Eric Mung'aũ Preston

04/14/24

CS 462: Cybersecurity Fundamentals

Professor Susan Zehra

Old Dominion University

Introduction

The society we live in has become synonymous with technology, which means human beings worldwide interact with technology daily. These interactions with technology include different sectors such as the government, finance, healthcare, and education (Bhosale, 2021). One of the most critical components of ensuring these interconnected entities are functional without interruption has been ensuring cybersecurity and free from cyberattacks. Cybersecurity includes technologies, processes, and practices designed to protect networks, devices, programs, and data from attack. While the integration with technology has been highly beneficial to humankind, and cybersecurity has become integral in protecting these systems, there continues to be a risk of cyberattacks that can have devastating effects and cause significant harm to individual users, organizations, infrastructure, and financial institutions (Bhosale, 2021). Some entities have experienced cyberattacks more than others. The healthcare industry has been a significant area that has experienced intimidation and cyber-attack incidents. These cyberattacks have caused significant damage and disruption to the healthcare industry, including breaching private medical information and leading to millions of dollars in loss when it comes to revenues and fines (Bhosale, 2021). This paper will focus on a recent cyberattack on Change Healthcare, the largest clearing house for insurance billing and payment in the United States, that significantly disrupted the healthcare industry and sectors connected to the industry. The paper

will address the breach itself, the immediate effect of the breach, vulnerabilities and attacks used, and societal effects and will end with a conclusion.

The Breach Itself (Change Healthcare)

On February 21st, 2024, the most significant and consequential cyberattack in American history occurred against Change Healthcare, the largest clearing house for insurance billing and payment in the United States. The BlackCat/ALPHV ransomware groups cyberattack led to the company taking its systems offline. Change Healthcare processes 15 billion healthcare transactions annually and interacts with one in every three patient records. On February 26th, the American Hospital Association (AHA) wrote a public letter to the Department of Health and Human Services (HHS) notifying them of the significant impact of the cyberattack. On the same date, BlackCat/ALPHV claimed responsibility for the attack. Additionally, the Medical Group Management Association (MGMA), representing over 60,000 medical practice administrators and executives, sent a public letter to the Department of Health and Human Services (HHS) asking the government to intervene and mitigate the attacks' impact.

This impact included the crippling of financial operations for multiple sectors that included hospitals, insurers, pharmacies and medical groups nationwide. Services that came to a halt included the inability to verify claims, check health insurance coverage, the inability of pharmacies to determine the price of medications, and lack of financial payments from health insurance companies for services rendered, resulting in nonpayment of salaries, wages, and contract fees owed to workers in the healthcare industry. Additionally, the breach caused anxieties related to the exposure of private medical information of millions of people. (Caminiti, 2024). On March 1st, the ransom, including 350 bitcoins worth $22 million, was made to BlackCat/ALPHV. On March 5th, HHS issued a public statement about the Change Healthcare

cyberattack and plans to help providers serve patients. By March 7th, prescription claim submissions and payment system services were restored, and on March 18th, substantial progress was made towards restoring the system to its full capacity. Also, the government provided at least 2 billion dollars to health care providers, and more secure software for medical claims (Kerner, 2024). The immediate effect of the cyberattack was felt far and wide.

Vulnerabilities and Attacks Used

According to security researchers, Change Healthcare has yet to be forthcoming with exactly how the cyberattack occurred. However, based on tactics previously deployed by the BlackCat/ALPHV, a prolific ransomware gang, it can be assumed that they gained initial access to Change Healthcare through the infiltration of Microsoft's remote desktop protocol and brute-force attacks against Active Directory (*What Is BlackCat Malware?*). Additionally, security researchers indicated vulnerabilities in the ConnectWise Screen Connect application. Once inside the Change Healthcare network, the attackers deployed ransomware attacks that rendered critical systems and data unavailable, disrupting key operations and forcing healthcare providers to implement workarounds to continue providing services. To stop further damage, Change Healthcare responded to the attack by disconnecting more than 111 services across its system. Additionally, the organization engaged cybersecurity companies and law enforcement to contain and rectify the ransomware risk (Kerner, 2024).

