U.S. HOUSE COMMITTEE ON ENERGY AND COMMERCE
Subcommittee on Health

Robert Sheldon
Sr. Director, Public Policy & Strategy
CrowdStrike

Testimony on Examining Health Sector Cybersecurity

April 16, 2024

Chairman Guthrie, Ranking Member Eshoo, members of the Subcommittee, thank you for the opportunity to testify today. Every week, we see news of healthcare entities like doctor's offices, hospitals, pharmacies, and insurance providers getting breached or disrupted by cyber threat actors. Each instance delays essential services, adds costs, poses difficult privacy challenges, and introduces uncertainty into the care of patients.

Some attacks against the sector have led to protracted, debilitating disruptions with national-level consequences. Once only theorized, reports are increasing in recent years of real casualties from these attacks.

While I'm unable to describe any particular breach, I'd like to share some observations and lessons from CrowdStrike's work protecting tens of thousands of customers globally–including many within the healthcare sector. Across these entities, we provide proactive defense through a variety of technical solutions, incident response services, and threat intelligence insights.

Before proceeding further, I'd like to acknowledge and thank healthcare workers and caregivers. Most enter the field to treat people–not to become cybersecurity professionals. Yet, as we've seen, cybersecurity is absolutely critical to the provision of medical care today. Many within the field are rising to the challenge–and there's more we can do as a community to help them.

The Threat Environment

Healthcare is one of the most heavily-targeted critical infrastructure sectors. Cyber threat actors attempt to breach these entities for a variety of reasons:

- Cyber criminal **(eCrime) actors** seek to monetize hacking these entities through ransomware, data extortion, Business Email Compromise (BEC), theft of medical records, and access to banking and payment information.
- **Nation-state actors** target the sector seeking information about specific individuals or broad populations for espionage purposes, and could leverage disruptive or destructive attacks to advance geopolitical aims.
- **"Hacktivist" actors** may also target entities in the sector, directly or inadvertently, to advance a social or political advocacy agenda.

Recent CrowdStrike research highlights the implications of threat actors' heightened attention on the sector. According to our 2024 Global Threat Report:

- 8% of all interactive intrusions–i.e., those with a human at the keyboard, not a bot or spam–in 2023 impacted the healthcare sector.
- Healthcare was one of the top sectors advertised by access brokers in 2023, which demonstrates how attractive the sector is to those monetizing breaches.
- Multiple "Ransomware as a Service" (RaaS) affiliates compromised healthcare entities and highlighted their access to — and provided previews of — sensitive data and records, including patient photos, in dedicated leak site (DLS) posts.

This reporting aligns with an increasing tempo of advisories shared by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS).[1] At present, eCrime actors represent the broadest threat to the sector. This could change under different political or geopolitical conditions.

Operational Environment

Healthcare cybersecurity is premised on an absolute need for continuity of operations. Health outcomes—even lives—are at stake and IT disruptions can be catastrophic. Practitioners in the space are acutely aware of these risks. However, there is a radical disparity in cybersecurity readiness and outcomes between the "haves" and "have nots" in the field. There are related but distinct challenges with respect to rural healthcare.

Healthcare IT environments can be incredibly complex. In addition to traditional enterprise infrastructure, a number of particular attributes are noteworthy. As in other sectors, cloud infrastructure is increasingly common. *Internet of Things* (IOT) and *Internet of Medical Things* (IOMT) devices as well as other esoteric endpoints extend the attack surface and may not support traditional visibility and security technologies. While some of these systems are cutting-edge, there remains widespread use of legacy technologies that present additional challenges to secure.

The healthcare business environment is also complex. Significant requirements exist for connectivity, integration, and/or interoperability between providers, insurers, and other actors. There is widespread use of Electronic Medical Records (EMRs) and increasingly, virtual treatment options. Each entails intense privacy considerations (see *Legal, Policy, and Regulatory Environment* section, below). There is meaningful payment activity both by consumers and on a business-to-business ("B2B") basis. A dynamic business environment means actors range from small startups to major hospital networks, and merger and acquisition (M&A) activity is common.

