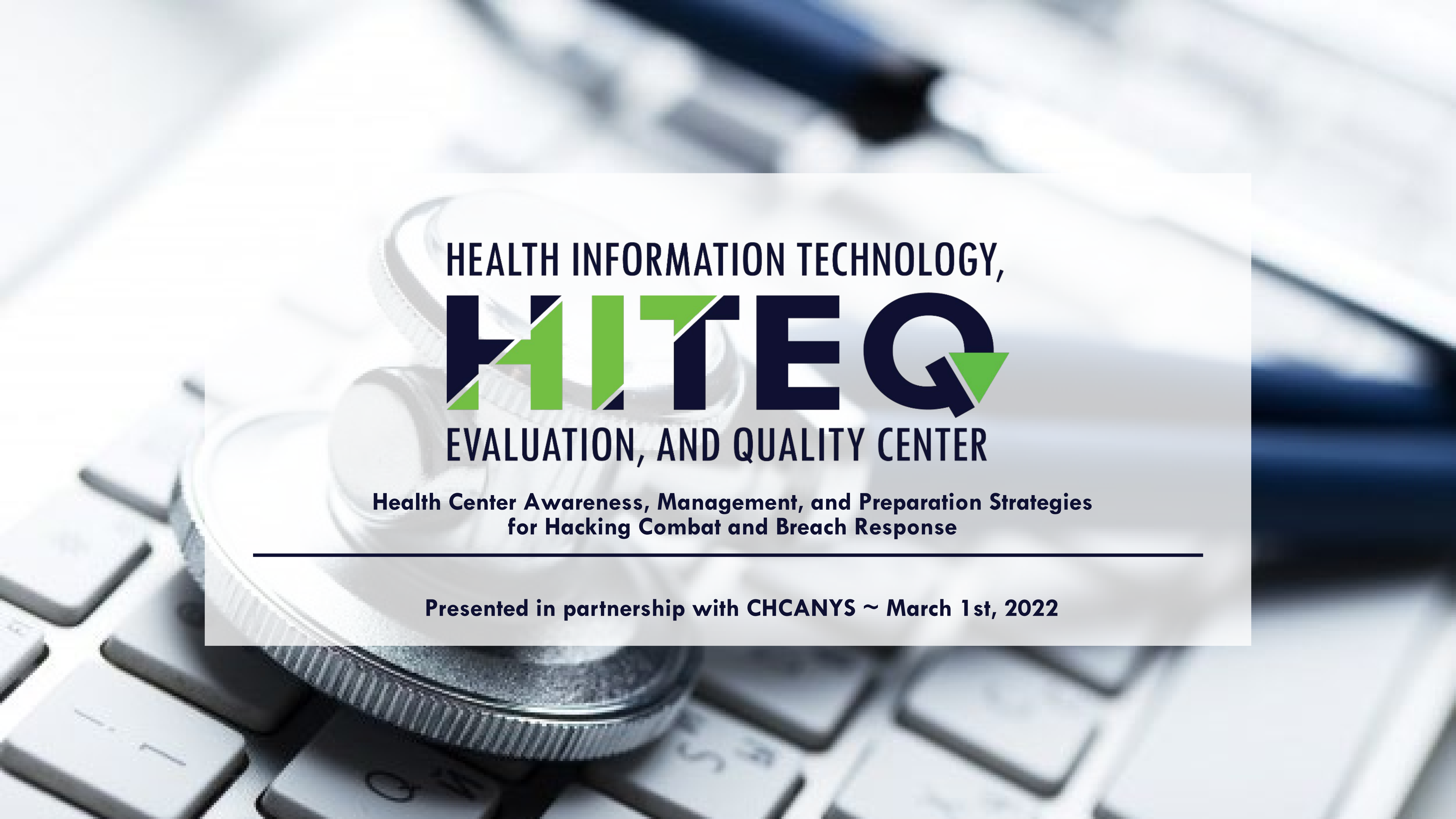


HEALTH INFORMATION TECHNOLOGY,

HITEQ

EVALUATION, AND QUALITY CENTER

Health Center Awareness, Management, and Preparation Strategies for Hacking Combat and Breach Response

Presented in partnership with CHCANYS ~ March 1st, 2022

About The HITEQ Center

The HITEQ Center is a HRSA-funded National Training and Technical Assistance Partner (NTTAPs) that collaborates with HRSA partners including Health Center Controlled Networks, Primary Care Associations and other NTTAPs to engage health centers in the optimization of health IT to address key health center needs through:

- A **national website** (**www.hiteqcenter.org**) with health center-focused resources, toolkits, training, and a calendar of related events.
- **Learning collaboratives**, **remote trainings**, and **on-demand technical assistance** on key topic areas.

HITEQ Topic Areas

Access to comprehensive care using health IT and telehealth

Privacy and security

Advancing interoperability

Electronic patient engagement

Readiness for value based care

Using health IT and telehealth to improve Clinical quality and Health equity

Using health IT or telehealth to address emerging issues: behavioral health, HIV prevention, and emergency preparedness

Legal Disclaimer

- The information included in this presentation is for informational purposes only and is not a substitute for legal advice.

- Please consult an appropriate attorney if you have any particular questions regarding a legal issue.

Session Agenda

Assessing Breach Risk

Strengthening Breach Defense, Mitigation and Response Plans

Operationalizing Cybersecurity

Questions and Discussion

Your Presenter

Nathan Botts, PhD, MSIS

- Senior Study Director, Westat – Healthcare Delivery, Research, and Evaluation
- Privacy & Security domain lead for the HRSA HITEQ Center
- Health informatics specialist, with over 15 years of clinical software and systems R&D experience.
- Knowledge Integrator for the Privacy and Security Community of Practice, for the ONC Regional Extension Centers.
- Co-lead of the HL7 Consumer Mobile Health Application Functional Framework for Privacy and Security Considerations
- Professor of Cybersecurity – Purdue University Global

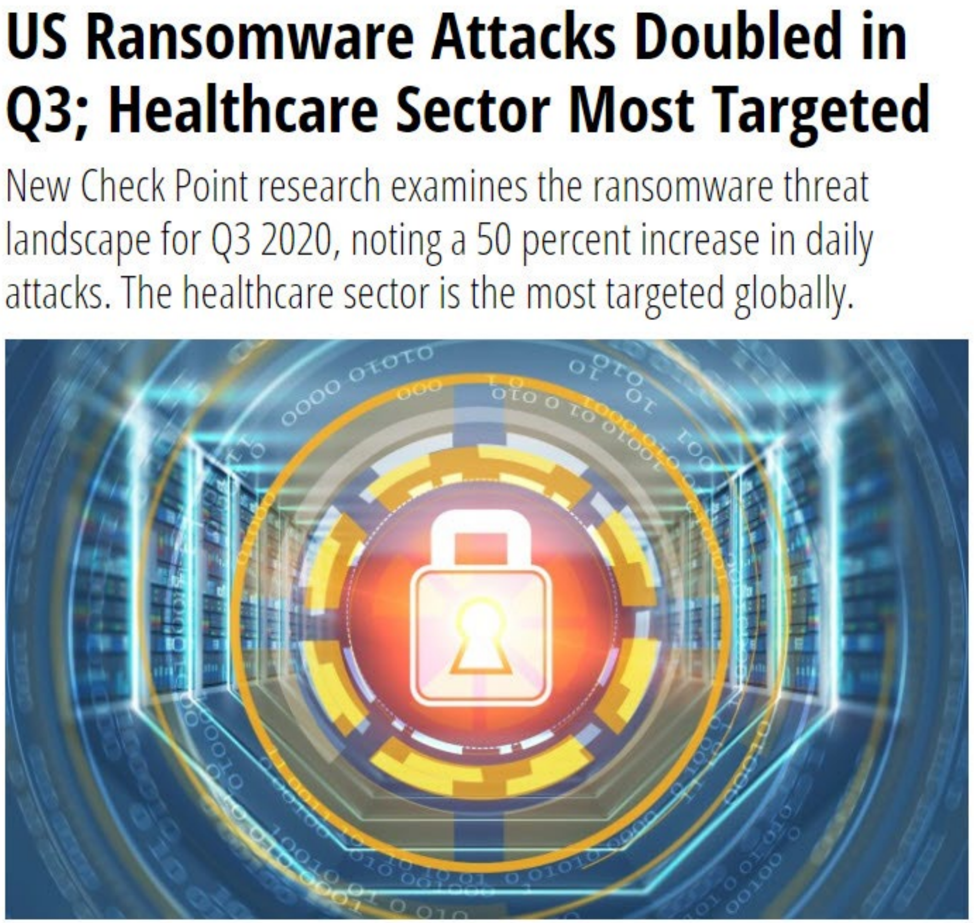
Assessing Breach Risk

Health Center Cybersecurity Problem Statement

- Increased use of electronic health record systems increases security risk
- Increased use of IoT enabled mobile health and medical devices increases security risk
- Increased use of internet-based systems increases security risk
- Increased numbers of users on a given system increases security risk
- *That can be a lot of security risks for small to medium-sized health centers to effectively manage!*

The Continued Rise of Ransomware

- The frequency of daily ransomware attacks increased 50 percent during the third quarter of 2020 from the first half of the year
- The effects can be seen in the ransomware attack on Universal Health Services, which impacted all 400 US sites
- Educating the healthcare workforce on how to identify and avoid potential ransomware attacks is considered the most important defense against these attacks as the threat becomes more targeted via social engineering



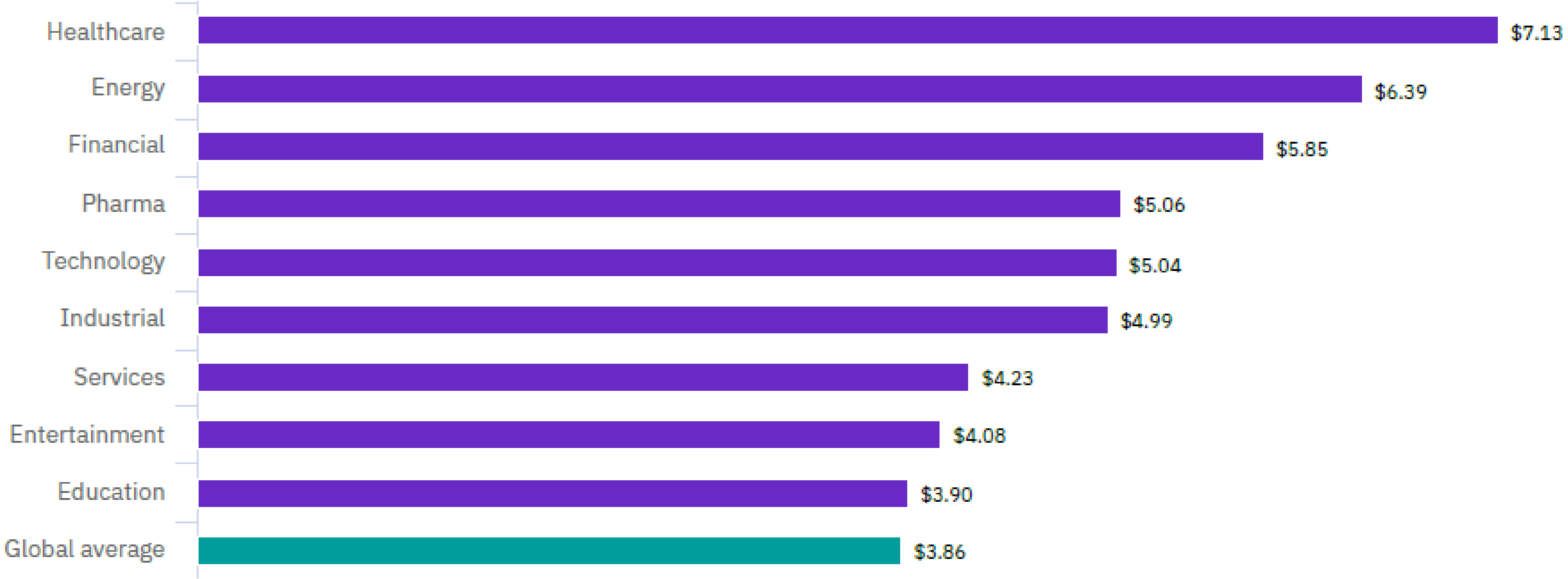
US Ransomware Attacks Doubled in Q3; Healthcare Sector Most Targeted

New Check Point research examines the ransomware threat landscape for Q3 2020, noting a 50 percent increase in daily attacks. The healthcare sector is the most targeted globally.

