The vCISO

Full Experience / Fractional Cost

Disproving The Infinite Monkey Theorem:

Because we just don't have that kind of time

UNCLASSIFIED / For Official Use Only (FOUO)

Updated: January 2025
Version 1.0

But first, the legal mumbo jumbo...

Disclaimer / Warning

The vCISO
Full Experience / Fractional Cost

- This presentation is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations.
- These opinions are not meant to defame, purge, humiliate, or injure anyone should you decide to act upon or reuse any information provided.
- All trademarks, service marks, collective marks, design rights, personality rights, copyrights, registered names, mottos, logos, avatars, insignias and marks used are the property of their respective owners.
- I the author of the content found herein assure you that any of the opinions expressed are my own and are the result of the way in which a mind uniquely wired as my own singularly interprets things.
- Objects in the mirror may be closer than they appear.
- Those of you with the home version, please feel free to follow along.
- As Dennis Miller used to say, this is just my opinion, I could be mistaken.
- As always, no wagering.
- Stay alert as this performance may feature loud noises, pyrotechnics, strobe lights, or indiscriminately thrown air-borne projectiles.

What's wrong with this picture?

Why are we here?

Introduction

The vCISO

Full Experience / Fractional Cost

- **Briefing Purpose:**
  - **Share experiences** so that we may learn from one another
  - **Reduce the likelihood** that any of us will more in the hot seat
  - Promote awareness of capabilities in support of **increased partnership**
  - Satisfy a few **control requirements** while we're at it.

- **Discussion Topics:**
  - NIST OCR HIPAA Security Summit (Scope, Scope, Scope)
  - Updated HIPAA Rules
  - AHA Content (Hint It's Not Hospitals)
  - AI Framework (Policy & Questions)
  - Supply Chain and TPRM (Std Clauses, Minimum Security Standards)
  - Cost Optimization Strategies (Microsegmentation, Scanning, Zero Client)
  - Incident Response (False Claims Playbook).

Which control objectives does this briefing helping us all address?

Controls Fulfillment

The vCISO
Full Experience / Fractional Cost

- **Third Party Risk Management / Supply Chain:**
  - PS-07: Third-Party Personnel Security
  - SA-04: Acquisition Process
  - SA-12: Supply Chain Protection
- **Change Management / Security Impact Assessments:**
  - CM-03: Configuration Change Control
  - CM-04: Security Impact Analysis
  - CM-05: Access Restrictions for Change
- **Incident Response:**
  - IR-02: Incident Response Training
  - IR-03: Coordination with Related Plans
  - SI-05: Security Alerts & Advisories
- **Device Authentication:**
  - CM-02: Baseline Configuration
  - IA-03: Device Identification and Authentication
  - IA-05: Authenticator Management
  - IA-08: Identification and Authentication (Non-Organizational Users)
- **Contingency Planning:**
  - CP-02: Contingency Plan
  - CP-07: Priority of Service
  - CP-08: Telecommunications Services
  - CP-10: Information System Recovery and Reconstitution
- **Resiliency By Design / Backup:**
  - CP-09: Information System Backup
  - SC-05: Capacity, Bandwidth, and Redundancy
  - SC-06: Resource Availability
  - SI-04: Information System Monitoring

Why do we have CSCOUT?

Our Shared Journey

The vCISO

Full Experience / Fractional Cost

- **The Path Taken**
  - Booz Allen (ARPANET, CERT, Intel/DoD, DoE, VA, NASA)
  - Ajilon/Adia/Adecco (FinTech, HHS/CMS, Commercial Healthcare Providers)
  - ViPS, WebMD, Emdeon, GDIT, Maricom, CSC, FEI (~60% of the Medicare Portfolio)
  - HITRUST
  - The vCISO
- **Achievements Realized**
  - Fully realized and compliant cybersecurity programs
  - Risk, Remediate, Refine Repeat
  - Met business needs without putting customers or data at risk
  - 38+ years without a compromise or reportable event
- **But we're in this together. And the last couple of years? Oh boy!**
- **So, Why? What Changed? What's the root cause?**
  - Regulators Need to be Seen to Act but are making things worse
  - Seemingly unable to leave well enough alone
  - Abject failure to recognize risk or price it in
  - Lack shared/mutual accountability
  - We've ignored too many things at our peril

"We've long since addressed the "Material Weakness" but the stakes have never been greater and IMHO, the CMS program, our shared mission, the beneficiaries, and their data have never been challenged by the risks we now (and will increasingly) face."

Background & Context

The vCISO

Full Experience / Fractional Cost

What do hospitals have to do with healthcare?

