Tab 1

Assignment #3  
For Class PUBP 6725 OCY/001 (Spring25)

Author Name: Dasaray Fyall  
dfyall3@gatech.edu

# 1 Introduction

Change Healthcare is a healthcare technology company that is known as one of the largest healthcare payment processors in the medical industry. In February 2024, the company experienced a cyberattack that affected its computer systems and disrupted the processing of medical claims and healthcare services for several weeks. This breach caused a backlog of unpaid claims which led to several medical facilities experiencing financial hardships nationwide.

# 2 Diamond Model

## 2.1 Adversary

It was later revealed that the breach was orchestrated by a Russian Ransomware group called ALPHV/ BlackCat. This group of attackers are known for targeting organization’s infrastructure within several industries such as government and healthcare in order to demand ransom from the victims with their Ransom as a service approach. Ransom as a service is a business model in which ransomware developers create ransomware and sell the malicious program to other potential hackers and cybersecurity criminals (Techtarget, 2024). The attack was financially motivated as the group encrypted sensitive data and demanded a large ransom in order to release the data.

## 2.2 Victim

Change Healthcare, a company that provides many services such as processing claims, payments and maintains other data for healthcare providers, is considered the primary victim of the attack. However, those who used Change Healthcare services such as the healthcare providers and patients were the secondary victims. This particular incident caused disruptions of services throughout the healthcare sector and exposed patients’ sensitive data such as personal and financial information that could possibly be exposed in the dark web.

### 2.2.1 Social political meta feature

The adversary attacked the victim mainly for financial reasons. Healthcare is known for its critical nature and its access to sensitive data; however, many providers use legacy systems which makes it a perfect target for exploitation. Since the incident caused major disruptions for many people, it highlights the need for stricter regulations throughout the entire healthcare industry to prevent future attacks and to maintain patient’s trust.

## 2.3. Infrastructure

The attackers were able to obtain access to Change Healthcare’s IT systems, which includes network, databases, and servers that stored electronic health records. It was later revealed that the organization did not follow best practices of cybersecurity standards such as using multifactor authentication and patching vulnerabilities within its systems and in some of the software such as ConnectWise ScreenConnect. As soon as the severity of the attack was known, the company disconnected its systems to prevent any additional harm.

## 2.4 Capability

The cybercriminals deployed ransomware to exfiltrate and encrypt the data. It was revealed that there were vulnerabilities that were not patched before the attack which made it easier for the ransomware to penetrate through the company system. Weeks later, it was mentioned that 6TB of data was stolen and the company paid the attackers’ $22 million ransom to not release the data into the dark web (HIPAA Journal, 2024).

### 2.4.1 Technology meta feature

While the details of how the attackers initially entered the system hasn’t been disclosed, cybersecurity professionals did reveal that the group was able to retrieve an employee’s login credentials to exploit the vulnerabilities which may have been obtained through social engineering tactics such as a phishing email. Due to the lack of security controls such as multi factor authentication and end point detection and response tools the group was able to gain access to the network and installed ransomware which penetrated throughout the system.

# 3 Policy Assessment and Recommendation

This particular incident shows how vulnerable the healthcare industry is and the need to strengthen cybersecurity measures in these entities. The investigation brought to light that the company's issues stem from the organization layer. While there are standards on the national level, this specific company was not prepared to defend itself from a breach. For example, policies and regulations such as HIPAA and HITRUST CSF require healthcare providers to have several security safeguards such as multi-factor authorization, end to end encryption, continuous software updates, etc. However, a few days before the attack, there were notifications that were ignored which stated that vulnerabilities needed to be patched on several software that may have been connected to the attack and multi-factor authorization was not enabled on the servers. Applying those security measures would have reduced the risk of experiencing an attack from happening. Additionally, the presence of endpoint detection and response tools would’ve allowed the company to stop the attack from moving through several layers of the network quicker. Also, since the attack was traced to an employee login credentials, it should be mandatory that all employees go through cybersecurity training on the continuous bases and the company should conduct phishing simulations so employees can be aware of what a phishing attempt looks like. In addition to that, incident response and recovery plans would’ve helped the company to respond quickly in order to continue operations. Although it took about a month to resolve 92% of the issue, many healthcare providers suffered financially which resulted in several lawsuits due to slow response.

# 4 Conclusion

By October 2024, the company was able to operate in full capacity as they continued to investigate the incident. However, the Change Healthcare breach has cost the company billions of dollars and led to the resignation of the CEO. Additionally, many government officials and industry experts call for stricter regulations, compliance, and penalties for non-compliance as the world continues to be reliant on technology.

# 

# 5 REFERENCES

1. American Hospital Association. (2024, February 22). *Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field*. American Hospital Association <https://www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and>
2. Government of Canada. (2023, March). *Profile: ALPHV/BlackCat ransomware.* Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/guidance/profile-alphvblackcat-ransomware>
3. HIPAA Journal. (2024, February). *Change Healthcare responding to cyberattack.* HIPAA Journal. <https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/#:~:text=In%20February%202024%2C%20Change%20Healthcare,an%20estimated%20190%20million%20individuals>.
4. Hyperproof. ( 2024, February 20). *Understanding the Change Healthcare breach.* Hyperproof. <https://hyperproof.io/resource/understanding-the-change-healthcare-breach/>
5. IS Partners, LLC. (2024, February 21). *Change Healthcare data breach* *2024.* IS Partner. <https://www.ispartnersllc.com/blog/change-healthcare-data-breach-2024/>
6. Techtarget. (2024, February 27). *The Change Healthcare attack: Explaining how it happened*. TechTarget. <https://www.techtarget.com/whatis/feature/The-Change-Healthcare-attack-Explaining-how-it-happened>
7. U.S. House of Representatives Committee on Energy and Commerce. (2024, February 26). *What we learned from the Change Healthcare cyberattack.* U.S. House of Representatives Committee on Energy and Commerce <https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack>

Tab 2

In September 2023, MGM Casino Resorts experienced a cyberattack throughout several of their properties. This attack affected services such as slot machines, ATMs, room access and it was later revealed that customers’ information may have been compromised during the attack. After conducting additional investigation, the company realized that customers’ information may have been compromised during the attack.

