Measuring Cybersecurity

as a Non-Technologist

LEVERAGING CYBERSECURITY FRAMEWORKS

ROGER W. LUTZ

JULY 19, 2019

Questions? https://mdcpa.participoll.com/

1

Agenda

- About me and my organization
- Cybersecurity past and present
- Cyber-threat Landscape
- Cybersecurity Frameworks
- Using frameworks as a guide to secure your organization -- *or* -- in your assessment of an organization's security
- What's this all mean to you
- Questions and discussion

Please, feel free to ask questions along the way!

Questions? https://mdcpa.participoll.com/

2

About me

- Chief Information Officer & Information Security Officer for Butler Health System
- Responsible I.T. Operations, Cybersecurity and the HIPAA Security program
- In my spare time, I teach Healthcare Ethics, Law, Privacy and Information Assurance as part of the M.Sc. Healthcare Informatics program at Slippery Rock University
- 20+ Years in information systems and networked communications

Questions? https://mdcpa.participoll.com/

3

Butler Health System

Independent community health system 30 miles north of Pittsburgh
IBM Watson Health 100 Top Hospitals and Everest Award winner
Named one of the best cardiac surgery programs in the country by U.S. News & World Report
The largest employer in Butler County

Questions? https://mdcpa.participoll.com/

4

Butler Health System I.T. Landscape

- 2600 employees

Questions? https://mdcpa.participoll.com/

5

Butler Health System I.T. Landscape

- 70+ wide-area networked Locations

Questions? https://mdcpa.participoll.com/

6

Butler Health System I.T. Landscape

- Over 500 servers in multiple data centers

Questions? https://mdcpa.participoll.com/

7

Butler Health System I.T. Landscape

- Over 2500 computers deployed throughout our many facilities

Questions? https://mdcpa.participoll.com/

8

Butler Health System I.T. Landscape

- ~500 WiFi Access Points providing coverage to well over a half-million square feet of clinical and business operations workspace.

Questions? https://mdcpa.participoll.com/

9

Butler Health System I.T. Landscape

- ~ 10,000 network ports

Questions? https://mdcpa.participoll.com/

10

Butler Health System I.T. Landscape

- *Hundreds* of clinical systems and devices networked to computer systems.

Questions? https://mdcpa.participoll.com/

11

Butler Health System I.T. Landscape

- Keeping our systems secure is a huge responsibility
- A responsibility we take very ***very*** seriously
- Yet, like many other non-profits, resources are limited.
  - An *intelligent, informed approach* to the application of those resources is critical to optimizing the ROI for our investments in security.
  - Modern cybersecurity programs operate on frameworks that provide just that approach!

Questions? https://mdcpa.participoll.com/

12

Cybersec circa 1990s

My first role in cybersecurity was at a local telecom company as a Network Engineer

Assigned to manage the new "*Ethernet network*"

At that time, our network was directly connected to the Internet with no firewall, only routers.

Our security strategy was "*Security through Obscurity*".

Remember when Warning Emails would circulate when a new virus came out to alert everyone not to click or open it?

Questions? https://mdcpa.participoll.com/

13

A brief word on terminology "Secure"

- My use of the word "secure", should not be interpreted as implying 100% impenetrability. No cybersecurity program is impenetrable.
  - Instead, think of "*Appropriately Secure*"…
- Defining what appropriately secure is for the organization should be a risk decision, and common sense comes in to play in this determination.
- Common sense,… guided by an expertly designed, structured approach.

- I will use the term cybersecurity and information security interchangeably throughout this presentation.

  *While there is a difference in pedantic sense, we approach cybersecurity broadly to address the full information security scope.

Questions? https://mdcpa.participoll.com/

14

A brief word on terminology "Cybersecurity vs. Information Security"

- Cybersecurity is about securing things that are vulnerable through **I**nformation and **C**ommunications **T**echnology, or ICT.
- Information security is about protecting the information on a broader sense beyond merely threats from the Internet.

Questions? https://mdcpa.participoll.com/

15

Cybersec progression circa 1990s…

- Firewalls were installed
- Anti-Virus was installed
- Early systems to safeguard networks and information were determined via *our* ***individual judgement***…
  - What had we read in the I.T. publications?
  - What did the sales rep convince us we needed?
- Limited commercial options were available for security devices and software.

