Health Industry Cybersecurity Practices
Managing Threats and Protecting Patients

HCCA - New Orleans Region

1

HACKERS CONVENTION

2

50,000 Hackers in Attendance

3

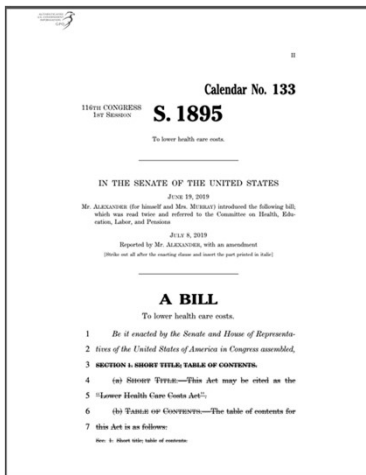Social-Engineer Village

4

5

6

7

8

2017

- Windows Vulnerability

- 300,000 computers shut down

- One fifth of the UK Health System Shut Down

2020

- Urgent 11 – Sept 2019 (CVSS 9.8)

- BlueKeep – Wormable like Wannacry

- 49 Windows Vulnerabilities – Jan 2020

- Many more…….

- COVID 19 – Healthcare Industry (Critical)

9

Lower Health Care Costs Act – Section 502

- Senate Bill 1895
- Recognition of Security Practices
  - ***Approaches promulgated under section 405(d) of the Cybersecurity Act 2015***
- Reduce Breach Exposure
  - Mitigate fines
  - Early favorable termination of an audit
  - Limit remedies from HHS
- Documentation for 12 months

10

10

Healthcare – #1 Target


"Bummer of a birthmark, Hal."

"FULLZ"

A compilation or package of information on a prospective fraud or identity theft victim.