The Cost of Healthcare Breach

Average total cost of a data breach by industry

Measured in US$ millions



Current Well Known Malware Exploits

Clop ransomware: This ransomware disables windows applications such as windows defender, effectively stopping you from receiving any new intruder alerts. While it does this the ransomware also encrypts your files.

Agent Tesla: This is a RAT (Remote Access Trojan) that exfiltrates credentials by logging keystrokes and taking screenshot from the infected system.

Snugy: PowerShell based backdoor which allows the attacker full access to the system using DNS tunneling. DNS tunneling exploits the DNS protocol to tunnel malware and other data through a client-server model.

ZeuS: Botnet that delivers malware, logs keystrokes, spreads other malware and reports back to the attacker.

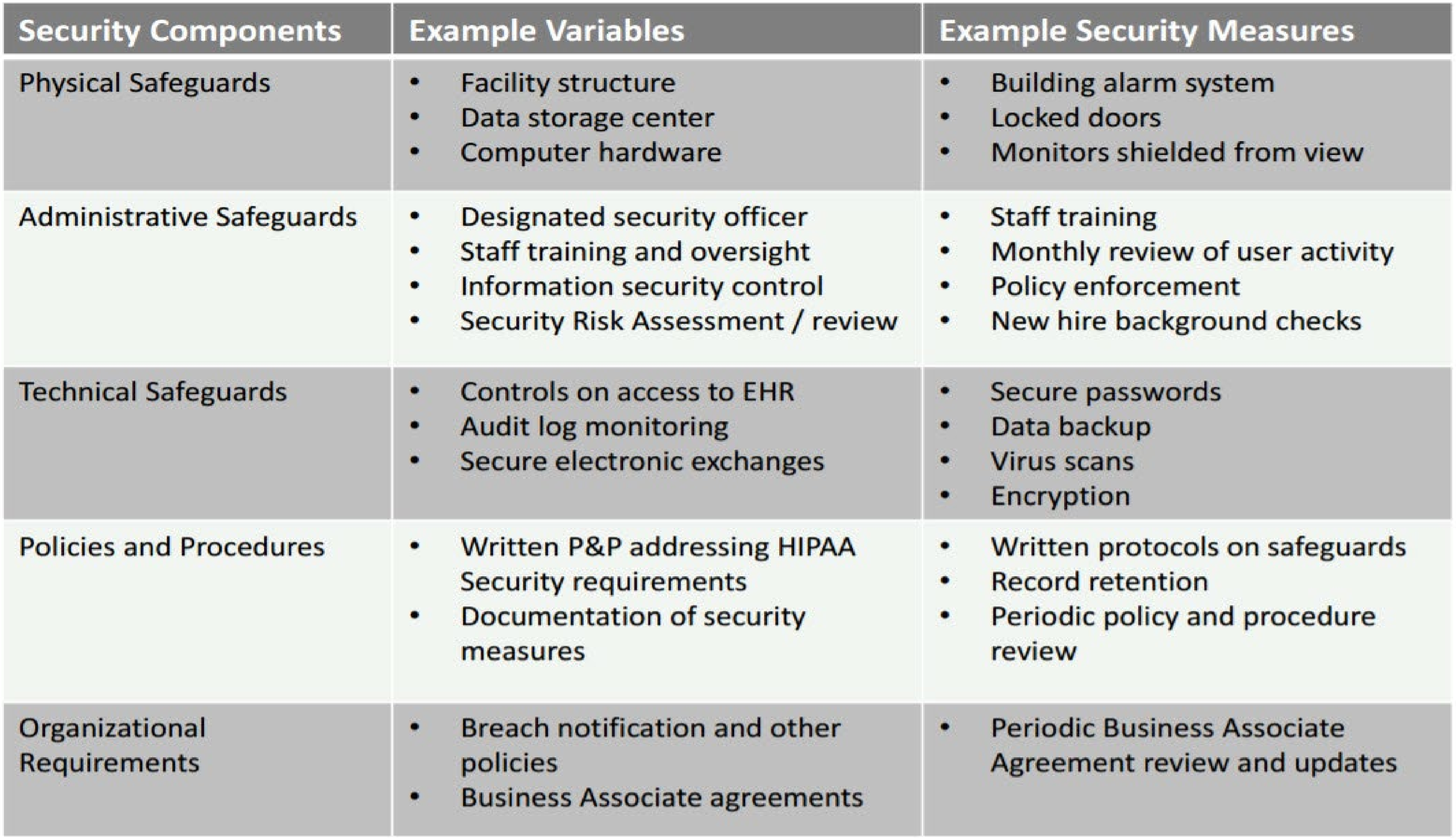
Dridex: a phishing trojan and botnet which uses malicious macros in Microsoft Office with either malicious embedded links or attachments

CoinMiner: A cryptocurrency miner that spreads throughout an enterprises network and uses the system resources to mine for cryptocurrencies.

Health Center Cyber Defense against the Dark Web Call to Arms!

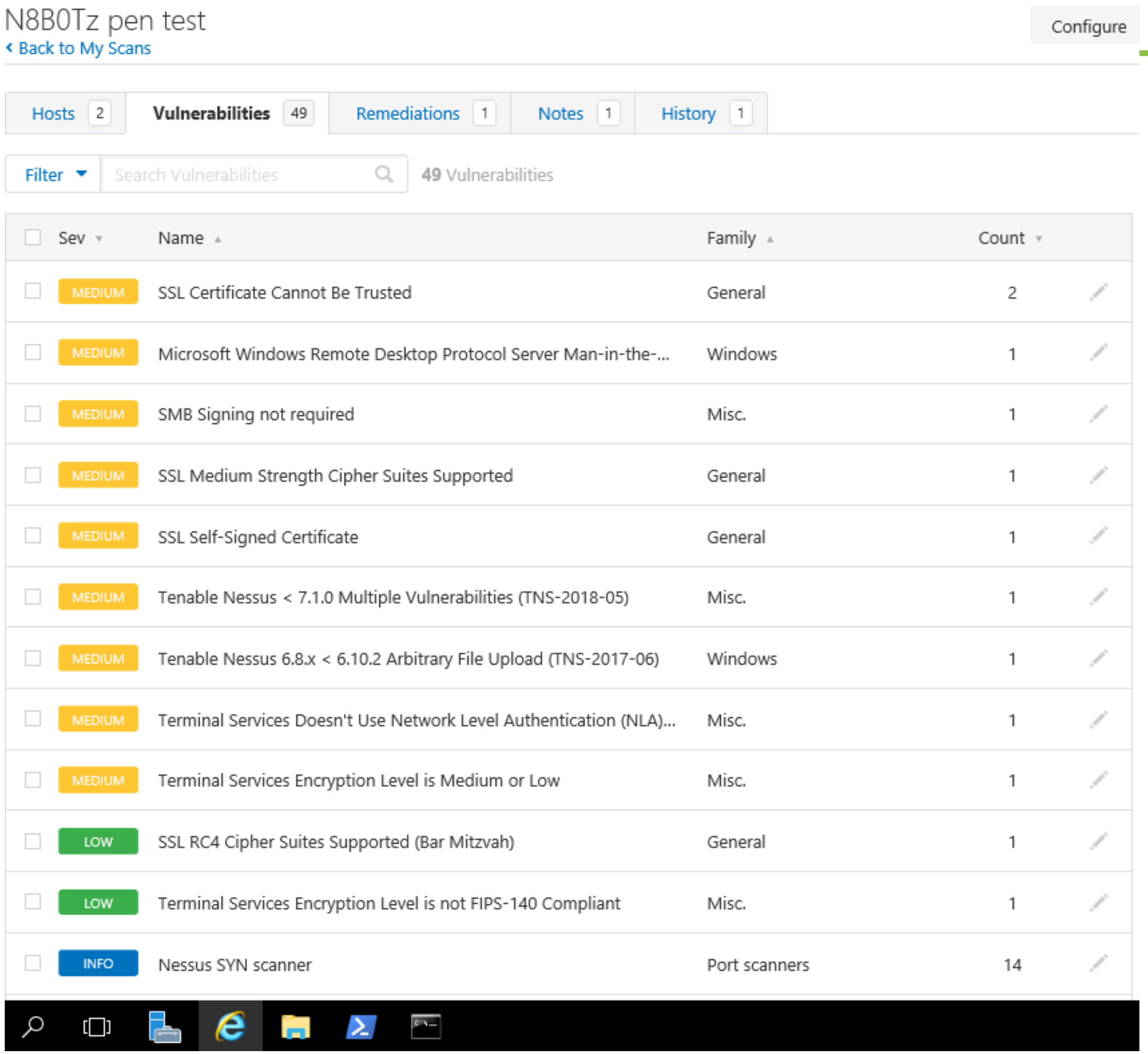
- An EHR system or medical device is essentially no different than any other type of computer program
- Except…that there is a greater chance that it could have a direct impact on someone's health
- "White Hat" initiatives for protecting the privacy and security of that data have steadily evolved.
- It is all of our responsibility, whether health IT staff, nurses, doctors, CEOs or patients to defend health information against the dark web
- Join the fight!