Questions? https://mdcpa.participoll.com/

16

Cybersec Butler Health System

- I came to BHS in 2009
- Various technical protections in place
  - Firewalls
  - Antivirus
  - Encrypted Virtual Private Networks (VPNs) tunnels
- Several policies defined, though largely regulatory centric (HIPAA/HITECH).
- Still… Technical safeguards were put in place through an individual's judgement.

Questions? https://mdcpa.participoll.com/

17

Securing Healthcare I.T. Systems
- Complexity

- Unique challenges to securing healthcare I.T.
- Most systems must be Always-on
- Very challenging to arrange downtime
- Patching security vulnerabilities is a never-ending task
- Modern authentication processes slow care workflows.
  - Longer or more complex p@sSw0rd$
  - 2-factor authentication
- Visibility across the large enterprise requires automation

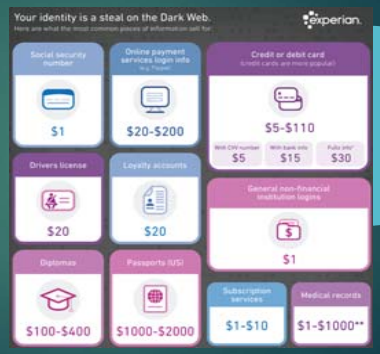
Questions? https://mdcpa.participoll.com/

18

Securing Healthcare I.T. Systems

- Threat Landscape

- The value of Information



Questions? https://mdcpa.participoll.com/

19

Securing Healthcare I.T. Systems

- Threat Landscape

Massachusetts Nonprofit Shelter Targeted by Ransomware

Father Bill's and MainSpring, a Brockton-based nonprofit homeless shelter, announced this week that it had been attacked by ransomware in April. Officials say they do not believe that personal information was stolen.

BY MARC LAROCQUE, THE ENTERPRISE, BROCKTON, MASS. / JUNE 28, 2019

- **Non-profits are a target**
- Ransomware is prolific
- Zero-day attacks render traditional prevention methods useless

Questions? https://mdcpa.participoll.com/

20

But doesn't HIPAA* Compliance keep us secure?

- HIPAA Privacy, Secure and Breach Notification regulations keep us ***busy***,.. and headed in the right direction.
- They're not a substitute for a Cybersecurity and/or Information Security program.
- HIPAA is a "Compliance Framework"

*Health Insurance Portability and Accountability Act

Questions? https://mdcpa.participoll.com/

21

Compliance Frameworks

- Health Insurance Portability and Accountability Act / HIPAA
- HIPAA is a compliance framework
  - Applies to the largest national health systems, *and* it applies to the smallest local dentist's practice.
- "Requires" organizations to assess risk
- "Requires" some basic security safeguards
- Much of it is deemed "Addressable"
  - Which is not to say it's optional, but rather that certain things must be considered by an organization and effectively addressed
- But… HIPAA Compliance does *not* guarantee an organization is secure from threats.

Questions? https://mdcpa.participoll.com/

22

What is Information Security?

- Information Security is a result of assuring CIA

  No, not the Central Intelligence Agency!
- CIA
  - **Confidentiality** (privacy)
  - **Integrity** (data integrity)
  - **Availability** (systems availability)

Questions? https://mdcpa.participoll.com/

23

The ***other CIA*** however…

by Shane McGlaun — Sunday, May 26, 2019

Stolen CIA Hacking Tools Unleash Mayhem On Baltimore's Computer Systems

TECHNOLOGY

A researcher made an elite hacking tool out of the info in the Vault 7 leak

Massive CIA Hacking Tool Leak: Ex-Agency Employee Charged

Questions? https://mdcpa.participoll.com/

24

How to assure CIA?

- Where to begin?
- We all have limited budgets…
- We all have limited resources….
- How do we avoid missing "something"?

Questions? https://mdcpa.participoll.com/

25

Safeguards assure CIA

- The HIPAA Security Rule describes those *"somethings"* as Safeguards
  - **Administrative Safeguards** – Policy, Procedures, Training
  - **Physical Safeguards** – Locks, Fire protection, Location
  - **Technical Safeguards** – normally we think of these. Firewalls, Anti-virus, etc…

Questions? https://mdcpa.participoll.com/

26

Safeguards assure CIA

- Which safeguards should we put in place?...
  - All that we can of course!... within the limits of what is reasonable for the assets that you're protecting.
    - But which first?...
    - How do we decide?...