- Most costly across industry - $408

- Most valuable record for hackers - $500

- Highest "Churn Rate" due to breach

- Longest "Identify and Contain" times – 358 days

- Records breached in 2019 increased 300% - 41 million

- Fines and Fees hit $28m in 2019

- Least investment in cybersecurity

- Medical Devices Security = Patient Safety

11

11

12

"WE'VE NARROWED OUR SECURITY RISKS DOWN TO THESE TWO GROUPS."
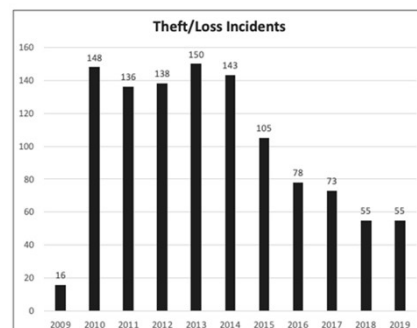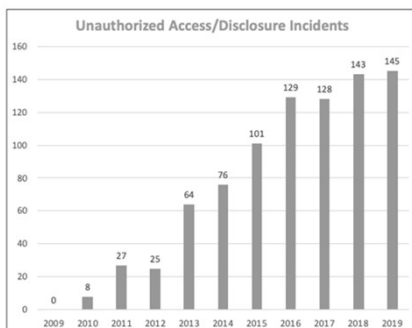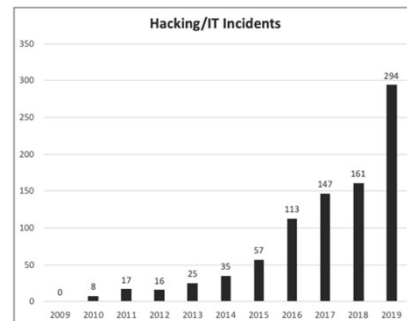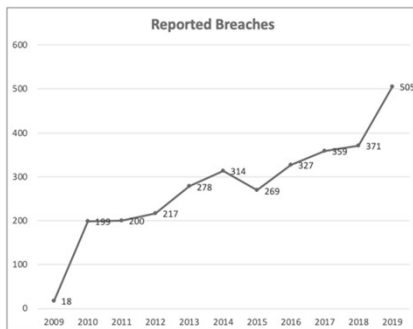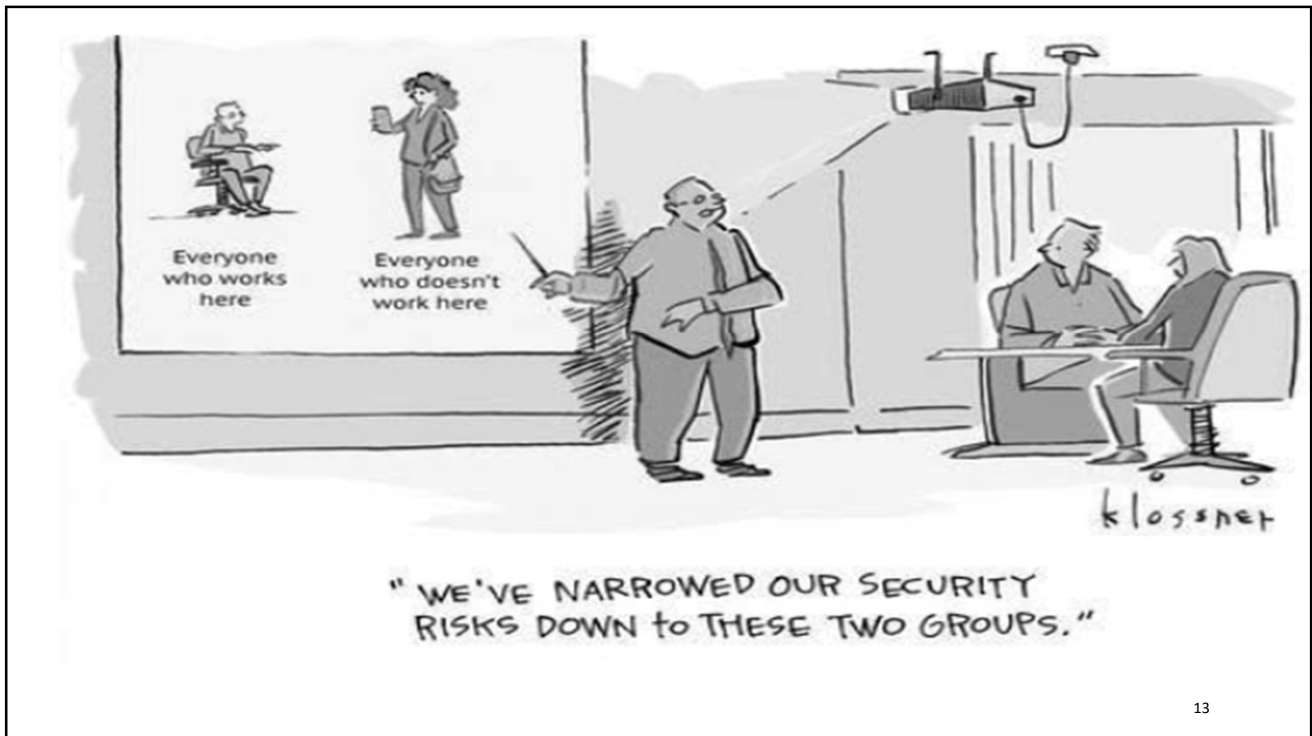
13

14

HHS 405(d)
Aligning Health Care
Industry Security Approaches

Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

Health Industry Cybersecurity Practices:
Managing Threats and Protecting Patients
"HICP"

2019 Winner
FedHealth**IT**
Innovation Awards

Ty Greenhalgh
ty@cybertygr.com

- Co-founder Cyber Tygr

- 30 years experience in HIM

- Henry Ford Health System – Most Innovative Technology of the Year

- Healthcare Information Systems & Privacy Practitioner (HCISPP) ISC^2

- HHS Joint Cybersecurity Workgroup

- NCHICA Biomedical Security Taskforce

- HHS led CISA 405(d) task group member

PROUD MEMBER

16

- Top 5 Current Threats
- 10 Mitigation Practices
- Traveling the 405
- Resources and Templates
- Where is the 405 going
- Questions

