Cybersecurity: Awareness and Preparedness

Alison Pingelski, New York State Department of Health

March 14, 2019

Discussion Topics

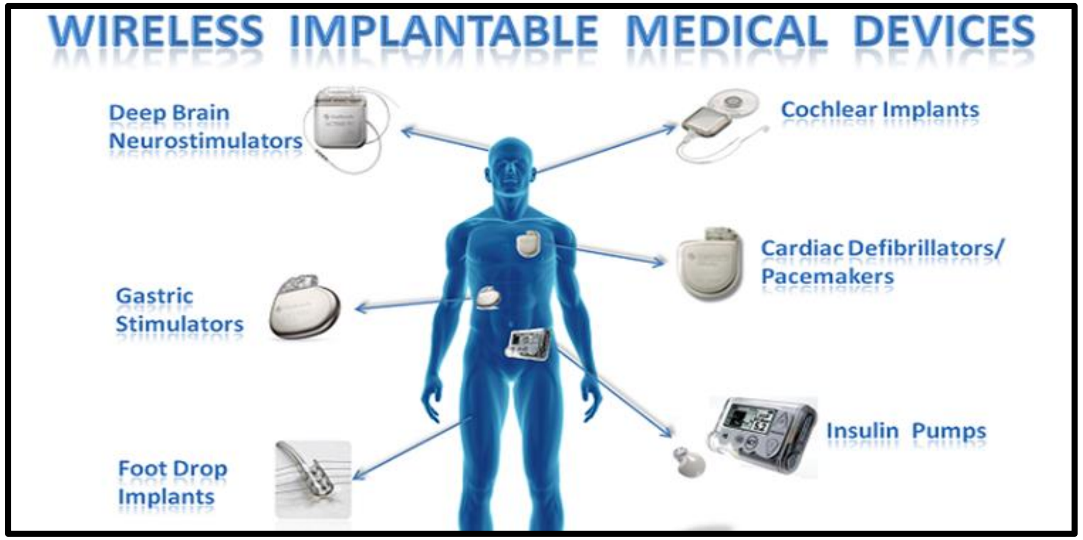
- Describe vulnerabilities
- Identify methods to increase protection from cyberattacks
- Review methods for reporting and responding to a cybersecurity incident

Vulnerabilities

What's in the Cloud?

Uncountable number of personal devices; ever increasing volume of connected medical devices; automated medication systems.

E.g., EHR data, Implanted medical devices;



Hackers recognize the “value” of the sector as a target that needs quick resolution to avoid potentially severe health impacts

- Recent U.S. government interagency report indicated average 4,000 daily ransomware attacks on the sector since early 2016;
- 300% increase of ransomware attacks over 2015 - more than any critical infrastructure sector).
  - Identified 23 different patient safety risks, 55% related to loss of PHI
- According to TrendMicro, health care was the sector that was hit the hardest by data breaches from 2010 through 2015. Two-thirds were due to the loss or theft of things like laptops, smartphones or thumb drives.

  https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/why-hackers-are-going-after-health-care-providers/?noredirect=on&utm_term=.4f1987c5e5ef

