VIEWPOINT

Cybersecurity Lessons From the Change Healthcare Attack

Hannah T. Neprash, PhD
Division of Health Policy and Management, School of Public Health, University of Minnesota, Minneapolis.

Christian Dameff, MD, MS
Department of Emergency Medicine, University of California San Diego; and Department of Computer Science and Engineering, University of California San Diego.

Jeffrey Tully, MD
Department of Anesthesiology, University of California San Diego.

Corresponding Author: Hannah T. Neprash, PhD, Division of Health Policy and Management, School of Public Health, University of Minnesota, 420 Delaware St SE, MMC 729, Minneapolis, MN 55455 (hneprash@umn.edu).

Cybersecurity is increasingly critical to the day-to-day delivery of health care. From mandatory institutional trainings to seemingly ubiquitous media reports of ransomware attacks, even the proudest clinical Luddites are likely aware of the threat posed by cyberattacks to the practice of medicine. Cybersecurity incidents affecting health care delivery organizations (HDOs) have become increasingly frequent and disruptive. From 2016 to 2021, the number of ransomware attacks (a common cyberattack in which computer networks and the data contained within them are held hostage for pecuniary gain) on HDOs more than doubled.[1] These cyberattacks come with immense financial costs and disruptions to patient care.[2,3]

The recent ransomware attack on the technology conglomerate Change Healthcare may herald a new era of cyber threats, wherein hackers target key elements of health care infrastructure rather than individual HDOs. Change Healthcare (a subsidiary of Optum Inc, a subsidiary of UnitedHealth Group) offers revenue and payment cycle management services. When a ransomware attack disabled many of their electronic systems, thousands of physicians (many previously unaware of the existence of the company) and hospitals across the country were suddenly unable to submit claims and receive payment. By some estimates, this meant $100 million per day in deferred patient care revenue for the more than 3 weeks required to restore Change Healthcare systems to full functionality.[4] As a result, many HDOs reported difficulties purchasing supplies, paying staff, and covering other expenses. Beyond delayed revenue, the Change Healthcare attack also disrupted many HDOs' ability to verify patients' insurance coverage, seek prior authorization, electronically exchange clinical information, and e-prescribe medications. In an informal survey fielded by the American Medical Association nearly 2 months after the attack, 60% of respondents reported continuing challenges in verifying patients' insurance details and 85% reported continuing disruptions in submitting and receiving claim payments for services rendered.[5]

Without directly affecting any patient-facing care, the Change Healthcare attack profoundly disrupted the US health care system. The byzantine complexity of the network of ancillary services, supply chains, systems, and vendors supporting every hospital in the country is a web instinctually appreciated by every physician, but it is only after such linchpins fail that we fully appreciate their importance.

The Change Healthcare attack hints at the existence of a tremendously consolidated and, therefore, vulnerable market for key health care infrastructure services. This particular attack was so disruptive because Change Healthcare processes an estimated 15 billion health care transactions and touches 1 in every 3 patient records.[6] Based on market share alone, it is not surprising that Change Healthcare presented an appealing target for hackers. Furthermore, the corporate anatomy of the company, evolving as a series of acquisitions, mergers, and consolidations, may have resulted in additional risk, as the disparate technology platforms, software collections, and networks of each individual subsidiary are subsumed into the larger whole. After an alleged $22 million ransom payment was made to the organization claiming responsibility for the attack,[7] the incentives for cybercriminals to target health care infrastructure services seem increasingly lucrative.

Given its unprecedented scale, the Change Healthcare attack has rightly garnered unprecedented attention from policymakers and regulators. The Centers for Medicare & Medicaid Services within the Department of Health and Human Services took the rare step of advancing Medicare payments for hospitals and physicians. The Office for Civil Rights within the Department of Health and Human Services launched an investigation into what is likely to be a massive breach of personal health information affecting millions of patients. Federal policymakers are pursuing multiple legislative and regulatory changes in response to the Change Healthcare attack and the broader cyberthreat facing health care.

