Monthly Cyber Briefing

February 2024

Clearwater

Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Recording and final slides shared within 48 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Agenda

- Cyber update
  - Healthcare breaches
  - Ransomware
  - HHS Cybersecurity Strategy and Performance Goals
  - OCR Enforcement Focus
  - Regulatory Changes

- Evolving guidance for medical device cyber-risk and the strategic management approaches for tackling legacy devices

Speakers

Steve Cagle
CEO
Clearwater

Jon Benedict
Director, Consulting Services,
IDN/Hospital Team
Clearwater

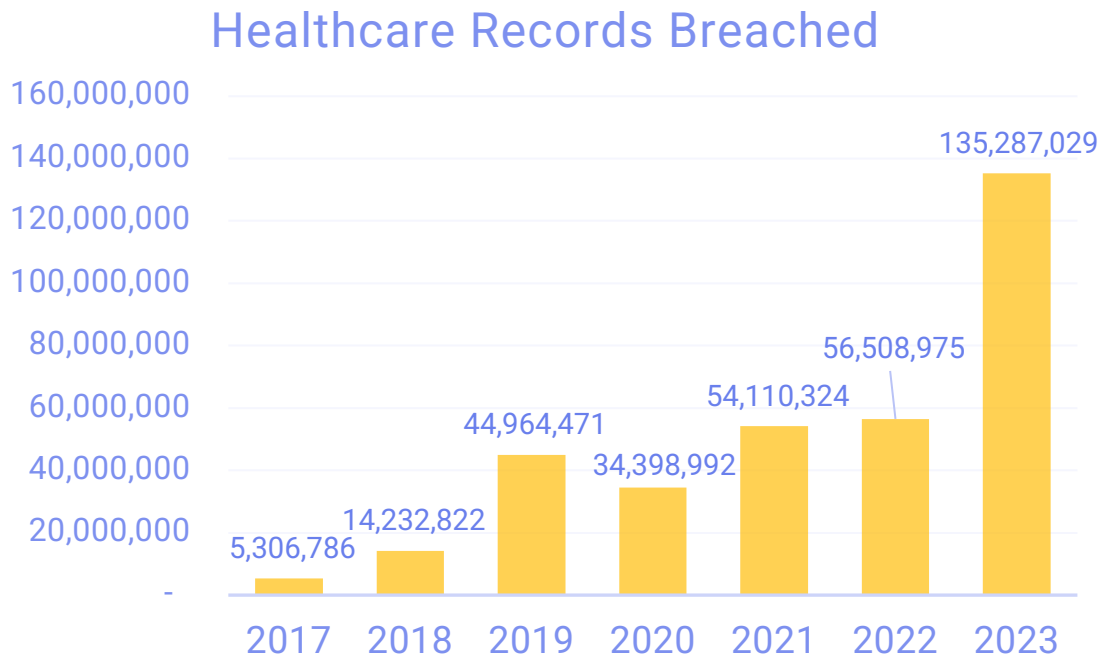
Cyber Update

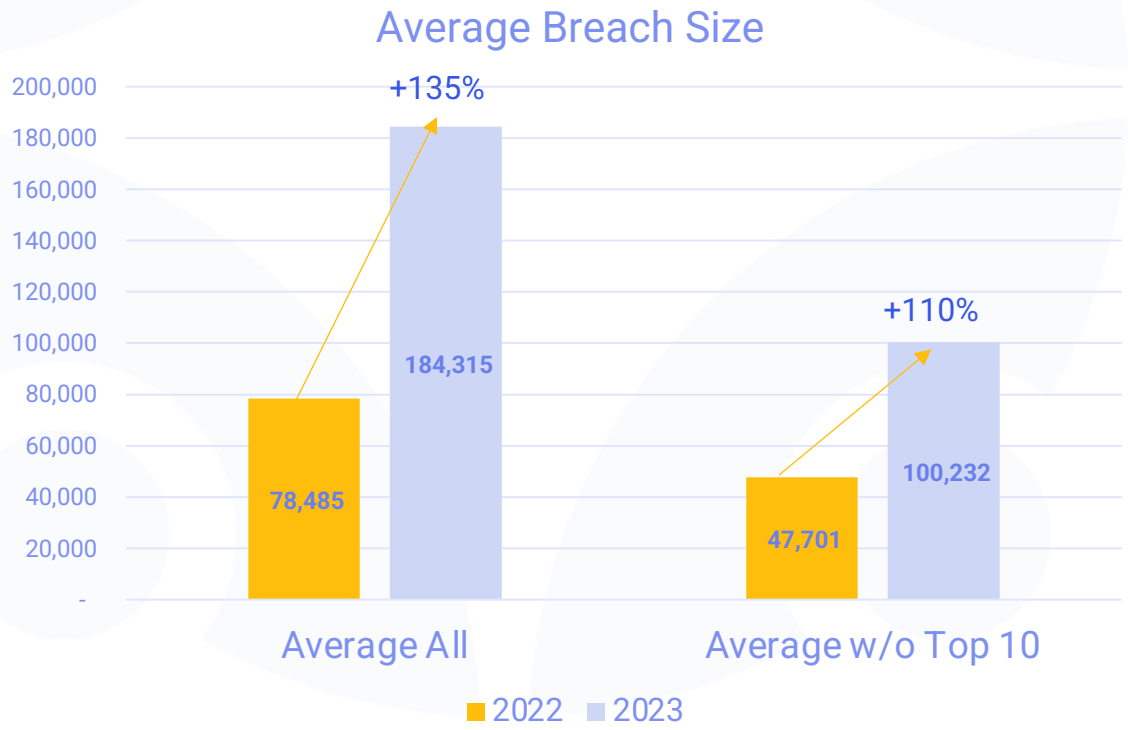
Steve Cagle

Clearwater

Recap of 2023 (Updated Data as of 1/31/24)

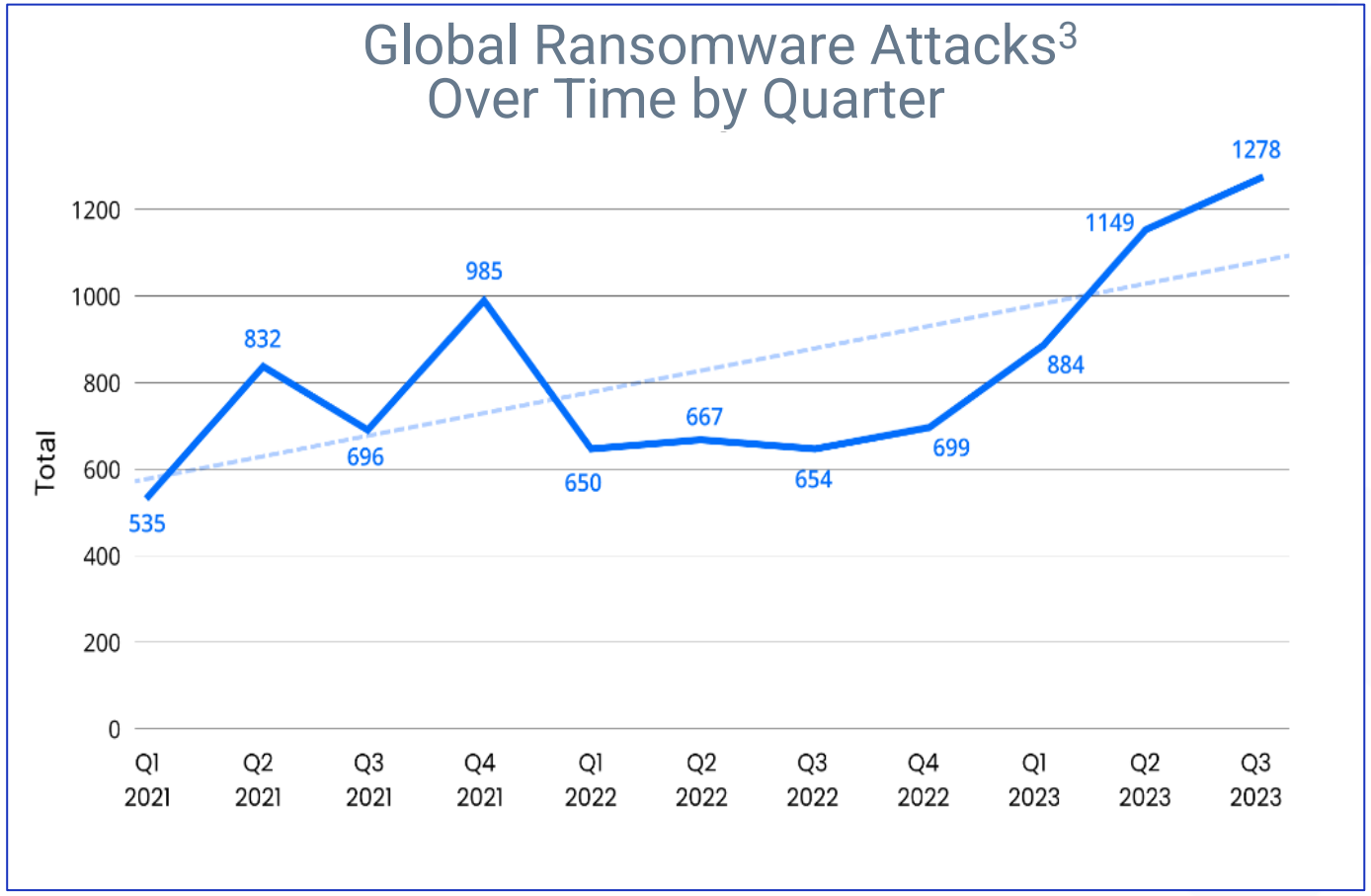
- 135.3M records reported breached in 2023, and increase of 139% vs 56.5 million in 2022[1]
- 734 breaches reported in 2023 vs 720 in 2022, a slight increase
- Average breach size has increased 135%, and 110% if removing top 10 breaches each year
- As of 1/31/24 5.6M records reported as breached in month of January, however, the majority are related to PJ&A (business associate) breach reported in November





