How The Change Healthcare Cyberattack is Impacting the Industry

Hassan Khan

Technology Consulting Partner

hkhan@grassiadvisors.com

212.223.5021

The ransomware attack targeting Change Healthcare, a part of Optum and owned by UnitedHealth Group, is one of the most disruptive in years, crippling pharmacies, medial groups and hospitals across the U.S. leading to serious delays in the delivery of prescription drugs nationwide.

The cyberattack carried out by a "suspected nation-state-associated" threat actor, has caused a network interruption and forced the company to shut down more than 111 services. This attack is the latest sign that the health care industry is under siege from bad actors. Now, a dispute within the criminal underground has revealed a new development in that unfolding: One of the partners of the hackers behind the attack points out that those hackers, a group known as AlphV or BlackCat, received a $22 million transaction that looks like a large ransom payment.

If Change Healthcare did pay a $22 million ransom, it would not only represent a huge payday for AlphV, but also set a dangerous precedent. Ransomware payments could fund future attacks and suggests to other predators that they should try the same, in this case, attacking critical health care services that patients depend upon.

The affiliated hacker wrote that in their penetration testing of Change Healthcare's network, they had also accessed the data of numerous other health care firms who partner with the company. If that claim is accurate, it creates additional risks, and the affiliate hacker still possesses sensitive medical information. Even if Change Healthcare did pay AlphV, the hacker affiliate could still demand additional payment or leak the data independently.

Regardless of whether Change Healthcare paid the ransom, the attack shows that AlphV pulled off a disturbing comeback. In December, it was the target of an FBI operation that seized its dark web sites and released decryption keys that foiled attacks on hundreds of victims. Yet, just two months later, it carried out the cyberattack that paralyzed Change Healthcare, triggering an outage whose effects on pharmacies and their patients have now stretched well beyond a week. As of last Tuesday, AlphV listed 28 companies on the dark web site it uses to extort its victims, not including Change Healthcare.

The following are key points regarding Federal relief efforts and actions taken:

Initial Security Incident:

- On February 21, 2024, Change Healthcare reported that its systems were compromised by a security breach.
- Providers were advised to contact their claims processing technology vendors and payors for updates to determine if they were affected.

- Strategies for requesting Medicare accelerated payments were suggested.
- A letter was submitted to the U.S. Department of Health and Human Services (HHS) requesting specific actions in response to the issue.

Impact on Providers:

- Initially, it appeared that the risk was limited to providers using software vendors integrated with Change Healthcare's clearinghouse services.
- However, further investigation revealed that many payors, including Medicare Advantage (MA) plans, some State Medicaid systems, and commercial payor claims processing systems, were also impacted.
- This disruption could lead to delays in provider payments.

Provider Relief Options:

- On March 1, UnitedHealth Group introduced a temporary funding assistance program through Optum Financial Services, but it only applies to providers whose payments are issued through Change Health systems.
- Unfortunately, this assistance may not cover most impacted AHCA/NCAL member providers.
- HHS has taken steps to assist affected providers, including those in the long-term and post-acute care community.
- Providers should continue working with payors for the latest updates on receiving timely payments.

Accelerated Payment Option:

- HHS announced that providers experiencing significant cash flow problems due to this situation can submit a request for an accelerated payment.
- While hospitals were specifically mentioned, this option is also available for skilled nursing facility (SNF) providers.

Steps to prevent cyber-attacks in healthcare

Build a Robust Cybersecurity Infrastructure – A robust cybersecurity infrastructure is the cornerstone of any defense strategy. This involves implementing firewalls, anti-malware software, data encryption and secure networks.

Employee Education and Training – Regular training of health care staff to identify and avoid potential cyber threats can significantly reduce the risk of attacks. This includes recognizing phishing emails, using strong passwords, and understanding the importance of regular software updates.

Effective Patient Data Management – Proper patient data management, including regular backups and secure data storage, can help prevent data loss in an attack. Using secure systems for data transfer and ensuring data encryption is also vital.

Regular System Updates and Patch Management – Keep all systems updated with the latest to protect against known vulnerabilities. A robust patch management process can help maintain the security of healthcare IT systems.

Deploy Network Security Measures – Implement network security measures like secure Wi-Fi, VPNs and intrusion detection systems can help safeguard against network-based attacks.

Use of Intrusion Detection and Prevention Systems – Intrusion detection and prevention systems can identify and stop cyber threats before they infiltrate the network, providing a valuable line of defense.

Implement an Incident Response Plan – Having a well-defined incident response plan can limit the damage in case of a breach and ensure a quick return to normal operations.

Efforts are underway to mitigate the impact of this security incident on health care operations, and providers are encouraged to stay informed and explore available relief options.

Preventing cyber-attacks is no small feat, but it is entirely possible with a proactive approach encompassing understanding, preparation and constant vigilance. By recognizing the importance of cybersecurity in healthcare, educating staff, maintaining up-to-date systems, and having a robust response plan, health care providers can help shield themselves and their patients from these threats.

Various payors who are impacted by this attack have reached out to providers advising that some of their systems for payment and issuing remittance advices have been, at least temporarily, modified and, in some cases, cash flow is expected to be impacted. Some payors have offered to advance payments to help providers through this period.

If your organization needs support, Grassi Healthcare Advisors (GHA) is prepared to help during this time. Please reach out to the GHA team for assistance with:

- Cash flow management during this period
- Revenue cycle modifications to accommodate transitional changes by payors
- Proactive review of your organizations defenses from future attacks