HHS 405(d)
Aligning Health Care
Industry Security Approaches

The 405(d) Post

Volume XXIII

A Word from the Task Group

The Health Sector Coordinating Council Cybersecurity Working Group Releases the Health Industry Cybersecurity Strategic Plan

By Greg Garcia- Executive Director, Health Sector Coordinating Council

In the face of evolving cyber threats, the healthcare sector stands at a pivotal juncture. The crafting of the Health Industry Cybersecurity Strategic Plan (2024-2029) marked a concerted effort to not only anticipate future challenges but to lay down a robust framework that ensures the resilience and security of healthcare delivery systems. Myself and many 405(d) Task Group members contributed to this monumental plan, and we've witnessed firsthand the complexities and the urgent need for a unified approach to secure the healthcare ecosystem against increasingly sophisticated cyber-attacks.

The Genesis of the Strategic Plan

The necessity for the Strategic Plan was born from a clear and present danger: cyber-attacks on healthcare systems. These attacks threaten patient safety, disrupt clinical operations, and risk the privacy and security of critical health data. The interconnected nature of modern healthcare delivery, amplified by the advent of telehealth and remote care models, has expanded the attack surface, making the development of a comprehensive cybersecurity strategy not just prudent but imperative.

A Collaborative Journey

The development of the Strategic Plan was a collaborative odyssey that spanned over 20 months, engaging more than 175 industry and government organizations. This journey underscored the shared responsibility across the health sector in protecting against cyber threats. The Health Sector Coordinating Council (HSCC) Cybersecurity Working Group spearheaded this effort, embodying a partnership that transcends organizational boundaries for the greater good of patient safety and data protection.

Envisioning the Future State of Healthcare Cybersecurity

The Strategic Plan outlines a future where cybersecurity measures are not just reactive but are an integral part of the healthcare ecosystem's fabric. It envisions a state where cybersecurity is synonymous with patient safety, where technology innovations are securely integrated into healthcare delivery, and where the health sector's resilience is bolstered by collective action and shared responsibilities.

Key Pillars of the Strategic Plan

The Plan is structured around several key pillars:

User-centric Security:

Emphasizing the development and deployment of user-friendly, secure, and compliant healthcare delivery services.

Shared Responsibility:

Highlighting the importance of collaboration across all subsectors of the healthcare ecosystem to ensure comprehensive cybersecurity measures.

Resilience & Rapid Response:

Establishing protocols for preparedness, response, and resilience to enable uninterrupted access to healthcare technology and services.

The Path Forward

Mobilizing the Strategic Plan requires concerted efforts across individual organizations, industry participation, and government policy support. The Plan serves as a blueprint for action, guiding C-suite executives, IT leaders, and other stakeholders toward strategic investments and implementations that fortify the sector's defenses against cyber threats.

Conclusion

The Health Industry Cybersecurity Strategic Plan (2024-2029) is more than a document; it is a call to action for a unified and resilient front against cyber threats to the healthcare sector. It embodies our collective commitment to safeguarding patient safety, securing sensitive health data, and ensuring the uninterrupted delivery of care. As we move forward, it is imperative that all stakeholders rally around the principles laid out in this plan, translating strategy into action for a more secure and resilient healthcare future.

HICP in the Spotlight

Where do I fit and How to Use HICP

The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients document provides a structured approach to enhancing the cybersecurity posture of various health organizations, big and small. This guide aims to assist healthcare entities in implementing effective cybersecurity measures tailored to their specific size and capabilities. Here's how to determine which size category your organization fits into and how to utilize the publication effectively once you know your organization's classification.

Understanding Organization Size

To effectively use the HICP publication, an organization must first identify its size category — small, medium, or large. This classification influences the approach and resources recommended. Here's how you can identify your organization's size:

Small Organizations:

Typically, these include single physician practices, small clinics, or outpatient facilities. Key characteristics include having minimal IT support, possibly outsourcing IT needs, and handling a smaller quantity of patient data.

Medium Organizations:

These are larger than small practices but not as extensive as a large hospital system. They might include multi-specialty clinics or small hospitals. Such organizations usually have dedicated IT staff and deal with larger data volumes requiring more robust cybersecurity measures.

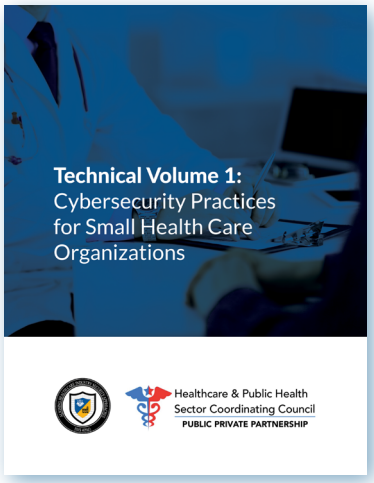
Large Organizations:

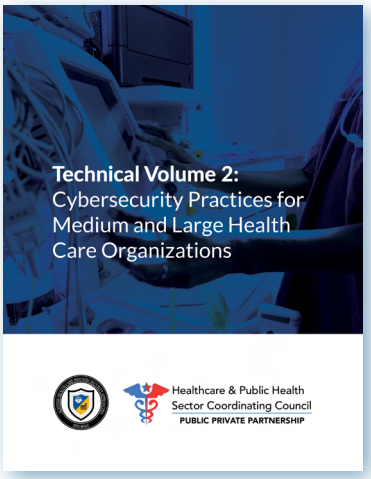
This category includes large healthcare systems and hospitals. They have comprehensive IT infrastructure, multiple locations, and handle extensive amounts of sensitive data across various departments.

The size determination is facilitated by a table within the publication, guiding you through attributes like the number of health information exchange partners, IT capabilities, provider attributes (e.g., number of beds or physicians), and complexity levels.