One thing is clear from the current policy conversations: physicians can anticipate cybersecurity measures becoming an even more important aspect of clinical practice and enterprise operations. While currently voluntary, the Department of Health and Human Services intends to enforce minimum cybersecurity performance goals for HDOs by the end of this decade.[8] These include implementing vendor and supplier cybersecurity requirements, strong encryption, and multifactor authentication. In light of the recent revelation that the Change Healthcare attack started when cybercriminals breached a server without multifactor authentication, there is reason to believe that incentivizing the adoption of basic cybersecurity measures may decrease the frequency of cyberattacks.[9]

As cyber threats evolve in sophistication, so too do the actions necessary to prevent and prepare for them. Specifically, the Change Healthcare attack suggests that HDOs would do well to answer the following questions: Who are your critical third-party vendors, financial intermediaries, and infrastructure dependencies? Do they engage in appropriate cybersecurity prevention and planning activities? In the event of multiweek third-party downtime, how would you minimize the effects on care delivery and business continuity? While discovering the answers to these questions is largely the responsibility of information security professionals and emergency managers, physicians know best how patient care workflows may depend on external entities. We suggest that clinicians work hand-in-hand with information security staff

to develop and refine cybersecurity incident response plans. Furthermore, we suggest that HDOs conduct cyber incident planning at the regional level, in recognition of the fact that cyberattacks affect patterns of care well beyond the entity experiencing the attack.[3]

While the Change Healthcare attack is the first example of large-scale disruption of critical health care infrastructure, it is unlikely to be the last. Market consolidation and a push for interoperability go hand in hand with the proliferation of cybersecurity vulnerabilities. Our ability to prevent, prepare for, and respond to cybersecurity incidents will depend on our ability to better understand the hidden connections within clinical infrastructure and keep our finger on the digital pulse of medicine.

ARTICLE INFORMATION

Published Online: September 9, 2024. doi:10.1001/jamainternmed.2024.3162

Conflict of Interest Disclosures: Dr Neprash reported receiving grants from the NIHCM Foundation during the conduct of the study. Dr Dameff reported receiving grants from Advanced Research Projects Agency for Health outside the submitted work. Dr Tully reported receiving grants from Advanced Research Projects Agency for Health outside the submitted work. No other disclosures were reported.

REFERENCES

1. Neprash HT, McGlave CC, Cross DA, et al. Trends in ransomware attacks on us hospitals, clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum*. 2022;3(12):e224873. doi:10.1001/jamahealthforum.2022.4873

2. Neprash HT, McGlave CC, Rydberg K, Henning-Smith C. What happens to rural hospitals during a ransomware attack? evidence from Medicare data. *J Rural Health*. 2024. doi:10.1111/jrh.12834

3. Dameff C, Tully J, Chan TC, et al. Ransomware attack associated with disruptions at adjacent emergency departments in the US. *JAMA Netw Open*. 2023;6(5):e2312270. doi:10.1001/jamanetworkopen.2023.12270

4. Moniuszko S. Health care providers may be losing up to $100 million a day from cyberattack: a doctor shares the latest. CBS News. 2024. Accessed March 10, 2024. https://www.cbsnews.com/news/change-healthcare-cyberattack-losing-up-to-100m-a-day/

5. American Medical Association. Change Healthcare cyberattack impact: key takeaways from informal AMA follow-up survey 2024. April 29, 2024. Accessed May 11, 2024. https://www.ama-assn.org/system/files/change-healthcare-follow-up-survey-results.pdf

6. US Department of Health and Human Services. Letter to health care leaders on cyberattack on Change Healthcare. 2024. Accessed March 27, 2024. https://www.hhs.gov/about/news/2024/03/10/letter-to-health-care-leaders-on-cyberattack-on-change-healthcare.html

7. Hackers behind the Change Healthcare ransomware attack just received a $22 million payment. Wired. 2024. Accessed March 12, 2024. https://www.wired.com/story/alphv-change-healthcare-ransomware-payment/

8. US Department of Health and Human Services. Fiscal year 2025: budget in brief. 2024. Accessed May 11, 2024. https://www.hhs.gov/sites/default/files/fy-2025-budget-in-brief.pdf

9. Murphy T. Change Healthcare cyberattack was due to a lack of multifactor authentication, UnitedHealth CEO says. Associated Press. May 1, 2024. Accessed May 11, 2024. https://apnews.com/article/change-healthcare-cyberattack-unitedhealth-senate-9e2fff70ce4f93566043210bdd347a1f