Agenda

17

Cybersecurity Act (CSA) 2015

CSA Section 405
Improving Cybersecurity in the Health Care Industry

Section 405(b): Health care industry preparedness report

Section 405(c): Health Care Industry Cybersecurity Task Force

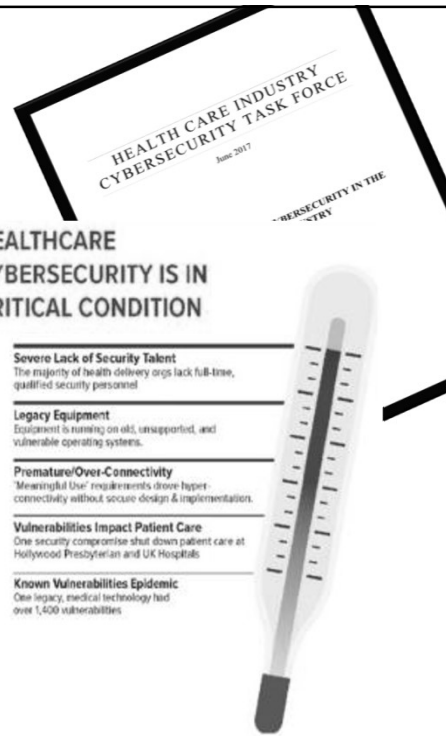Section 405(d): Aligning Health Care Industry Security Approaches

18

CSA 405(c)
Health Care Industry Cybersecurity Task Force Report
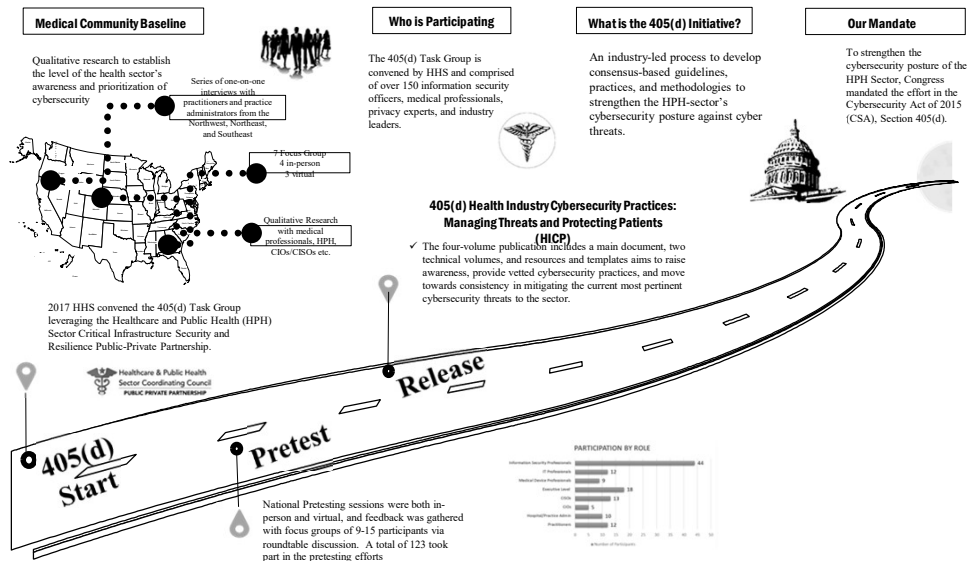
6 IMPERATIVES

1. NIST CSF for leadership and governance
2. Security and resilience increased
   - *medical devices & Health IT*
3. Improve information sharing
4. Cybersecurity training & awareness
5. Develop workforce
6. Protect R&D and Intellectual Property

HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE
June 2017
CYBERSECURITY IN THE INDUSTRY

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities

19

CSA 405(d)
Aligning Health Care Industry Security Approaches

Medical Community Baseline

Qualitative research to establish the level of the health sector's awareness and prioritization of cybersecurity

Series of one-on-one interviews with practitioners and practice administrators from the Northwest, Northeast, and Southeast

7 Focus Group
4 in-person
3 virtual

Qualitative Research with medical professionals, HPH, CIOs/CISOs etc.

