HealthManagement
Promoting Management and Leadership

A New Strategic Plan For Health Industry Cybersecurity

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a collaboration of private-sector healthcare infrastructure entities, working with governmental bodies to identify and tackle threats to healthcare delivery services. Within HSCC, the Cybersecurity Working Group (CWG) consists of almost 1,000 members from 425 organizations, working together to combat cybersecurity issues in the healthcare sector.

New threats call for an industry-wide strategic plan

Cyber threats are pervasive in the healthcare sector, affecting various areas including patient care, medical technology, pharmaceuticals, and public health. These attacks exploit vulnerabilities in digital infrastructure, posing risks to patient safety, data privacy, and healthcare operations. With the increasing adoption of digital technologies and remote care models, the healthcare ecosystem faces complex and evolving cybersecurity challenges. CWG's tactics include developing best practices, policy recommendations, and a strategic plan to enhance cybersecurity across the healthcare sector. Recognizing that cyber safety is crucial for patient safety, the plan aims to guide stakeholders in implementing measures to mitigate risks and strengthen the resilience of the healthcare system. Collaboration between the HSCC, government partners, and healthcare entities is essential to achieve these goals and safeguard public health infrastructure.

Industry cyber resilience: what is the goal for 2029?

The targeted state of healthcare cybersecurity for 2029 envisions several key elements laid out in the strategic plan. Healthcare cybersecurity is dynamic, readily accessible, and adhered to by both practitioners and patients alike. Responsibility for secure technology implementation spans the entire healthcare ecosystem and is a collaborative effort. Healthcare leadership takes ownership of cybersecurity as a critical enterprise risk and technological necessity. A Cyber Safety Net offers financial, policy, and technical support to ensure equitable cybersecurity practices across the sector. Continuous cybersecurity education and application are integrated into the infrastructure's wellness framework. A responsive "911 Cyber Civil Defense" mechanism guarantees reflexive, cooperative, and constant early warning, incident response, and recovery capabilities.

A plan relying on industry-specific operational and governance principles

The strategic plan's development was guided by the following operational and governance principles.

Prioritizing Patient Safety: Patient safety is paramount, with cybersecurity playing a crucial role in ensuring it.

Embracing Shared Responsibility: Cybersecurity goals involve all sectors of healthcare and public health, encouraging each organization to identify their role in achieving strategic objectives.

Balancing Security and Interoperability: Protecting sensitive data goes hand in hand with promoting data sharing and interoperability for informed care delivery.

Integrating Privacy and Security: Cybersecurity efforts support data privacy, with privacy requirements aligning with cybersecurity objectives.

Fostering Cybersecurity Innovation: Cybersecurity requirements should encourage innovation and meet evolving business needs in healthcare.

Adapting Globally: While primarily focused on the U.S. healthcare system, cybersecurity objectives should be adaptable to global healthcare cybersecurity standards.

Cultivating a Cybersecurity Culture: Cybersecurity goals are part of a lifelong commitment, not limited by existing habits or short-term perspectives.

All healthcare stakeholders participate in the plan's objectives

The following cybersecurity objectives aim to realize the proposed cybersecurity goals tailored to address current healthcare trends. These objectives form a comprehensive cybersecurity plan for organizations, both individually and collectively, to enhance the security and resilience of healthcare data, operations, and patient care. Each objective corresponds to specific stakeholders within the health sector, and is associated

with measurable outcomes consultable in the plan report: https://healthsectorcouncil.org/wp-content/uploads/2024/02/Health-Industry-Cybersecurity-Strategic-Plan-2024-2029.pdf

- Ensure products and services meet safety and resilience standards, focusing on secure-by-design and secure-by-default concepts.
- Simplify access to resources for adopting regulatory standards for securing devices, services, and data.
- Establish uniform privacy standards to protect personal data and encourage ethical data practices.
- Forge partnerships with public/private entities to safely adopt emerging technologies.
- Educate health sector leaders about cybersecurity and hold them accountable for fostering a secure culture.
- Promote cybersecurity practices among public health and smaller healthcare organizations.
- Support education and certification programs in healthcare cybersecurity.
- Use automation and AI to streamline cybersecurity processes.
- Develop specific cybersecurity profiles for the health sector.
- Create strategies for managing third-party cybersecurity risks.
- Share information about cyber disruptions to improve readiness.
- Establish mutual aid support for responding to cybersecurity incidents across sectors

Source : HSCC CWG

Image Source: HSCC CWG

Published on : Tue, 5 Mar 2024