Selfishly Serving the Entire Industry

The vCISO
Full Experience / Fractional Cost

1. Johns Hopkins Health System
2. University of Maryland Medical System
3. MedStar Health
4. Adventist HealthCare
5. LifeBridge Health
6. Luminis Health
7. TidalHealth
8. Holy Cross Health
9. Mercy Health Services
10. Sheppard Pratt Health System
11. Frederick Health
12. Calvert Health
13. Garrett Regional Medical Center
14. Doctors Community Health System
15. Meritus Health.
16. UM Shore Regional Health
17. UM Capital Region Health

CHiME®

AEHiS

American Hospital Association™
Advancing Health in America

Maryland Hospital Association

Maryland State Healthcare Cybersecurity Working Group

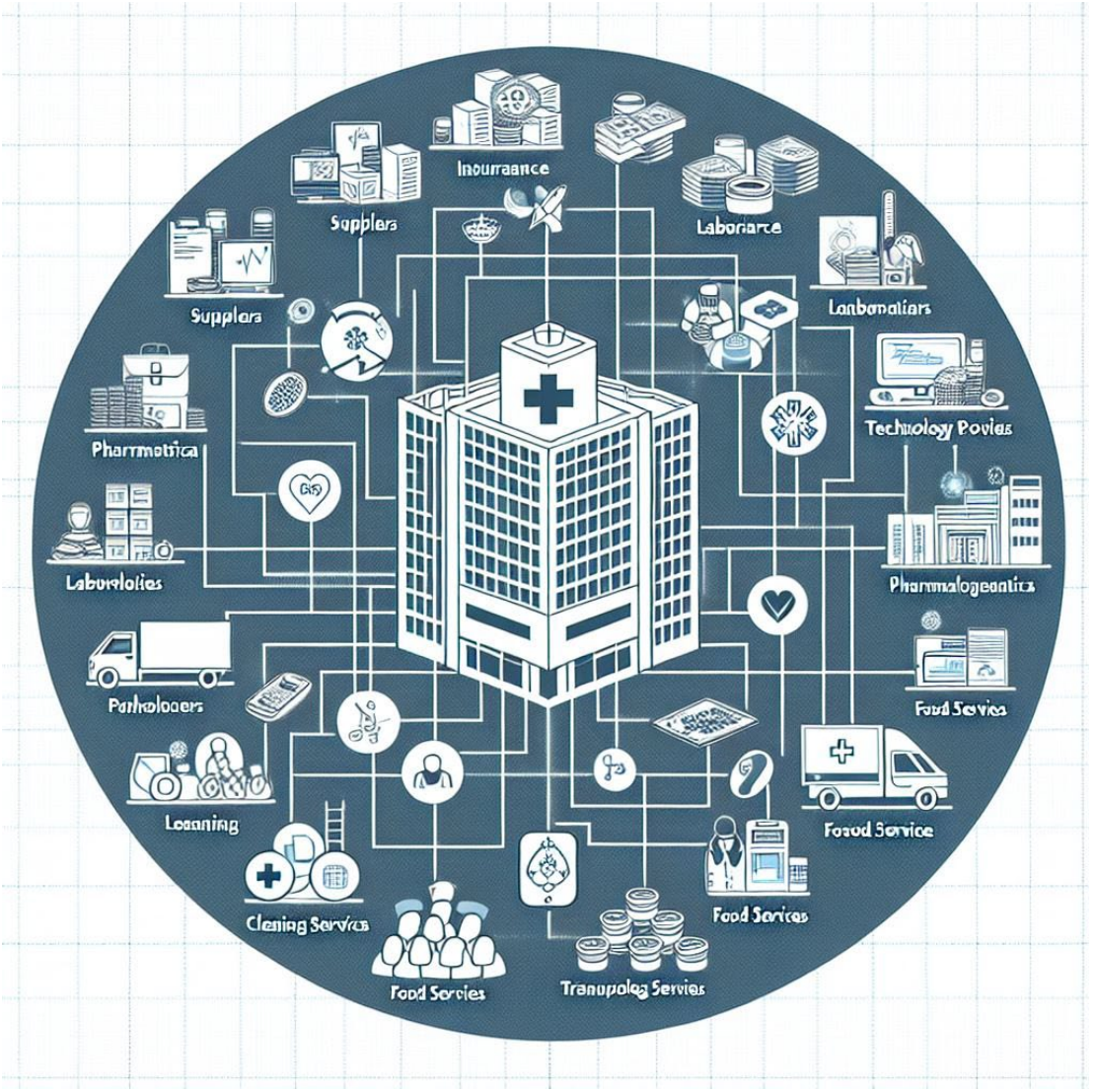
Think you've got your hands full?

Scope

The vCISO

Full Experience / Fractional Cost

- **Entire Healthcare Ecosystem**
  - Numerous Hospitals
  - Psychiatric Care
  - Ambulatory Sites
  - Data Centers
  - Colocation Facilities
  - Research Institute
- **Third & Fourth Parties**
  - Joint Ventures
  - Clearinghouses
  - Payers
  - External Cloud and Service Providers
  - Supply Chain