2017 HHS convened the 405(d) Task Group leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership.

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

405(d)
Start

Pretest

National Pretesting sessions were both in-person and virtual, and feedback was gathered with focus groups of 9-15 participants via roundtable discussion. A total of 123 took part in the pretesting efforts

Release

Who is Participating

The 405(d) Task Group is convened by HHS and comprised of over 150 information security officers, medical professionals, privacy experts, and industry leaders.

What is the 405(d) Initiative?

An industry-led process to develop consensus-based guidelines, practices, and methodologies to strengthen the HPH-sector's cybersecurity posture against cyber threats.

405(d) Health Industry Cybersecurity Practices:
Managing Threats and Protecting Patients
(HICP)
✓ The four-volume publication includes a main document, two technical volumes, and resources and templates aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in mitigating the current most pertinent cybersecurity threats to the sector.

Our Mandate

To strengthen the cybersecurity posture of the HPH Sector, Congress mandated the effort in the Cybersecurity Act of 2015 (CSA), Section 405(d).

PARTICIPATION BY ROLE

20

20

- **HICP - Main Document**
  - Industry cybersecurity threats and vulnerabilities
  - Explores five (5) current threats
  - Presents ten (10) practices to mitigate those threats

- **HICP - Technical Volume 1**
  - Small healthcare organization
  - Ten (10) detailed cybersecurity mitigation practices
  - Nineteen (19) detailed sub-practices

- **HICP - Technical Volume 2**
  - Medium and Large healthcare organizations
  - Ten (10) detailed cybersecurity mitigation practices
  - Seventy (70) detailed sub-practices

- *HICP - Resources and Templates*
  - Mappings to the NIST Cybersecurity Framework
  - An HICP assessment process
  - Sample Templates

Top 5 Threats

1. **Email Phishing Attacks**
2. **Ransomware Attacks**
3. **Loss or Theft of Equipment or Data**
4. **Internal, Accidental, or Intentional Data Loss**
5. **Attacks Against Connected Medical Devices that May Affect Patient Safety**

21

Cybersecurity Mitigation Practices

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response & SOC
9. Medical Device Security
10. Cybersecurity Policies

