When Healthcare Gets Hacked: The Change Healthcare Cyberattack and Why It Became Personal to Me

When most people think about going to the doctor, filling in a prescription, or getting blood work done, cybersecurity is probably the last thing on their minds. We expect our doctors, hospitals, laboratories, insurance companies, and the businesses working with them to protect our personal information. Unfortunately, healthcare has become one of the biggest targets for cybercriminals.

The Change Healthcare cyberattack of 2024 is a perfect example of how one cybersecurity attack can affect an entire country. The attack did not just involve hackers stealing information from a computer. It interfered with prescriptions, medical claims, payments to healthcare providers, insurance processing, and other services that patients depend on.

This subject is also personal to me because this is not my first experience seeing what can happen when healthcare information is compromised. Years before the Change Healthcare attack, I received a notification that my own information had been affected by the American Medical Collection Agency (AMCA) data breach involving LabCorp. I was one of the millions of LabCorp patients whose information was stored in the affected AMCA system.

The AMCA attack compared with the 2024 Change Healthcare attack shows something disturbing, here we are years later, and healthcare organizations and their third-party companies are still struggling to protect the enormous amount of personal information entrusted to them.

The Change Healthcare incident also demonstrates how something as simple as a stolen username and password, combined with a missing security feature, can contribute to a nationwide cybersecurity disaster.

What Is Change Healthcare?

Before understanding the attack, it is important to understand Change Healthcare. Change Healthcare is a healthcare technology company that became part of UnitedHealth Group. Most patients probably would not recognize the company's name even though its systems have played an important role behind the scenes in American healthcare. Change Healthcare processes healthcare transactions connecting doctors, pharmacies, hospitals, insurance companies, and other organizations. According to the American Hospital Association, Change Healthcare processes about “15 billion healthcare transactions each year” and touches approximately “one out of every three patient records” (AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals’ Finances, 2024). This helps explain why attacking one company caused such a large problem. Change Healthcare was not just another website. It was part of the infrastructure that allowed different parts of the healthcare system to communicate and conduct business.

What Happened?

On February 21, 2024, UnitedHealth Group reported that Change Healthcare was experiencing a cybersecurity incident. A ransomware organization known as “ALPHV, or BlackCat”, claimed responsibility for the attack. The Congressional Research Service reported that BlackCat/ALPHV was a Russia-linked cybercriminal organization (Jaikaran, 2024). Investigators eventually learned that the criminals had actually gained access before February 21. The attackers entered the Change Healthcare environment on approximately February 12, 2024. They used compromised credentials to access a remote-access application. That means the attackers did not necessarily have to perform some complicated hack to get through the front door. They had a working username and password but there was another major problem, the remote-access system did not have multi-factor authentication enabled (this was extremely important).

What Is Multi-Factor Authentication?

Multi-factor authentication, commonly called MFA, is one of the most important security controls involved in this incident. Most of us have probably used MFA without realizing how important it is. Suppose I log into my bank account, and I enter my username and password. The bank then sends a six-digit code to my phone and requires me to enter that code before I can access the account, that second step is multi-factor authentication. The idea is simple have 2 different ways to verify it’s you 1. Take something you know like your password, and 2. something you have like your phone or security device or, sometimes something you are, such as a fingerprint or facial recognition to authenticate access. Therefore, the benefit is that stealing my

password alone would not be enough to access my account. That extra security layer was missing from the remote access system involved in the Change Healthcare attack.

According to reporting based on UnitedHealth CEO Andrew Witty's congressional testimony, the attackers used compromised credentials to access a Citrix portal that did not have MFA enabled (Siddiqui, 2024). In simple terms, imagine a building that normally requires an employee badge and a PIN to enter. A criminal steals someone's badge, If the building requires both the badge and PIN, the stolen badge alone should not be enough. But imagine that one entrance only requires the badge and the criminal finds that entrance and walks in. That is similar to why MFA matters.

The Citrix Remote-Access Technology

The attackers accessed Change Healthcare through a Citrix remote-access portal. Citrix technology can allow authorized employees and users to remotely connect to applications and organizational resources. Remote access is extremely useful because employees do not always work inside the physical building containing the organization's computer systems. The problem is that anything available through the Internet can also become a target for attackers. The portal itself was designed to let authorized people enter remotely. If criminals obtain valid credentials and there is no second authentication requirement, those criminals may appear to be legitimate users. This is one reason authentication security is so important.

What Did the Attackers Do After Getting Inside?

Getting into a network is only the beginning of an attack. Once cybercriminals establish access, they may attempt to explore the environment, find valuable systems, steal information, obtain additional permissions, and move between systems. The Change Healthcare attackers reportedly entered on February 12. The ransomware portion of the attack occurred approximately nine days later, on February 21. That gap is significant; it shows why cybersecurity is not only about preventing someone from getting inside. Organizations also need systems capable of detecting suspicious activity after someone enters. This is where technologies such as security monitoring, access logs, intrusion detection, endpoint detection and response, and Security Information and Event Management systems can become important. A company needs to be able to recognize behavior that does not look normal. These warning signs can help cybersecurity teams detect an attacker before the final stage of an attack occurs.

What Is Ransomware?

