Cyber Security and Health Data/EHR: Perspectives from Clinicians, Patients & Family

ANNA SCHOENBAUM, DNP, RN-BC
DIRECTOR, PORTFOLIO EPIC CLINICAL APPLICATIONS
UNIVERSITY OF MARYLAND MEDICAL SYSTEM

ROBYN ECKERLING, JD, MPH
CHIEF PRIVACY AND SECURITY COUNSEL
ALLSCRIPTS

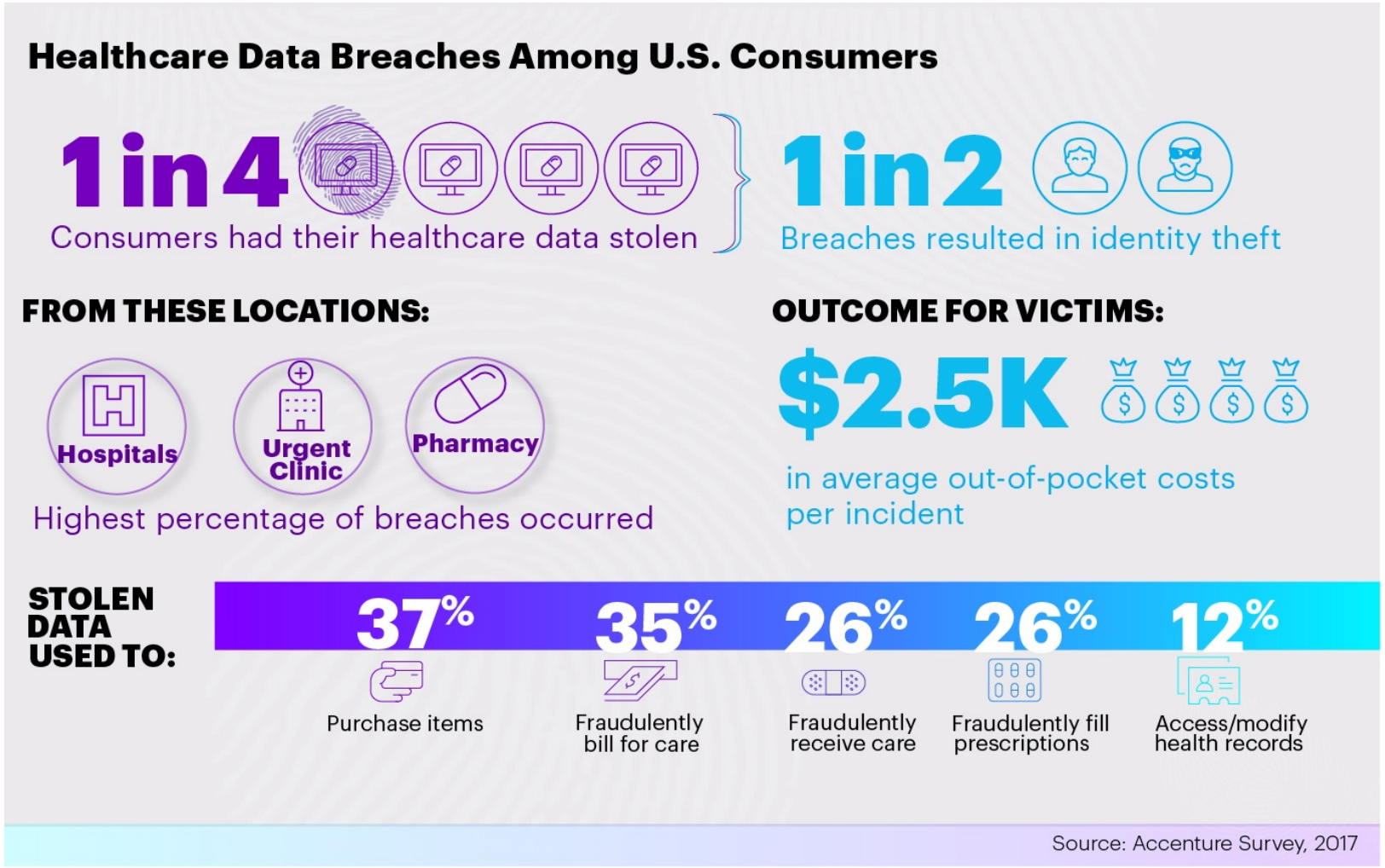
Disclaimer

The views expressed in this presentation are our own and do not represent the opinions of the entities for which work or any entities with which we have been affiliated. Nothing in this presentation should be construed to create an attorney-client relationship or constitute legal advice.