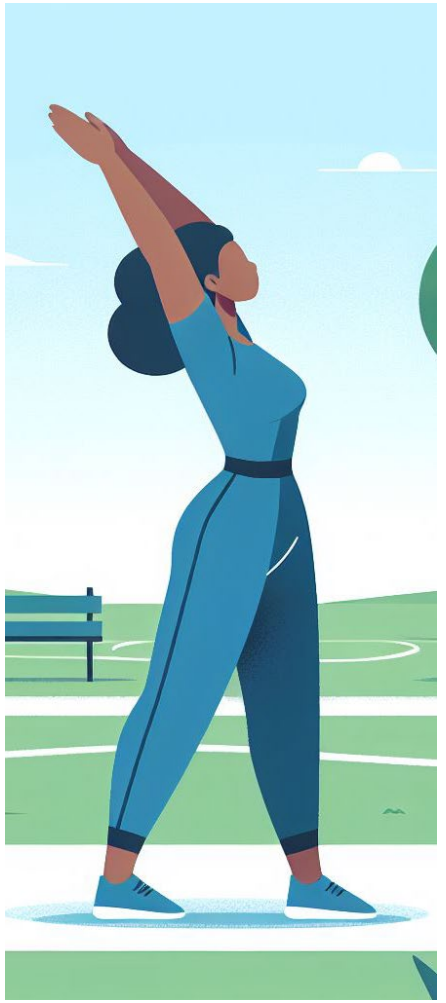
Let's see who is awake and paying attention

Audience Poll

The vCISO

Full Experience / Fractional Cost

- **Please stand up at your seats if you/your organization:**
  - Lacks documented playbooks for all critical scenarios you might encounter
  - Lacks 100% true MFA on all apps, all assets, all remote access, all privileged accounts, and all productivity accounts)
  - Has more than 1 persistent VPN Tunnel
  - Has any outstanding unpatched vulnerabilities
  - Has any configuration baseline variances
  - Are not 100% confident that you know where all PHI entrusted to your organization is located.
  - Do not have a 100% current asset management databases (for any hardware, software, or firmware installed on or interconnected with your domain). Contact information must also be accurate and current.
  - Has any generative AI components, whether yours or your vendors/partners.
  - Subscribes to any third party threat intelligence/sharing services including the US CERT or the H-ISAC.



What is our end state objective?

Mission Success

The vCISO

Full Experience / Fractional Cost

- **How do we define success?**
  - Perfect Security?
  - Regulatory Compliance?
  - No audit findings?
  - No events?
  - No reportable incidents?
  - No breaches?

NOPE, NOT ENOUGH

- **CISOs define success through a combination of objective metrics and subjective perceptions. Here are some key aspects:**
  - Alignment with Organizational Goals
  - Partnership Engagement
  - Security Culture
  - Incident Response and Recovery
  - Comprehensive identification, assessment, and mitigation of risks
  - Continuous Improvement.

People are our biggest threat, but not for the reasons you think

Oday Oday Oday Oday

The vCISO

Full Experience / Fractional Cost

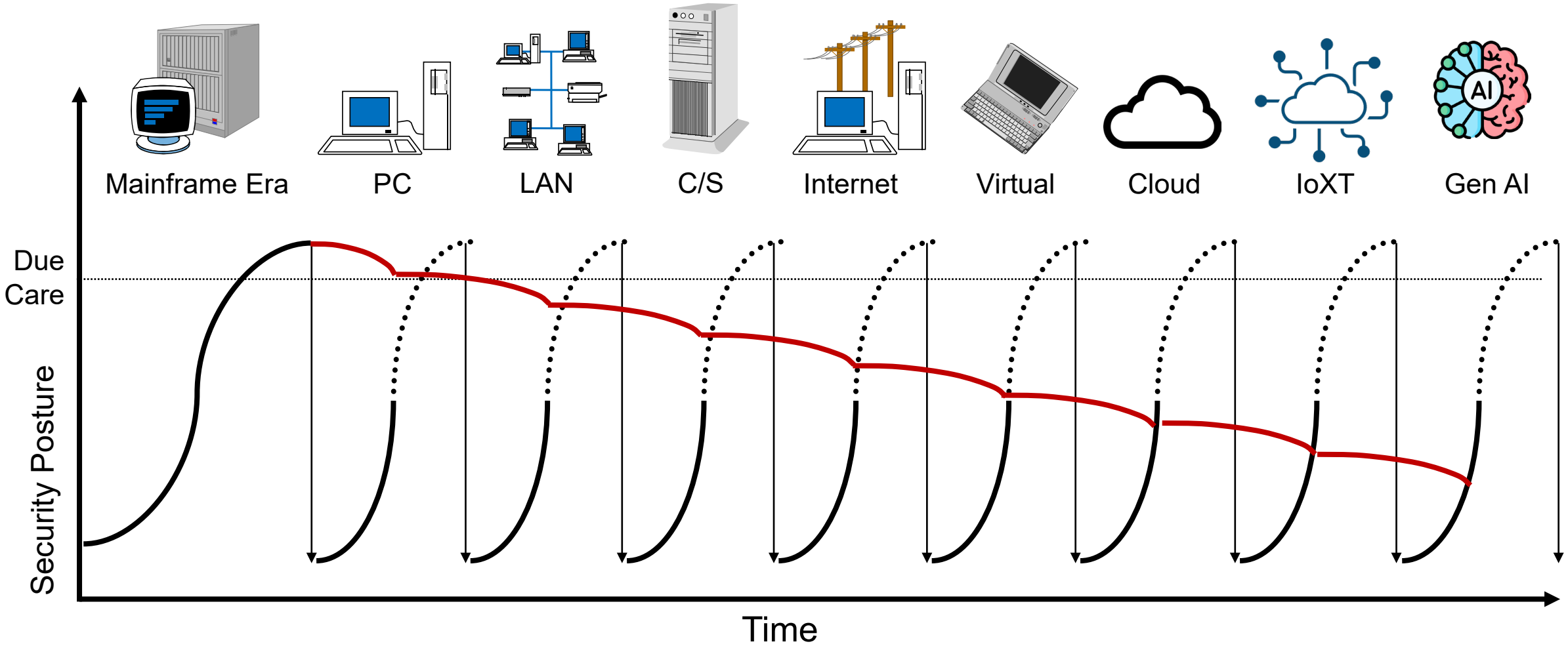
- What is our single biggest blind spot?
- This has not always been the case.
- Cyber has evolved like everything else.
- No Trust Among Thieves Necessitated Brokers
- The brokers have now morphed into market makers
- Hackers are now relegated to the role of lead gen
- Realistically, who can afford to buy a $200M Zero day?