**Diamond Model**

Adversary- The breach was orchestrated by a group of young individuals from the US and UK that goes by the name Scattered Spider. The group collaborated with

Tab 3

Change Healthcare is a healthcare technology company that is known as one of the largest healthcare payment processors in the medical industry. In February 2024, the company experienced a cyberattack that affected its computer systems and disrupted the processing of medical claims and healthcare services for several weeks. This breach caused a backlog of unpaid claims which led to several medical facilities experiencing financial hardships nationwide.

Diamond Model

Adversary-It was later revealed that the breach was orchestrated by a Russian Ransomware group called ALPHV/ BlackCat. This group of attackers are known for targeting organization’s infrastructure within several industries such as government and healthcare in order to demand ransom from the victims with their Ransom as a service approach. Ransom as a service is a business model in which ransomware developers create ransomware and sell the malicious program to other potential hackers and cybersecurity criminals. The attack was financially motivated as the group encrypted sensitive data and demanded a large ransom in order to release the data.

Victim- Change Healthcare, a company that provides many services such as processing claims, payments and maintains other data for healthcare providers, is considered the primary victim of the attack while those who used Change Healthcare services such as the healthcare providers and patients were the secondary victims. This particular incident caused disruptions of services throughout the healthcare sector and exposed patients’ sensitive data such as personal and financial information that could possibly be exposed in the dark web.

Social political meta feature- The adversary attacked the victim mainly for financial reasons. Healthcare is known for its critical nature and its access to sensitive data; however, many providers use legacy systems which makes it a perfect target for exploitation. Since the incident caused major disruptions for many people, it highlights the need for stricter regulations throughout the entire healthcare industry to prevent future attacks and to maintain patient’s trust.

Infrastructure- The attackers were able to obtain access to Change Healthcare’s IT systems, which includes network, databases, and servers that store electronic health records. It was later revealed that the organization did not follow best practices of cybersecurity standards such as using multifactor authentication and patching vulnerabilities within its systems and in some of the software such as ConnectWise ScreenConnect. As soon as the severity of the attack was known, the company disconnected its systems to prevent any additional harm.

Capability- The cybercriminals deployed ransomware to exfiltrate and encrypt the data. It was revealed that there were vulnerabilities that were not patched before the attack which made it easier for the ransomware to penetrate through the company system. Weeks later, it was mentioned that 6TB of data was stolen and the attackers were paid $22 million to not release the data.

Technology meta feature- While the details of how the attackers initially enter the system hasn’t been disclosed, cybersecurity professionals did reveal that the group obtained an employee’s login credentials to exploit the vulnerabilities. After gaining access to the network, the group installed ransomware which penetrated throughout the system.

Policy Assessment and Recommendation

This particular incident shows how vulnerable the healthcare industry is and the need to strengthen cybersecurity measures in these entities. The investigation brought to light that the company's issues stem from the organization layer. While there are standards on the national level, this specific company was not prepared to defend itself from a breach. For example, policies and regulations such as HIPAA and HITRUST CSF require healthcare providers to have several security safeguards such as multi-factor authorization, end to end encryption, continuous software updates, etc. However, a few days before the attack, there were notifications stating that vulnerabilities needed to be patched on several software may have been connected to the attack and multi-factor authorization was not enabled on the servers. Applying those security measures would have reduced the risk of experiencing an attack from happening. Also, since the attack was traced to an employee login credentials, it should be mandatory that all employees go through cybersecurity training on the continuous bases and the company should conduct phishing simulations so employees can be aware of what a phishing attempt looks like. In addition to that, incident response and recovery plans would’ve helped the company to respond quickly in order to continue operations. Although it took about a month to resolve 92% of the issue, many healthcare providers suffered financially which resulted in several lawsuits.

Conclusion- By October 2024, the company was able to operate in full capacity. However,the Change Healthcare breach has cost the company billions of dollars and led to the resignation of the CEO. Additionally, many government officials and industry experts call for stricter regulations, compliance, and penalties for non-compliance as the world continues to be reliant on technology.

**Reference List**

1. American Hospital Association. (2024, February 22). *Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field*. American Hospital Association <https://www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and>
2. Government of Canada. (2023, March). *Profile: ALPHV/BlackCat ransomware.* Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/guidance/profile-alphvblackcat-ransomware>
3. HIPAA Journal. (2024, February). *Change Healthcare responding to cyberattack.* HIPAA Journal. <https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/#:~:text=In%20February%202024%2C%20Change%20Healthcare,an%20estimated%20190%20million%20individuals>.
4. Hyperproof. ( 2024, February 20). *Understanding the Change Healthcare breach.* Hyperproof. <https://hyperproof.io/resource/understanding-the-change-healthcare-breach/>
5. IS Partners, LLC. (2024, February 21). *Change Healthcare data breach* *2024.* IS Partner. <https://www.ispartnersllc.com/blog/change-healthcare-data-breach-2024/>
6. Techtarget. (2024, February 27). *The Change Healthcare attack: Explaining how it happened*. TechTarget. <https://www.techtarget.com/whatis/feature/The-Change-Healthcare-attack-Explaining-how-it-happened>
7. U.S. House of Representatives Committee on Energy and Commerce. (2024, February 26). *What we learned from the Change Healthcare cyberattack.* U.S. House of Representatives Committee on Energy and Commerce <https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack>