Devastating Hack Sends Shock-Waves Through Healthcare

ARTICLE 03.07.24 GUI COZZI

The cybersecurity situation in healthcare looked bad throughout 2023 when 1 in every 3 Americans had their health information breached. But now it looks even worse.

A ransomware attack—currently still in progress—on a UnitedHealth Group subsidiary has caused chaos for patients and providers from coast to coast. It will also have implications for everyone, suggesting that the future of healthcare cybersecurity will be even more difficult and destructive than in the past.

What's Happening?

An announcement on February 21 revealed that Change Healthcare, which acts as a clearinghouse in the healthcare ecosystem and processes 15 billion transactions annually, had its billing and payment portals affected by a cyber attack.

As a result, the electronic portals that patients, providers, and insurers depend on to quickly process claims were no longer available, sending shock waves through the status quo. Faced with no other option, some offices have returned to paper forms and manual filing methods—but this has done little to alleviate the issues.

Patients are waiting to get necessary prescriptions and delaying important appointments while the mess gets sorted out. Providers are waiting to bill for their services, causing revenue to slow or stop entirely in some cases. Insurers, sitting in-between, must contend with mountains of paperwork while experiencing their own financial strains.

No wonder the American Hospital Association has called this "the most serious incident" ever to strike America's healthcare system.

UnitedHealth Group has faced its own consequences. Reports suggest the company paid $22 million to the cyber criminals to end the attack, but to what extent they honor that commitment remains to be seen. Regardless, the financial fallout of the attack will be much larger than that figure once all the technical costs, legal fees, regulatory sanctions, revenue losses, and brand damage are added up.

The systems affected by the hack are still down. They will eventually be restored. As a result of this hack, though, the US healthcare system will never be the same.

What's Next for Healthcare Cybersecurity?

The long-term effects of this attack will take many forms, but two are worth highlighting here.

First, cybercriminals repeat their tactics until they stop working. Since these criminals just secured an eight-figure payout by putting pressure on a healthcare organization, expect to see a wave of copycat attacks, and no one is exempt. More aggressive cyber attacks in higher volumes will be a source of stress for the entire industry. Far worse, they could put lives at risk.

Second, regulators at the United States Department of Health and Human Services have been called on to provide subsidies and relieve restrictions, and the agency issued an official statement on the attack. It has their attention. In line with other trends, this incident may eventually result in higher cybersecurity standards required by regulators, insurers, vendors, or most likely all three.

Cybersecurity was already an urgent issue in healthcare, but the risk is even greater now, and it's poised to keep rising with no signs of stopping. What steps is your organization taking to prepare?

Contact Dean Dorton for expertise in healthcare, cybersecurity, and the dynamic place where they intersect.