How did we get here?

Security Exposure

The vCISO

Full Experience / Fractional Cost

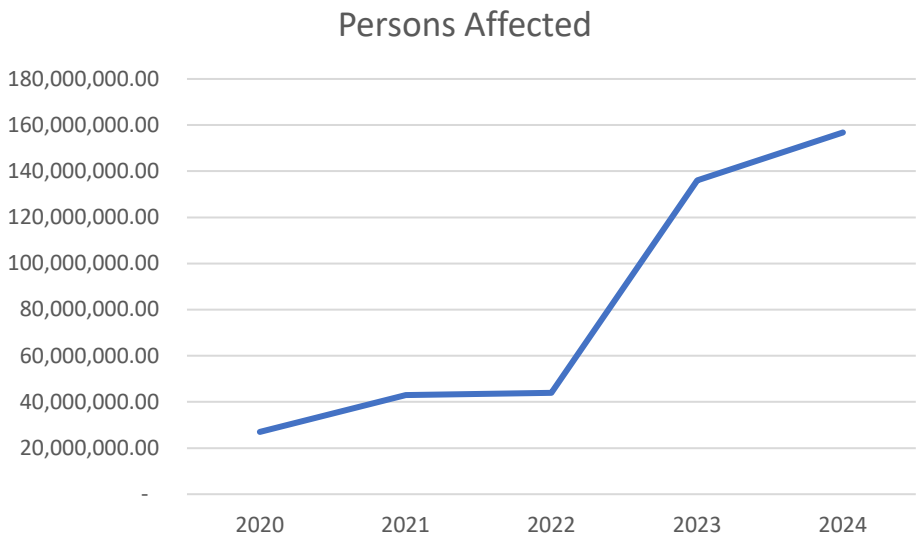


How bad is all this really?

Hacking Incidents Reported to OCR

The vCISO
Full Experience / Fractional Cost

- **2020 Total:**
  - 425 Hacks Impacting 27 Million Individuals
- **2021 Total:**
  - 518 Hacks Impacting 43 Million Individuals
- **2022 Total:**
  - 556 Hacks Impacting 44 Million Individuals
- **2023:**
  - 591 Hacks impacting 136 Million individuals
- **2024 (First 11 Months)**
  - 531 Hacks Impacting a Record 156.8 Million* Individuals



  - **Entire U.S population (some more than once) impacted by hacks of their PHI since 2020**
  - **Ransomware attacks up 278% since 2020 per HHS – OCR**
  - **Healthcare is the most attacked sector by ransomware per the FBI**

Sources : HHS, OCR website data accessed 01/11/2021, 01/15/2022, 01/15/2023 and 12/03/2024 www.ocrportal.hhs.gov. Active and archived breaches 2024 FBI Internet Crime Complaint Center

Regulation

The vCISO

Full Experience / Fractional Cost

Where is the Government in all this?

NIST OCR HIPAA Security Summit

The vCISO
Full Experience / Fractional Cost

- **On October 23-24, 2024, NIST and OCR hosted their annual security summit for the first time in 5 years since Covid.**
  - The current state of cybersecurity in healthcare is characterized by evolving threats and challenges faced by the industry.
  - Presentations covered the latest cybersecurity threats to the healthcare community, emphasizing the importance of staying updated and proactive in defense measures2.
  - Strategies, techniques, and best practices for complying with the HIPAA Security Rule were presented with a focus on IoT and AI.
  - Updates from both federal healthcare as well as enforcement agencies provided insights into regulatory changes (including HIPAA2) and upcoming initiatives (HPH CPGs) aimed at enhancing healthcare cybersecurity.
  - 2024 set new records for # of breaches and # of individuals affected
- **Settlements reached over the past 5 years were reviewed:**
  - Overall, the most common theme was that **regulated entities failed to adequately address scope in** their risk assessments and programs. IT but not OT, First Party not 3rd or 4th party, and On-Prem but not the cloud (New BOD 25-01)
- **Recordings and proceeds are available for download online.**

Can you be more specific?

