November 1, 2019
Columbia Convention Center

HIMSS
SOUTH CAROLINA Chapter

- Conflict of Interest Disclosure

Darren W. Carroll

Has no real or apparent

conflicts of interest to report.

- **While hacks of major retail businesses will continue to occur with frightening regularity, it will be the health care industry that will be the source of many, if not most, major data breaches**. (WHY?)
- Due to a perfect storm of vulnerability caused by large amounts of stored electronic data shared by many users within the health care system, the health care industry has become a major target for hacking, with the stolen personal information used for identity theft, including medical identity theft.
- The effects of that can be particularly harmful when an identity thief's medical records become mixed with the victim's medical records. The FBI has warned the health care industry that its cyber security is not presently sufficient to protect the information it stores.

Understanding HIPAA

Understanding HIPAA

Covered Entities and their Business Associates need to protect the privacy and security of protected health information (PHI).

There are 4 rules that you will need to be aware of.

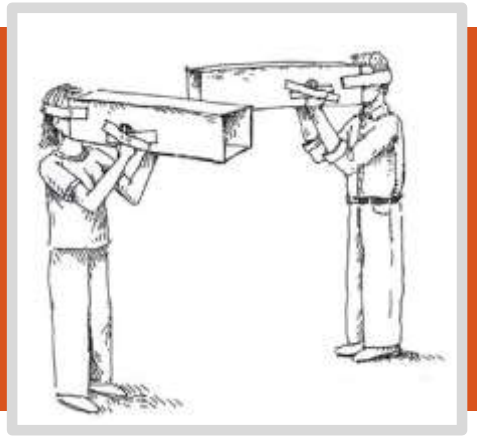
1.HIPAA Privacy Rule
2.HIPAA Security Rule
3.HIPAA Enforcement Rule
4.HIPAA Breach Notification Rule

We're going to focus on this one, but they're all important

As far as action items are concerned, you need to follow the HIPAA Privacy Rule and the HIPAA Security Rule. And, you need to provide notification following a breach of unsecured protected health information (the Breach Notification Rule).

What is Situational Awareness?

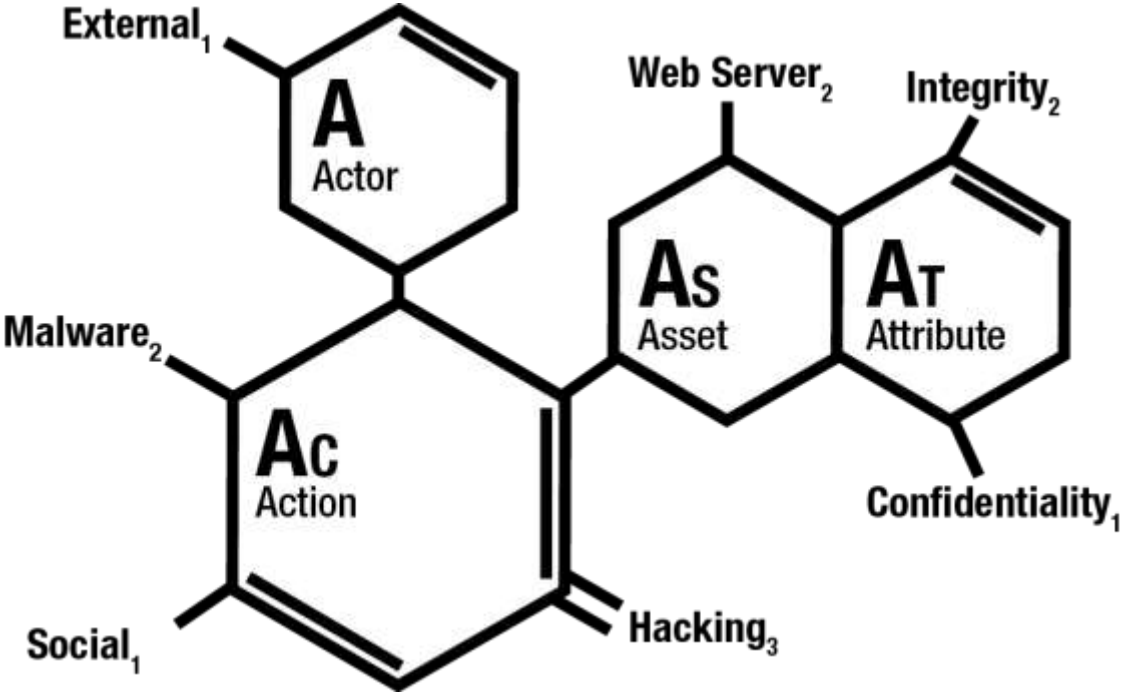
- ***Situational Awareness*** is the ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regards to the mission. More simply, it's knowing what is going on around you.