Security Rule Requirements



Security Components	Example Variables	Example Security Measures
Physical Safeguards	• Facility structure • Data storage center • Computer hardware	• Building alarm system • Locked doors • Monitors shielded from view
Administrative Safeguards	• Designated security officer • Staff training and oversight • Information security control • Security Risk Assessment / review	• Staff training • Monthly review of user activity • Policy enforcement • New hire background checks
Technical Safeguards	• Controls on access to EHR • Audit log monitoring • Secure electronic exchanges	• Secure passwords • Data backup • Virus scans • Encryption
Policies and Procedures	• Written P&P addressing HIPAA Security requirements • Documentation of security measures	• Written protocols on safeguards • Record retention • Periodic policy and procedure review
Organizational Requirements	• Breach notification and other policies • Business Associate agreements	• Periodic Business Associate Agreement review and updates

Example: Use of Vulnerability Scanners



N8B0Tz pen test

‹ Back to My Scans

Hosts 2 | Vulnerabilities 49 | Remediations 1 | Notes 1 | History 1

Filter ▾ | Search Vulnerabilities

49 Vulnerabilities

□	Sev ▾	Name ▴	Family ▴	Count ▾
□	MEDIUM	SSL Certificate Cannot Be Trusted	General	2
□	MEDIUM	Microsoft Windows Remote Desktop Protocol Server Man-in-the-...	Windows	1
□	MEDIUM	SMB Signing not required	Misc.	1
□	MEDIUM	SSL Medium Strength Cipher Suites Supported	General	1
□	MEDIUM	SSL Self-Signed Certificate	General	1
□	MEDIUM	Tenable Nessus < 7.1.0 Multiple Vulnerabilities (TNS-2018-05)	Misc.	1
□	MEDIUM	Tenable Nessus 6.8.x < 6.10.2 Arbitrary File Upload (TNS-2017-06)	Windows	1
□	MEDIUM	Terminal Services Doesn't Use Network Level Authentication (NLA)...	Misc.	1
□	MEDIUM	Terminal Services Encryption Level is Medium or Low	Misc.	1
□	LOW	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	1
□	LOW	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.	1
□	INFO	Nessus SYN scanner	Port scanners	14

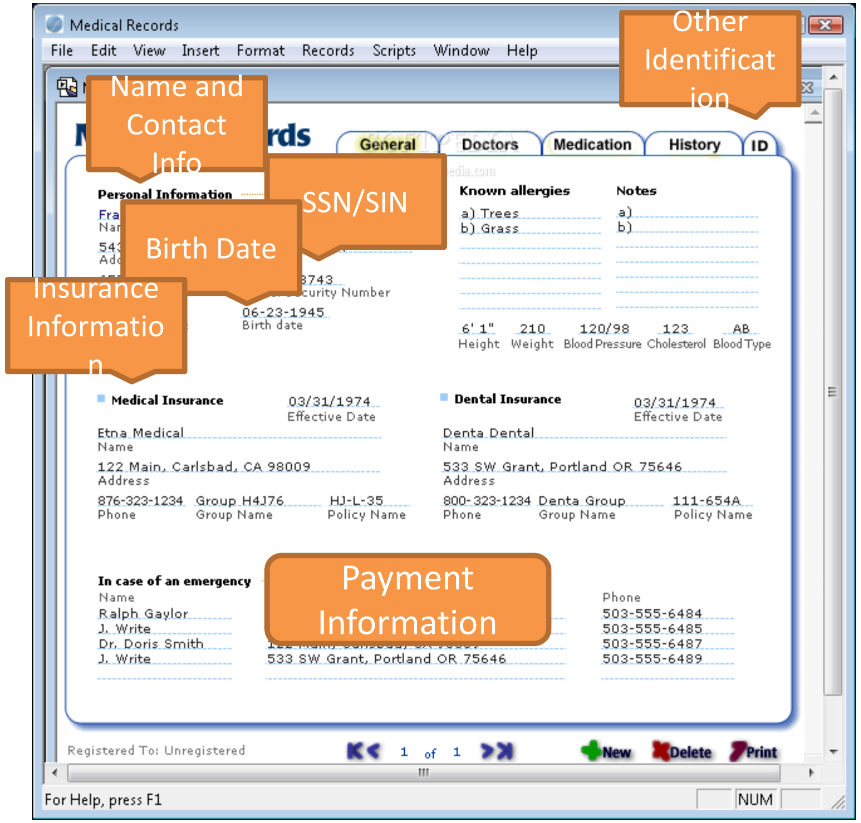
Allows for vulnerability, configuration and compliance assessments

Prevents network attacks by identifying the vulnerabilities and configuration issues

Uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools

Utilizes attack scripting languages that describes individual threats and potential attacks

Why do they want our Health Center data so badly?



Personal Information

3743
curity Number

06-23-1945
Birth date

Known allergies
a) Trees
b) Grass

Notes
a)
b)

6' 1"	210	120/98	123	AB
Height	Weight	Blood Pressure	Cholesterol	Blood Type

Medical Insurance
03/31/1974
Effective Date
Etna Medical
Name
122 Main, Carlsbad, CA 98009
Address
876-323-1234 Phone
Group H4J76 Group Name
HJ-L-35 Policy Name

Dental Insurance
03/31/1974
Effective Date
Denta Dental
Name
533 SW Grant, Portland OR 75646
Address
800-323-1234 Phone
Denta Group Group Name
111-654A Policy Name

In case of an emergency

Name		Phone
Ralph Gaylor		503-555-6484
J. Write		503-555-6485
Dr. Doris Smith		503-555-6487
J. Write	533 SW Grant, Portland OR 75646	503-555-6489

Registered To: Unregistered

For Help, press F1

	Medical Record	Credit Card
Black Market Value per record	~$5	~$.50
Demographics	Yes	Maybe
Payment Information	Yes	Yes
Lifetime of Information	Forever	Short
Risk to Consumer	High	Low
Privacy Concerns	High	Moderate

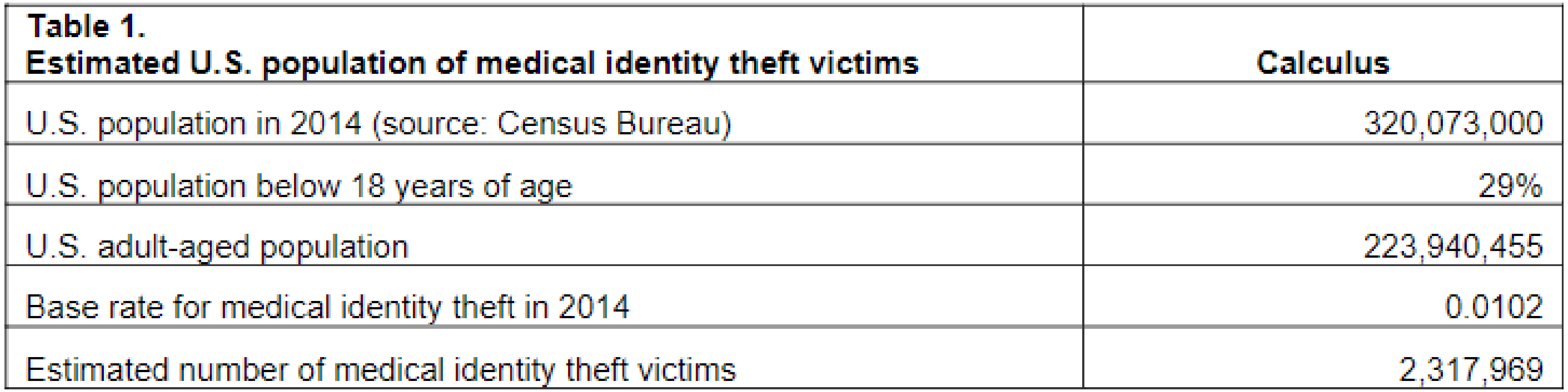
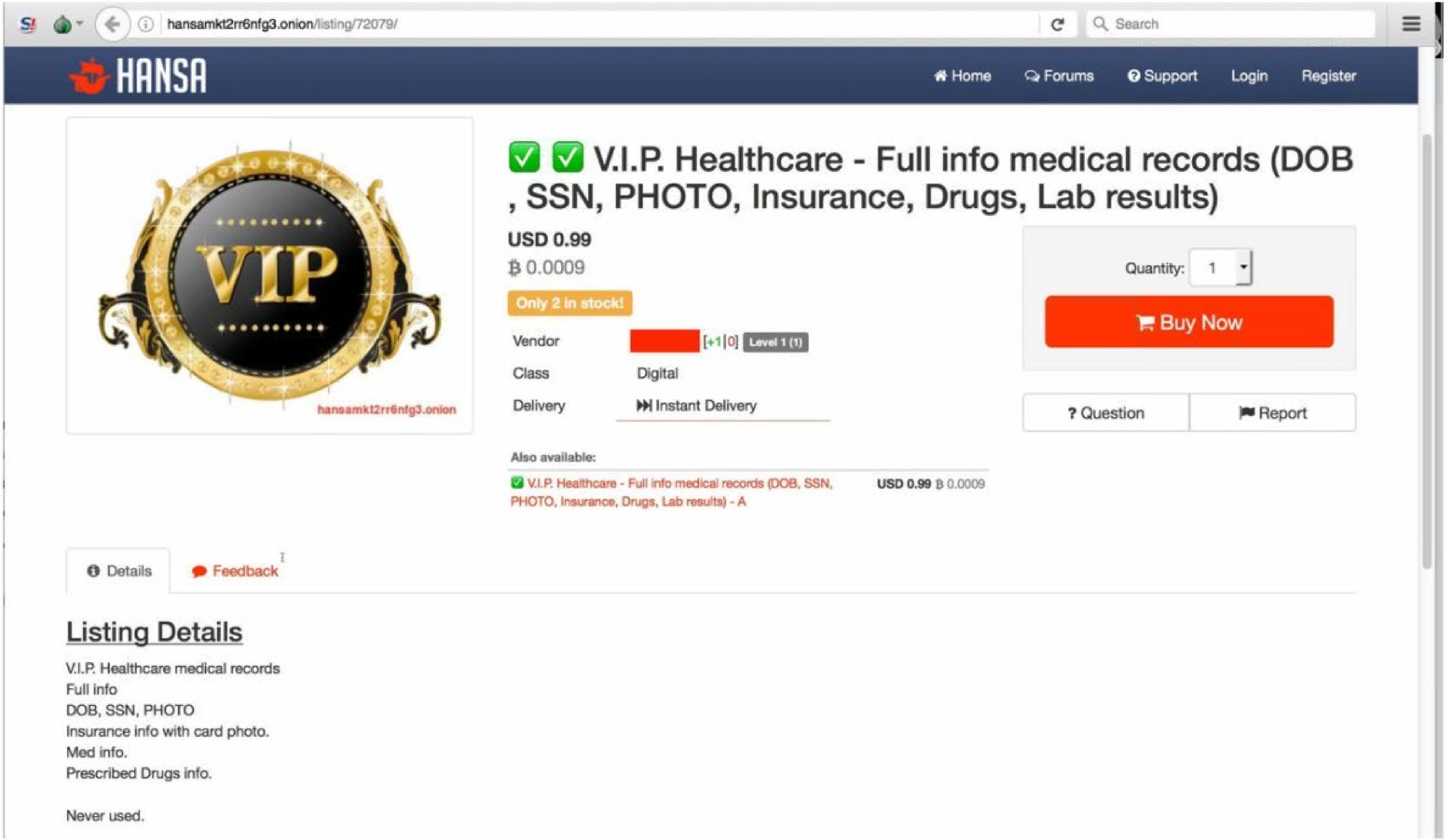


Table 1. **Estimated U.S. population of medical identity theft victims**	**Calculus**
U.S. population in 2014 (source: Census Bureau)	320,073,000
U.S. population below 18 years of age	29%
U.S. adult-aged population	223,940,455
Base rate for medical identity theft in 2014	0.0102
Estimated number of medical identity theft victims	2,317,969



✅ ✅ V.I.P. Healthcare - Full info medical records (DOB , SSN, PHOTO, Insurance, Drugs, Lab results)

USD 0.99

฿ 0.0009

Only 2 in stock!