Would you be convinced?

https://www.youtube.com/watch?time_continue=127&v=opRMrEfAIiI

Healthcare Breaches: Impact Snapshot



Objectives

- Understand hospital and outpatient landscape vulnerabilities to security threats, damage to hardware, software or electronic data
  - People
  - Process
  - Technology
- Understand possible threats
- Understand potential solutions

Threats to the Clinical Landscape

- Threats both internal and external

Frequency	750 incidents, 536 with confirmed data disclosure
Top 3 patterns	63% of incidents within Healthcare • Miscellaneous Errors • Crimeware • Privilege Misuse
Threat actors	43% External, 56% Internal, 4% Partner and 2% Multiple parties (breaches)
Actor motives	75% Financial, 13% Fun, 5% Convenience, 5% Espionage (all incidents)
Data compromised	Medical (79%), Personal (37%), Payment (4%)

2018 Data Breach Investigations Report, Verizon, 11th Edition

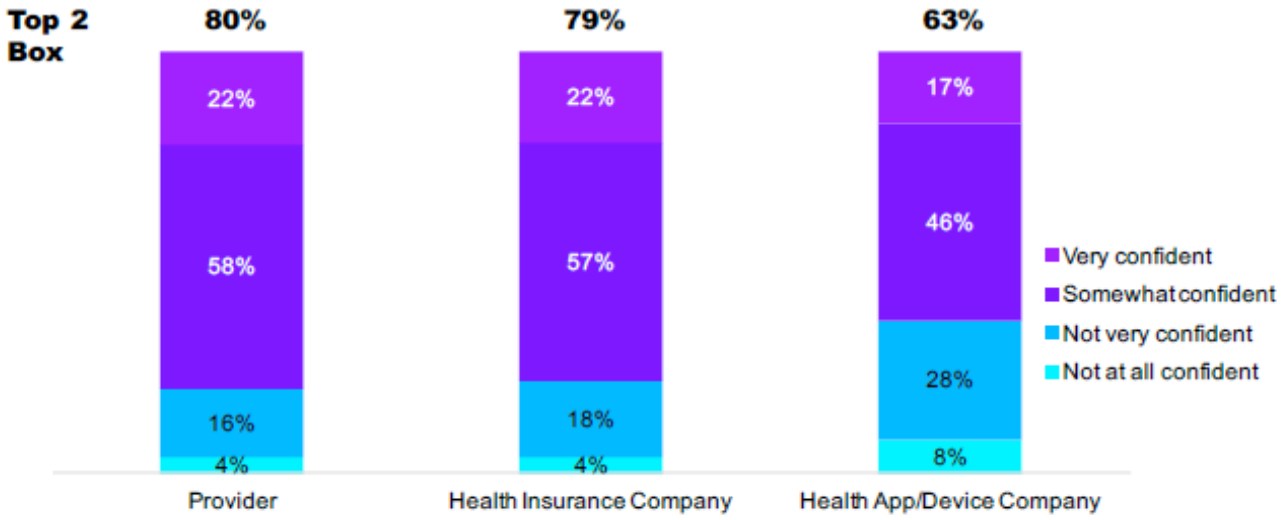
Patient Perspective

Some Degree of Trust

Yet, according to the Accenture study, **25% of patient changed healthcare providers**

The majority of the US consumers have at least some confidence in the digital data security measures taken by their providers and insurers and somewhat fewer by the companies that make health apps or devices; relatively few have high confidence in any of these organizations.

Confidence in Security Measures to Protect Privacy and Security of Health Data



BASE: ALL QUALIFIED RESPONDENTS (n=2000)
Q525/Q545/Q560 How confident are you that your healthcare providers/health insurance company/health app/device company's security measures will protect the security and privacy of your digital healthcare data?

Hospital & Outpatient Landscape: People

- Identify key players
  - What are their roles?
- Who has access to your systems?
  - Staff (all levels and departments) - Executives, Clinicians, Non-clinicians
  - Third Party, including vendors and contractors
  - Patients
    - Access to records
    - Patient entered data
    - Personal health record
  - Other Family Members/Guardians
- What is the scope of their access?