22

Top 5 Threats

23

23

#1 Threat

CURRENT ATTACK VECTOR:
COVID 19

RomoloTavani / Getty Images / Thinkstock

Email Phishing Attack

- Spear Phishing
- Executive Whaling
- Social Engineering
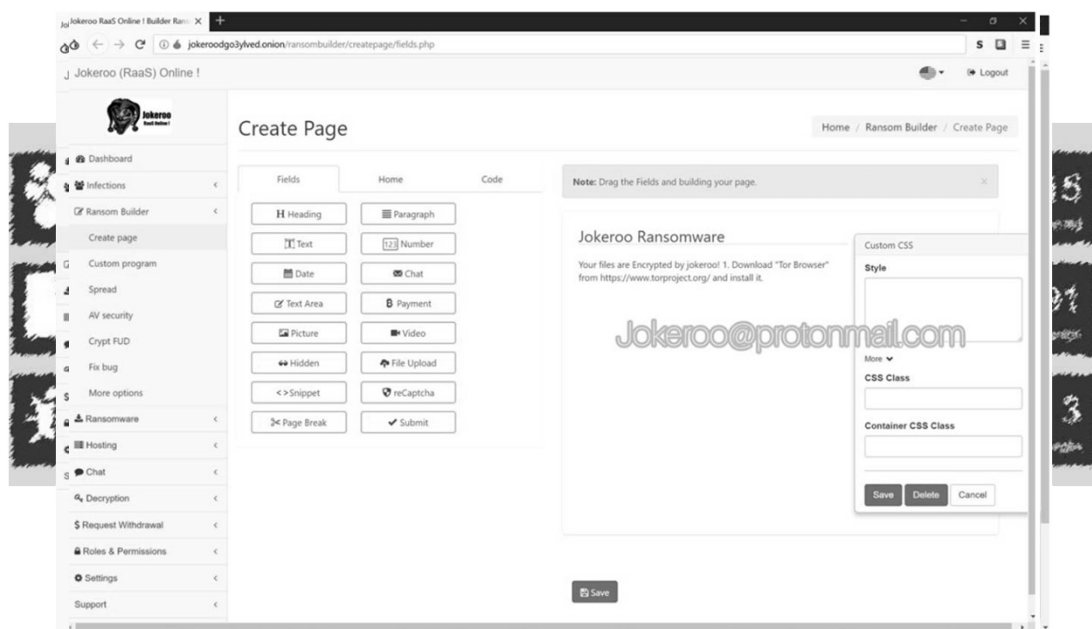- Malvertising

24

#2 Threat

Ransomware

- Email
- Drive by Download
- Free Software
- Remote Desktop Protocol (RDP)
- Ransom - Bitcoin
- Held Hostage

25

Ransomware-As-A-Service

Ransom Note Creator

26

Loss or Theft of Equipment or Data

- Laptops, drives, etc.
- Data sensitivity
- Business disruption

27

27

Insider – Accidental or Intentional Data Loss

- Accidental Insider
  - Honest mistakes
  - Procedural errors
  - Emailing sensitive data
- Intentional Insider
  - Personal gain
  - Inflict harm
  - Impersonating staff
  - Disgruntled employee

28

#5 Threat

Medical Device Security: Patient Safety

- Inventory control
- Software patches
- Device monitoring
- Remote access
- Anti-malware
- Urgent 11 – VxWorks OS

29

Top 10 Cybersecurity Practices

30

Top 10 Cybersecurity Practices

Doctors and nurses know that hand sanitizing is critical to prevent the spread of germs. That does not mean healthcare workers wash up as often as they should.

Similarly, cybersecurity practices reduce the risk of cyber-attacks and data breaches. Just as we are able to protect our patients from infection, we should all work towards protecting patient data to allow physicians and caregivers to trust the data and systems that enable delivery of quality health care.

Cyber Hygiene >>> **Patient Safety**

31

31

Email Protection Systems

- Education
- Phishing Simulation
- E-mail Protection Controls
- Domain Key Identified Mail (DKIM)
- E-mail Encryption

SPAM FILTER

#1 Practice

32

32

Endpoint Protection Systems

- Micro-segmentation
- Mobile Device Management
- Host Based Intrusion Detection/Prevention Systems
- Endpoint Detection and Response
- Application Whitelisting

#2 Practice

33

33

Access Management

- Identity
- Automate Provisioning
- Authentication
- Multifactor Authentication for Remote Access
- Single-Sign On

#3 Practice

34

34

Data Protection and Loss Prevention

- Policies & Procedures
- Classification of Data
- Data Use Procedures
- Data Security
- Backup Strategies
- Data Loss Prevention
- Mapping of Data Flows