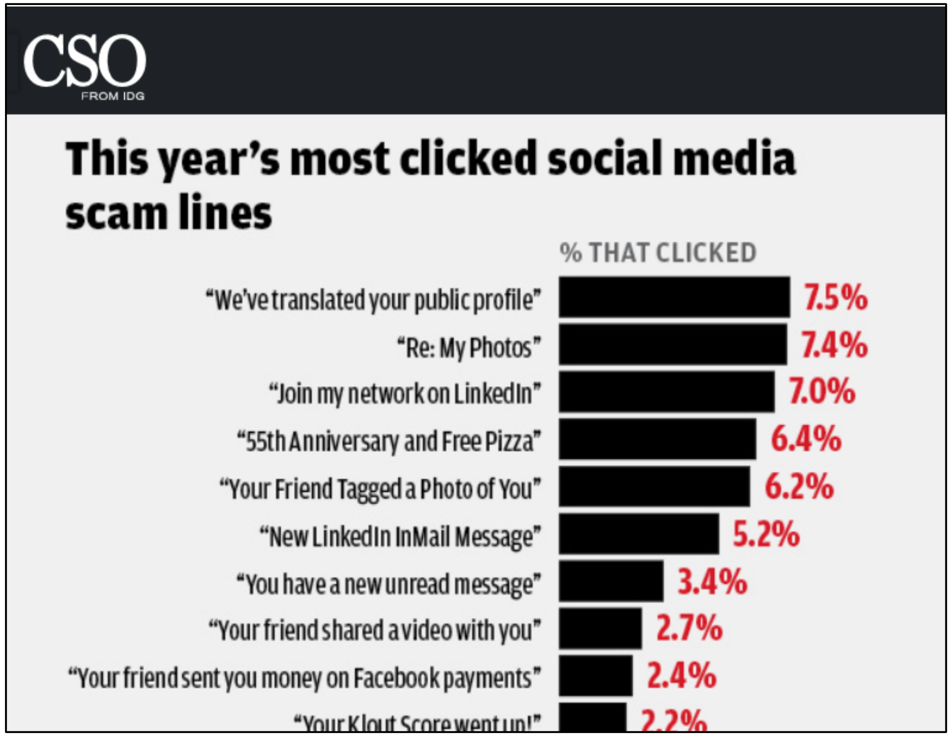
Hackers exploit fairly common vulnerabilities in the healthcare sector:

- Legacy equipment, technology, software – outdated/no longer supported operating systems; no security patches available;
  - one legacy system was found to have over 1400 vulnerabilities;
- Nature of the work: increased need for interconnectivity/internet connected devices
- Rapid roll out without proper secure design or testing
- Lack of workforce training on cyber and network security
- Exploit the human element in a dynamic healthcare environment with frequent staff changes

The Human Element

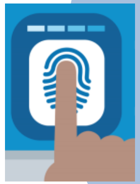
Many security breaches occur when users:

- Don’t follow policies; unaware of risks
- Don’t have strong passwords and multi-factor authentication
- Security roles are not modified or removed upon change in responsibility
- Fall victim to social engineering: visit questionable websites and download questionable software; open emails/attachments from unknown sources
- Leave workstations unlocked
- Use unencrypted devices that when lost could expose sensitive data
- Don’t have an established backup process



Increase Protection from Cyberattacks

Focusing on the Basics



Who?

- Has access to your systems and data
- How are you managing access?

What?

- External entities and data consumers are you supporting

Where?

- Are our systems located or hosted?