Questions? https://mdcpa.participoll.com/

27

Cybersecurity Frameworks

"The Plan"

Year after year, investigations performed after breaches and other security incidents reveal that the majority of security incidents occur because well-known security controls and practices were not implemented or were not working as organizations had assumed. …

*… **the major problem in cyber security remains a lack of defined and repeatable processes for selecting, implementing and monitoring the security controls that are most effective against real-world threats.*** *-- A SANS Spotlight April 2018*

Questions? https://mdcpa.participoll.com/

28

Cybersecurity Frameworks

- Cybersecurity frameworks are roadmaps
- Frameworks aid in setting priorities
- They cover each area of safeguards – Administrative, Physical, Technical
- Expert driven
- Assure CIA -- Confidentiality, Integrity, Availability

Questions? https://mdcpa.participoll.com/

29

Cybersecurity Frameworks

There are many!

- Payment Card Industry Data Security Standard (PCI DSS) | 47%
- National Institute of Standards and Technology (NIST) | 35%
- Center for Internet Security Critical Security Controls | 32%
- International Organization for Standardization (ISO) | 35%

Source: Tenable trends in security framework adoption (2016)

Questions? https://mdcpa.participoll.com/

30

Example Framework

CIS: Critical Security Controls

- Center for Internet Security (CIS) is a non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.
- The CIS Controls are a recognized best practices for securing IT systems and data against the most pervasive attacks.
- These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals.

Questions? https://mdcpa.participoll.com/

31

CIS: Critical Security Controls

- 20 high level controls that map to many sub-controls
- Generally Prioritized
- Define specific defenses against known cyber attacks
- Provide actionable tasks in clear language
- First six (Basic) are said to address *80% of the most common threats!*

Questions? https://mdcpa.participoll.com/

32

Critical Security Control 1

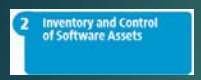
Inventory and Control of Hardware Assets

- Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
- Attackers, who can be located anywhere in the world, are continuously scanning the network addresses of target organizations, waiting for new and possibly unprotected systems to be attached to the network.

Questions? https://mdcpa.participoll.com/

33

Critical Security Control 2



Inventory and Control of Software Assets

- Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and that unauthorized and unmanaged software is found and prevented from installation or execution.
- Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited.

Questions? https://mdcpa.participoll.com/

34

Critical Security Control 3

Continuous Vulnerability Management

- Continuously acquire, assess, and take action on new vulnerability information/announcements in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
  - ***Think PATCHING!***
- Attackers have access to the same information and can take advantage of gaps between the appearance of new knowledge and the remediation of the new vulnerability.

Questions? https://mdcpa.participoll.com/

35

Critical Security Control 4

Controlled Use of Administrative Privileges

- Use processes and tools to track and control the assignment and use of administrative privileges on computers, networks, and applications.
  - *The keys to the Kingdom*
- The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise.
  - Malware that is executed on a computer logged-in with these administrative privileges can inherit these administrative privileges.

Questions? https://mdcpa.participoll.com/

36

Critical Security Control 5

Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

- Establish, implement, and actively manage the security configurations of mobile devices, laptops, servers, and workstations using a configuration management and change control process in order to prevent attackers from exploiting poorly configured settings.
- Out of the box, the default configurations for most technology lean towards ease-of-use and not security.

Questions? https://mdcpa.participoll.com/

37

Critical Security Control 6

Maintenance, Monitoring and Analysis of Audit Logs

- Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.
- Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Sometimes logging records are the only evidence of a successful attack.
  - Attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.

Questions? https://mdcpa.participoll.com/

38

Critical Security Control 7 - 16

Foundational

- Technology oriented
- Defenses
- Countermeasures
- *Many of the items most people think of when they think cybersecurity*

Questions? https://mdcpa.participoll.com/

39

Critical Security Control 17 - 20

Organizational

- Administrative oriented
- People
- Planning
- Preparation

Questions? https://mdcpa.participoll.com/

40

CIS CSC at BHS

- We found we were very strong on Foundational controls (Technical)
- We were weaker on some of the Basic controls
  - Large organization, limited resources
  - Challenged to know all devices and software that existed on our network.
  - Technical individuals were attracted to technical controls
    - *REMEMBER – We were previously guided by our **individual** judgement*

-- and we I.T. folks do like gadgets!