#4 Practice

35

35

Asset Management

- Inventory Details
- Decommissioning
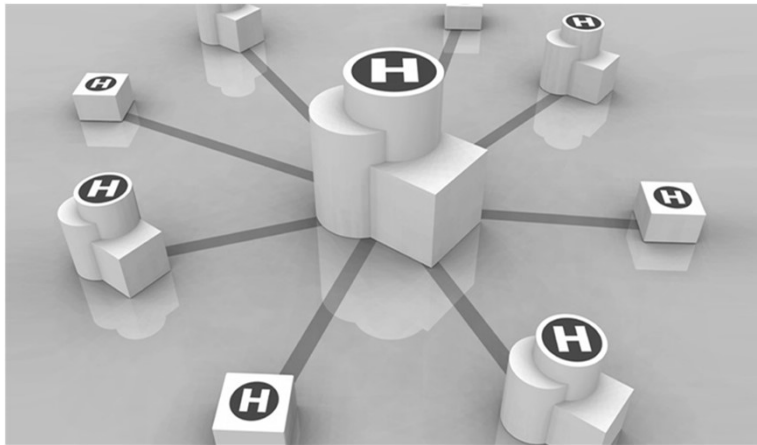- Automated Discovery and Maintenance
- Procurement – HIC-SCRiM

    https://healthsectorcouncil.org/hic-scrim/

#5 Practice

36

36

Network Management

- Network Segmentation
- Physical Security
- Intrusion Prevention
- Network Profiles and Firewalls
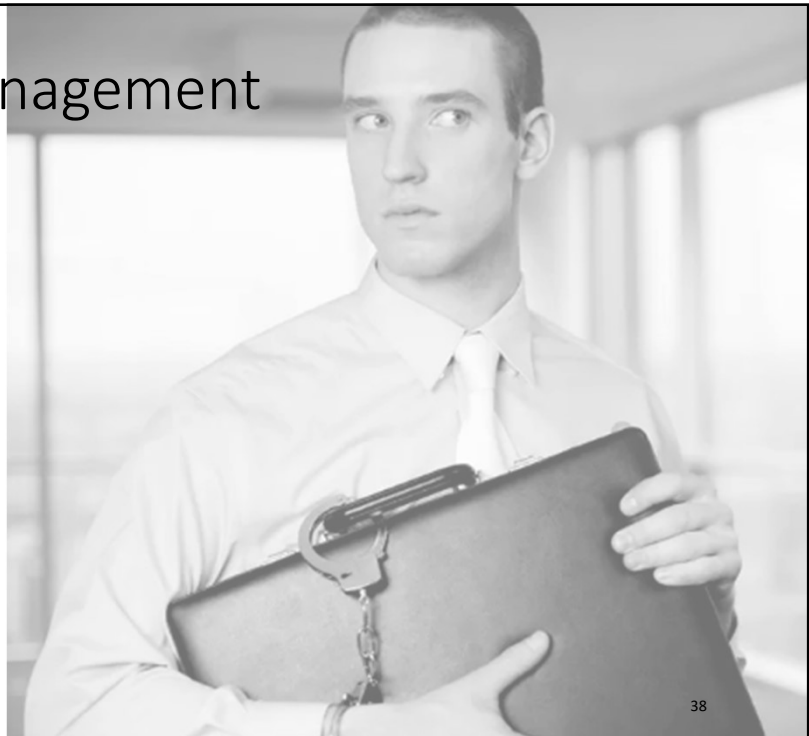- Network Access Control

#6 Practice

37

37

Vulnerability Management

- Scanning
- Data Classification
- Patch Management
- Configuration Management
- Penetration Testing

#6 Practice

38

38

Incident Response

- Incident Response
- ISAC/ISAO Participation
- Security Operations Center (SOC)
- Baseline Network Traffic
- User Behavior Analytics
- Deception Technologies

Our Incident Response Plan goes something like this...

HELP! HELP!

#8 Practice

39

39

Medical Device Security

- Procurement and Security Evaluations
- Practice #2
- Practice #3
- Practice #5
- Practice #6
- Practice #7
- Practice #8
- Practice #10
- Contacting the FDA

#9 Practice

40

40

Cybersecurity Policies

- Policies

#10 Practice

41

So You Want A Recipe For Cybersecurity?