Hospital & Outpatient Landscape: Access

- Identify your access points
- Identify what tools your practice uses
  - Laptops, tablets, smart phones, etc.
- Third-party applications
  - Internet of Things
  - Scheduling
  - Financial
  - Etc.
- Health Information Exchange
- Patients
  - Patient Portals
  - Personal Health Records

Hospital & Outpatient Landscape: How to Protect Data

- Process
  - Identify your data
  - Identify what your practice is doing with data (ex. Research, Data Analytics)
  - Identify where you maintain your data
  - Identify how you protect your data
- Cybersecurity framework and program
  - Pick one!
    - National Institute for Standard and Technology
    - International Organization for Standardization

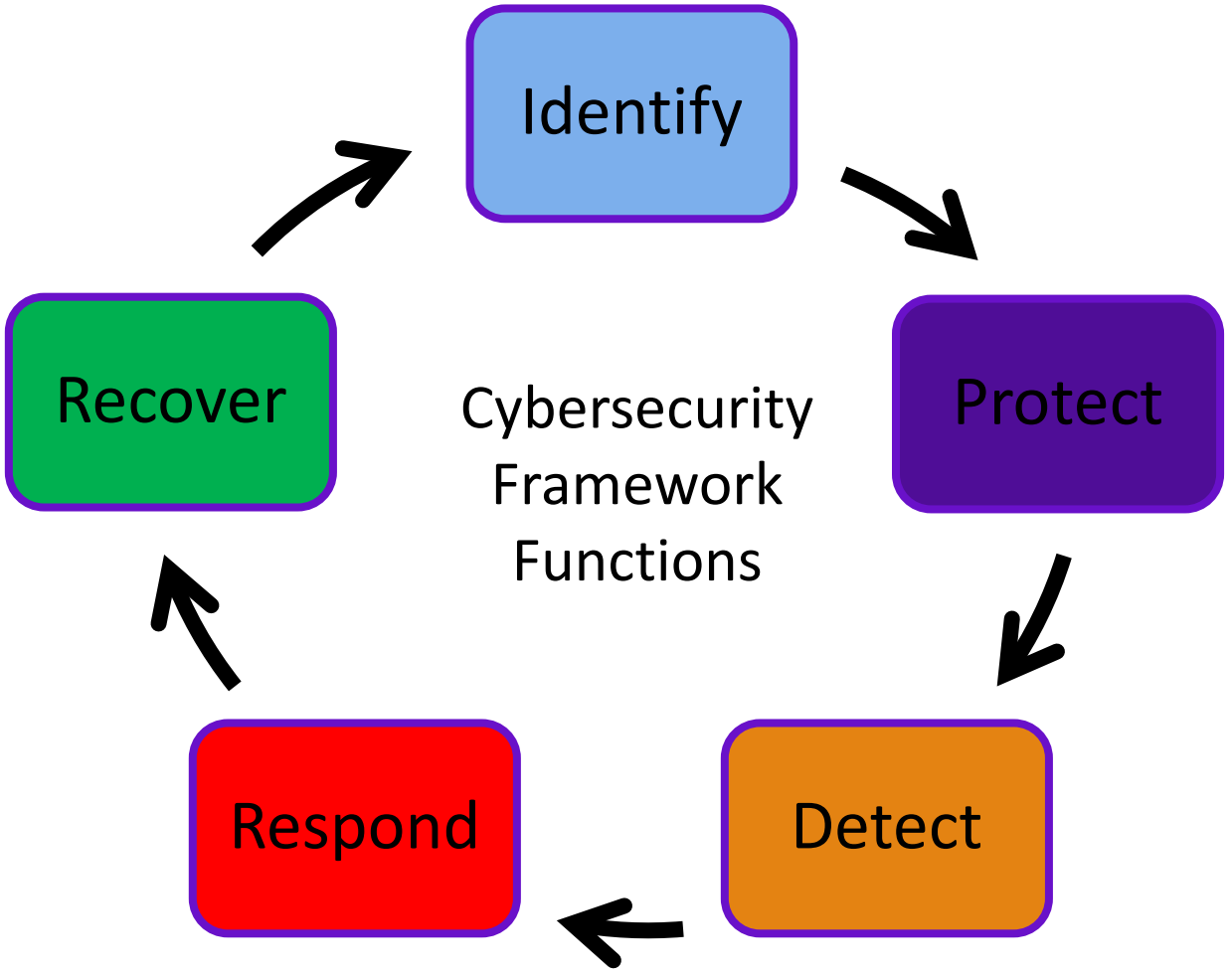
NIST National Institute of Standards and Technology

