Bolster safeguards after health care cyberattack

May 6 2024

Credit: CC0 Public Domain

Unfortunately, hackers didn't need sophisticated skills to pull off one of the nation's most alarming and consequential health care ransomware attacks.

Instead, the cybercriminals who crippled a UnitedHealth Group subsidiary earlier this year took advantage of a basic and obvious security oversight, a revelation made public Wednesday at two congressional hearings.

The subsidiary is called Change Healthcare. It acts as the Visa/Mastercard payment system for wide swaths of health care and is entrusted with patient data. Disturbingly, it did not have multi-factor authentication (MFA) in place across all of its systems.

MFA requires users, such as employees, to have two or more credentials to log in. If one credential is stolen or compromised, it provides a second layer of security to prevent bad actors from accessing networks, databases or hardware. It's a standard at many companies protecting far less vital data.

Not having it, especially in health care, is a basic error, the equivalent of not having a deadbolt on the back door in a high-crime neighborhood. With ransomware attacks hard to trace and likely to continue, the nation's lawmakers urgently need to put in place stronger information security requirements to prevent other hackers from bringing much of health care to a standstill, as the Change Health attack did.

The work to do that commendably got underway this week in Congress. Two hearings, one in the Senate and one in the House, put a timely and necessary spotlight on the ransomware attack. Andrew Witty, CEO of Minnesota-based UnitedHealth Group, testified solo throughout Wednesday.

As these events go, the hearings were unusually productive, with informed questions asked and political grandstanding at a minimum. Clarity came on some key issues, such as: How did this happen? The unsatisfying answer: UnitedHealth had completed its acquisition of

Change Health in October 2022. With the company came outdated security systems, though it seems like United should have had time to ensure comprehensive MFA was in place. Hackers using stolen credentials took advantage when it did not.

Other troubling questions, such as how many patients have had their health care data compromised, are alarmingly still unknown. UnitedHealth said last week "a substantial proportion" of Americans may have had their personal data compromised, the Star Tribune reported.

Answers are urgently needed from UnitedHealth, with lawmakers rightly pointing out that potentially compromised patient records may belong to those serving in the military. There are national security implications if their medical data are sold on the dark web, for example, and gets into the wrong hands.

These concerns are legitimate. They not only underscore the need for stronger information security requirements, but should spur Congress to move swiftly on this important reform.

Clearly, the two hearings on Wednesday are just the start of the lawmakers' work. The vulnerability exposed by an attack on just one company raises broader questions about health care consolidation and UnitedHealth's size.

The company is the "nation's largest private health insurer and largest employer of physicians" and is rapidly expanding into other areas, such as outpatient surgery centers and home health services, according to the Washington Post.

"For decades, UnitedHealth's staggering growth attracted relatively little Washington scrutiny, particularly compared with drugmakers repeatedly summoned to Congress to testify on price increases. Federal antitrust officials also traditionally focused on blocking companies from gobbling up direct competitors, known as horizontal integration, while being more permissive of the strategy practiced by UnitedHealth, which involves buying a stake in different sectors of the same industry, known as vertical integration," the Post reported this week.

While this strategy has been good for UnitedHealth, it's less clear that it's benefited consumers and health care. This phenomenon seems likelier to inhibit competition than foster it. How is that helpful in an era of rapidly rising medical costs?

For too long, rapid health care industry consolidation has been written off by many as just "the way it is." It's time to look more deeply into this. Fortunately, Minnesota has a U.S. senator, Amy Klobuchar, who is an antitrust expert (she wrote a book on it) and has clout on Capitol Hill. This week, Klobuchar provided an editorial writer with a commendable statement about her intent to continue probing the hack and the issues it raises.

"There are still a number of outstanding questions after the Finance Committee hearing in the Senate, and it is clear UnitedHealth and Change Healthcare need to do more to secure their systems and ensure that providers are getting the payments they need," Klobuchar said in the statement.

"In June, I will be holding a hearing on the role of competition policy in promoting economic resilience. As our economy has become more concentrated, the U.S. has become more susceptible to single points of failures that can create systemic issues. The UnitedHealth/Change Healthcare hack is an example of this and will be one of the topics of the hearing."

That's the right course of action. Stronger security requirements should be a priority, but other serious questions also need an airing. This is the time to begin this important work, and Klobuchar should lead it.

2024 StarTribune. Distributed by Tribune Content Agency, LLC.

Citation: Bolster safeguards after health care cyberattack (2024, May 6) retrieved 18 June 2024 from https://techxplore.com/news/2024-05-bolster-safeguards-health-cyberattack.html