Public Cloud

Vendor Hosted

On-Premised Servers

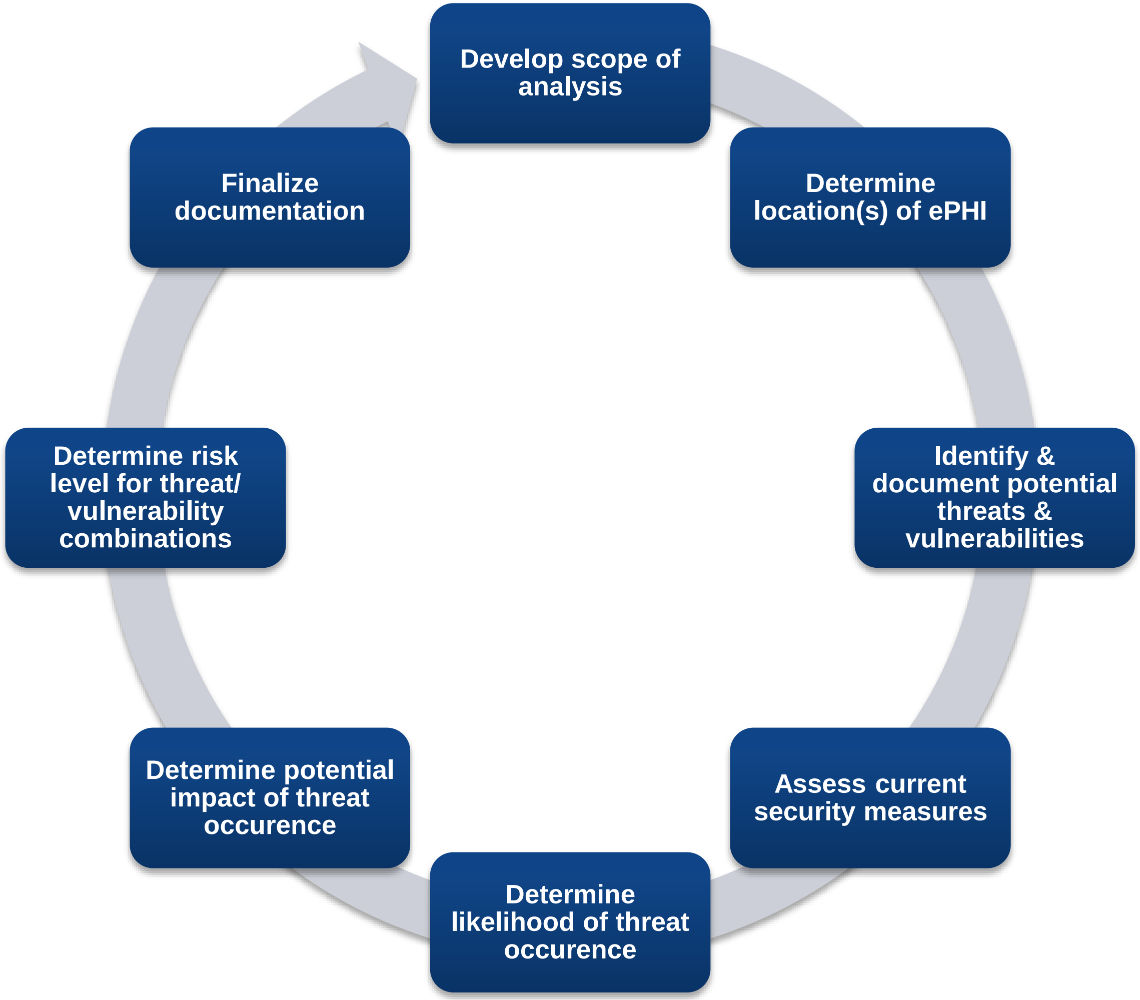
Conduct Risk Assessment

Covered entities have greater responsibilities to secure their systems, medical devices and patient data to mitigate this risk.

The Security Management Process standard of the HIPAA Security Rule (https://www.hhs.gov/hipaa/for-professionals/security/index.html) requires all covered entities and business associates to:

- conduct an accurate and thorough **risk analysis** of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of the ePHI the entities create, receive, maintain, or transmit.
- implement security measures sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level.

Guidance on Risk Analysis from HHS



HIPAA Provisions

- **Conduct Security Awareness Training** – security reminders, protection from malicious software, log-in monitoring, password management.
- **Develop Security Incident** policies and procedures to identify and respond to suspected or known security incidents and mitigate harmful effects to the extent practicable.
- **Implement Access** controls to ensure appropriate access to ePHI.
- **Encryption** is heavily recommended – but not mandated under HIPAA in all cases. Determine what is reasonable and appropriate.
- **Conduct Information System Activity Review** procedures and Audit controls to regularly review and record information system activity (e.g., audit logs, access reports, and security incident tracking reports).

Develop a Cybersecurity Strategy

- Develop a **cybersecurity strategy** that is well-constructed, deliberate, and consistent with best practices for an healthcare organization.
  - Sample https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf
- Conduct a table top exercise to simulate a Breach or Security Incident.
  - Focus on incident management and response
  - Evaluate decision-making readiness
  - Review response plans, line up trusted providers
  - Prepare your message(s) to the public and key stakeholders
  - Identify and involve your counsel.
- Determine if your organization outsources certain functions and identify involved stakeholders.
  - Focus on "high risk" data
  - Not limited to IT department