[1]Source: HHS Breach Portal. Data pulled January 7, 2024.

Ransomware Attacks Spiked in 2023



2023 ransomware attacks up more than 95% over 2022[1].

46 U.S. hospital systems suffered ransomware attacks in 2023, up from 25 in 2022 and 27 in 2021.[2]

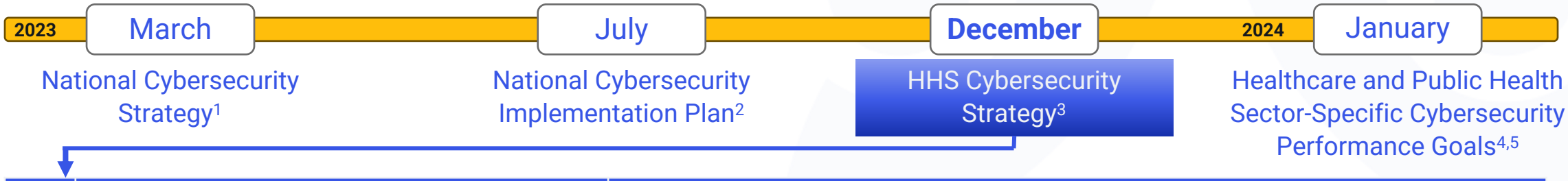
New Trends

- Dwell time from 4.5 days -> < 1 day[4]
- "New" ransomware groups targeting healthcare: Hunters International, Inc. Ransom, Money Message
- Contacting patients directly (swatting)

Clearwater

[1]2023 Ransomware Attacks Up More Than 95% Over 2022, According to Corvus Insurance Q3 Report (darkreading.com)
[2]The State of Ransomware in the U.S.: Report and Statistics 2023 (emsisoft.com)
[3]Q3 Ransomware Report: Global Ransomware Attacks Up More Than 95% Over 2022 (corvusinsurance.com)
[4]Ransomware Dwell Time Hits Low of 24 Hours | Secureworks

HHS Cybersecurity Strategy



#	Step	Details
1	Establish voluntary cybersecurity performance goals	• Prioritize "high impact" practices that drive desired outcomes • Remove "confusion" as to which practices to implement • Essential and "enhanced" goals
2	Provide resources and incentives	• Upfront investment program for low-resourced hospitals • On-going incentives (financial consequences) for meeting goals
3	Greater enforcement and accountability	• CMS will propose new cybersecurity requirements for hospitals through Medicare and Medicaid • OCR will begin update to HIPAA Security Rule to begin in spring 2024 • OCR will ask Congress to increase HIPAA violation penalties • OCR is seeking funding for more resources for enforcement actions, auditing
4	Expand and mature one-stop shop withing HHS	• Mature cybersecurity support function for sector within the Administration of Strategic Preparedness and Response (ASPR) • Enhance coordination within HHS and the Federal Government

Clearwater

1 National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov)
2 National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf (whitehouse.gov)
3 Healthcare Sector Cybersecurity (hhs.gov)
4 HPH Cybersecurity Gateway (hhs.gov)
5 Healthcare and Public Health Sector-Special: Cybersecurity Performance Goals (hhs.gov)

HHS Releases Voluntary Healthcare Specific Cybersecurity Performance Goals (CPGs)[1,2]

- Mapped to 405(d) health industry cybersecurity practices (HICP), NIST CSF v1.1, NIST 800-53 Rev5, and CISA CPGs
- Appears to seek to more clearly define what is required to achieve a desired outcome
- May ultimately just create more confusion?

