CSC 2.0

Healthcare Cybersecurity Needs a Check Up

By Michael Sugden and Annie Fixler

Executive Summary

In May 2021, San Diego-based hospital system Scripps Health suffered a massive ransomware attack lasting almost four weeks. The attack compromised the personal data of roughly 150,000 patients, and all five hospitals operated by Scripps Health faced significant limitations on their ability to provide care. With their data-sharing systems offline, hospital staff had to use paper records. Patients requiring emergency care had to be diverted to other hospitals. Not only did the attack cost Scripps Health a record $112 million in remediation costs and lost revenue,[1] but the diversion of patients to other facilities resulted in overcrowding and degraded care. A case study of the incident found that nearby emergency departments saw patient volumes spike along with "significant increases in … waiting room times, patients left without being seen, [and] total patient length of stay." In short, the attack caused a "regional disaster."[2]

Local healthcare providers are not the only ones threatened by cyberattacks. In February 2024, a ransomware attack on healthcare payment processor Change Healthcare disrupted payments to providers across the country for weeks.[3] The disruption affected patient care at almost three-quarters of all hospitals, and more than half reported a significant or serious financial impact.[4] An impact of this magnitude can threaten national security.

The frequency of cyberattacks against the healthcare and public health sector has increased rapidly since the onset of the COVID-19 pandemic. Ransomware in particular has become the biggest threat.[5] Ransomware attacks can block access to electronic patient records, databases, and equipment, creating a higher incidence of patient mortality and morbidity in otherwise treatable circumstances.[6] Rural hospitals face a particularly high risk.[7] Such facilities face more financial constraints, leaving them with insufficient funding to invest in cybersecurity.[8] Patients relying on these hospitals are at greater risk of complication if a cyberattack occurs, as alternative hospitals tend to be farther away than their urban or suburban counterparts.

The safe and efficient provision of health services is a matter of both personal safety and national security. This is why the federal government designated the healthcare and public health sector as a critical infrastructure sector. The U.S. government must collaborate with stakeholders in this sector to increase providers' resiliency against cyberattacks.

This report provides 13 recommendations directed at the executive branch, Congress, and the healthcare sector to guide the sector into a safer, more resilient future. Industry must invest more in cybersecurity, including by properly resourcing security teams, implementing organization-wide cyber hygiene training, and developing contingency response plans for destructive cyberattacks. The executive branch must update its strategy for the sector, provide roadmaps to secure key lifesaving services, incorporate stakeholder feedback on cybersecurity goals, and address the rural cybersecurity workforce gap. Finally, Congress should fund relevant executive agencies and programs so they can better support the sector. These recommendations are not exhaustive but serve as a starting point to address the pervasive cybersecurity issues facing the sector. The health and welfare of the American people depend on it.

Recommendations

For the Executive Branch

1. Develop New, Long-Term Sector-Specific Cybersecurity Objectives
2. Work With Industry to Identify, Prioritize, and Secure Life-Saving Services
3. Iteratively Update HHS's CPGs
4. Accelerate the CPG Compliance Incentivization Program's Timeline
5. Create a Rural Hospital Cybersecurity Workforce Development Strategy
6. Reassess Systemically Important Entities List

For Congress

7. Ensure SRMA Resources and Organizational Structure Are Optimally Efficient
8. Increase Funding for HHS's SRMA Capabilities
9. Fund HHS's CPG Resourcing and Incentive Program
10. Direct and Resource HHS to Establish a Rural vCISO Pilot Program

For Industry

11. Spend More on Cybersecurity
12. Provide Cyber Hygiene Training to All Employees
13. Develop Regional Contingency Plans for Healthcare Providers

---

1. Robert King, "May cyberattack cost Scripps nearly $113M in lost revenue, more costs," *Fierce Healthcare,* August 11, 2021. (https://www.fiercehealthcare.com/hospitals/may-cyber-attack-cost-scripps-nearly-113m-lost-revenue-more-costs)
2. Christian Dameff, Jeffrey Tully, Theodore C. Chan, Edward M. Castillo, Stefan Savage, Patricia Maysent, Thomas M. Hemmen, Brian J. Clay, and Christopher A. Longhurst, "Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US," *JAMA Network Open*, May 8, 2023. (https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585)
3. James Rundle, Catherine Stupp, and Kim S. Nash, "Medical Providers Fight to Survive After Change Healthcare Hack," *The Wall Street Journal Pro*, March 1, 2024. (https://www.wsj.com/articles/medical-providers-fight-to-survive-after-change-healthcare-hack-328c2e5a)
4. "AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances," *American Hospital Association*, March 2024. (https://www.aha.org/2024-03-15-aha-survey-change-healthcare-cyberattack-significantly-disrupts-patient-care-hospitals-finances)
5. Joel Witts, "Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know," *Expert Insights*, February 9, 2024. (https://expertinsights.com/insights/healthcare-cyber-attack-statistics)
6. Ibid.
7. Kat Jercich, "Rural hospitals are more vulnerable to cyberattacks – here's how they can protect themselves," *Healthcare IT News*, September 8, 2021. (https://www.healthcareitnews.com/news/rural-hospitals-are-more-vulnerable-cyberattacks-heres-how-they-can-protect-themselves)
8. "Rural Hospital Closures Threaten Access: Solutions to Preserve Care in Local Communities," *American Hospital Association*, September 2022, pages 3-4. (https://www.aha.org/system/files/media/file/2022/09/rural-hospital-closures-threaten-access-report.pdf)