Vendor	[redacted] [+1|0] Level 1 (1)
Class	Digital
Delivery	⏭ Instant Delivery

Also available:

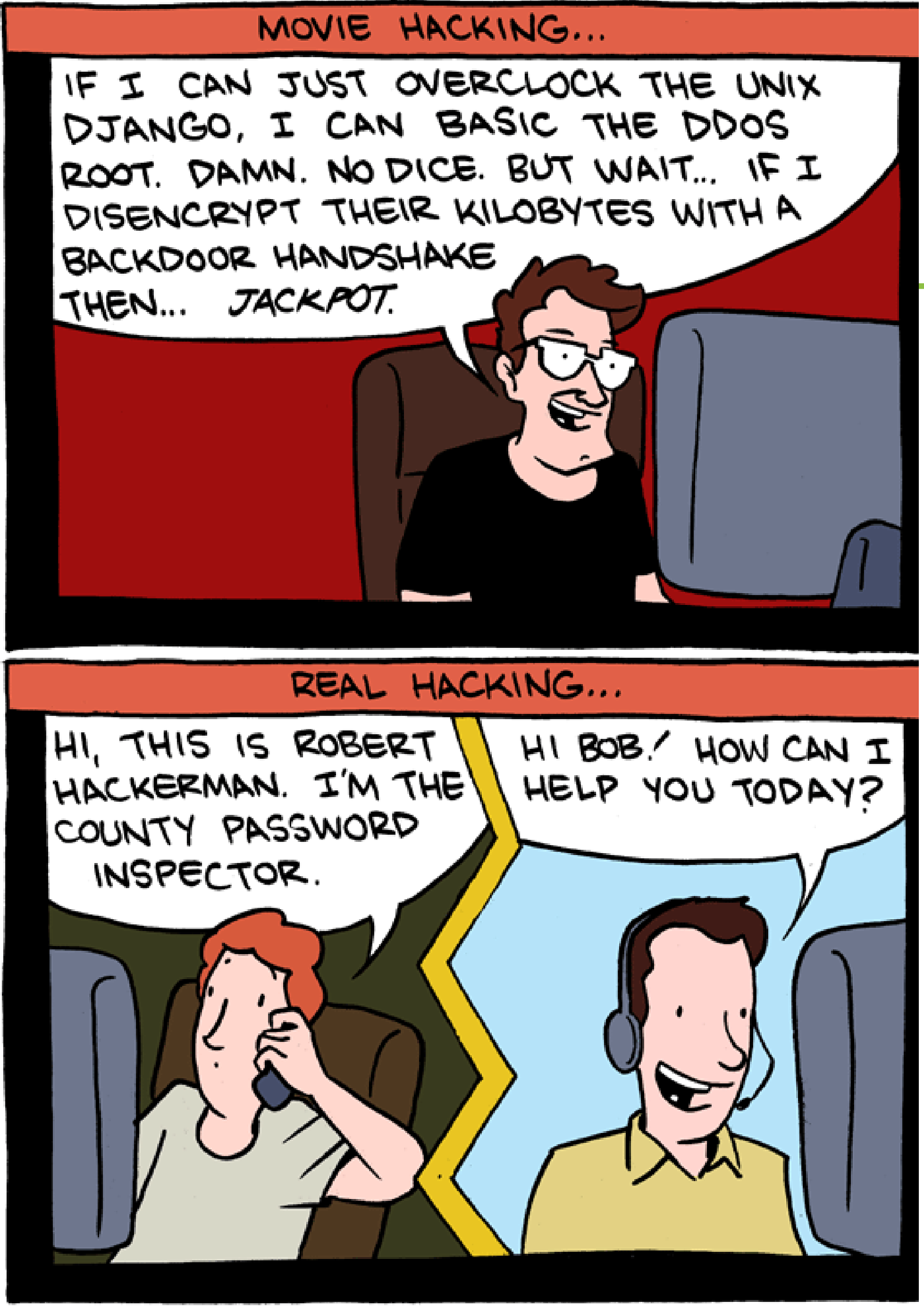
✅ V.I.P. Healthcare - Full info medical records (DOB, SSN, PHOTO, Insurance, Drugs, Lab results) - A	USD 0.99 ฿ 0.0009

Details Feedback

Listing Details

V.I.P. Healthcare medical records
Full info
DOB, SSN, PHOTO
Insurance info with card photo.
Med info.
Prescribed Drugs info.

Never used.


MOVIE HACKING...
IF I CAN JUST OVERCLOCK THE UNIX DJANGO, I CAN BASIC THE DDOS ROOT. DAMN. NO DICE. BUT WAIT... IF I DISENCRYPT THEIR KILOBYTES WITH A BACKDOOR HANDSHAKE THEN... JACKPOT.
REAL HACKING...
HI, THIS IS ROBERT HACKERMAN. I'M THE COUNTY PASSWORD INSPECTOR.
HI BOB! HOW CAN I HELP YOU TODAY?

Entry Points

- Phishing
- Ransomware
- Connected Medical Devices (IoT)
- Social Engineering
- Misconfigured Servers
- Inadvertent Disclosures
- Unpatched Systems
- Vendors and Business Associates
- Facilities and other supporting systems

Preach SRA Love!

- Make everyone in your health center a part of conducting an SRA
- By conducting an SRA regularly, providers can identify, and document potential threats and vulnerabilities related to data security and develop a plan of action to mitigate them.
- An SRA is the first step of a continuous, comprehensive Risk Management Program that will benefit your patients and your practice
- You cannot protect what you are unaware of!

Breach Protection and OCR Implications

Breach Protection High Level Strategy

- Build a culture motivated and dedicated to securing patient data
- Hire external consultants to help you build a strategy and test that strategy frequently
- Clarify related policies and determine gaps
- Gamify – Find ways to make sure your organization doesn’t fall asleep at the wheel

General OCR HIPAA Settlements

Primary Issues:

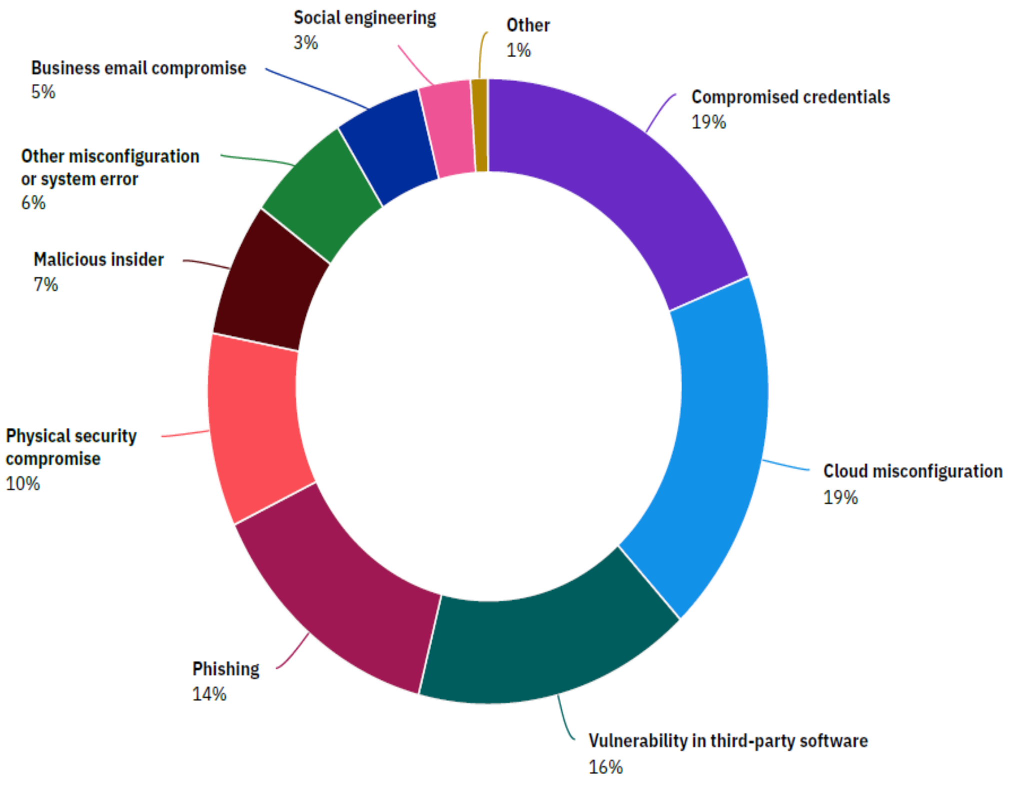
- Lack of risk analysis/risk management
- Large breaches (e.g., 300,000 or more)
- Improper disposal
- Unencrypted mobile devices
- Widespread snooping

Triggers:

- Media attention
- Breach report
- DOJ/OIG referral
- Consumer/Business Associate Complaints

Reference: http://www.dwt.com/people/adamhgreene/

Primary Breach Factors



1. Compromised Credentials
2. Cloud misconfiguration
3. 3rd-party software vulnerabilities
4. Phising attacks
5. Physical security compromise

The Baseline: Encryption

- Provides safe harbor for HITECH breach notification
- Addressable standard in HIPAA Security Rule however many consider it a defacto standard because with today's technology, it's hard to say that encryption would not be reasonable or appropriate.
- Lessens breach impact