ID	Goals	Desired Outcomes (NIST CSF V1.1)	HICP Practices	HICP Sub-Practices	NIST 800-53 REV5 Controls	Threats Mitigated
1	**Mitigate Known Vulnerabilities:** Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet	**ID.RA-1:** Asset vulnerabilities are identified and documented **PR.IP-12:** A vulnerability management plan is developed and implemented **DE.CM-8:** Vulnerability scans are performed **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks **RS.AN-5:** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) **ID.RA-6:** Risk responses are identified and prioritized **PR.AC-3:** Remote access is managed	**Vulnerability Management** **Endpoint Protection**	**Host/Server-Based Scanning** 7.M.A **Web Application Scanning** 7.M.B **Basic Endpoint Protection Controls** 2.M.A	CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 RA-1, RA-3, RA-5, SI-2 CA-5, PM-4, PM-9, PM-28, RA-7 CA-1, CA-2, RA-1, PM-4, PM-15, RA-7, SI-5, SR-6 AC-1, AC-17, AC-19, AC-20, SC-15	Ransomware Social engineering Insider threat Attacks on network connected devices

Clearwater

1 HPH Cybersecurity Gateway (hhs.gov)
2 Healthcare and Public Health Sector-Special: Cybersecurity Performance Goals (hhs.gov)

HHS CPGS – Our View & Recommendation

- The establishment of well-defined, healthcare-specific cybersecurity performance goals is a positive step forward in helping less mature organizations prioritize important security practices.
- We are glad to see that the CPGs provide references to specific outcomes from existing frameworks, control sets, and practice guides already used in healthcare, such as the 405(d) HICP, NIST CSF v1.1, and NIST Special Publication 800-53 rev5.
- The CPGs reflect intended outcomes of a very basic subset of security practices. We at Clearwater are concerned that this might create further confusion and lure some organizations into a false sense of security.
- Our recommendation does not change – leverage the NIST CSF using 405(d) HICP and continue to perform on going risk analysis of all information systems with ePHI.

How Is Clearwater Addressing?

- HPH CPGs are mapped to the NIST CSF and 405(d) HICP, and therefore understanding an organization's status relative to the CPGs is achievable by analyzing outcomes from our existing NIST CSF and 405(d) HICP evaluations, and **we can provide this output from our existing assessments.**
- Clearwater uses NIST CSF and 405(d) HICP for its ClearAdvantage® Program, or to help organizations create their strategy roadmaps. As such, clients who subscribe to the ClearAdvantage program, and implement our recommendations, are, by definition, achieving and exceeding these goals.

We Expect OCR to Continue Enforcement Focus in These Areas in 2024

Enforcement related to

- Phishing attacks
- Ransomware attacks
- Failure to conduct OCR Quality Risk Analysis
- Right of Access
- Embedded Tracking Technologies

HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation

OCR Settles with Business Associate in attack affecting over 200K individuals

HHS' Office for Civil Rights Settles First Ever Phishing Cyber-Attack Investigation

Louisiana Medical Group settles after investigation reveals large cybersecurity breach affecting nearly 35,000 patients

HHS' Office for Civil Rights Settles Multiple HIPAA Complaints With Optum Medical Care Over Patient Access to Records

This Settlement with Optum marks the 46th Enforcement Action in the OCR Right of Access Initiative

HHS Office for Civil Rights Settles with L.A. Care Health Plan Over Potential HIPAA Security Rule Violations

$1.3M settlement after failure to conduct OCR Quality Risk Analysis

HHS Office for Civil Rights and the Federal Trade Commission Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies

Other Regulatory Updates

- OCR Initiaitives[1]
  - NPRM on April 12, 2023 to prohibit the use or disclosure of PHI to identify, investigate, prosecute, or sue patients, providers, and others involved in the provision of legal reproductive health, including abortion
  - Update to HIPAA Privacy Rule expected this year
  - Updates to HIPAA and Part 2 related to disclosures and penalties for substance use disorder (SUD) patients
  - Update to HIPAA Security Rule per cybersecurity strategy
- CMMC rules released for comment in December 2023, and regulation expected to be in effect in 2024[2]
- The Federal Acquisition Regulatory (FAR) Council on Oct. 3, 2023, issued two proposed rules for incident reporting and new cybersecurity requirements[3,4]
- SEC Cybersecurity incident reporting regulation in effect since December 18th for SEC registered companies[5]
- CIRCIA Notice of Proposed Rulemaking, which is required to be published no later than March 2024[6]

[1] Clearwater January 2024 Cyber Briefing
[2] Cybersecurity Maturity Model Certification Program Proposed Rule Published > U.S. Department of Defense > Release
3 2023-21328.pdf (govinfo.gov)
4 2023-21327.pdf (govinfo.gov)
5 Tighter SEC Cybersecurity Incident Disclosure Requirements Go into Effect Today | Locke Lord LLP - JDSupra
7 Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) | CISA

Other Regulatory Updates – State Level

- NY State proposed cybersecurity regulation and $500m in grant money for hospitals in November 2023[1]
  - Rules are out for public comment period – ends 2/5/24
  - Grant money in the budget for 2024 – applications due March 13th[2]
- The Florida Cybersecurity Incident Liability Act (H.B 473) has been introduced in the Florida legislature
  - Aims to introduce a “safe harbor” that limits liability for all businesses that implement reasonable and appropriate cybersecurity measures that meet industry standards and cybersecurity frameworks

1 Clearwater January 2024 Cyber Briefing
2 GO_5002669_fupGOFullPDFUpload.pdf (sachspolicy.com)

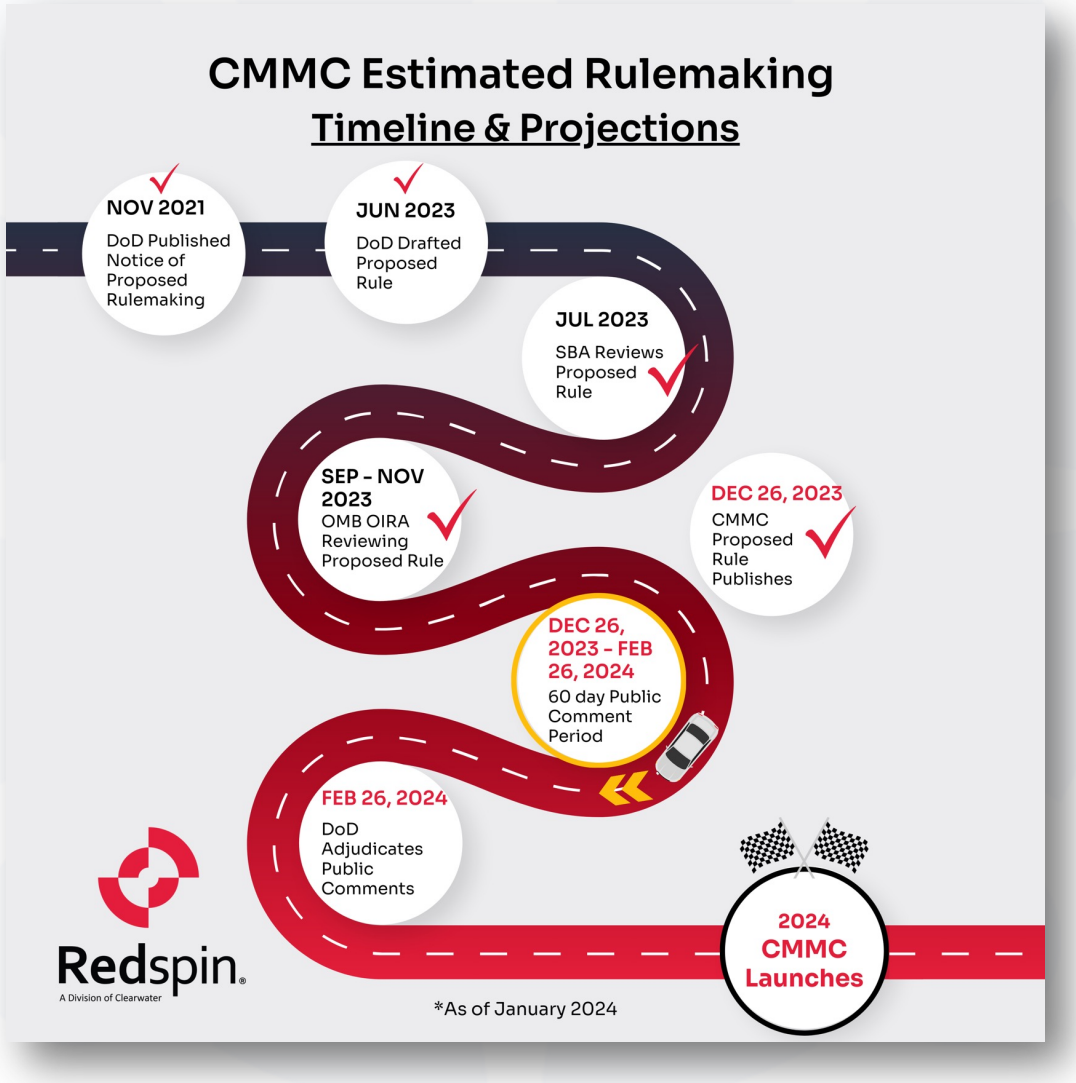
Recommendations Based on Current Threat & Regulatory Enforcement Environment

Areas where you may want to “turn up the dial”:

- *Increase* cadence of vulnerability scanning, and prioritize remediation of high-risk vulnerabilities
- *Ramp sophistication* of social engineering tests to reflect more current TTPs
- *Scrutinize* your capabilities to *detect and respond* to attacks – orchestration of end point detection, log management, and vulnerabilities, coverage, incident response process and timelines
- *Execute* security controls validation assessments that are aligned to current attack scenarios taking place in healthcare
- *Update and exercise* incident response and test recovery plans
- Conduct on *on-going* risk analysis – *at the information system level*
- *Prioritize* security projects based *on YOUR risk* – NOT someone else’s checklist
- *Conduct a third-party compliance* assessment to ensure you are meeting requirements

Latest Resources

Healthcare's Incident Response Playbook



A roadmap of CMMC estimated rulemaking timeline projections.

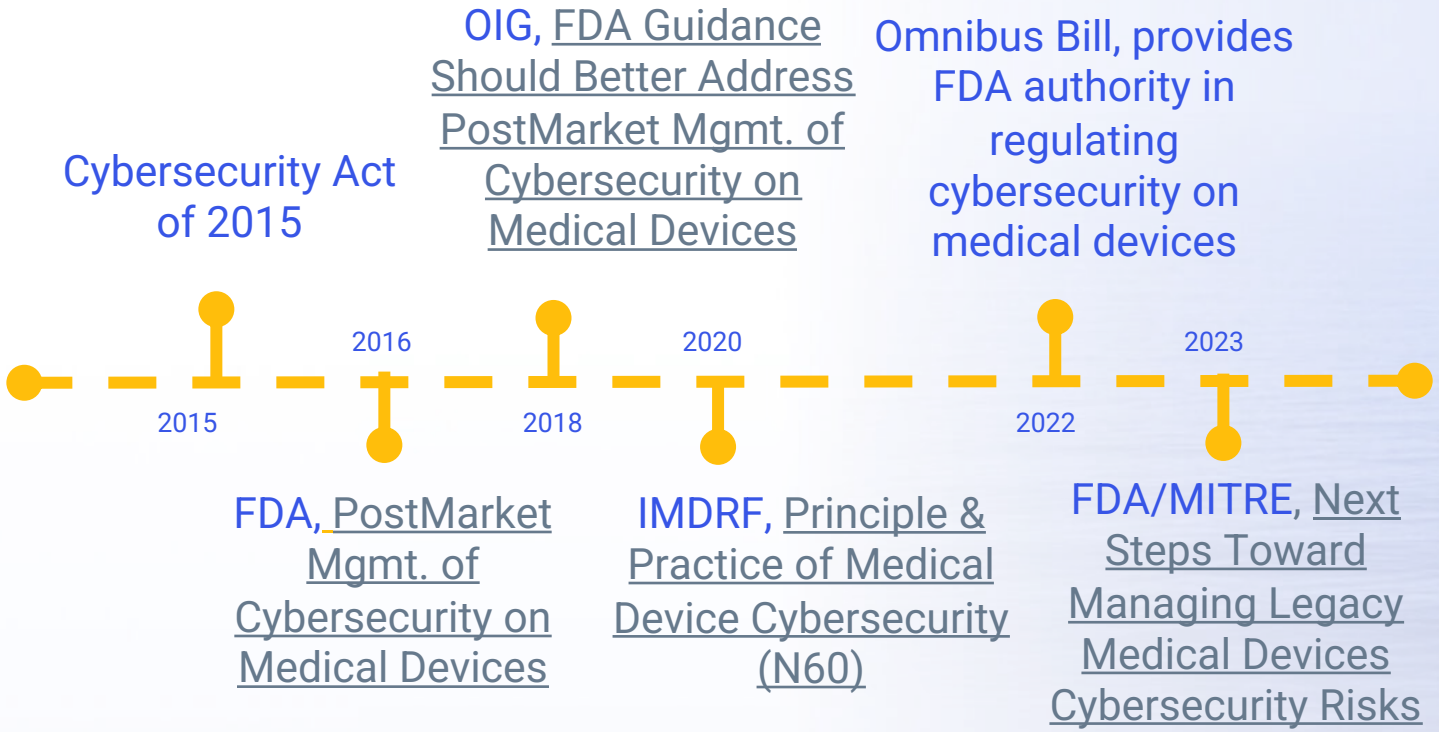
Clearwater

Evolving Guidance for Medical Device Cyber-Risk

Jon Benedict

Clearwater

Guidance Updates for Legacy Medical Device Cybersecurity



Legacy is a Today problem not Tomorrow

- Most Devices would currently be considered Legacy – not meeting the cybersecurity lifecycle guidance.
- Many still have a useful life that lasts beyond the declared “end of support” or “end of life” status by mfg.

Definition of Legacy

A legacy medical device is any device that cannot be reasonably protected against cybersecurity threats.

How do we address?

- Recommendations to address legacy medical device challenges:
  - Shared responsibility of all stakeholders, including MDMs, HCPs, users, regulators, and software vendors throughout the medical device lifecycle
  - Vulnerability Management
  - Workforce Development

The Risk-Informed Challenge

- Data is needed to inform strategic decisions for your MDS Program
- SBOM
  - Understand the risks associated with all components of a medical device
  - Required for all new FDA submissions after 10/1/2023
- Vulnerability Management
  - Must be a shared responsibility
- Workforce Management
  - Templates for Roles and Responsibilities

Medical Device Vulnerability Management

- The current vulnerability management process is resource intensive and time consuming for HDOs & MDMs
- Focus on streamlining and improving the process
- Ensuring information is actionable and is directed to the appropriate individuals within the affected organizations.
- Identifying areas for automation
- Leveraging SBOMs and other databases

Workforce Management / Competency Models

- Managing the risks of legacy devices and minimizing the impact of devices becoming unsupported requires a skilled workforce
- Competency Models can be used to determine what skills and knowledge are required for different roles supporting critical functions that manage legacy risk
- HDO Competency Model Template
  - Cybersecurity core competencies
  - Critical areas and functions
- Resources for workforce development
  - CISA provides a collection of cybersecurity training resources
    - https://www.cisa.gov/cybersecurity-training-exercises
  - The Federal Virtual Training Environment
    - https://fedvte.usalearning.gov/public_fedvte.php

Clearwater

The Practical Outcome of Risk Management

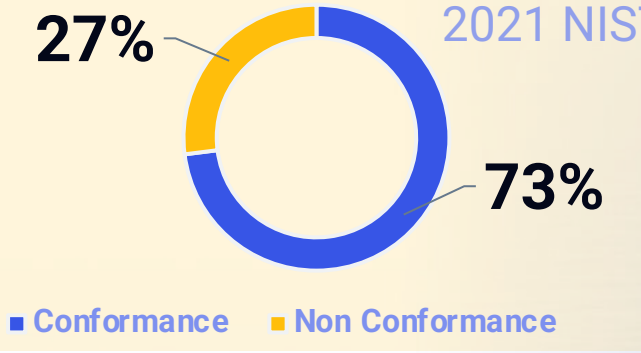
- One size does not fit all:

- What a large hospital system did:
  - Deep tech stack, discovery tools integrated with CMDB and ticketing system

- What a small hospital did:
  - Not as mature tech stack, well thought out policies and procedures with a well-trained staff that understands and executes the program

Maturity Score – 3 Year Comparison

of the 23 Categories assessed scored 3 or higher



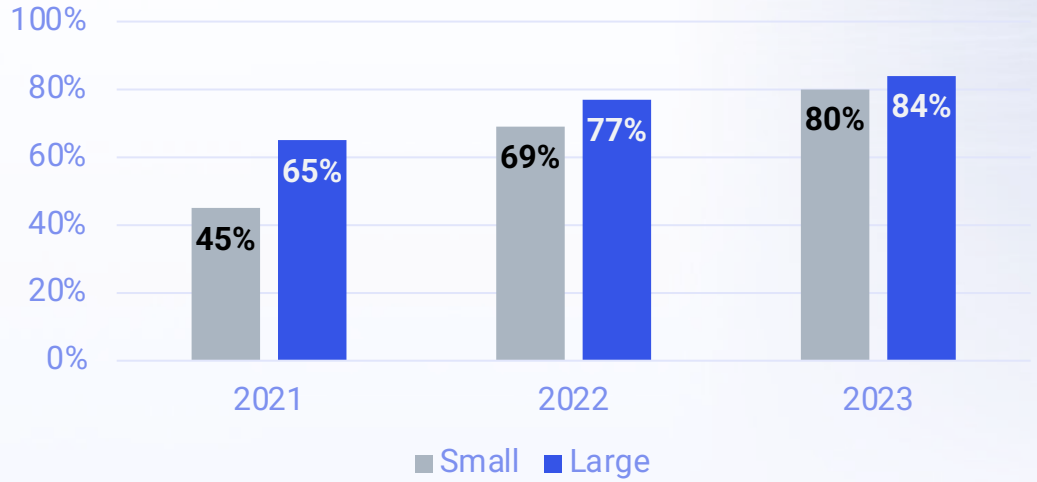
2021 NIST CSF Assessment Results

2.9

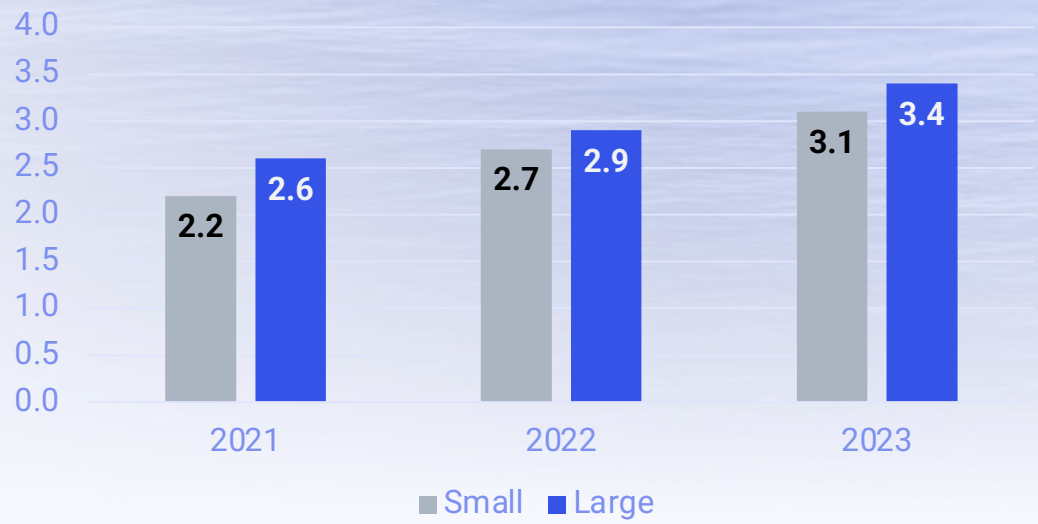
The average maturity score of each of the 23 Categories assessed was #

Client Average Maturity of each Category

Maturity Comparison



Industry Average COBIT Maturity of CSF 1.1



Clearwater

Staying Resilient to Medical Device Attacks

- Have a current, accurate inventory of all medical devices connected to your network
- Know who is responsible for working with manufacturers and vendors to confirm security settings and approved patches
- Ensure software updates are properly and timely maintained on each device.
- Segmentation is one of the most scalable and effective defenses
- Document and know what your plan is when medical devices are compromised.
  - Communicate how patients should notify you if they suspect a compromise.
- Regularly practice your organization's protocols in case of a potential shutdown or attack against medical devices.

Q&A

Clearwater

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Upcoming Events

ViVE | February 25-28, 2024
Booth #1549, Cybersecurity Pavilion

HIPAA Summit | February 27-March 1
Cybersecurity Roundtable on Feb. 28

HIMSS | March 11-15
Booth #1618, Cybersecurity Command Center

HCCA | April 14-17
Andrew Mahler presenting "How Safe Is 'Safe Harbor'? Balancing De-identification, Anonymization, and Pseudonymization of Health Data with Privacy Risks" on April 15

Clearwater

Clearwater

Healthcare – Secure, Compliant, Resilient

Contact us

info@clearwatersecurity.com

www.clearwatersecurity.com

1.800.704.3394

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Twitter | @clearwaterhipaa

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.