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

CYBERSECURITY COOKBOOK

Mitigating Email Phishing Recipe
1. 5 oz Basic E-Mail Protection Controls (1.M.A)
2. A dash of Multi-Factor Authentication (1.M.B)
3. 1 cup of Incident Response plays (8.M.B)
4. 1 tsp of Digital Signatures for authenticity (1.L.B)
5. Advanced and Next General Tooling to taste (1.L.A)
6. 2 cups of Workforce Education (1.M.D)

Preheat your email system with some basic email protection controls, building a foundation for your dish. Mix in MFA for remote access, protecting against potential credential theft. Place in oven at high temp for incident response plan testing.

When finished baking sprinkle with additional tooling to provide next level protection to taste. Let cool several hours while providing the workforce training on reporting phishing attacks in the new system. Garnish with education on how digital signatures demonstrate authenticity of the sender.

Just like with any cookbook the recipes provide the basic ingredients to making a meal. It does not instruct you how to cook, instruct you on what recipes to use or limit your ability for substitutions. The skill of the cook is what makes the dish!

42

HICP is…	HICP is **not**…
• A call to action to manage real cyber threats	‣ A new regulation
• Written for multiple audiences (clinicians, executives, and technical)	‣ An expectation of minimum baseline practices to be implemented in all organizations
• Designed to account for organizational size and complexity (small, medium and large)	‣ The definition of "reasonable security measures" in the legal system
• A reference to "get you started" while linking to other existing knowledge	‣ An exhaustive evaluation of all methods and manners to manage the threats identified
• Aligned to the NIST Cybersecurity Framework	– You might have other practices in place that are more effective than what was outlined!
• Voluntary	‣ Your guide to HIPAA, GDPR, State Law, PCI, or any other compliance framework

43

What Size is My Organization?

Factors Determining Size:
– Health Information Exchanges
– IT Capability
– Cybersecurity Investment
– Size (provider)
– Size (acute/post-acute)
– Size (hospital)
– Complexity

Main Document – page 11

Best Fit		Small	Medium	Large
Common Attributes	Health information exchange partners	One or two partners	Several exchange partners	Significant number of partners or partners with less rigorous standards or requirements. Global data exchange
	IT capability	No dedicated IT professionals on staff, IT may be outsourced on a break/fix or project-by project-basis	Dedicated IT resources on staff. No or limited dedicated security resources on staff	Dedicated IT resources with dedicated budget. CISO or dedicated security leader with dedicated security staff
	Cybersecurity investment	Nonexistent or limited funding	Funding allocated for specific initiatives. Potentially limited future funding allocations. Cybersecurity and IT budgets are blended	Dedicated budget with strategic roadmap specific to cybersecurity
Provider Attributes	Size (provider)	1–10 physicians	11–50 physicians	Over 50 physicians
	Size (acute / post-acute)	1–25 providers	26–500 providers	Over 500 providers
	Size (hospital)[15]	1–50 beds	51–299 beds	Over 300 beds
	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated delivery networks. Participate in accountable care organization or clinically integrated network
Other Org Types			Practice Management Organization. Managed Service Organization. Smaller device manufacturers. Smaller pharmaceutical companies	Health Plan. Large Device Manufacturer. Large pharmaceutical organization

