5 CRITICAL CYBERSECURITY ACTIONS FOR THE HEALTHCARE SECTOR IN 2024

digicert®

Every year, the Health Information Sharing and Analysis Center (H-ISAC) gathers for the Fall Americas Summit. Here, the world's leading cybersecurity minds in the healthcare sector collaborate to build a strategy for preventing, detecting and responding to cybersecurity and physical security threats to improve outcomes and save lives. This is what the brightest healthcare experts see coming in the next year—and what you should do to protect your organization and patients.

1. IDENTITY FOR USERS, SERVERS, ENTERPRISE DEVICES AND MEDICAL DEVICES

"Without identity, you can't have trust within your ecosystem."

- New regulatory measures from the FDA—as well as the proliferation of connected medical devices—are driving an increased focus on establishing strong identity.
- Manufacturers are looking for new ways to get identity onto medical device endpoints so they can be tracked, secured, and mutually authenticated.
- Healthcare Delivery Organizations (HDOs) also require strong identity for traceability and management of the device from onboarding through the entire device lifecycle.

84%

increase in healthcare breaches from 2018 to 2021 (source HHS)

89%

of healthcare organizations reported an average of 43 cyber attacks per year, nearly one a week (source Ponemon Institute)

53%

of connected and IoT devices in hospitals have vulnerabilities (source FBI)

2. SECURE SOFTWARE SUPPLY CHAIN

"It's vital to have security and integrity throughout the lifecycle of the development of software."

- The FDA has a variety of new mandates for healthcare software that require scanning and signing throughout every stage of development, as well as the submission of a software bill of materials (SBOM).
- SBOMs ensure continuous integrity from source, to build, to packaging and distribution.
- SBOMs are vital to defend against the growing prevalence of software supply chain attacks, prevent loss from data breaches, and ensure compliance with new regulations. However, many organizations are struggling to effectively create and submit an SBOM.

3. SECURITY VENDOR CONSOLIDATION

"I'm managing 10,000 relationships. I'm challenging my team to do more with less."

- The current economic situation is driving many organizations to extract more value from their current approach while reducing complexity and redundancy.
- Public Key Infrastructure (PKI) is a prime example of a solution that can be easily consolidated.
- By bringing multiple PKI providers under a single management platform, organizations can quickly gain more efficiency.

4. GAINING CONTROL OVER BROAD AND DIVERSE INFRASTRUCTURE

"Five years ago, it was the wild, wild west. Today, we're seeing a move toward centralized control. It's a much better approach."

- Corporate product security teams are establishing policies and governance models to ensure more control when organizations deploy new security initiatives.
- Centralized control delivers better transparency, visibility, and control for organizations, streamlines reporting and audits, and simplifies rights management and access controls.
- Due to the increasing burden of managing certificate expiration and renewal, many organizations are moving toward a centralized Certificate Lifecycle Management system that enables end-to-end discovery and automation.

5. COMPLIANCE AND REGULATORY AGILITY

"A lot of organizations see FDA best practices and don't know where to start."

- The FDA has released a stringent framework of security best practices and now has regulatory authority to deny submissions, which has led the industry to make compliance a key focus.
- PKI is the technology underpinning many of the recommended practices, including authentication, code signing, whitelisting, and vulnerability scanning.
- A centralized PKI strategy is an excellent starting point for hardening security and ensuring compliance.
- The key to long-term success is standing up a CA with the ability to scale and grow as needed so your organization has the agility to rapidly adapt to changing requirements and evolving threats.

ABOUT DIGICERT

Digital trust has become the backbone for security in the connected world. DigiCert is the leading provider of digital trust, enabling companies and individuals around the globe to navigate the connected world with the confidence that their digital footprint is secure.

RESOURCES

- To learn more about security for medical device manufacturing, click here.
- To learn more about payer, provider, or supporting enterprise IT initiatives, click here.
- To learn more about supply software to the healthcare sector, click here.
- To learn about how quantum computing will impact healthcare security, click here.
- Access DigiCert's quantum safe playground here to generate PQC certificates and experiment with singing, authentication and encryption using NIST-approved algorithms, free of charge