The Change Healthcare attack involved ransomware. Ransomware is malicious software designed to prevent an organization from accessing its systems or information, usually by encrypting files. Encryption normally has legitimate purposes. It mathematically changes readable information into a form that cannot easily be read without the correct key. Cybercriminals turn that useful technology into a weapon. Imagine having 10,000 important files stored on a computer. A criminal installs ransomware and encrypts all 10,000 files. The files still

exist, but the company can no longer use them normally. The attacker then demands money in exchange for helping restore access. The Change Healthcare attacks were even worse because the criminals stole information before encrypting the systems. This created two threats 1. Pay us if you want access to your systems again, and 2. Pay us or we may expose the information we stole. This technique is commonly called double extortion.

The Attack Did More Than Steal Information

One reason the Change Healthcare attack stands out is that its impact went far beyond stolen information. Healthcare providers use systems such as Change Healthcare to submit insurance claims and receive payments. When those services became unavailable, healthcare organizations experienced serious problems. The Centers for Medicare & Medicaid Services acknowledged that providers were experiencing cash-flow problems because facilities were unable to submit claims and receive normal payments through the Change Healthcare platform (Change Healthcare Payment, 2024). This possibility affected the doctor who had employees to pay, the hospital cost to order supplies, the pharmacy still needs to process prescriptions, the medical office that still had rent, utilities, and other expenses. A cybersecurity attack against a technology company can therefore turn into a financial emergency for healthcare providers that were never directly hacked.

How It Affected Patients

The American Hospital Association surveyed nearly 1,000 hospitals shortly after the attack. Approximately 74% reported an impact on patient care, and 94% reported some financial impact. Hospitals reported problems involving areas such as insurance verification, prior authorization, claims processing, and cash flow (Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances, 2024). This demonstrates why cybersecurity in healthcare can potentially become a public-safety issue. If a hospital's healthcare technology becomes unavailable, the consequences can involve medication, medical treatment, patient records, insurance approval, and payment systems.

Privacy Information Sharing

AMCA attack and Change Healthcare attack happened years apart, but they share an important connection. Both demonstrate the danger of third-party risk in healthcare. With AMCA, patients may have received services from LabCorp without thinking much about the outside collection company that later received some of their information. Similarly, many Americans affected by Change Healthcare may never have knowingly done business with a company called Change Healthcare. That is one of the biggest problems with modern data privacy. We give our information to one organization, but that does not necessarily mean our information stays there. A doctor's office may use an insurance company, the insurance company may use a claims processor, another business may provide billing services, another company may host information in the cloud, another vendor may collect unpaid bills, and each connection creates another place

where information must be protected. My experience with the AMCA breach taught me that a company can compromise my information I did not intentionally choose to do business with. The Change Healthcare attack shows that this problem still exists on an even larger scale.

How Could an Attack Like This Be Prevented?

The most obvious lesson from Change Healthcare is the importance of MFA. An Internet-accessible system containing or providing access to sensitive healthcare resources should have strong authentication. Organizations should also limit employee access according to the principle of least privilege. Employees should have access only to the systems and information necessary to perform their jobs. Networks should also be segmented, network segmentation is like putting locked doors inside a building, if a criminal gets through the front door, that does not automatically mean every room in the building should be open.

Organizations also need:

- strong passwords,
- multi-factor authentication,
- network segmentation,
- updated and patched software,
- endpoint protection,
- encryption,

- continuous security monitoring,
- secure backups,
- employee cybersecurity training,
- incident-response plans, and
- regular security assessments.

Companies must also evaluate the cybersecurity practices of vendors and companies they acquire. Cybersecurity cannot be treated as something that only the IT department worries about after a problem occurs.

Conclusion

The 2024 Change Healthcare ransomware attack demonstrates how one cybersecurity weakness can contribute to consequences across an entire industry. Attackers obtained compromised credentials and entered a remote-access environment that did not have multi-factor authentication enabled. Once inside, they were able to establish access before ransomware was deployed and information was stolen. The result was not simply a computer problem. Healthcare providers had difficulty submitting claims and receiving payments. Patients experienced disruptions. Sensitive information belonging to approximately 192.7 million people was ultimately reported as impacted.

The Change Healthcare attack shows that the same larger problem continues today. We live in a connected society where hospitals, laboratories, insurance companies, pharmacies, collection agencies, payment processors, cloud providers, and technology companies exchange enormous amounts of information. That connectivity makes healthcare faster and more efficient, but it also creates risk. The lesson I take from both attacks is simple; our information is only as secure as the weakest organization or system trusted with it. Cybersecurity is therefore no longer about protecting computers. It is about protecting people's identities, finances, privacy, healthcare, and sometimes their ability to receive essential services.

References

AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances. (2024, March). Retrieved from American Hospital Association: https://www.aha.org/2024-03-15-aha-survey-change-healthcare-cyberattack-significantly-disrupts-patient-care-hospitals-finances

Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances. (2024, March 15). Retrieved from American Hospital Association: https://www.aha.org/2024-03-15-aha-survey-change-healthcare-cyberattack-significantly-disrupts-patient-care-hospitals-finances

Change Healthcare Payment. (2024, March 9). Retrieved from Centers for Medicare & Medicaid Services: https://www.cms.gov/newsroom/fact-sheets/change-healthcare-optum-payment-disruption-chopd-accelerated-payments-part-providers-advance

Jaikaran, C. (2024, April 24). *The Change Healthcare Cyberattack and Response Considerations for Policymakers*. Retrieved from Congressional Research Service: https://www.congress.gov/crs-product/IN12330

Siddiqui, Z. (2024, April 30). *Unired Health Hacker Used Stolen Login*. Retrieved from Reuters: https://www.reuters.com/technology/cybersecurity/unitedhealth-hackers-took-advantage-citrix-vulnerabilty-break-ceo-says-2024-04-29/