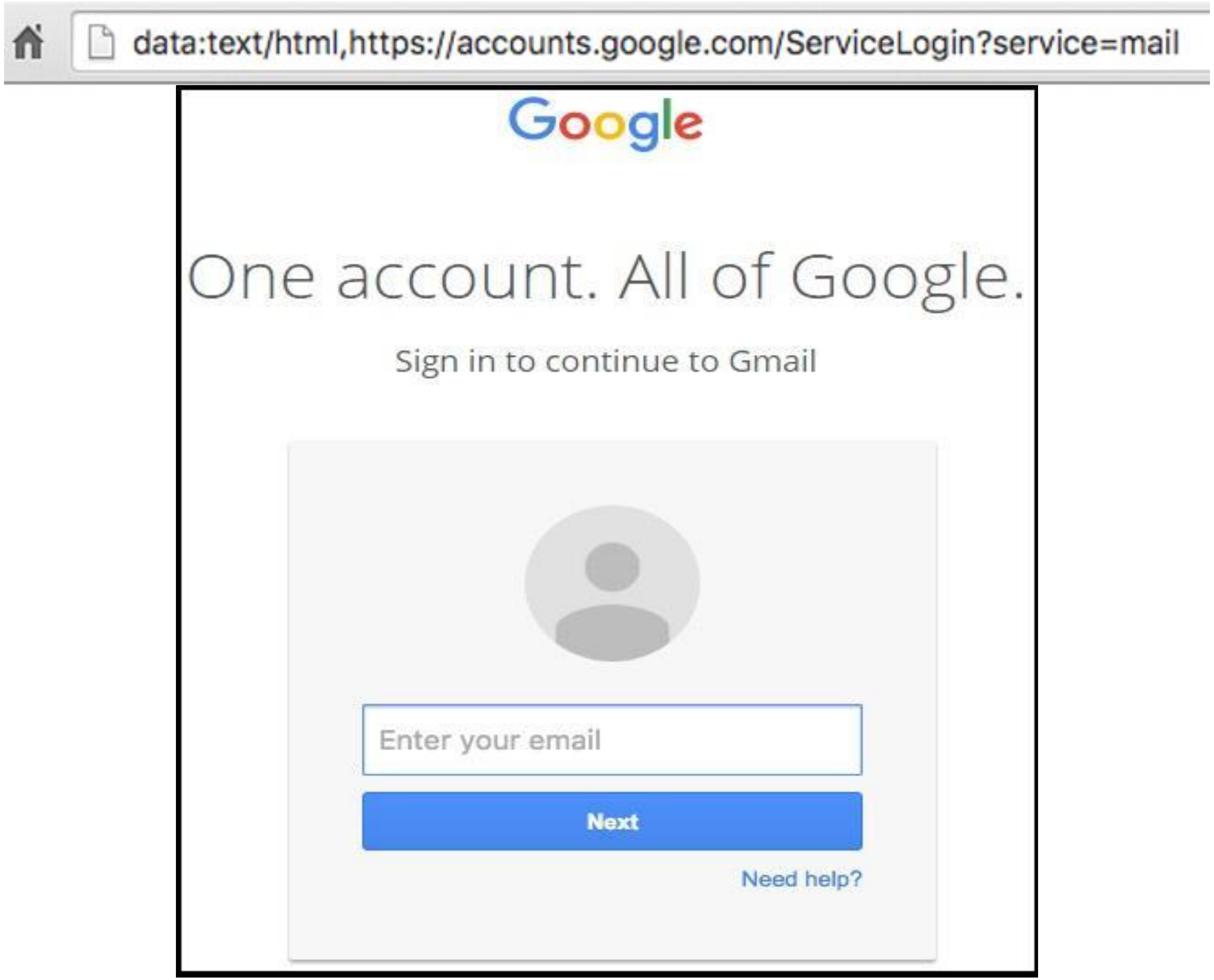
Phishing

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

http://www.phishing.org/what-is-phishing

Phishing Facts

- According to the SANS Institute, 95% of all attacks on enterprise networks are the result of successful spear phishing
- According to Wombat Security State of the Phish, 83% of businesses reported being a victim of a phishing attack in the last year as a result of successful spear phishing, up 7% from 2017
- According to the Verizon Data Breach Investigations Report, 30% of phishing messages get opened by targeted users and 12% of those users click on the malicious attachment or link