Breach Management Tools

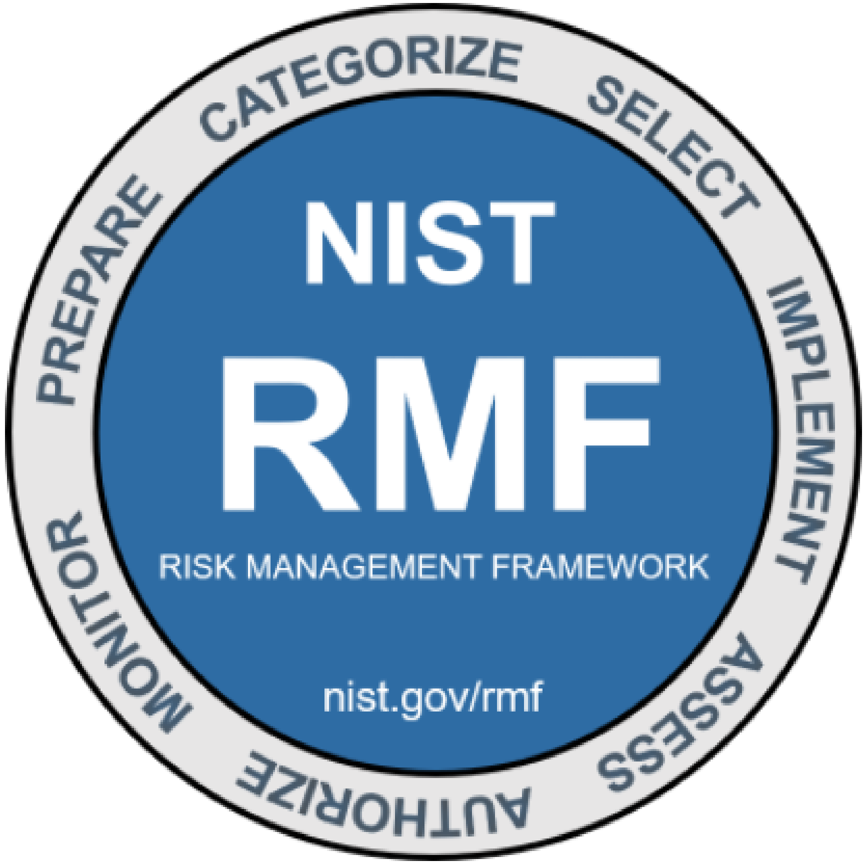
- **Technical Measures**
  - Security Information and Event Management (SIEM) Services
    - provide real-time analysis of security alerts generated by network hardware and applications
    - used to log security data and generate reports for compliance purposes
  - Intrusion Prevention/Detection Systems
  - Vulnerability Scanners
  - Next Generation Firewalls
- **Organizational Measures** - Attack Practice
  - Phishing/Whaling Attacks
  - Domain Spoofing
  - USB Drive Protection

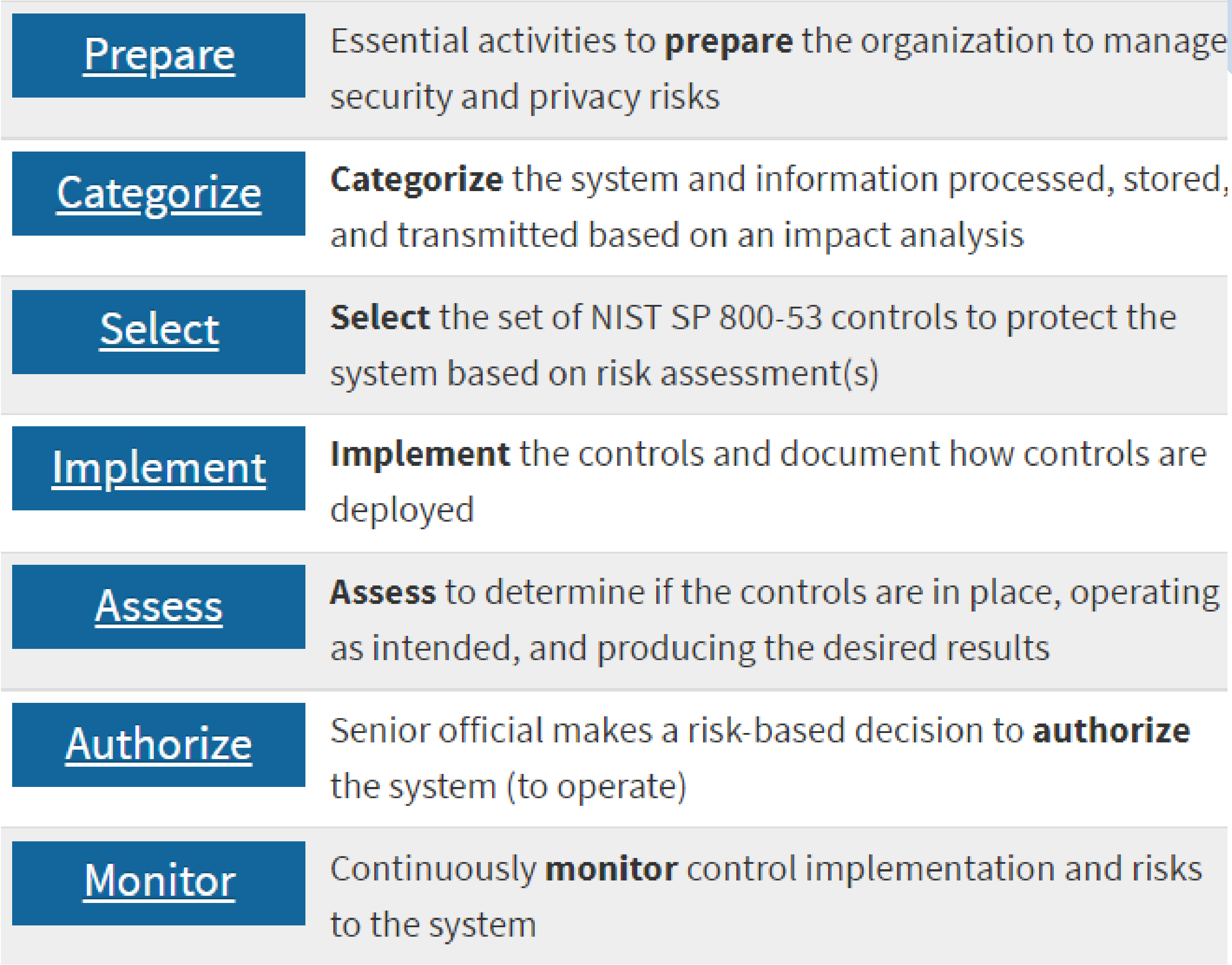
Strengthening Risk Management, Breach Defense, Mitigation, and Response Plans

Risk Management Frameworks

In general, there are four steps to the cybersecurity risk management process:

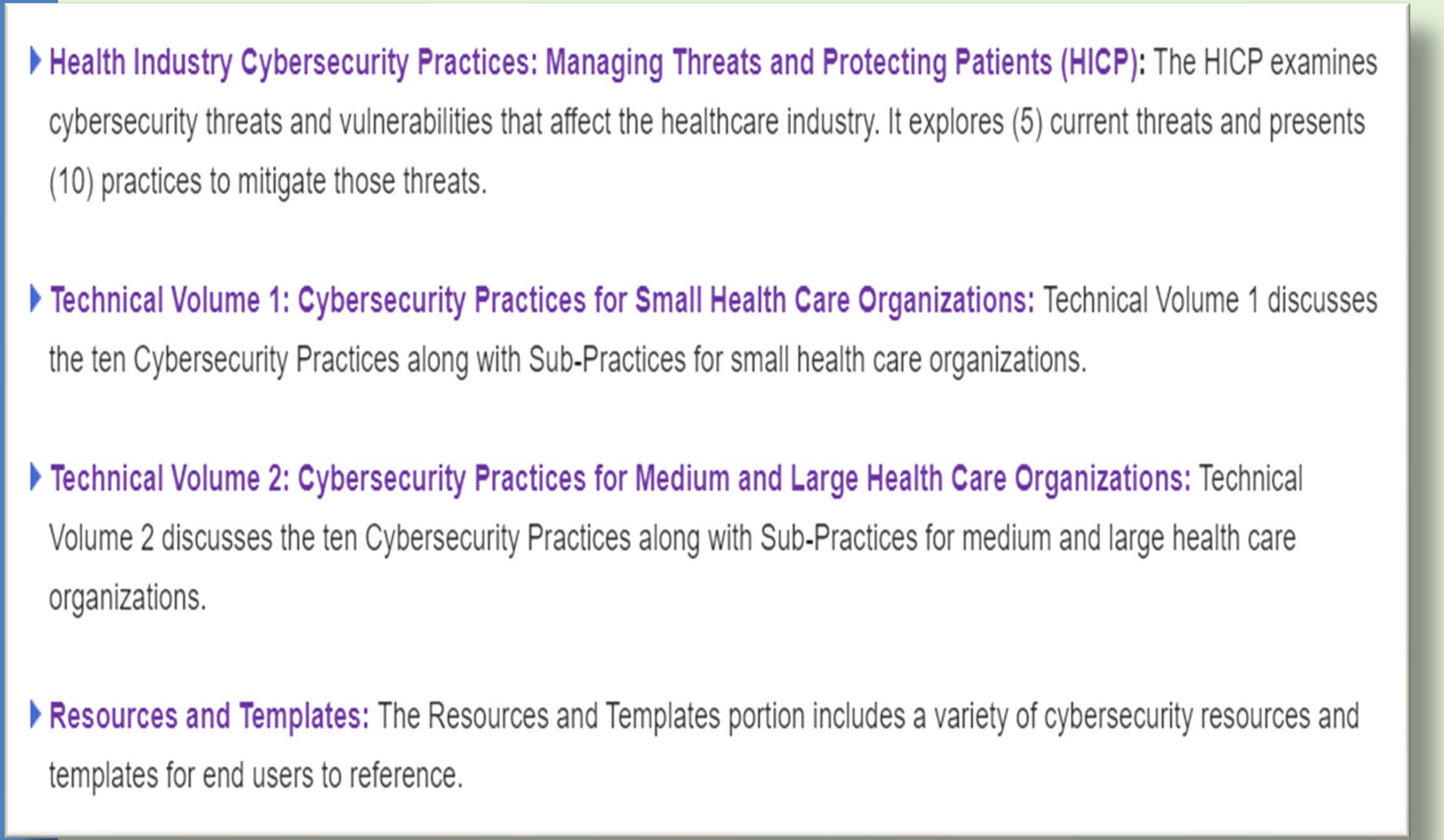
1. **Identify Risk** - entails assessing the organization's surroundings in order to detect present or potential threats to its operations.
2. **Assess Risk** - examining identified risks to determine how probable they are to have an impact on the company, as well as the magnitude of that impact.
3. **Control Risk** - Define strategies, processes, technology, or other steps that can assist the company in mitigating risks.
4. **Review Controls** – security controls are reviewed on a regular basis to see how effective they are at mitigating risks, and controls are added or adjusted as appropriate.





