Corewell Health™

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector

Witness Testimony of Scott Dresen
Senior Vice President, Information Security &
Chief Information Security Officer

Before the Senate Homeland Security
and Governmental Affairs Committee

March 16, 2023

Chairman Peters, Ranking Member Paul, and members of the Homeland Security and Governmental Affairs Committee: thank you for inviting me to testify this morning. It is an honor and privilege to be speaking with you about this very important issue. I am the Chief Information Security Officer for Corewell Health which, as the largest integrated health system and largest employer in Michigan, is committed to health and wellness so that people can live their healthiest life possible.

In the spirit of our mission to improve health, instill humanity, and inspire hope, I am here to talk about cybersecurity threats to the healthcare sector which could compromise our health system's ability to effectively provide access to and deliver healthcare services to our patients and members. Of particular concern are high impact ransomware attacks which disrupt and delay health care delivery, may cause risk to patient safety, and used to conceal activity by threat actors to exfiltrate personal health information.

Healthcare is digitally dependent; we are in a world where healthcare is highly digital and highly connected. And that makes us vulnerable given the value of the data we manage. We have a responsibility to protect the data of our patients and members. This obligation and the associated risks are of the highest priority across our system leadership and Board of Directors.

Healthcare is a complex business model whereby multiple, often independent, entities come together to form what the patient sees as a cohesive care delivery process. Over time and often out of necessity, this model has evolved in ways that has made us more vulnerable to cyber-attacks. For example, the rapid expansion of network-connected technologies to provide telehealth during the COVID-19 pandemic increased the attack surface targeted by criminals. Other examples include increased use of third parties to provide services, expanded use of Software as a Service, and other cloud-based solutions. This has expanded the footprint of healthcare systems that must be protected and increases the opportunities for threat actors to compromise an organization.

Media reports of cyber-attacks, data breaches, and unintended exposure of sensitive data underscores the vulnerability of healthcare systems to these disruptive incidents and the impact to our patients and members. Operational disruption prevents patients from being able to receive the care they need when they need it. Material financial impact in the form of fines, penalties, and associated remediation costs increase financial pressures significantly. Brand and reputational impacts can have lasting consequences on organizations victimized by cyber-attacks. These issues only serve to undermine the trust our communities have in our healthcare system and our ability to serve them in their most vulnerable time of need.

A comprehensive information security program is critical to manage these risks. Yet there exists significant disparity in the healthcare sector for organizations to resource an effective security team and the necessary technology to provide the requisite protections to reduce the risk of an attack. Small and medium sized healthcare systems are at a significant disadvantage compared to larger systems to be able to recruit, retain, instrument, and fund an effective information security program. And despite the advantage larger organizations have in comparison, the increasing trend of attacks prove even the largest organizations are vulnerable and can be compromised.

The increasing frequency of attack from nation state actors and organized crime has created a sense of urgency within the healthcare sector and we need help from the United States government to respond to these threats more effectively. Requirements for inter-agency sharing of cybersecurity threat intelligence is a productive step forward. We need more of this and need that enhanced collaboration to include critical infrastructure sector participation including the ability to automate threat intelligence data sharing with sector participants enabling rapid, near real time automatic ingestion of threat intelligence into the technologies participating members use to protect their respective organizations. The United States government has actionable intelligence that would be of immediate value to the healthcare sector. While there is some degree of automated intelligence sharing, we need to make more of that intelligence accessible.

We are in an environment where keeping up with the technology to defend against advanced persistent threat is extremely expensive. Many of these technologies aren’t an option for financially disadvantaged healthcare systems due to cost. We recommend creating incentives to make technology more affordable and accessible to the entire healthcare sector.

We recommend reforms on the penalties healthcare entities face because of cyberattacks and related data breaches. We understand and support the legislative intent to encourage adoption of best practices and the implementation of appropriate protections to safeguard our data. However, penalizing victims of cyberattack, when defensive measures can’t keep up with the sophistication of hackers, is not the fair approach.

We are at our best and most capable when it comes to caring for our patients and members. That is our expertise. Our adversaries are at their best and most capable when they are attacking us. They are extremely well-funded, extremely talented, and highly motivated. Many are either nation state actors or sponsored and supported by nation states. We can’t beat them alone.

In conclusion, we can be more effective by enhancing existing partnerships with and between U.S. government agencies, expanding the sharing of actionable threat intelligence, incentivizing access to affordable technology to defend against advanced threats, and reforming legislation to encourage the adoption of best practices while not penalizing the victims of cyberattacks.

Thank you for this opportunity to testify and I look forward to your questions.