The Office of the National Coordinator for Health Information Technology

Department of Health & Human Services · USA — Office for Civil Rights

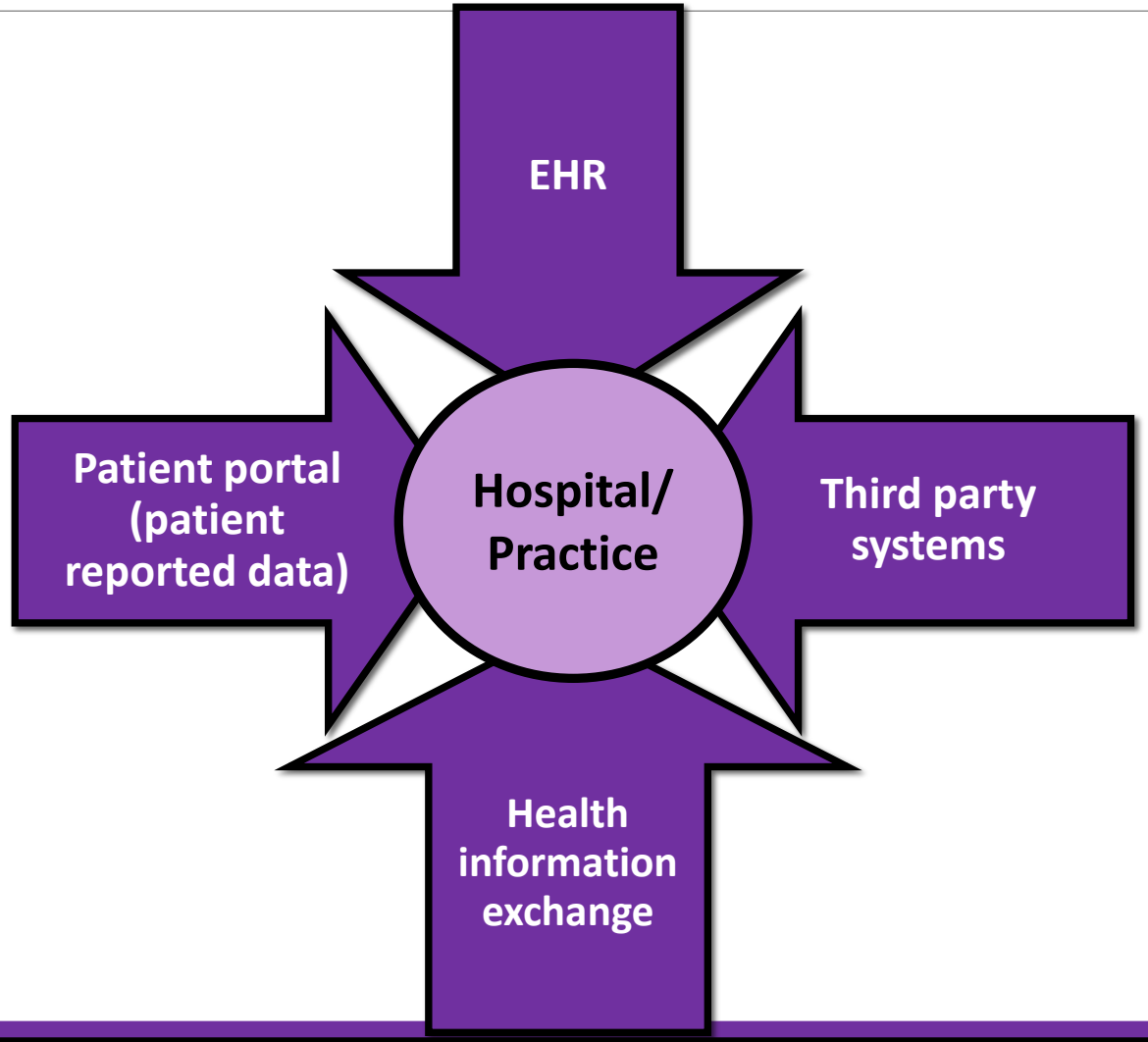
ISO

National Institute for Standard and Technology (NIST)



Identify	Identify and understand critical business functions, resources & cybersecurity risks
Protect	Develop & implement the appropriate safeguards to ensure delivery of critical infrastructure services
Detect	Develop & implement the appropriate activities to identify the occurrence of cybersecurity event
Respond	Develop & implement the activities to take action regarding detected cybersecurity event
Recover	Develop & implement the activities to restore any capabilities or services that were impaired due to a cybersecurity event