Prepare	Essential activities to **prepare** the organization to manage security and privacy risks
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis
Select	**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	**Implement** the controls and document how controls are deployed
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)
Monitor	Continuously **monitor** control implementation and risks to the system

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

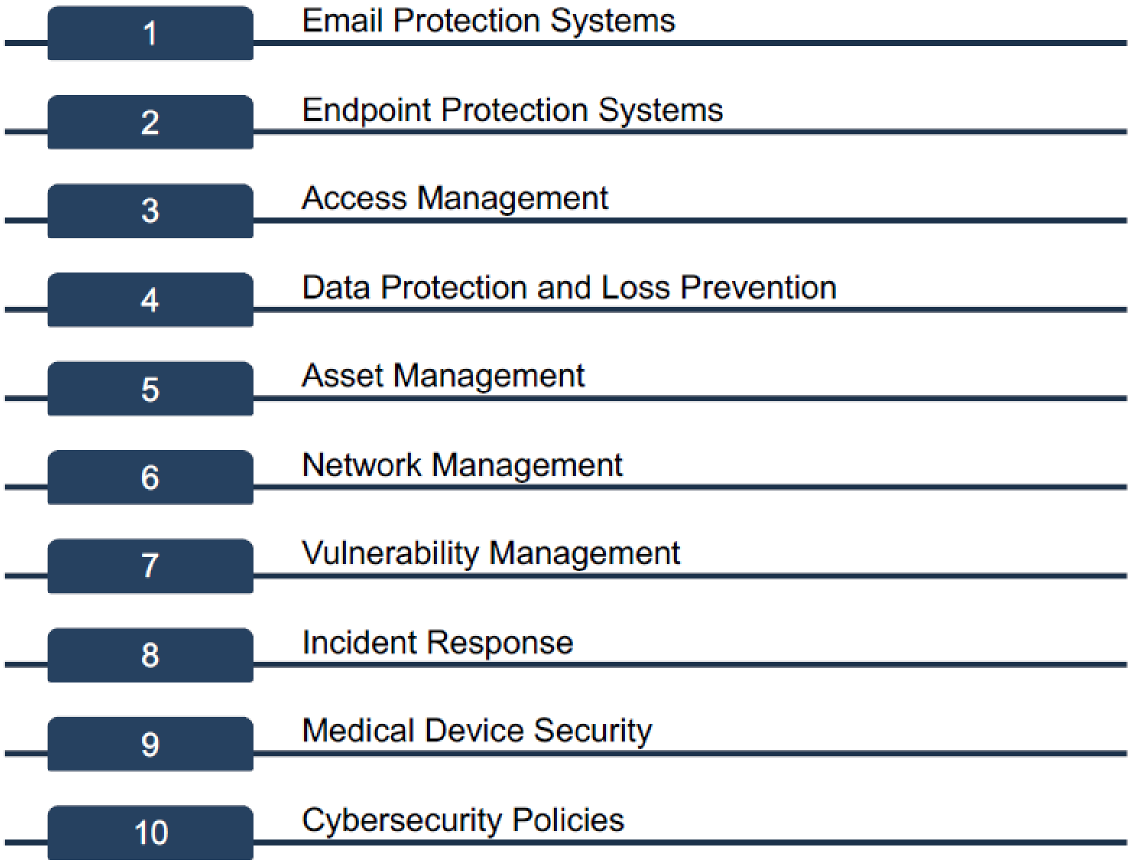


- **Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP):** The HICP examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores (5) current threats and presents (10) practices to mitigate those threats.
- **Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations:** Technical Volume 1 discusses the ten Cybersecurity Practices along with Sub-Practices for small health care organizations.
- **Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations:** Technical Volume 2 discusses the ten Cybersecurity Practices along with Sub-Practices for medium and large health care organizations.
- **Resources and Templates:** The Resources and Templates portion includes a variety of cybersecurity resources and templates for end users to reference.

https://405d.hhs.gov

405(d) HICP Publication – Ten Practices

- HICP identifies ten (10) practices, which are tailored to small, medium, and large organizations
- Budget, investment, grant funding decisions should consider cybersecurity risk, its impact on enterprise-wide risks and most importantly its impact to patient safety and uninterrupted care delivery.



1 Email Protection Systems

2 Endpoint Protection Systems

3 Access Management

4 Data Protection and Loss Prevention

5 Asset Management

6 Network Management

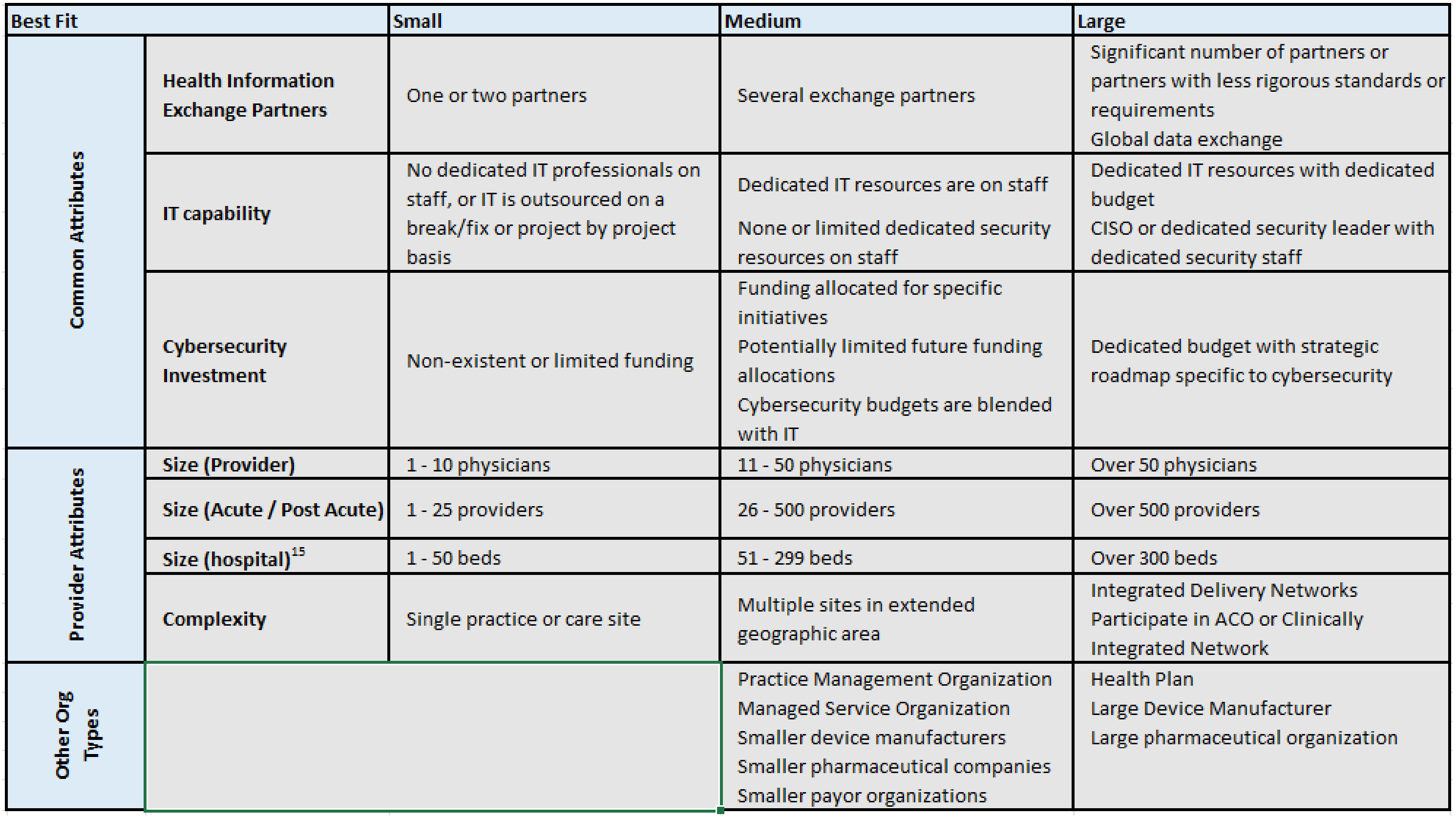
7 Vulnerability Management

8 Incident Response

9 Medical Device Security

10 Cybersecurity Policies

HICP Cybersecurity Self-Assessment Tool



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, or IT is outsourced on a break/fix or project by project basis	Dedicated IT resources are on staff None or limited dedicated security resources on staff	Dedicated IT resources with dedicated budget CISO or dedicated security leader with dedicated security staff
	Cybersecurity Investment	Non-existent or limited funding	Funding allocated for specific initiatives Potentially limited future funding allocations Cybersecurity budgets are blended with IT	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 ACO or Clinically Integrated Network
Other Org Types			Practice Management Organization Managed Service Organization Smaller device manufacturers Smaller pharmaceutical companies Smaller payor organizations	Health Plan Large Device Manufacturer Large pharmaceutical organization

This toolkit is designed to be a supplement to the main document of the Healthcare Industry Cybersecurity Practices (HICP) guide.

Specifically, Appendix E of the Main Document outlines an assessment methodology.

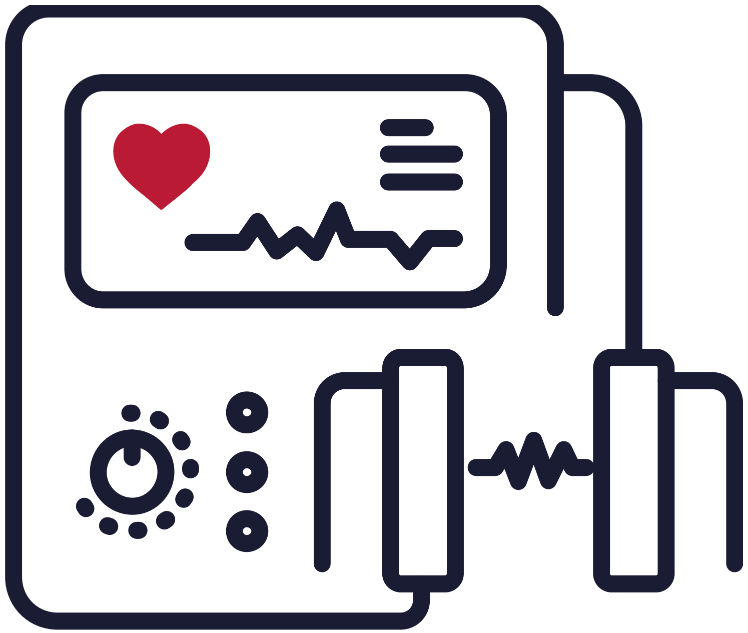
After you have identified the size of your organization, review the threats and determine the level of concern your organization faces.

Protect Your Assets

- Implement a hardware asset management system or Mobile Device Management (MDM) system
- As users have moved to remote work, ensure asset management is capable of identifying and managing remote devices
- Protect
  - **Configuration** – Authentication (MFA, Biometrics), Encryption, Lockdown, restrict Admin access
  - **Patch Management**
  - **Endpoint Protection**
- Offsite/Cloud Backup

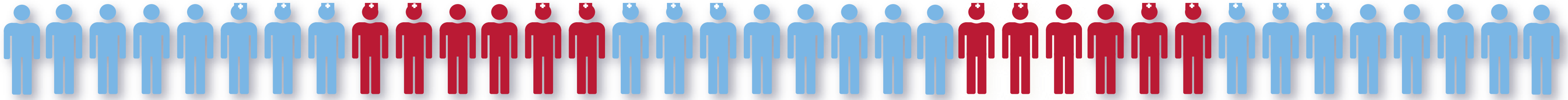
Protect Your Medical Devices

- **Asset Management** – Procurement, Contracting, Asset Inventory, Destruction Procedures
- **Technical Controls** – Patching, Network Isolation, Monitoring



Organizational Security

- **Assessment** – Conduct a Security Risk Assessment, Assess new technologies such as telehealth, remote access, or remote patient monitoring
- **Risk Management** – Can help determine which security investments will provide the most value
- Conduct an Incident Response or Disaster Recovery Exercise
- Enhance Identity and Access Management Procedures



Safeguard your EHR

- **Assessment –** Conduct as assessment of security configuration of your EHR. Consider:
  - Authentication (MFA for remote access?)
  - Encryption
  - Logging/Monitoring
  - User Access Controls
- **User Access Review**
- **System Activity Review –** Implement systems to report on or alert on suspicious activity. It's required by the HIPAA Security Rule!