[1] Joint Cybersecurity Advisory "#StopRansomware: ALPHV Blackcat," Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Department of Health and Human Services (HHS), December 19, 2023. https://aspr.hhs.gov/cyber/Documents/stopransomware-508.pdf

Legal, Policy, and Regulatory Environment

Of all critical infrastructure sectors, healthcare is governed by one of the most complex regulatory landscapes. Of particular note from a cybersecurity perspective:

- **Health Insurance Portability and Accountability Act (HIPAA)**[2] under the **Health Information Technology for Economic and Clinical Health Act (HITECH)**[3] has required security and breach reporting for more than a decade.
- The **Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)**[4] requires cybersecurity incident reporting from entities whose disruption would impact economic security or public health and safety, including healthcare organizations.
- The **Security and Exchange Commission (SEC) Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule**[5] applies to publicly-traded entities within the healthcare space.
- General privacy and specific healthcare regulations are advancing at the state-level. New York State, for example, recently introduced **hospital cybersecurity requirements**[6] which helpfully mirrored some of the best practices outlined in Executive Order (EO) 14028.[7]
- **Healthcare and Public Health (HPH) Cybersecurity Performance Goals (CPGs)** is a voluntary, industry-specific set of cybersecurity best practices sector members should consider.[8]
- Going forward, the **FY25 President's Budget Request** for HHS includes reference to possible penalties starting in FY29 for hospitals that fail to adopt "essential cybersecurity practices."[9]

Technology and Policy Recommendations

I'd like to offer a few recommendations to improve healthcare cybersecurity outcomes. First, small- and medium- sized entities in particular, including those with resource constraints, should strongly consider leveraging a trusted Managed Security Services Provider (MSSP). The focus should be increasing speed and efficiency in dealing with threats. At best, this type of partnership enables

---

[2] Summary of the HIPAA Security Rule, U.S. Department of Health and Human Services https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

[3] Omnibus HIPAA Rulemaking, U.S. Department of Health and Human Services https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/omnibus-hipaa-rulemaking/index.html

[4] Cyber Incident Reporting for Critical Infrastructure Act of 2022, U.S. Cybersecurity and Infrastructure Security Agency https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

[5] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Securities and Exchange Commision. https://www.sec.gov/files/rules/final/2023/33-11216.pdf

[6] *CrowdStrike Comments to Proposed New York Hospital Cybersecurity Requirements,* CrowdStrike, February 2, 2024. https://www.crowdstrike.com/wp-content/uploads/2024/02/NY-Hospital-Cybersecurity-Comments.pdf

[7] Executive Order on Improving the Nation's Cybersecurity. The White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity /

[8] Health and Public Health Cybersecurity Performance Goals, U.S. Department of Health and Human Services. https://hphcyber.hhs.gov/performance-goals.html

[9] Providing Cybersecurity Support to Hospitals, Page 82. Fiscal Year 2025 Budget in Brief, U.S. Department of Health and Human Services. https://www.hhs.gov/sites/default/files/fy-2025-budget-in-brief.pdf

MSSPs to focus on security and healthcare providers focus on healthcare. Resident security talent within user organizations also saves time and can focus on esoteric security challenges (like those presented by integrating new IOMT solutions); broad security program maturity enhancements; and leadership communication.

Entities in the sector that already have sophisticated security programs should focus on the frontiers. These include:

- Leveraging Artificial Intelligence for security-related tasks;
- Implementing robust identify threat protection solutions;
- Driving enterprise-wide operational efficiency through the use of Next-Generation Security Incident and Event and Management (Next-Gen SIEM) solutions;
- Adopting a "shared services" architecture where appropriate to enforce security measures across federated or multiple associated entities;[10]
- Addressing concentration risks from overreliance on one vendor across multiple parts of the enterprise IT environment.

For their part, policymakers should identify mechanisms to support the outcomes identified above. One often-overlooked opportunity is the use of a tax mechanism (e.g., credits) to promote adoption of cybersecurity measures. These measures could be proscribed and/or targeted to selected beneficiaries (e.g., small providers, rural providers, etc). Given the issuance of a variety of new regulatory obligations to report cyberattacks, policymakers should "double down" on harmonization efforts to ensure small entities in particular are not distracted from breach response by duplicative compliance requirements.

Finally, I'd like to acknowledge the Full Committee's efforts under Chairwoman Rogers and Ranking Member Pallone to pass Federal privacy legislation. Among other important benefits, a Federal approach to privacy has the potential to simplify breach reporting obligations. This is a very important issue for the healthcare sector and beyond.

Thank you again for the opportunity to testify today and I look forward to your questions.

###

[10] The rationales outlined here are also applicable across federated entities in the healthcare sector. See Drew Bagley, "Embracing the Whole-of-State Approach to Cybersecurity," State Tech, December 5, 2023. https://statetechmagazine.com/article/2023/12/embracing-whole-state-approach-cybersecurity.