44

Self Assessment - Practices & Sub Practices

FULL LISTING OF CYBERSECURITY SUB-PRACTICES BASED ON ORGANIZATION SIZE SELECTED			Self Assessment		
Cybersecurity Sub-Practice Title	Short Description	Current State	Gaps	Action Plan	
.A Basic Endpoint Protection Controls	Basic endpoint security controls to enable	Encryption at 80%, AV in place, baseline image, all users with admin rights	Encryption gaps and admin rights	Finish encryption, remove rights	
.A Identity	Establish a unique identifier for all users, leveraging systems of record	All users provided accounts, not tied to ERP	No identity, can allow for orphaned accounts and failure to term	Establish identity program	
.B Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination	User accounts created directly into Active Directory manually, when terminal access requested	Access rights might cumulate and administrators might fail to remove access	Establish accounts based on identity, automate provisioning and de-provisioning	
.C Authentication	Implement and monitor secure authentication for users and privileged accounts	Authentication bound to central authentication source	No gaps	No gaps	
.D Multi-Factor Authentication for Remote Access	Implement multi-factor authentication for remote access to resources	VPN accessible, no MFA	MFA not enabled, which can allow for a theft of credentials to access sensitive data	Implement MFA	
.A Security Operations Center	Establish a SOC to prevent, discover and respond to cyber attacks	Dedicated team to manage and respond to cyber incidents	No gaps	No Gaps	
.B Incident Response	Establish formal incident response playbooks for responding to cyber attacks	Playbooks exist, but no playbook for lost/stolen device	In the case of a stolen device teams might not execute investigation properly	Establish playbook for stolen devices, get approval from leadership	
.C Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information	Not a current member of an ISAC/ISAO	By not participating in ISAC/ISAOs cyber teams might be missing out on leading practices	Join ISAC/ISAO	

Cybersecurity Practices Assessment Toolkit

45

45

Prioritization Tool

- Approach
  - Threat - apply combination of Practices and Sub-Practices
  - Practice - applicable to multiple Threats

Factor		
Select your organizations size		Medium
Prioritize the threats (5 being highest priority, 1 being lowest priority)		
A	Email Phishing Attack	1
B	Ransomware Attack	4
C	Loss or Theft of Equipment or Data	5
D	Insider, Accidental or Intentional Data Loss	3
E	Attacks Against Connected Medical Devices that may affect Patient Safety	2

CP #	Cybersecurity Practices	Priority Rank Based on Threat Model Inputs
8	Incident Response	28
3	Access Management	23
2	Endpoint Protection Systems	23
5	Asset Management	20
6	Network Management	16
7	Vulnerability Management	16
10	Cybersecurity Policies	15
1	Email Protection Systems	13
9	Medical Device Security	11
4	Data Protection and Loss Prevention	11

46

46

Templates

- Glossary of Terms
- NIST Cybersecurity Framework Crosswalk
- Assessment Methodology
- Toolkits

- Examples
  - Portable devices policy
  - Incident response policy
  - Access control procedure
  - Security incident report sample
  - Onboarding and Offboarding policy
  - TECFA Do's and Don'ts

47

47

405(d) Awareness Materials

The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! These 5 threat posters were created in support of Cybersecurity Awareness Month in October 2019 to be used in hospitals, doctor's offices and even in email threads!

405(d) Outreach

The 405(d) Program produces Bi-monthly Newsletters and Spotlight Webinars to increase cybersecurity awareness. They also present on new emerging cybersecurity news and topics, to include highlighting the HICP Publication!

405(d) Social Media

The 405(d) Program is now live on Twitter, Instagram, and Facebook at @ask405d. Follow us to receive up to date 405(d) News and cybersecurity tips and practices!

Request materials – cisa405d@hhs.gov

48

HHS 405(d) Group

➢ Collaboration center for HHS Office of the CIO
➢ HICP
  ➢ Update current information
  ➢ Add additional detail
➢ 405(d) Communications
  ➢ Videos
  ➢ Newsletter
  ➢ How to guides (S,M,L)
➢ Executive Leadership's role
➢ Impactful metrics

49

49

Resources and Solutions

HICP Documents - https://cybertygr.com/resource.html or
https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

Business Case for Medical Device Security

Free Medical Device Security ROI
https://cybertygr.com/connectedmd.html

Automatically Document Security Efforts
Governance, Risk & Compliance Software
https://cybertygr.com/hipaamanage.html

Thank you

Ty Greenhalgh – Ty@CyberTygr.com

50