The Immediate Effect

The initial impact included the ransomware group BlackCat/ALPHV, claiming responsibility for the attack Olsen & Vogel, 2024). Additionally, the healthcare system became vulnerable as the private medical information of millions of Americans became at risk of being leaked. In addition, hospitals and health systems could not pay salaries to medical providers and

other team members of care teams. Other disruptions included healthcare systems being unable to acquire necessary medicines and supplies and being unable to pay for critical contract work in areas such as environmental services, physical security, and food services.

Furthermore, interruption of care due to lack of information related to co-pays for prescription medications forced medical providers to estimate payments, sometimes overcharging patients for medical care. Emily Dowsett, the associate director of public affairs at the Medical Group Management Association, summed up the effect by stating, “They’re employed by a variety of groups, health systems, health plans, and vendors, and as a result, the impacts of the cyberattack were incredibly significant and far-reaching” (Olsen & Vogel, 2024). Upon realizing the effect and disruption would take longer than expected, other immediate effects occurred. Medical providers attempted to apply manual workarounds that included manually inputting claims in other clearing houses.

While these workarounds were adequate, the process was time-consuming and tedious, leading to labor being diverted from more critical tasks to manually inputting claims to speed up payments by insurance companies (Olsen & Vogel, 2024). Change Healthcare also attempted to resolve the crisis by providing a temporary funding assistance program to the healthcare industry to keep it afloat. The attack began on February 21st, and by March 15th, there was an estimated 6.3 billion in delayed payments to healthcare providers in the United States. An alleged payment of 350 bitcoins worth $22 million was made to a Bitcoin cryptocurrency wallet associated with the BlackCat/ALPHV to regain control of the Change Healthcare system (Kerner, 2024). To understand the security gaps that led to the attack, vulnerabilities, and attacks are addressed below.

Societal Effects

While the cyber attack's immediate effect on the organization and its users was prevalent, other significant societal effects occurred and are worth noting. One important effect was the heightened awareness of needed cybersecurity changes within the healthcare industry. After the attack, multiple aspects such as risk analysis, vendor security protocols, recovery plans, and transparency were some of the many factors criticized as not being secure and effectively in place (Olsen, 2024b). Firstly, for a critical institution like Change Healthcare to suffer a cyberattack of this scale showed how proper risk analysis is necessary for protecting health information, which is a much more valuable target for cybercriminals. Furthermore, with the healthcare industry having third-party vendors heavily reliant on its business model, foundational cybersecurity standards are critical for mitigating potential vulnerabilities. Next, UnitedHealth Group's unsteady approach in fixing the damage over the past few weeks proved there was a clear lack of a recovery plan if an attack happens. Lastly, while a lack of transparency is understandable within the healthcare industry for legality, a change between the industry and the government would greatly improve technological flaws and prevent similar attacks in the future (Adams, 2024).

However, a glaring issue was the cascading effect of this attack on smaller healthcare providers like community health centers. These centers function on much fewer resources than large health institutions, and this attack forced them to take lines of credit, which depleted resources quickly. While reserve funds may exist for similar situations, the average amount of on-hand cash for health centers is typically 64 days. Another societal effect was the challenge of shifting to more antiquated ways of filing claims. For example, by March 25th, even though UnitedHealth Group was progressing towards billing, the number of claims to file took up more time and continued to strain these centers. This hardship experienced by small health centers and

providers shows how vital cybersecurity is for large industries due to how much damage can spread from a massive cyber attack (Hellmann, 2024).

Fortunately, changes are being implemented to mitigate these issues via the HHS's cybersecurity goals for 2024 and the Biden administration's proposed budget for 2025. For example, getting an improved risk analysis is essential to understand what is critical to invest in. In addition to that, the capacity to change service vendors unwilling to change cybersecurity protocols, and the federal government providing funding to finance cybersecurity for smaller healthcare providers. These goals for the industry can enforce a foundation of improved cybersecurity standards for vendors and the implementation of recovery plans. The increased budget is intended to "put cyber protections in place, with penalties towards those not in compliance rolling out in coming years." These protections will help secure lower levels of the healthcare industry and provide more resources to improve their financial situation after an attack (Olsen, 2024a).