Strengthen Your Infrastructure

- **Implement technology:**
  - Segment your network
  - Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS)
  - Aggregate Logs into a SIEM
  - Contract with a 3rd party to monitor logs

- **Vulnerability Assessment & Penetration Testing**

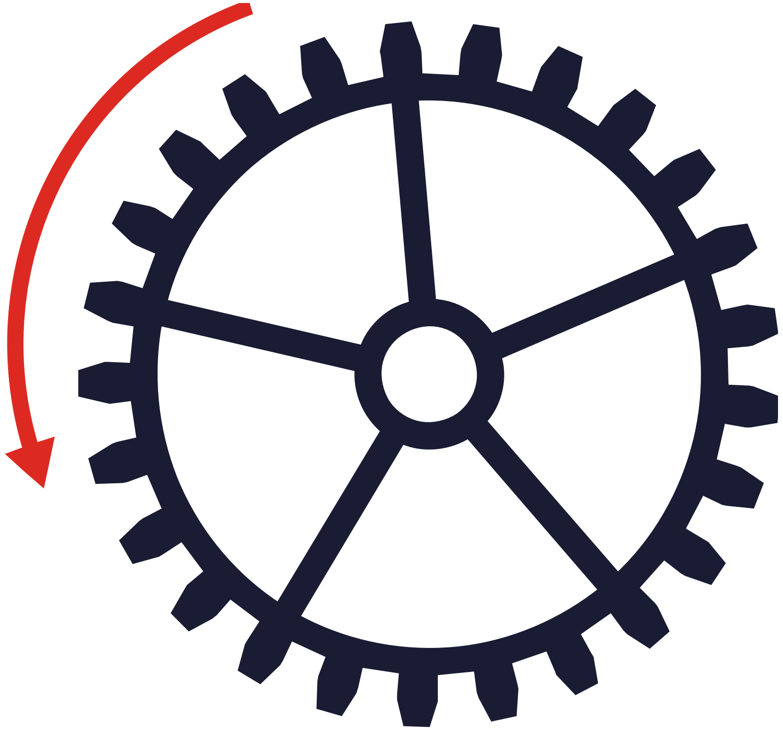
- **Enhance Physical Security** – badge access, security cameras, fire suppression, redundant power

In the Cloud

- **Security Configuration:**
  - Consider security configuration of cloud email and storage systems
  - Access Controls
  - Document Sharing
  - Logging
  - DLP
  - Email encryption

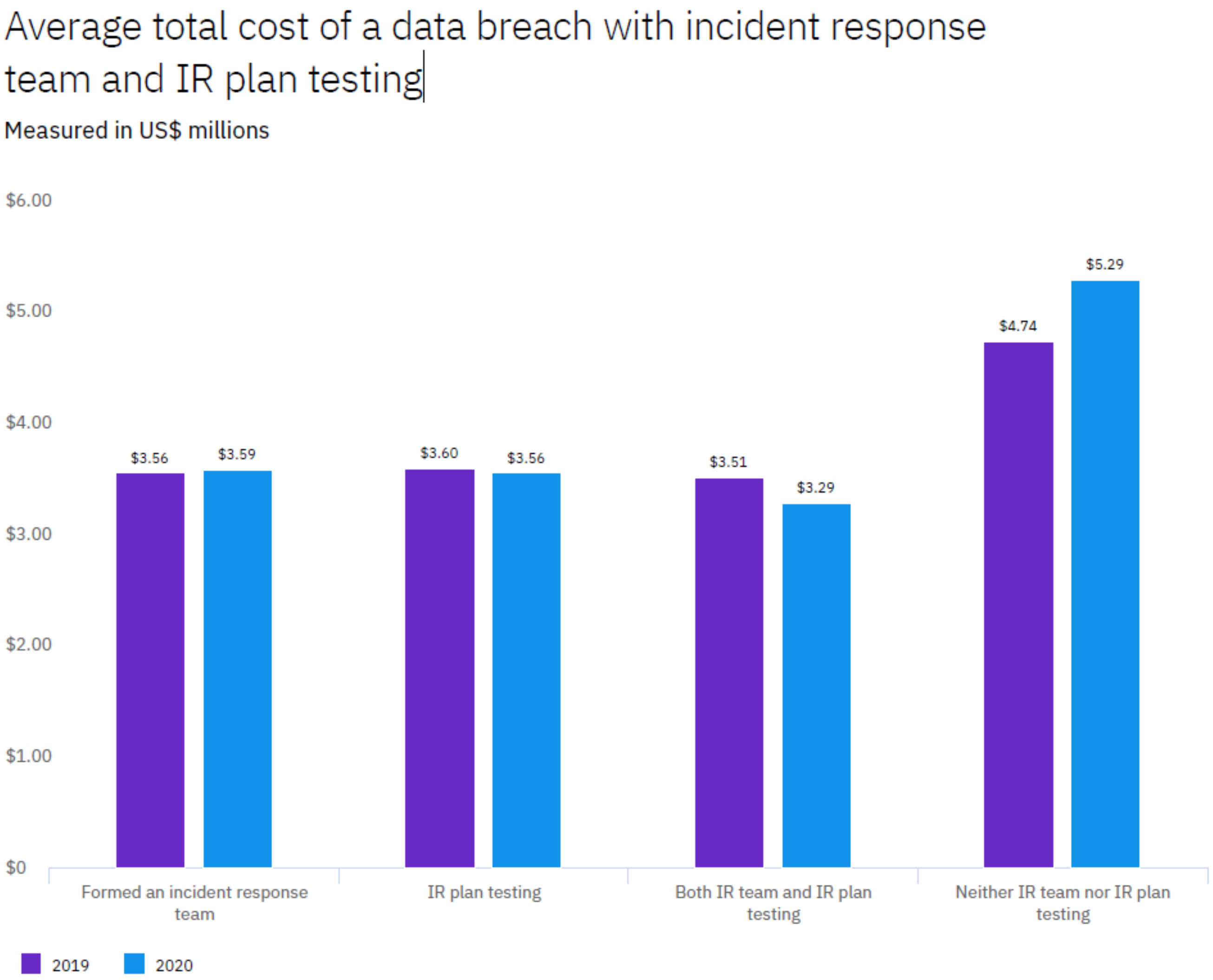
Monitor Your Assets

- Implement a Security Incident & Event Monitoring (SIEM) system
- Contract with a 3rd party to monitor your SIEM



Operationalizing Cybersecurity

The Cost of Not Being Prepared



Average total cost of a data breach with incident response team and IR plan testing

Measured in US$ millions

Cybersecurity Rugged DevOps

Defensible infrastructure: Better configuration and security controls in place, with more consistency overall.

Operational discipline: Changes and code pushes managed collaboratively and with heightened awareness and interaction.

Situational awareness: All changes and systems monitored proactively to determine any adverse impacts or potential attack surface created.

Countermeasures: Quick response, with proper preventive controls enabled and sound communication strategy maintained.

Incident Response Readiness Table Top Exercise Activity

HIPAA – Security Incident Response

Security Incident Procedures - §164.308(a)(6)

"Implement policies and procedures to address security incidents."

RESPONSE AND REPORTING (R) - §164.308(a)(6)(ii)

"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."

Security Incident Response Plan

NIST SP 800-53 (IR-8) Incident Response Plan:

1. Provides the organization with a roadmap for implementing its incident response capability;

2. Describes the structure and organization of the incident response capability;

3. Provides a high-level approach for how the incident response capability fits into the overall organization;

4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

5. Defines reportable incidents;

6. Provides metrics for measuring the incident response capability within the organization;

7. Defines the resources and management support needed to effectively maintain and mature an incident response capability

Readiness Questions

Questions to ask yourself:

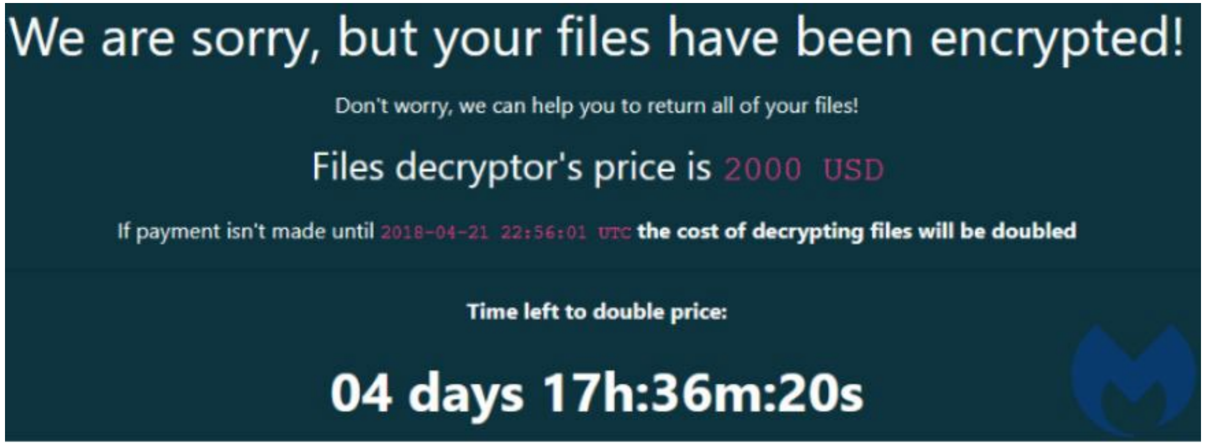
- How are we documenting security incidents?
- What is our communications plan? Internal/External?
- Who are the decision makers? For example, who has ultimate authority to shut down critical systems such as EMR in order to prevent further infection of malware?
- Do all employees know how to recognize a security incident, know their obligation to report, and know how to report?

Exercise Overview

- For those of you unfamiliar with the term, a Table Top Exercise is a small but inclusive exercise that occurs as part of Information Security's attempt to be better prepared to respond to potential cyber related incidents.

- The Table Top Exercise serves to exercise preparedness, validate plans, test operational capabilities, maintain leadership effectiveness, and examine the ways the organization works with the larger community outside of the company to prevent, protect from, respond to, recover from, and mitigate cyber related incidents.

Incident Response Scenario – Ransomware Attack



We are sorry, but your files have been encrypted!

Don't worry, we can help you to return all of your files!