NIST/DHHS HIPAA Conference Take-Aways

The vCISO
Full Experience / Fractional Cost

WHAT WE ALREADY KNOW:

- Increasingly Sophisticated Attacks
  - APT
  - Ransomware
  - Cybercrime Syndicates
- Rising Geopolitical Tension
- Evolving Attack Vectors
  - AI-Driven
  - Supply Chain Attacks
  - IoT Vulnerabilities
  - Cloud Threats
  - Open Source Infiltration
  - Zero-Day to Zero-Click

WHAT WE MAY NOT YET KNOW:

- FTC Act Extends to HIPAA CEs
- Health Breach Notification Rule
- FDA FD&C Act (Medical Devices)
  - FDA Final Premarket Guidance
  - FDA Final Cybersecurity Guidance
- SP 800-66 R2 (2/24)
  - Updated Risk Assessment Process
  - Scope, Scope, Scope
- Proposed HIPAA Security Rule Update
- Prioritizing Investigations
  - Hacking
  - Ransomware
  - Right of Access Enforcement
  - Risk Analysis Enforcement
- ASTP AI in Healthcare
  - 1/1/25 EHR Vendor “Nutrition Labels”

Resources

- **Standard Security Clauses**
  - Data Security and Protection
  - Compliance with Laws and Regulations
  - Incident Response and Reporting
  - Access Controls
  - Audit and Assessment Rights
  - Third Party Risk Management
  - Cyber Insurance
  - Data Return and Destruction
  - Confidentiality
  - Indemnification
  - Continuity and Disaster Recovery
  - Malware Free
  - Malware Remediation

- **Legalese versions are available for fee from Westlaw. Contact me directly for a plain language version**

Wait, say that again…

HITECH Amendment

The vCISO

Full Experience / Fractional Cost

Public Law 116-321 (H.R. 7898), enacted on January 5, 2021, amends the Health Information Technology for Economic and Clinical Health (HITECH) Act. Here are the key points:

- Directs HHS to provide regulatory relief for HIPAA covered victims of cyber attacks
- Recognized Cybersecurity Practices in Place Previous 12 months
- Reduced Fines
- Early, Favorable Termination of Audits
- Mitigation of other penalties
- No Increased Penalties for Not Having Recognized Cybersecurity Practices in Place

That's a great idea!

AHA Threat Intelligence Briefing

The vCISO
Full Experience / Fractional Cost

- **Board/Senior Leadership Engagement:**
  - As a reminder, Cybersecurity teams are not solely responsible for an organization's posture nor are they solely to blame for breaches that may occur.
  - Various regulations, industry sector guidance, and legal precedents make it clear that responsibility for cyber rests at the top with the Senior Leadership Team and Board of Directors.
  - Our Role as Cybersecurity practitioners is to ensure that decision making conversations are fully informed.
  - One strategy for conveying this important message and engaging your board is to schedule an "education session" during a board dinner.
  - By selecting the right external "messenger" who has credibility with your board allows you and your team to "come to the rescue."
- **Education Content:**
  - NDAs and other restrictions preclude me from directly sharing AHA content.
  - I can share however, that:
    - Cyber crime against hospitals is now a "threat to life crime"
    - Downtime presumptions must be upwards of 4 weeks or longer

They giveth and they taketh away…

Updated HIPAA Security Rule

The vCISO
Full Experience / Fractional Cost

On December 27, 2024, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) issued a Notice of Proposed Rulemaking (NPRM) to update the HIPAA Security Rule. This update aims to strengthen cybersecurity protections for electronic protected health information (ePHI). Here are the key points:

- Implementation Specifications – The distinction between "required" and "addressable" implementation specifications will be removed, making all specifications required with limited exceptions.
- Documentation Requirements – All Security Rule policies, procedures, plans, and analyses must be documented in writing.
- Technology and Terminology Updates – Definitions and implementation specifications will be updated to reflect changes in technology and terminology.
- Compliance Time Periods – Specific compliance time periods will be added for many existing requirements.
- Network Segmentation – Implement network segmentation to isolate ePHI from other parts of the network
- Technology Asset Inventory – Regulated entities must develop and maintain a technology asset inventory and a network map illustrating the movement of ePHI, updated at least annually or in response to significant changes.
- Risk Analysis Specificity – Greater specificity will be required for conducting risk analyses.
- Mandatory 72 Hour RTO -- Establish written procedures to restore the loss of certain relevant electronic information systems and data within 72 hours.
- Mandatory 12 Month Audit – Require regulated entities to review and test the effectiveness of certain security measures at least once every 12 months, in place of the current general requirement to maintain security measures.
- Third Party Oversight -- Require that BAs verify at least once every 12 months that they have deployed technical safeguards required by the Security Rule to protect ePHI through a written analysis of the business associate's relevant electronic information systems by a subject matter expert and a written certification that the analysis has been performed and is accurate.

