News Brief

MST INSURANCE SOLUTIONS

Change Healthcare Cyberattack Causes Unprecedented Disruptions

On Feb. 21, 2024, Change Healthcare, a subsidiary of UnitedHealth Group (UHG) and one of the largest platforms for managing health insurance billing and payments in the United States, experienced a large-scale cyberattack. This attack forced the company to shut down over 100 services across its system for multiple weeks, affecting millions of health care providers and patients across the country.

Due to its magnitude, cybersecurity experts have deemed the incident one of the most disruptive attacks in history, showcasing the devastating impacts of cyber events in the health care sector. This article provides more information on the Change Healthcare cyberattack and offers guidance to help organizations prevent similar incidents.

> **“We continue to make significant progress in restoring the services impacted by this cyberattack. We know this has been an enormous challenge for health care providers and we encourage any in need to contact us.”**
>
> - *Andrew Witty, CEO of UHG*

Cyberattack Overview

The attack began when BlackCat (also known as ALPHV), a sophisticated cybercriminal group responsible for executing several major data breaches, infiltrated Change Healthcare’s system. Although it’s currently unknown how BlackCat gained this unauthorized access, cybersecurity experts presume it was likely via remote desk protocol (RDP), brute-force techniques or application vulnerabilities. From there, the cybercriminal group deployed ransomware to render a variety of sensitive data and essential operations across Change Healthcare’s system unavailable. BlackCat then demanded the company make a large payment in exchange for restoration.

In response to the attack, Change Healthcare immediately disconnected more than 111 of its services to prevent further damage and contacted law enforcement for additional remediation assistance. From Feb. 21-28, the company’s services remained disconnected, ultimately leaving doctors and hospitals unable to bill, manage and issue prescriptions for medical procedures; preventing pharmacies from filling prescriptions; and restricting patients from making health insurance claims and receiving prescribed medications. According to digital health risk assurance firm First Health Advisory, this downtime may have cost health care providers up to $100 million per day.

During this time, several health care organizations, such as the American Hospital Association and the Medical Group Management Association, released public statements emphasizing the severity of the cyberattack and urging the U.S. government to get involved in mitigation efforts. Shortly afterward, BlackCat took responsibility for the attack, claiming they compromised more than six terabytes of health care provider, insurance program and patient data, including personally identifiable information.

On March 1, Change Healthcare began to show signs of recovery as the company made temporary funding available to health care providers in its system.

The content of this News Brief is of general interest and is not intended to apply to specific circumstances. It should not be regarded as legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice.

By March 5, the federal government announced its involvement in the remediation process, with the U.S. Department of Health and Human Services outlining a detailed plan for investigating the incident and supporting the health care sector in multiple recovery initiatives. A few days later, Change Healthcare restored services related to prescription claim submissions and payment operations. The company expects to reinstate the remainder of services impacted by the cyberattack during the week of March 18.

Altogether, the attack contributed to several weeks of considerable operational disruptions, financial challenges and health care complications for both Change Healthcare and its stakeholders. Furthermore, the company may have compounded its losses from the attack by complying with BlackCat's ransom demand. Although Change Healthcare has not confirmed this speculation, some cybersecurity experts reported that a recent Bitcoin transaction of $22 million to an account affiliated with BlackCat via the cryptocurrency's publicly visible blockchain platform proves that the company paid the ransom.

Prevention Guidance

As ransomware incidents like the Change Healthcare cyberattack become more frequent and costly, it's important for organizations to take steps to prevent similar losses. Here are some ransomware prevention tips for organizations to keep in mind:

- **Protect sensitive data.** By keeping confidential information secure, organizations can make it more difficult for cybercriminals to access this data and use it against them amid ransomware incidents. This entails selecting safe locations to store critical information, establishing routine data backup protocols and implementing access control policies (e.g., the principle of least privilege and multifactor authentication).
- **Utilize effective security software.** Various security solutions can help defend organizations' systems against potential ransomware threats. These include antivirus software, patch management plans, endpoint detection and response solutions, and email authentication technology.
- **Prioritize technical procedures.** In addition to security solutions, certain technical procedures may help organizations minimize ransomware risks. This may involve setting up RDP safeguards to limit possible attack avenues, segmenting and segregating different networks to stop the spread of attacks, and prioritizing end-of-life software management to reduce attack exposures from outdated technology.
- **Educate employees.** Because employees are widely considered the first line of defense against cyberattacks, they should be regularly educated on the latest ransomware threats, detection practices and response methods.
- **Have a plan.** Cyber incident response plans help organizations act swiftly and limit total losses when attacks occur. Organizations should include ransomware attack scenarios in their cyber incident response plans and periodically evaluate these plans through tabletop exercises and penetration testing to ensure their effectiveness.
- **Approach ransom demands with caution.** The FBI generally advises against complying with ransom demands, as there is no guarantee that cybercriminals will follow through with their end of the negotiations, potentially exacerbating overall losses. Further, organizations that pay ransom demands may be more likely to be targeted in future ransomware attacks, as cybercriminals will remember their willingness to deliver payments in the past.
- **Purchase proper coverage.** It's imperative for organizations to secure adequate cyber insurance to maintain financial protection against losses resulting from ransomware attacks. Organizations should consult insurance professionals to discuss specific coverage needs.

Contact us for additional risk management resources.