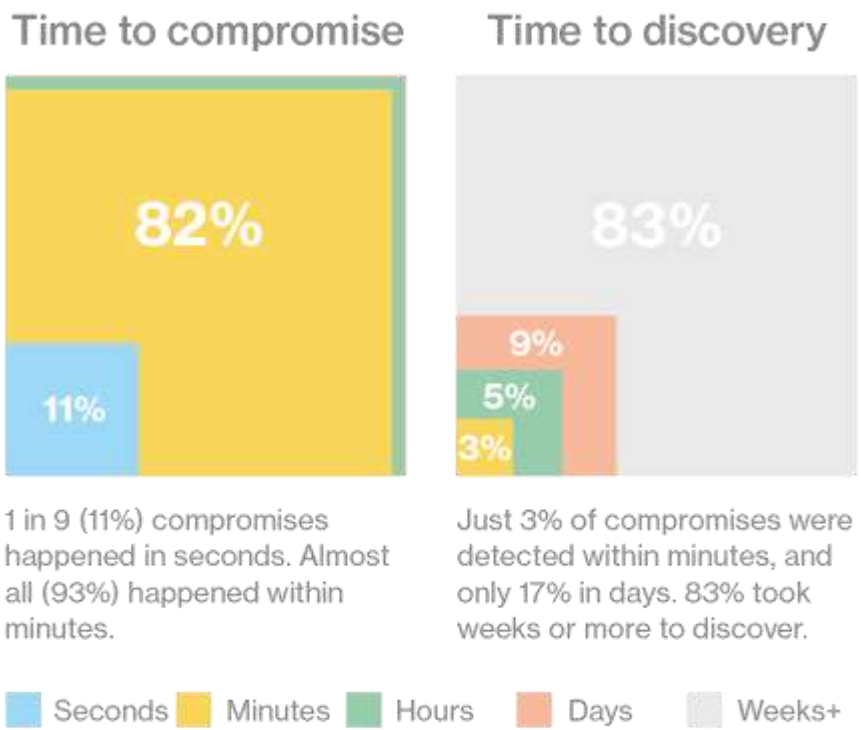
HIMSS SOUTH CAROLINA Chapter

Vocabulary to start the discussion

Welcome to VERIS



Cyber Crime Innovation Gap



HIMSS SOUTH CAROLINA Chapter

Failing to plan…

Fewer respondents have well-resourced incident response handling teams, down from just under one-third to 25%.

Consider it a part of your DR/BC plan:

- ✓ *Plan*
- ✓ *Do*
- ✓ *Check*
- ✓ *Act*

HIMSS SOUTH CAROLINA Chapter

Even the PCI DSS got it right

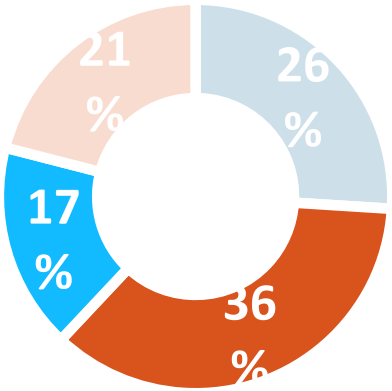
- *1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*

So did HIPPA (sort of)

- **Part 2 – Recommended configuration guidelines**
- The following are 7 of the most common and critical hardware devices that maybe part of a medical center Information Systems environment and are of the highest concern and applicability to HIPAA Security regulations for systems certification and accreditation.

The at-risk component is the human element

Causes of Data Loss



Electronic Media
(Email, web, social networking, instant messaging)

Portable Devices/Electronic media
(Mobiles, Laptops, PDS's, USB)

Papers & Files
(Confidential documents, unsecure printing & document disposal)

External Attacks
(Hackers, viruses, spamming, phishing, interception of communication devices)