Files decryptor's price is 2000 USD

If payment isn't made until 2018-04-21 22:56:01 UTC **the cost of decrypting files will be doubled**

Time left to double price:

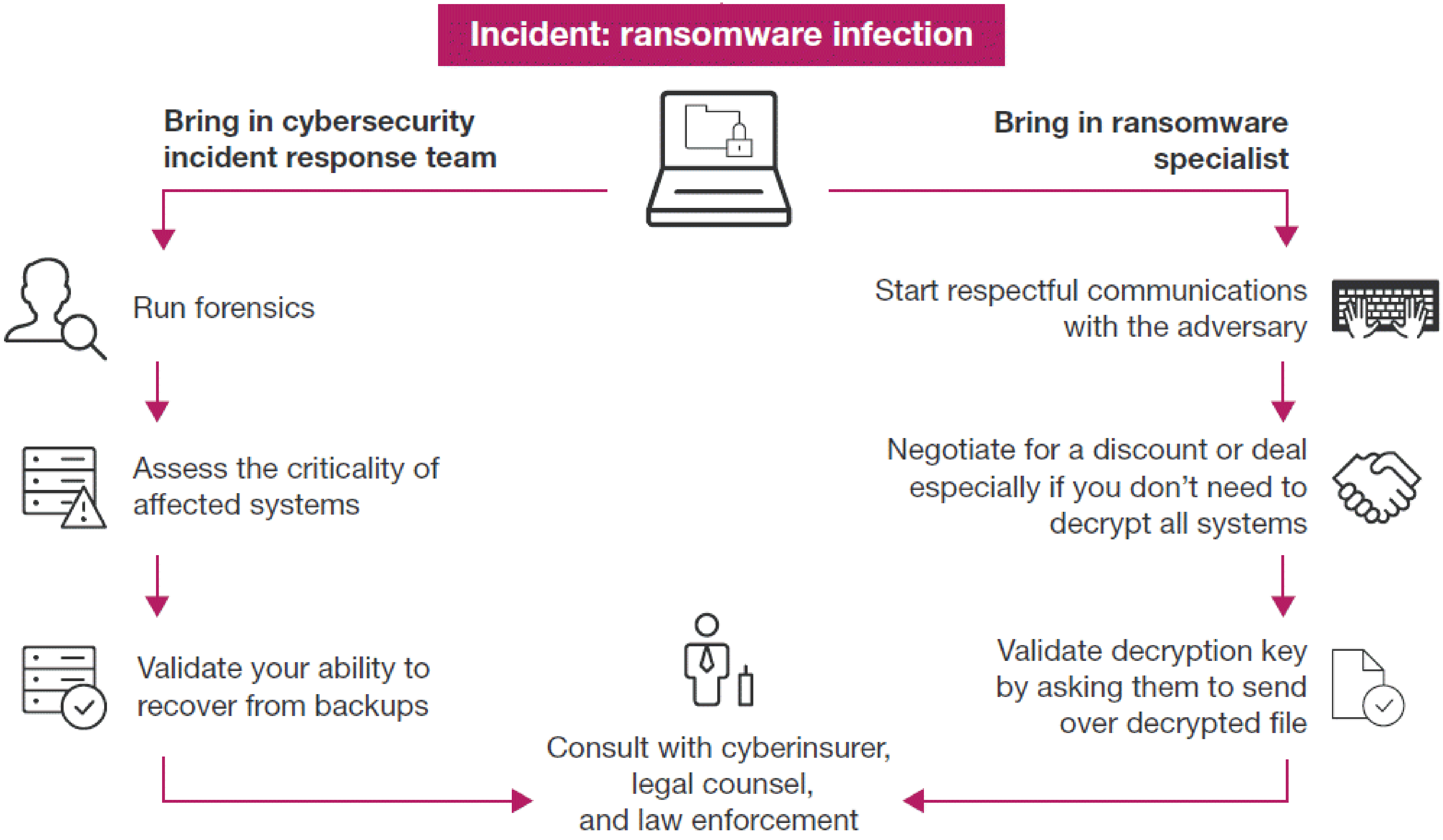
04 days 17h:36m:20s

- A phishing email was sent to numerous members of the medical practice
- One person clicked on the link and entered their credentials into the attacker's fake website
- Shortly after, the victim's computer displayed a ransom message
- The user reported the incident to the IT helpdesk

Potential Questions to Ask

- If you are the one who receives the ransomware notification what is the first thing you should do?
- How are you going to document the steps that are taken?
- Do you have a crisis management team that should be activated? If yes, who would initiate the activation?
- When should Senior Leadership be notified?
- When do you contact law enforcement? Who?
- What would your strategy be if it looks like you will only lose one day's worth of data?
- Assume a recent backup is not recoverable. The 6-week backup appears to not be impacted but it may take 1½ weeks to recover the data. Is using a 6-week backup a viable option to pursue?
- What would be the strategy to continue business for 1½ weeks?
- What actions should non-IT areas consider? How will these actions be coordinated with other key partners?

Debrief: Ransomware Response Report



Incident: ransomware infection

Bring in cybersecurity incident response team

Run forensics

Assess the criticality of affected systems

Validate your ability to recover from backups

Bring in ransomware specialist

Start respectful communications with the adversary

Negotiate for a discount or deal especially if you don’t need to decrypt all systems

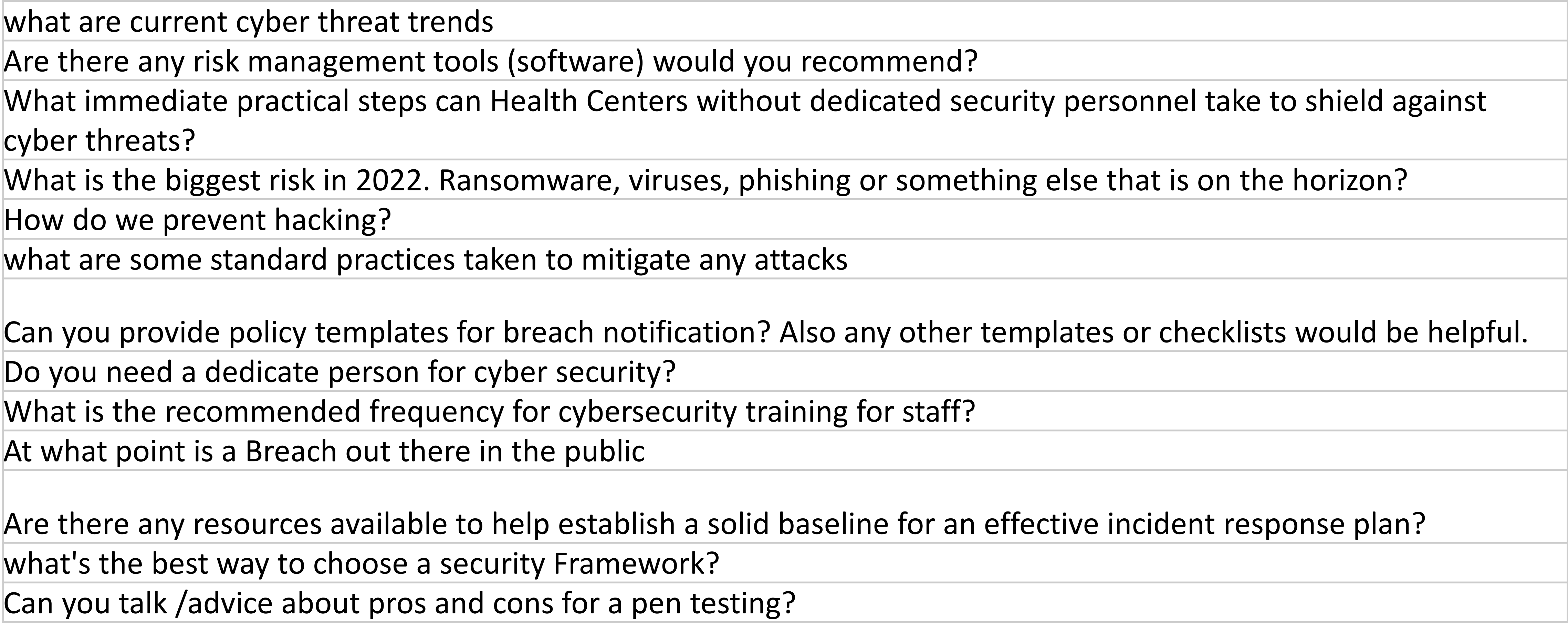
Validate decryption key by asking them to send over decrypted file

Consult with cyberinsurer, legal counsel, and law enforcement

Post Incident Response Due Diligence

- Exactly what happened and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What new or different resources do we now need in order to improve the emergency planning/response process?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- In what ways can the organization prepare external audiences for a situation like this, in an effort to minimize the amount of damages or losses?

Questions Asked at Registration



what are current cyber threat trends
Are there any risk management tools (software) would you recommend?
What immediate practical steps can Health Centers without dedicated security personnel take to shield against cyber threats?
What is the biggest risk in 2022. Ransomware, viruses, phishing or something else that is on the horizon?
How do we prevent hacking?
what are some standard practices taken to mitigate any attacks
Can you provide policy templates for breach notification? Also any other templates or checklists would be helpful.
Do you need a dedicate person for cyber security?
What is the recommended frequency for cybersecurity training for staff?
At what point is a Breach out there in the public
Are there any resources available to help establish a solid baseline for an effective incident response plan?
what's the best way to choose a security Framework?
Can you talk /advice about pros and cons for a pen testing?

Questions Asked at Registration

- What are current cyber threat trends and risks in 2022?
- Are there any risk management tools (software) would you recommend?
- Do you need a dedicated person for cyber security?
- What practical steps can Health Centers without dedicated security personnel take?
- What are some standard practices taken to mitigate any attacks
- Can you provide policy templates for breach notification?
- What is the recommended frequency for cybersecurity training for staff?
- Are there any baseline resources available to establish an incident response plan?
- What's the best way to choose a security Framework?
- Can you talk /advise about pros and cons for a pen testing?

Incident Response Wrap-up

Increased threats are creating a higher number of attacks making incident response capabilities a requirement of organizational information security programs.

Prepare (Pre-Incident)

- Plan ahead for the incident events

Respond (Active Incident Response)

- Determine what you are fighting
- How to stop it from spreading
- How to get rid of it
- Coordinated response requires following established processes

Report (Post-Incident)

- Remediate the root cause to minimize future issues
- Learn from every opportunity and update your plan for future improvement

Conclusion

- Health Center Privacy and Security is everyone's responsibility
- Security Risk Analysis is your #1 tool for protecting your health information systems from breach
- There are known best practices and frameworks that can be followed to help ensure information security is addressed appropriately
- Effective incident response is about planning and practice
- Help defend your Health Centers against the Dark Web!

Get Your Badge!

1. Visit: http://bit.ly/hiteq-defender
2. Read through the suggested resources:
   - Ransomware Guidance Presentation for Health Centers
   - Creating and Managing Strong Passwords at Your Health Center
   - The Health Center CIO's Guide to HIPAA Compliant Text Messaging
   - Health IT Privacy & Security Skill Sets
   - Breach Protection Overview Presentation for Health Centers
3. Fill out the Health Center Defender Against the Dark Web Badge Confirmation form
4. Receive your badge!

Comments, Questions, and Discussion

Questions? Feedback?

Email: hiteqinfo@jsi.com

Phone: 1-844-305-7440

This project is supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as part of an award totaling $778,000 with 0 percentage financed with non-governmental sources. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by HRSA, HHS, or the U.S. Government. For more information, please visit HRSA.gov.