These changes are part of broader efforts to enhance cybersecurity in the healthcare sector, aligning with the Biden-Harris Administration's commitment to improving the cybersecurity of critical infrastructure.

Story Time

The vCISO

Full Experience / Fractional Cost

Hackers are taking a page from the Terrorist playbook

False Claim

The vCISO

Full Experience / Fractional Cost

- **CONTEXT:**
  - After successfully avoiding it for almost 40 years, I finally received the call every CISO dreads.
  - The FBI contacted me to alert me to a social media posting that alleged my organization had been the subject of a successful ransomware attack.
- **ISSUE:**
  - The post was false, no such attack took place (nor had any ransom been requested)
  - The H-ISAC picked up and rereported the false report without verifying bona fides
  - The social media company took 6 weeks to remove the criminal posting
  - A fourth party payer summarily severed connections to a related but completely different legal entity from the one allegedly affected
  - Despite our efforts to explain matters, they refused to restore connections until we proved the impossible negative proposition
- **RESOLUTION:**
  - We have since modelled and documented an additional playbook for this scenario
    - Greater prioritization of Alert Feeds (augmented with searches for our “brands”)
    - Deep Web / Social Media Monitoring
    - Established Liaisons with FBI and Social Media Outlets
    - Updated Crisis Management Plans and Templates

Actions have consequences

Severed Connections

The vCISO
Full Experience / Fractional Cost

- **CONTEXT:**
  - Secondary to the Change Healthcare event, and only after Change Healthcare acknowledged and widely reported their issue, affected organizations properly severed connections to avoid further spread of the contagion.
- **ISSUE:**
  - Which systems and/or connections are in scope?
    - Change Healthcare
    - Optum
    - United Health
    - McKesson
    - Other Third Parties who may not yet have severed their connections
  - What about connections in the cloud that we don't directly control ourselves?
  - Classic disconnects between IT and both business units and contracts/legal contributed to the issue.
- **RESOLUTION:**
  - Organizations had to cut into the bone erring on the side of caution severing connections that "might" be involved owing to outdated, absent, or incomplete asset management information.
  - Expanded Asset Management Systems
  - New Workflows from Contract Management Systems to CMDB
  - Updated contract clauses to hold providers accountable for the integrity of their updates and/or requiring device manufacturers to test patches before deployment.

You can outsource the work but not the accountability…

Gone Phishing

The vCISO

Full Experience / Fractional Cost

- **CONTEXT:**
  - The organization is engaged in a major upgrade, migration, and enterprise standardization to a new core back office system (think old school ERP project).
  - Given the enormous size and complexity of the effort, to say nothing of the IT challenges, board level impact, and stakes, the services of a reputable third-party solution provider partner were engaged to facilitate the migration.
- **ISSUE:**
  - An employee of the third party fell prey to a phishing attack aimed at his account on the provider partner's domain. The bad actor leveraged intel found in emails in the compromised account inbox to gain unauthorized access to the pre-prod environment for the system being stood up.
  - Root cause was a variance request to disable MFA combined with user reuse of identical credentials.
- **RESOLUTION:**
  - Our go-live / technical readiness review process uncovered this issue and we were able to restore the unauthorized changes made to hundreds of user accounts in the new system averting what would have otherwise been a catastrophe.
  - All variance requests for third parties are now routed to our Governance Council (5 members 3 of whom must approve).

The student is still going to school

Generative AI

The vCISO

Full Experience / Fractional Cost

- **CONTEXT:**
  - Healthcare professionals, especially clinicians measure success in time.
  - IT/Cyber's job is to help providers serve more patients (or beneficiaries) in less time.
- **ISSUE:**
  - A purchase request was submitted to acquire an AI tool that would assume responsibility for the mundane tasks of responding to emails in provider inboxes.
- **RESOLUTION:**
  - We questioned the use case
  - We reminded the organization of our AI policy
  - We deployed the tool in a sandbox and **the solution took the bait and interacted with one of our monthly anti-phishing exercises.**
  - Request deferred; vendor seeking partnership to resolve.

How can I defend a choice to use Gen AI?

AI Resources

The vCISO

Full Experience / Fractional Cost

Category	Question
Accuracy and reliability	What is the accuracy rate of your AI model? How does it handle ambiguous or complex queries?
Bias	Do you have processes in place (e.g., human review) to address algorithmic bias?
Compliance and ethics	Does your solution comply with relevant regulations (e.g., GDPR, CCPA HIPAA)? How do you address ethical concerns, such as bias in AI?
Cost	How do you manage context windows (i.e., AI memory span) effectively to reduce cost?
Cost structure	What is the pricing model for your solution? Are there any additional costs or fees for extra features or services?
Customization and integration	How customizable is your solution to specific industry needs or business requirements?
Data handling and privacy	Do contractual agreements exist that address enterprise data privacy assurances for enterprise data sent to the vendor's model environment?
Data handling and privacy	How does your solution handle user data? How do you support a users request to opt-out?
Future roadmap	What are the future development plans for your solution? How do you plan to stay ahead of technological advancements in AI?
IP	How do you respect, protect or develop intellectual property?
IP	Does enterprise content get used by the provider to improve the provider offering?
IP	Does the vendor screen out copyright materials on the outputs?