Questions? https://mdcpa.participoll.com/

41

CIS CSC at BHS

- This is a reality for many organizations
  - Individually driven choices made with good intentions
  - Often compelled by news, marketing, sales reps
  - Somewhat random impacts compared to a prioritized framework
- Working the CSCs in order, we began to improve our posture
- We began to improve our **Cybersecurity Maturity**

Questions? https://mdcpa.participoll.com/

42

CIS CSC at BHS

Today

- Fully operational framework *and* Information Risk Management program.
- Some remaining lower risk details are still targeted for improvement – *But we KNOW about them, and have a plan!*
- Still managing on s*ame-as* staff that runs operations.
- Making better decisions on where we focus

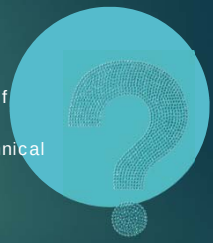
Questions? https://mdcpa.participoll.com/

43

What's all this mean to you?...

Cyber-risk is a business-risk

- Non-technologists are often charged with oversight of cybersecurity
- Financial leaders and auditors aren't *necessarily* technical security experts
- How to assure your not missing anything?
- Are the I.T. staff on top of it all?
- How can you feel confident that the appropriate measures are in place?



Questions? https://mdcpa.participoll.com/

44

What to ask?

- Organizations should be executing -- ***and constantly striving to improve*** -- their cybersecurity maturity.
- What was enough 10 years ago is not enough now.
- Our job may *not* be to verify that the org has applied every safeguard to ensure that the org secure.
- Our job is to determine if ***the organization*** is assuring that they are appropriately secure.

Questions? https://mdcpa.participoll.com/

45

No one person has all of the answers

- Those charged with cybersecurity should be guided by a plan
  - A recipe with all of the right ingredients
  - A roadmap prioritizing available resources to the greatest impact
  - A living document describing where they are in their ongoing journey
- Ideally, they should be able to provide this to those charged with oversight.
- In addition they should understand their risks – ideally through a risk assessment.
- They should have policies and plans for how to deal with incidents (Administrative Safeguards)

Questions? https://mdcpa.participoll.com/

46

Remember CIA

Information Security through --

- **C**onfidentiality of information
  - The privacy of Protected Health Information (PHI)
  - The privacy of Personally Identifiable Information (PII)
  - The privacy of Intellectual Property (IP)
  - The privacy of Financial Information
- **I**ntegrity of information
  - Preventing corruption, data loss, malicious modification
- **A**vailability of information
  - What are the financial implications of a gap in availability?
  - How are we prepared/positioned to assure this doesn't occur

Questions? https://mdcpa.participoll.com/

47

What should *YOU* look for?

- Varies by the organization, industry, etc.
  - Assets/Capability
  - Stakeholders
  - Any unique business requirements and risks
- Avoid focusing too hard on the individual technical detail.
  - *Do you have a firewall to secure you from the Interweb?*
  - *Do yinz guys have antivirus?*
  - *You have passwords,.. right?...*
- Technical questionnaires and spreadsheets have their place, but…

Questions? https://mdcpa.participoll.com/

48

The better question

- Verify that the org has assigned someone – *at a minimum one named individual* -- with the clear responsibility to remain informed and engaged in cyber security with respect to their industry
- This person or team should be able to describe the assets that might be targeted and to describe the risks that they in their specific industry face.
  - *Perhaps you should be familiar with this as well.*
- Have they assessed and documented their risk?
  - Threat x Likelihood = Impact
- Do they use a cybersecurity framework? Perhaps they should!

Questions? https://mdcpa.participoll.com/

49

Be prepared

- Because they probably don't use a framework.
- That's ok *(for now)*
  - Particularly in smaller resource-constrained organizations, some of these mechanisms may be more advanced than their current-state.
  - But the prescriptiveness of frameworks is exactly **why** they can be so impactful to the risk profile of these kinds of organizations.

Questions? https://mdcpa.participoll.com/

50

Other Considerations

What can we do with Risk?

- Avoid
- Mitigate – Through Safeguards
- Transfer – Cyber insurance
- Accept -- Sometimes

Questions? https://mdcpa.participoll.com/

51

Even the finest masterpiece had a beginning, a middle, and then an

Questions? https://mdcpa.participoll.com/

52

End

Questions? https://mdcpa.participoll.com/

53

Questions

Questions? https://mdcpa.participoll.com/

54

Resources

- https://www.nist.gov/cyberframework
- https://www.cisecurity.org/controls

Questions? https://mdcpa.participoll.com/

55

Thank you

- Roger Lutz
- Roger.Lutz@butlerhealthsystem.org

Questions? https://mdcpa.participoll.com/

56