Healthcare Provider	2000	04/01/2016	Theft
Healthcare Provider	869	04/01/2016	Unauthorized Access/Disclosure
Healthcare Provider	15625	03/25/2016	Hacking/IT Incident
Healthcare Provider	3000	03/24/2016	Hacking/IT Incident
Healthcare Provider	524	03/23/2016	Theft
Business Associate	2483	03/22/2016	Hacking/IT Incident
Healthcare Provider	1124	03/21/2016	Unauthorized Access/Disclosure
Healthcare Provider	2000	03/18/2016	Hacking/IT Incident
Healthcare Provider	773	03/18/2016	Theft
Healthcare Provider	647	03/17/2016	Unauthorized Access/Disclosure
Healthcare Provider	2200	03/17/2016	Loss
Health Plan	2373	03/15/2016	Unauthorized Access/Disclosure
Healthcare Provider	1154	03/14/2016	Hacking/IT Incident
Healthcare Provider	726	03/11/2016	Theft
Healthcare Provider	1654	03/11/2016	Unauthorized Access/Disclosure
Healthcare Provider	2808	03/10/2016	Loss
Healthcare Provider	677	03/10/2016	Unauthorized Access/Disclosure
Healthcare Provider	897	03/10/2016	Unauthorized Access/Disclosure
Healthcare Provider	500	03/10/2016	Unauthorized Access/Disclosure
Healthcare Provider	26588	03/08/2016	Hacking/IT Incident
Healthcare Provider	5883	03/07/2016	Hacking/IT Incident

HHS OCR Breach Portal aka *"HIPAA Wall of Shame"*

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

HIMSS SOUTH CAROLINA Chapter

Data Classification for Information Security

- ***Data Classification*** is a critical component of a good DLP implementation.

Who creates the data?

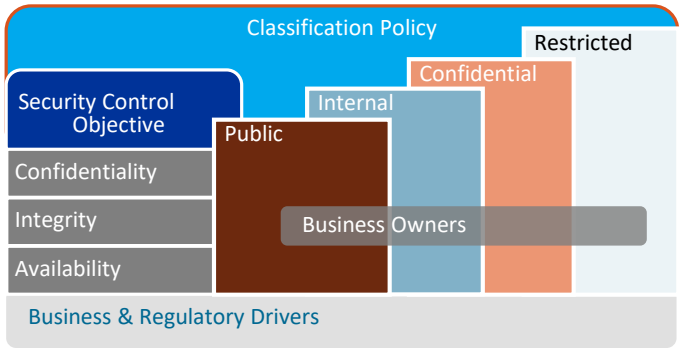
Who can see it?

Who can modify it?

Who can delete it?

Do you want pictures of last year's company BBQ on solid-state Tier 1 application storage?...

…No more so than you want to disclose sensitive information, but for different reasons



Structured* vs. *Unstructured

Ask me about the international hotel management company and their unstructured data set.

HIMSS SOUTH CAROLINA Chapter

Understanding HIPAA

Understanding HIPAA

HIPAA, the Health Insurance Portability and Accountability Act, sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network, and process security measures are in place and followed.

This includes covered entities (CE), anyone who provides treatment, payment and operations in healthcare, and business associates (BA), anyone with access to patient information and provides support in treatment, payment or operations. Subcontractors, or business associates of business associates, must also be in compliance.

Understanding HIPAA

3 Domains under the Security Rule

Technical Safeguards
- Access Control
- Audit Controls
- Integrity
- Authentication
- Transmission Security

Unique User Identification (required): Assign a unique name and/or number for identifying and tracking user identity.

Implement a mechanism to encrypt ePHI whenever deemed appropriate.

Physical Safeguards
- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.

Administrative Safeguards
- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

Perform and document a risk analysis to see where PHI is being used and stored in order to determine all the ways that HIPAA could be violated.

Deep Thoughts

Knowledge is power.

- Devices generate logs
- Logging leads to data
- Data leads to correlation
- Correlation leads to knowledge

One of my goals is to remove the word "policy" from our lexicon and replace it with the single concept of "Enforceable Policy".

Brush your teeth. Comb your hair.

Good security hygiene is critical.

- Log / Monitor / Correlate / Notify
- North/South & East/West
- Internal Segmentation
- A-End, B-End, and everything in between
- Don’t just scan, remediate (rolling 90 days)
- Frequent, Persistent Awareness Training
- Complex Passwords and why 3M still makes Post-It notes
- ACT!

“Verizon found that Target had a comprehensive vulnerability scanning program in place, using Tenable Security Center,” the report notes. “However, the Verizon consultants discovered that remediation procedures did not address findings discovered by the vulnerability scanning program in a timely fashion, if at all.” – Krebs on Security

Thanks for joining!

Discussion

HIMSS SOUTH CAROLINA Chapter