Using the Publication

Once the size is determined, organizations can follow specific guidelines laid out for their category:





Main Document Overview:

This document provides a general overview of current cybersecurity threats and sets the stage for detailed strategies. It is designed for executives and decision-makers to understand the urgency and nature of cybersecurity threats.

Technical Volumes:

Technical Volume 1: Tailored for small organizations, offering practical steps and simpler cybersecurity practices that do not require extensive technical expertise.

Technical Volume 2: Designed for medium to large organizations, this volume presents more complex strategies that fit the capabilities and risks associated with larger entities.

Implementation:

Depending on the organization's size, the corresponding technical volume will provide specific practices to implement. These range from basic email protection systems to advanced incident response strategies.

Customization:

It's crucial to adapt the practices to the specific needs and capabilities of your organization. This might involve focusing on particular vulnerabilities or threats that are more relevant based on your patient data and service scope.

Continuous Improvement:

Cybersecurity is an ongoing process. The publication encourages regular updates and reassessment of the cybersecurity practices in place. Engaging with new training programs, updating software and defenses, and staying informed about emerging threats are pivotal steps.

In conclusion - HICP is a dynamic tool designed to safeguard patient information and the technological infrastructures of healthcare providers. By understanding where your organization fits within the defined size categories and utilizing the specified volume tailored for your needs, you can significantly enhance your defenses against cyber threats. This strategic approach not only protects patient data but also ensures the continuity and reliability of healthcare services in the face of rising cyber challenges.

For more information, check out the full publication at 405d.hhs.gov.

HICP Chronicles

Last month during the HHS 405(d) Spotlight Webinar, CISA joined 405(d) and shared information on CISA's Priority Telecommunication Services. See below for an overview and if you would like to watch the webinar watch HERE or download the slides from our website HERE.

Ensuring Uninterrupted Communication with CISA's Priority Telecommunications Services

In today's hyper-connected world, the ability to maintain communication during crises is not just advantageous — it's essential. The Cybersecurity and Infrastructure Security Agency (CISA) recognizes this imperative and offers Priority Telecommunications Services (PTS) to ensure that essential personnel can stay connected even when network infrastructures are strained by natural disasters, cyber-attacks, or other disruptive events.

Overview of Priority Telecommunications Services

CISA's PTS are designed to prioritize communications for critical personnel, enhancing connectivity resilience during emergencies. These services are pivotal for organizations that require reliable communication for mission-critical functions. The best part? Enrolling in these services is generally cost-effective, often available at little to no expense to the organization.

Components of PTS

1. **Government Emergency Telecommunications Service (GETS)**

   GETS provides prioritization for voice calls over landlines when networks are congested or degraded. This service is crucial during widespread emergencies where traditional communication infrastructures might fail. Calls can be made from any phone worldwide, and no special equipment is needed to access the service. Notably, there is no charge to enroll in or use GETS.

2. **Wireless Priority Service (WPS)**

   Similar to GETS but for mobile networks, WPS ensures that voice calls get through even when cellular networks are overwhelmed or impaired. This service covers all nationwide and some regional networks, making it incredibly robust for national operations. WPS carriers typically waive the charges associated with this prioritization service.

3. **Telecommunications Service Priority (TSP)**

   TSP focuses on the prioritization of critical telecommunications infrastructure. This service is essential for the rapid repair and installation of voice and data circuits that are vital to operational continuity, whether in emergency or non-emergency situations. Organizations utilizing TSP are subject to minimal enrollment charges and monthly fees, which are generally offset by the high stakes of maintaining uninterrupted communications.

The PTS Dialer App

To streamline the use of GETS and WPS services, CISA offers the PTS Dialer App. This app simplifies the process of making priority calls by storing a user's GETS PIN, automatically adding necessary access numbers and codes, and integrating seamlessly with the user's phone contacts. Available on iOS and Android through the Apple App Store, Google Play, and the FirstNet® App Catalog, the PTS Dialer App is a critical tool for anyone enrolled in these services.

Enrollment and Information

Organizations looking to bolster their communications infrastructure can start by visiting CISA's dedicated Priority Telecommunications Services page. Enrollment is straightforward, with guidance available through the CISA Priority Telecommunications Service Center.

Conclusion

For organizations whose operations are critical to public safety and national security, maintaining communication during emergencies is non-negotiable. CISA's Priority Telecommunications Services offer an essential suite of tools that enhance resilience and ensure that vital communications can continue unabated during crises. To learn more about these indispensable services or to begin the enrollment process, visit CISA's website or contact the Priority Telecommunications Service Center directly. These services are not just about maintaining communication; they're about securing the continuity of operations when it matters most.

Other Links

Letter to Health Care Leaders on Cyberattack on Change Healthcare

HPH Cybersecurity Gateway

Russian Threat Actors Targeting the HPH Sector Presentation

Office of Civil Rights

HHS Office for Civil Rights Imposes a Civil Monetary Penalty on New Jersey Nursing Facility for Failing to Provide Timely Access to Patient Records

HHS Office for Civil Rights Issues Letter and Opens Investigation of Change Healthcare Cyberattack

About The 405(d) Post

This newsletter is for information purposes only and aims to broaden awareness and align healthcare security approaches. The "A Word from the Task Group" and the "405(d) Chronicles" is written by a different 405(d) Task Group Member each issue and does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute to this newsletter. The news articles are not an endorsement of any product/viewpoint/entity. Use of this document is neither required by nor guarantees compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations.

Need To Contact Us? Email us at cisa405d@hhs.gov

Follow us!

Facebook X

Instagram LinkedIn

Visit our website at 405d.hhs.gov!