessments to identify and mitigate potential cybersecurity vulnerabilities within your network. These assessments should consider your specific IT infrastructure, data security practices, and employee behavior.

Vendor Risk Management:

When selecting third-party vendors, ensure they have adequate cybersecurity measures in place to protect your data. Evaluate their security practices and inquire about their incident response protocols.

By implementing these measures and fostering a culture of cybersecurity awareness within your organization, healthcare providers can significantly reduce the risk of cyberattacks and protect sensitive patient data. Remember, cybersecurity is an ongoing process, and vigilance is key to staying ahead of evolving threats

Protect Your Healthcare Practice **with Capline**

The Change Healthcare attack highlights the importance of strong cybersecurity. Capline offers a complete solution:

- **Remote Data Backup:** Secure, HIPAA-compliant back-ups safeguard your data from cyberattacks, disasters, and hardware failures.

- **Anytime, Anywhere Access:** Ensure healthcare practice continuity with remote access to your data, facilitating remote work.

Combined with Capline's Healthcare Compliance Services:

- **Targeted Staff Training:** Minimize human error, a leading cause of breaches.

- **Reduced Penalty Risk:** Maintain compliance and avoid HIPAA fines.

Gain peace of mind with Capline's comprehensive data protection and ensure your practice thrives in the digital healthcare world.

Contact Info

888-444-6041 thinkgrowth@caplineservices.com

3838 N Sam Houston Pkwy E, Ste 290, Houston, TX 77032

Apr 10, 2024