Hospital & Outpatient Landscape: Technology



Potential Threats

- Size and scope of organization
  - Hospital
  - Clinic
- Errors
  - Ex. Data sent to incorrect recipient
- Malware
  - Trojans, spyware, virus, worm, ransomware
  - Exposure through Phishing, Social engineering,
    Whaling, Potential Security Vulnerabilities

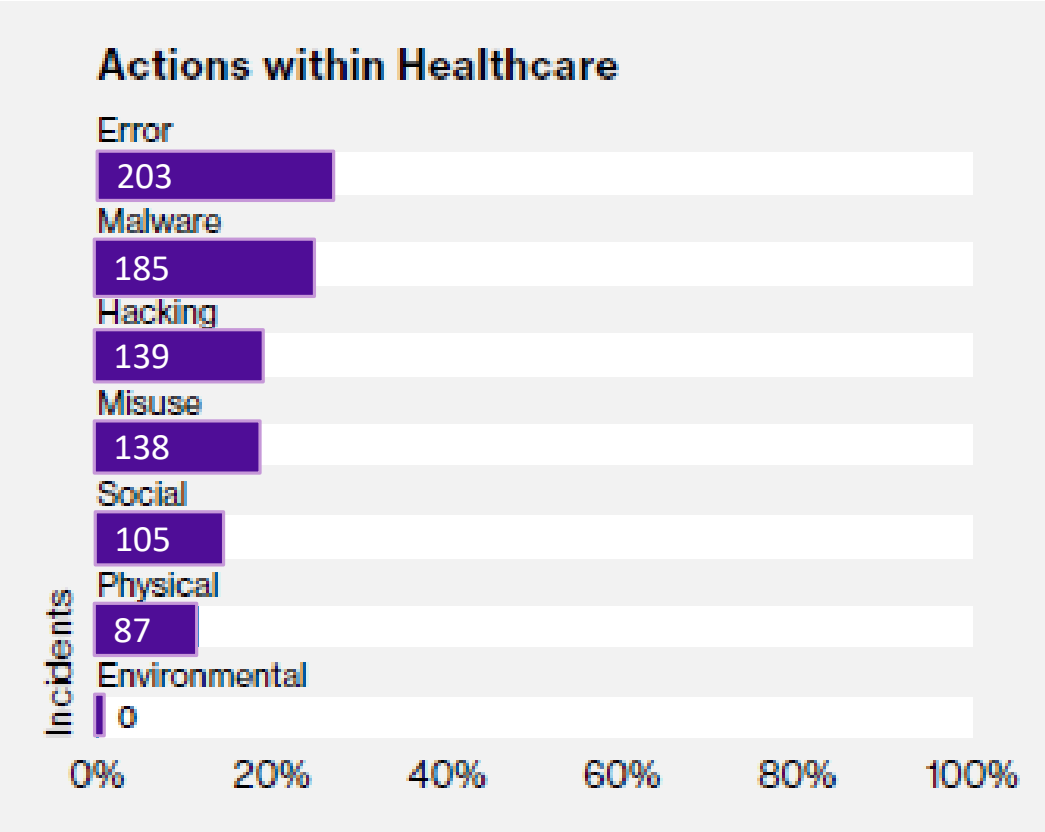


Figure 32. Threat action categories within Healthcare incidents (n=750)

2018 Data Breach Investigations Report, Verizon, 11th Edition

Solutions: People

- Training
- Engagement
- Education
- Physical Security
- Exit Interviews / Exiting Checklists