How can I defend a choice to use Gen AI?

AI Resources Continued

The vCISO

Full Experience / Fractional Cost

Category	Question
IP	Does the vendor have T&C informing the user of copyright (e.g., not responsible for data that is used and subject to copyright)?
IP	What open-source content is used?
IP	How do you help me develop assets?
Model training and updates	How was your AI model trained, and what data was used?
Moderation	Does the solution offer I/O filtering?
Performance metrics and reporting	What metrics are used to measure the performance of your AI? Does your solution provide detailed reports or analytics?
Real-world applications and case studies	Can you provide examples or case studies where your solution has been successfully implemented?
Risk	Can the enterprise disable the storage of prompts?
Scalability	How well can your solution scale with increasing demands or users?
Security	Is content encrypted at rest and in transit?
Security	Does the model have the ability to interpret unclear text data? If so, how?
Security	Do you have tools to detect PHI/PII on content in and out of the model?

AI Resources Continued

Category	Question
Support and maintenance	What kind of customer support and maintenance services do you offer? Are there any additional costs for these services?
Training	What corpora (i.e., raw material) was the model trained on?
Training	What is the frequency?
User experience and accessibility	How user-friendly is the interface? Is your solution accessible to users with disabilities?

Shouldn't we be updating the processes we've been using since WWII?

Supply Chain

The vCISO
Full Experience / Fractional Cost

- **CONTEXT:**
  - We haven't designed with resiliency in mind since the Hoover Dam
  - Just-In-Time is dated and is no longer appropriate in many industries
  - Supply chain issues that first surfaced during COVID have now become critical.
- **ISSUE:**
  - Baxter plant in Asheville leaves providers in dire need of IV fluids
  - DME providers cannot meet demand
  - Challenges exist not just in manufacturing but in logistics and distribution as well.
- **RESOLUTION:**
  - Increase stock on hand
  - Adjust reorder points
  - Have multiple providers
  - Prop up middle tier "connective tissue" players in our sector
  - Measure/oversee and alert on downward trends.

It's Not Hopeless

- **Microsegmentation:**
  - BMS, HVAC, and other such flows should neither be on nor interconnect with the data network.
  - OT, IOMT, Bioengineering, etc. should be on their own dedicated network with a select few tightly controlled interconnection points to the data network.
  - The data network should be further segmented by geography, facility, floor/unit, and function.
- **Zero Clients**
  - Specialized devices that afford streamlined access to virtual desktops and applications
  - Unlike thin clients, zero clients do not retain an operating system or configuration settings in flash memory. Instead, they use an onboard processor optimized for specific protocols like Microsoft RDP, VMware, or Citrix HDX
  - Due to their dedicated hardware, zero clients can boot up quickly and handle the decoding and display of virtual desktops efficiently
  - Zero clients reduce the costs of other security controls (e.g., there is no need for an XDR agent)
- **PHI Scanning:**
  - Currently if asked where is your PHI, many HCOs would answer "everywhere."
  - There is nothing wrong with this response, provided of course that organizations also fully harden all of their environments.
  - A better alternative would be to establish policies that restrict PHI to select specifically sanctioned locations.
  - To ensure that PHI does not find its way into unsanctioned locations, a PHI scanning solution (that can identify both structured and unstructured PHI in all forms/formats – including opaque images) can be deployed.

It sounded good at the time…

"Reasonable and Appropriate"

The vCISO

Full Experience / Fractional Cost

- **CONTEXT:**
  - The SolarWinds case, which was settled in October 2024, involved the U.S. Securities and Exchange Commission (SEC) issuing fines totaling nearly $7 million against four global digital service providers. These companies were impacted by the 2020 SolarWinds compromise, where malicious code was inserted into SolarWinds' Orion software, potentially allowing unauthorized access to affected systems
  - The SEC accused the companies of making misleading cybersecurity statements to investors. The allegations included downplaying the scope of the breach, omitting material information, and failing to update cybersecurity risk disclosures appropriate.
- **ISSUE:**
  - Having been bound to CMS for all these years, we have been trained to view security events differently.
  - It is not about right or wrong, neither is this about what can realistically be accomplished with the limited resources we have available.
- **RESOLUTION:**
  - It's all about defensibility. Make sure that whatever you do, you evaluate your options ensuring that they are carefully reasoned, fully scoped, and defensible.
  - Remember, it's a jury of non-technical members of the public who determine what is or is not reasonable.