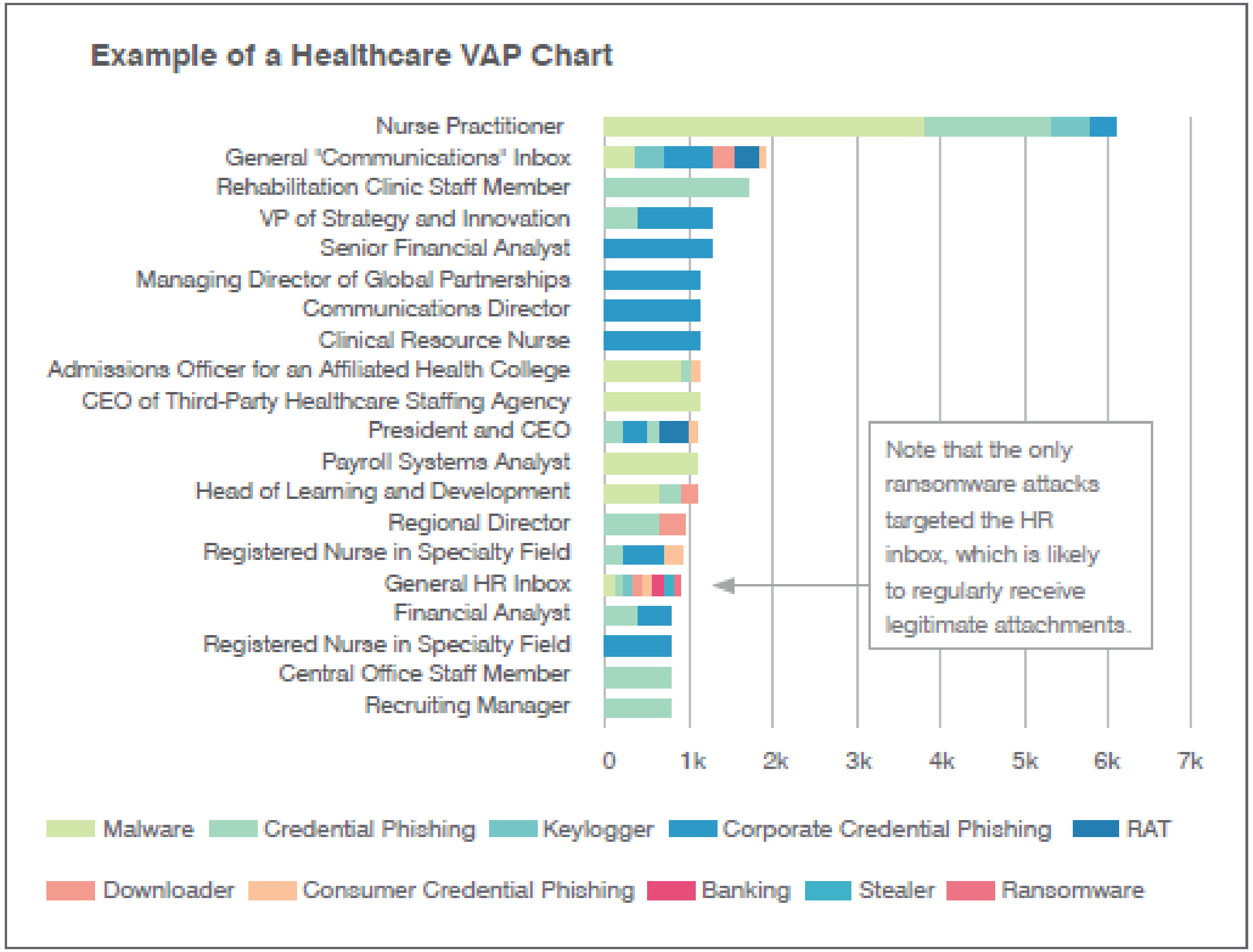


https://blog.dashlane.com/phishing-statistics

Implement Phishing Awareness & Prevention

- Educate users
  - Do you recognize the sender
  - Is the message from outside my organization
  - Is the email address suspicious
  - Is there a hyperlink (hover and look at the address) or attachment
    - Is there a consequence or reward for clicking link
  - Was the email sent outside of normal business hours
  - Does the subject line match the content in the body
  - Are there misspellings/typos or bad grammar
  - Does the message seem unusual
  - Is the email in reply to something you didn't send or request
  - Is the email suggesting there is a compromising or embarrassing picture of yourself or someone you know
- Conduct tests
- Ensure spam filters are enabled

Common Targets for Phishing



https://info.wombatsecurity.com/hubfs/Wombat_Proofpoint_2019%20State%20of%20the%20Phish%20Report_Final.pdf

NEW YORK STATE OF OPPORTUNITY. | Department of Health

Vendor Contracts: Key Tasks

- Identify actual/full scope of dependencies on **third-party IT service providers**, such as data center operators and cloud services.
- Ensure contracts are reviewed by knowledgeable personnel.
  - Ensure contract reviewers are adequately trained regarding standards and risk areas.
- Design standards for assessing vendor risk:
  - Checklists for business team when considering vendors
  - "Disclosure" form for vendors to complete prior to review of service agreement
- Devise reasonable process for review of information collected.
- Coordinate underlying contract and BAA review for high-risk arrangements.