Solutions: Process

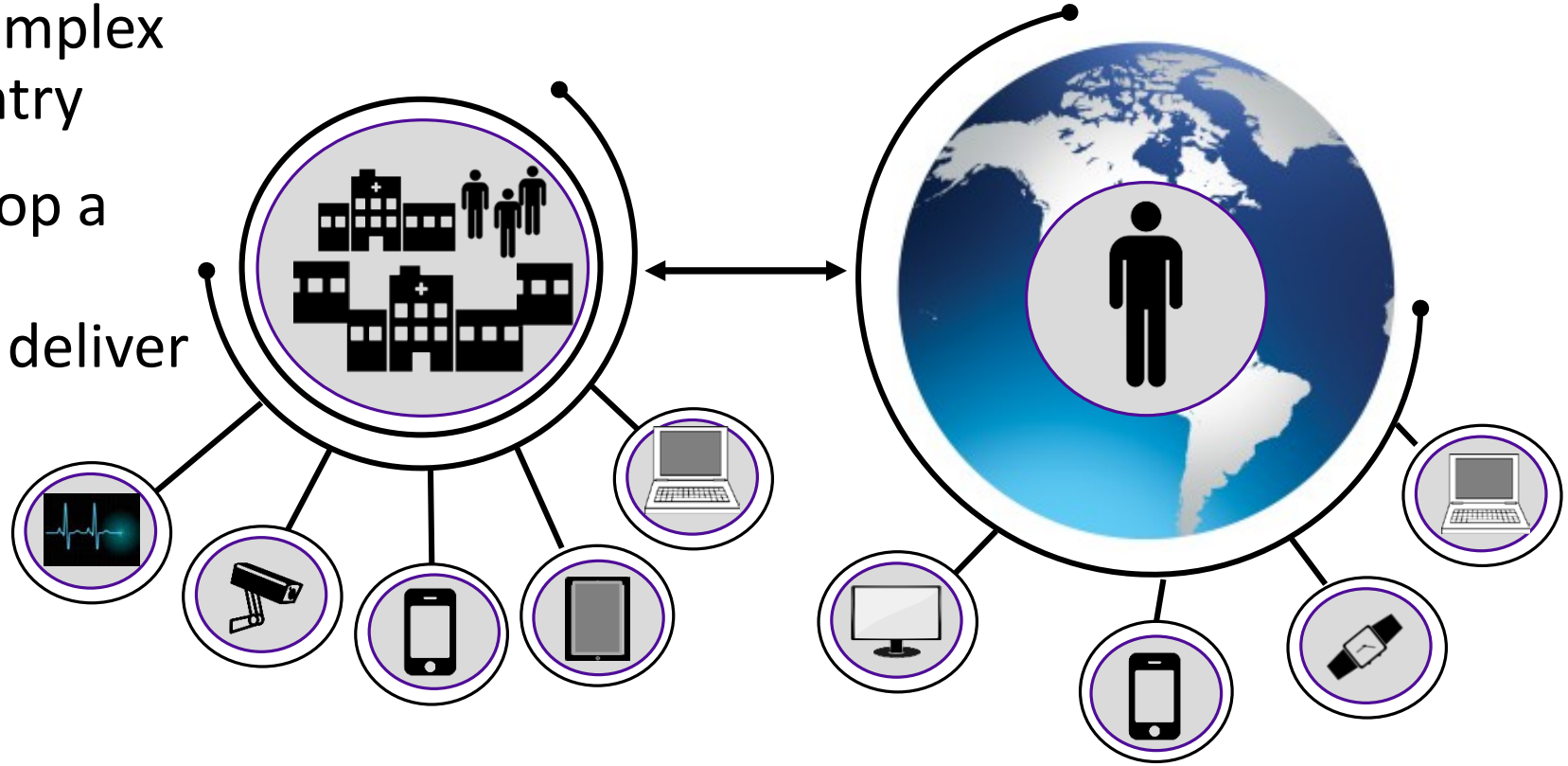
- Evaluate internal risk structure
- Collaborative governance process (security council)
  - Operations
  - Privacy & Security officer
  - Compliance
  - Information Technology
  - Clinical Leaders
- Perform risk assessments at least annually
- Application whitelisting
- Playbook, security audits, & drills
- Perform regular data backups
- Vendor identification
- Access Controls
  - Limiting Access (IT, secure areas, locked/limited access digital, prohibiting recording devices, disabling USB ports, etc.)
- Identify / Document / Inventory

Solutions: Technology

- Backups
- Password management
- Multi-factor authentication
- Firewalls
- Data encryption
- Security information and event management tools
- Anti-Malware
- Network Intrusion Prevention System (NIPS)
- Data loss prevention software
- Vulnerability scanning and penetration testing
- Denial of service mitigation (DDoS)

Pulling it TOGETHER

- An healthcare organization's Cybersecurity model is complex with multiple points of entry
- Organizations must develop a holistic business driven cybersecurity program to deliver safe and quality care
  - **People**
  - **Process**
  - **Technology**



Questions?

Contact Information

Anna Schoenbaum, DNP, RN-BC
Director, Portfolio Epic Clinical Applications
University of Maryland Medical System
aschoenbaum@umm.edu

Robyn Eckerling, JD, MPH
Chief Privacy and Security Counsel
Allscripts
Robyn.Eckerling@allscripts.com