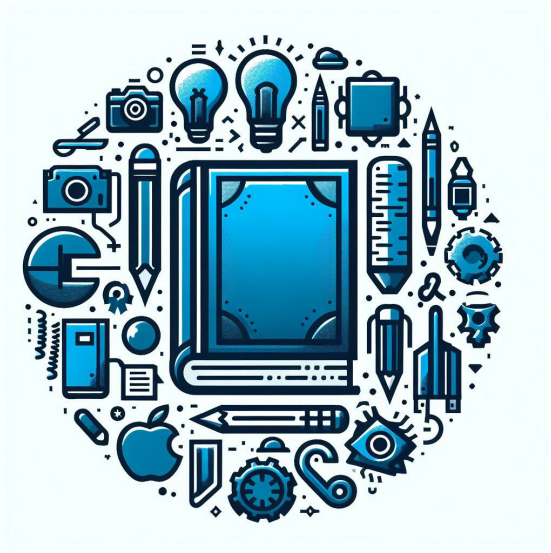
Where can I get more information?

Resources

The vCISO

Full Experience / Fractional Cost

- Proposed HIPAA Security Rule Update
  - https://public-inspection.federalregister.gov/2024-30983.pdf
- HHS HIPAA Security Rule Fact Sheet
  - ttps://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html
- Public Law 116-321 (H.R. 7898)
  - https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf
- H.R. 7898 Fact Sheet
  - https://www.govtrack.us/congress/bills/116/hr7898/summary
- BOD 25-01: Implementing Secure Practices for Cloud Services
  - BOD 25-01: Implementation Guidance for Implementing Secure Practices for Cloud Services | CISA
- Safeguarding Health Information: Building Assurance thru HIPAA Security:
  - https://www.nist.gov/itl/safeguarding-health-information-building-assurance-through-hipaa-security-2024r
- About IGEL Zero Clients
  - https://kb.igel.com/__attachments/90493873/About%20IGEL%20Zero%20Clients_10.6.pdf?inst-v=9cebe0e8-6fe9-415f-8a86-aaae9c9a03fb
- Tausight PHI Scanning
  - Tausight.com



What are the key take-aways?

Conclusion

The vCISO
Full Experience / Fractional Cost

- **Summary:**
  - The Healthcare Sector is one of (if not the) most vulnerable to cyber attack.
  - The events of the past year demonstrate that even compliant organizations can fall prey to compromise
  - Only by adopting a follow the data approach can we ensure full coverage
  - Perfection is unreasonable, what matters is what we do as a result
  - Defensibility is achieved by asking tough questions (think AI deployments), imposing strict demands on your ecosystem participants, by anticipating new types of attacks, having practiced containment and response playbooks, and implementing cost containment strategies that are broader than cyber alone.

- **Thank you for this opportunity!**
- **Who has the first question?**

What are your qualifications to serve?

The vCISO

The vCISO

Full Experience / Fractional Cost

Jason Taule

CCISO, CCSFP, CDH-E, CDPS, CDPSE, CGEIT, CHISL, CHSIII, CISM, CMC, CPCM, CRISC, HCISPP, NSA-IAM

PRAGMATIC CULTURALLY ATTUNED PROVEN INFORMATION SECURITY LEADERSHIP

Jason Taule is an information assurance and cybersecurity industry executive with a record of success who has worked in both the intelligence community and commercial sectors first consulting to Federal agencies and then serving as inside Chief Information Security Officer / Chief Privacy Officer both within Government and at large systems integrators like General Dynamics and CSC.

LinkedIn profile

Mr. Taule's leadership contributions have advanced the science and practice of information security and risk management. With passion and integrity, his communication/interpersonal skills and numerous accomplishments have earned him recognition as Industry Luminary. Ever mindful of the need to balance security with utility, he has successfully adapted security controls in countless real-world implementations; this pragmatism cause many to consider him a voice of reason. His unique background enables him to incorporate both business and technical perspectives in integrated solutions. For example, Mr. Taule helped create the US-CERT, authored various State Data Privacy Laws, led a multi-million dollar global cyber security practice for a large international consulting firm, ran the team responsible for HIPAA complaint investigations for OCR for 3 years, for the last two decades has been a luminary in the US Health IT space supporting numerous OpDivs in DHHS, served as the CISO & VP of Standards for HITRUST, and more recently has been supporting organizations in all industries and geographies grapple with these issues delivering CISO services on a fractional basis.

Mr. Taule is a graduate of the FBI Citizen's Academy, is member of the Homeland Security Preparation and Response Team, Chairs the Advisory Council of the Maryland Innovation Center, is the driving force behind the Maryland Innovation Center's CISO-In-Residence program, sat on the US Health IT Standards Committee's Transport and Security Workgroup and was a White House invitee to the Security Policy Roundtable for the President's Precision Medicine Initiative.

Mr. Taule received his Bachelors in Business Management from William & Mary and his Masters of Science in Information Technology Management from Johns Hopkins. He resides in Reisterstown, Maryland.

Developed By:

The vCISO
Full Experience / Fractional Cost

The vCISO appreciates the opportunity to partner with you and welcomes any questions you may have.

The vCISO

(410) 340-5385
Jason.taule@thevciso.net