Vendor Contracts & Business Associate Agreements (BAAs)

- Specific data security/protection issues to review include:
  - Security and data protection expectations
  - Substantive notification obligations (e.g., information to be provided and shared by vendor)
  - Coordination of security incident response
  - Sharing of information regarding/performance of ongoing risk assessments and audits
  - Vendor data storage and data destruction practices
  - Level of customer data segregation
  - Termination/ unwinding/ transition requirements
  - Indemnification, limitation of liability, and insurance provisions
- Ensure BAAs are negotiated in light of the scope of services being provided and the level of risk related to PHI.

NEW YORK STATE OF OPPORTUNITY. Department of Health

Assessing Current Cyberliability Coverage

- Ensure coverage levels are evaluated in light of actual risk exposure (requires proper people are participants in any gap analysis process).
  - Organizational risks continue to evolve, as do potential sources of data breaches.
- Coverage exclusions seem to be the rule – avoid surprises by understanding policy exclusions.
- May need layers of coverage to get to appropriate limits.
  - Layers still may not cover all costs of a data breach.

Reporting & Responding to Cyberattacks

Healthcare sector attacks can very quickly spread to become a “community” level event, beyond the initially breached office/facility…

May cause major disruption of the healthcare delivery system in a city, county, region, involving thousands of providers, patients and residents:

- Interconnected/interdependent provider networks; communications between referring providers deliver multiple access points for attack;
- disparity between organizations’ ability to address cybersecurity issues; health care as a whole will only be as secure as the weakest link
- locations not expecting to be a target can serve as doorways to other, more complex partners with greater cyber risks and rewards for the hacker

What is the Role of the State Health Department?

- Engage with the provider to learn and assess the impact of the cyber event to the larger public health landscape
- Facilitate communication with State, Federal and third-party resources as the need arises
- Advise providers of alternative methods of continuing critical aspects of their operations during an IT outage
- Collect and share general information on the cyber threats with other providers to prevent and protect other providers from similar vulnerabilities
- Establish and maintain a trusted collaboration with all types of providers, associations, other stakeholders
- Liaise with Health Information Technology community as needed
- Protect State IT resources as necessary

Sample Incident Tracking Report (Mock Data)

Abbreviation key:
XYZ - Western Memorial Hospital
NNRC – Northeast Nursing & Rehabilitation Center

Area	Department	Issue	Status	Patient Impact
XYZ	Pharmacy	4/1/18: Loss of inventory control system, barcode scanners remain intact 4/2/18: Remain on critical override, 60% patched remotely with 40% requiring hands on, in progress today. 4/3/18 Scanner intermittent connectivity issues - Vendor on site to reimage and patch. Over 80% of all devices have returned to network. Remaining will remain on override.	In progress.	No impact.
XYZ	Medical Imaging MRI	4/1/18: Multiple vendors. Back online by noon up but some issues with quality. Off network, burning to disk at XYZ 4/2/18: In progress. Continuing to work off-network. 4/9/18: Fully Operational	In progress.	Patients rescheduled. Operational.
ER	Pharmacy	4/1/18: Computer down. Off network. Low-volume. Alternative method work-around continues. 4/2/18: Alternative method work-around continues. 4/3/18: Back on-line	In progress.	No impact.

Resources

- www.HealthIT.org
- https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html
- US Department of Health & Human Services Public Health Emergency Cybersecurity Reports and Tools https://www.phe.gov/Preparedness/planning/405d/Pages/reportandtools.aspx
- Healthcare & Public Health Sector Coordinating Councils Medical Device and Health IT Joint Security Plan https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-v1.pdf
- KnowBe4 – security awareness and simulated phishing https://www.knowbe4.com/

Questions?