Conclusion

In conclusion, the cyber attack on Change Healthcare has proven to be one of the most damaging in the U.S. healthcare industry's history. BlackCat's ransomware effectively shut down one of the biggest clearinghouses, which processes 15 billion claims annually, creating a ripple effect for all healthcare providers due to the scale of Change Healthcare as an institution. While details about the breach have not been made public, the potential vulnerabilities that led to the attack lie in Microsoft's remote desktop protocol and an improperly secure Active Directory. This attack had the immediate effect of compromising the health information of millions of people, preventing healthcare providers from getting salaries, and forcing providers to estimate their prices, potentially overcharging patients on prescriptions. Furthermore, that financial

blockage severely affected smaller community health centers, which function on much fewer reserves than bigger institutions, and the extended time for processing claims at the time wasn't helping either. However, this attack generated a beneficial discussion on the need for improved cybersecurity aspects such as risk analysis, vendor security protocols, recovery plans, and transparency within the healthcare industry. Additionally, with the HHS cybersecurity goals and the Biden administration's plan for cybersecurity funding in the industry, there will be a more enforced cybersecurity foundation and beneficial resources for the lower levels of the industry to function. While this ransomware has been devastating, increases in resources and the implementation of new cybersecurity protocols will help make this critical infrastructure more prepared for the future.

References

Adams, K. (2024, April 7). *4 Lessons We Learned From The Change Healthcare Cyberattack*. MedCity News. https://medcitynews.com/2024/04/change-healthcares-cyberattack-cybersecurity/#:~:text=Given%20the%20massive%20scale%20of

Bhosale, K. S., Nenova, M., & Iliev, G. (2021, September 1). *A study of cyber attacks: In the healthcare sector*. IEEE Xplore. https://doi.org/10.1109/Lighting49406.2021.9598947

Caminiti, S. (2024, March 15). *Why UnitedHealth, Change Healthcare were targeted by ransomware hackers, and more cybercrime will hit patients, doctors*. CNBC. https://www.cnbc.com/2024/03/15/why-unitedhealth-change-healthcare-were-targets-of-ransomware-hackers.html

Emerson, J., & Wilson, R. (2024, March 26). *The Change Healthcare cyberattack: A timeline*. Www.beckershospitalreview.com. https://www.beckershospitalreview.com/cybersecurity/the-change-healthcare-cyberattack-a-timeline.html#:~:text=Change%20Healthcare%20confirmed%20ALPHV%2FBlackCat

Hellmann, J. (2024, March 25). *Hack poses financial problems for community health centers*. Roll Call. https://rollcall.com/2024/03/25/hack-poses-financial-problems-for-community-health-centers/

Kerner, S. M. (2024). *The Change Healthcare attack: Explaining how it happened*. WhatIs; TechTarget. https://www.techtarget.com/whatis/feature/The-Change-Healthcare-attack-Explaining-how-it-happened

Olsen, E. (2024a, March 13). *Biden's proposed budget for 2025 boosts cybersecurity funds, extends ACA subsidies*. Healthcare Dive. https://www.healthcaredive.com/news/biden-hhs-budget-proposal-2025-cybersecurity-aca-medicare-drug-negotiation/710086/

Olsen, E. (2024b, April 4). *Change cyberattack serves as wake-up call for healthcare cybersecurity*. Healthcare Dive. https://www.healthcaredive.com/news/change-healthcare-cyberattack-cybersecurity-resilience-planning/711650/

Olsen, E., & Vogel, S. (2024, March 5). *Change Healthcare cyberattack having "far-reaching" effects on providers*. Cybersecurity Dive. https://www.cybersecuritydive.com/news/change-healthcare-providers-impact/709236/

What Is BlackCat Malware? (n.d.). Www.blackberry.com; Blackberry Limited. Retrieved April 13, 2024, from https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/blackcat