Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

The Change Healthcare Cyberattack and Response Considerations for Policymakers

Updated April 24, 2024

On February 21, 2024, UnitedHealth Group Incorporated disclosed that one of its companies' units—Change Healthcare—was experiencing a cyberattack. The BlackCat/ALPHV ransomware group—a Russia-linked cybercrime organization—claimed responsibility. Repercussions from this cyberattack are reportedly affecting some individuals' ability to access health care services nationwide.

Attack Background

In December 2023, the Department of Justice (DOJ) announced that it disrupted the operations of the BlackCat/ALPHV/Noberus ransomware group. The government developed a tool to help victims decrypt and regain control of their systems—saving them from paying an estimated $68 million in ransom payments. The Federal Bureau of Investigation (FBI) also disrupted BlackCat's infrastructure by infiltrating its systems and seizing websites. The Cybersecurity and Infrastructure Security Agency (CISA) worked with other federal agencies to update a ransomware advisory with technical indicators of compromise as well as mitigation strategies. Following the FBI's campaign, BlackCat declared that it would retaliate against the United States by targeting health care providers with ransomware.

In the subsequent two months, BlackCat was able to reconstitute its infrastructure and compromise Change Healthcare. Change Healthcare facilitates transactions in the health care system (e.g., ensuring pharmacies receive payment from insurers for medications). BlackCat allegedly used stolen credentials to gain access to Change Healthcare's systems and deploy ransomware while also exfiltrating data. Upon discovery, Change Healthcare disconnected the affected system and took other systems offline to stem the ransomware's spread. The disruption of these networks has led to a cascade of real-world consequences across the nation, with individuals unable to leverage their insurance coverage for prescriptions and cash flow issues for pharmacies as payments were frozen.

This ransomware attack bears similarities to the 2021 attack against Colonial Pipeline. Both attacks began with ransomware, led the victim to disconnect systems thereby causing operational disruptions, which resulted in physical consequences.

Congressional Research Service
https://crsreports.congress.gov
IN12330

Attack Response

As the effects of the attack have transpired, concerns over the federal response and the attack's resolution have grown.

Change Healthcare reverted to manual processes and other workarounds to continue business operations while restoring digital system. UnitedHealth has retained cybersecurity firms to investigate the attack, and has shared information with the U.S. government. They also paid roughly $22 million in bitcoin (350 bitcoins) in ransom. For some organizations, paying a ransom is cheaper than addressing response and recovery costs. But the ransom payment did not alleviate total costs related to response, system reconstitution, or business losses. UnitedHealth estimates that this breach could cost the company in excess of $1.5 billion.

The health sector has generally been critical of the federal response, calling for the U.S. Department of Health and Human Services (HHS) to take action, especially with regards to the impact on the pharmaceutical supply chain.

On March 5, 2024, HHS said it would help Medicaid and Medicare program participants switch clearinghouses for claims, encourage relaxing policies related to prior authorization, and allow accelerated payments. On March 13, HHS opened an investigation related to compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

Policy Considerations

Arguably, the incident itself is not remarkable as ransomware attacks are common. The entity that was targeted, and its effect on the broader ecosystem, however, is notable. This incident highlights the health care system's interconnected nature and nationwide reach, and the broader impact of the disruption on economic activity.

Congress and the *National Cybersecurity Strategy* created a unique response structure for cyber incidents because traditional response structures were not inclusive enough to account for the complexities of a cyber incident. Unlike physical disasters, cyber incidents do not start with an apparent, singular event. They occur and develop over time, and downstream effects (which may include physical consequences) may be more severe. The Government Accountability Office highlighted that these challenges complicate a unified federal response.

In terms of federal activity, an almost decade-old domestic cyber response policy dictates a two-pronged approach with the FBI investigating the malicious actor and DHS assisting the victim. The policy also established the concept of a Cyber Unified Coordination Group (UCG) which would bring interagency resources together in response to a specific event. This is further elaborated in the *National Cyber Incident Response Plan* (NCIRP), which is now over seven years old. The National Security Council (NSC) reportedly has convened meetings of agency deputy heads to discuss responses to the Change Healthcare cyberattack, but it is unclear whether a UCG has been established, as would be expected under the policy.

The 2023 *National Cybersecurity Strategy* directs CISA to update the NCIRP, which the agency claims is in progress—a responsibility that Congress also requires. It is unclear if the NCIRP is being used in its current state or if it is being used with some new conditions to test potential changes.

The Infrastructure Investment and Jobs Act (IIJA) authorized the Secretary of Homeland Security to declare a *significant incident* related to cybersecurity (which accounts for harm to public confidence and safety). A declaration allows the National Cyber Director to coordinate interagency activities to respond

to the incident. Such declarations need to be published in the *Federal Register* within 72 hours. To date, none have been.

The IIJA also authorized a cyber response and recovery fund to help finance technical responses to significant incidents, but funding does not extend to addressing real-world consequences of the incident.

Information Parity

This incident raises potential matters concerning information parity.

- **Coordination of offensive and defensive actions.** The FBI conducted an offensive campaign against a known bad actor. Policymakers may want consider to what extent CISA and other sector risk management agencies (SRMAs) knew about the operation, the capabilities of the actor, the probability of retaliatory actions, and the capabilities the government could bring to impede a subsequent attack. If an SRMA does not have protective capabilities, policymakers may want to consider whether the SRMA can partner with another agency, or the private sector, to respond.
- **Knowledge of conditions in decisionmaking.** CISA may not have access to the requisite information needed to declare an incident "significant." The responsibility for such declaration does not lie with the NSC, where current deliberations are occurring. If CISA does not have access to requisite information, Congress may choose to consider whether future reporting, industry partnerships, or interagency collaboration be needed to ensure a complete picture of the incident and response.
- **Information Sharing Reach.** CISA and the FBI have both released information on ransomware and its threat to hospitals, but the health care sector includes many other players (e.g., physicians and pharmacies). HHS is the SRMA for the Healthcare and Public Health sector and arguably better positioned to ensure cyber threat information can reach all sector actors. However, awareness and distribution of information to the right parties is an ongoing challenge.

Author Information

Chris Jaikaran
Specialist in Cybersecurity Policy

Disclaimer

as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.