American Hospital Association™

Advancing Health in America

Strategic Cybersecurity and Risk Issues for Healthcare Providers

2019 AIRNet

Allied Association Information Resources Network

Presented by John Riggi, Senior Advisor, Cybersecurity and Risk Advisory Services

American Hospital Association

Agenda

- Healthcare Cyber Threats
- Data and Cyber Adversaries
- Anatomy of a Hack
- Healthcare Cyber Risk Factors
- Leadership Considerations
- Incident Response Exercise Elements
- The AHA’s Cybersecurity and Risk Advisory Services
- ***Discussion and questions***

American Hospital Association™

Advancing Health in America

The Cyber Threat Landscape

Major Healthcare Cyber Threats

Crypto Hijacking: Increasing threat in 2018. Cyber criminals infiltrate and takeover high computing power resources for crypto currency mining. Attack threat fluctuates with the price of digital currency. *Detection capabilities and impact on patient care?*

Internal Threat: From 2013 – 2017, internal actors were responsible for 56% cyber incidents, half of which were intentional, half accidental.

External Actors are still responsible for the vast majority of records stolen.

Ransomware: Incidents appear to be down in 2018 compared to peak in 2017. However, ***impact*** remains significant to those victimized. FBI received 1,493 complaints in 2018. *Reported* dollar losses up from \$2.3m in 2017 to \$3.6m in 2018.

Impact on hospital operations, medical devices, backups and incident response plan!

Sources: FBI Internet Crime Report (4/19/2019) Verizon 2018 PHI Data Breach Report; 2017 Data Breach Study: United States, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC

Major Healthcare Cyber Threats

Business E-mail Compromise: In 2018, the FBI received 20,373 complaints of U.S. victims with adjusted losses of $1.3 billion. Contact the FBI immediately at www.ic3.gov 75% recovery rate if reported within first 24 – 48 hours.

Vendor agreements, MFA and verbal payment authentication procedures!

Supply Chain Attacks: Vendor networks, products, services and ***software*** targeted by a cyber attacker as a pathway to compromise the network of the customer of the vendor.

Vendor risk management program, business associate agreements, patient care impact?

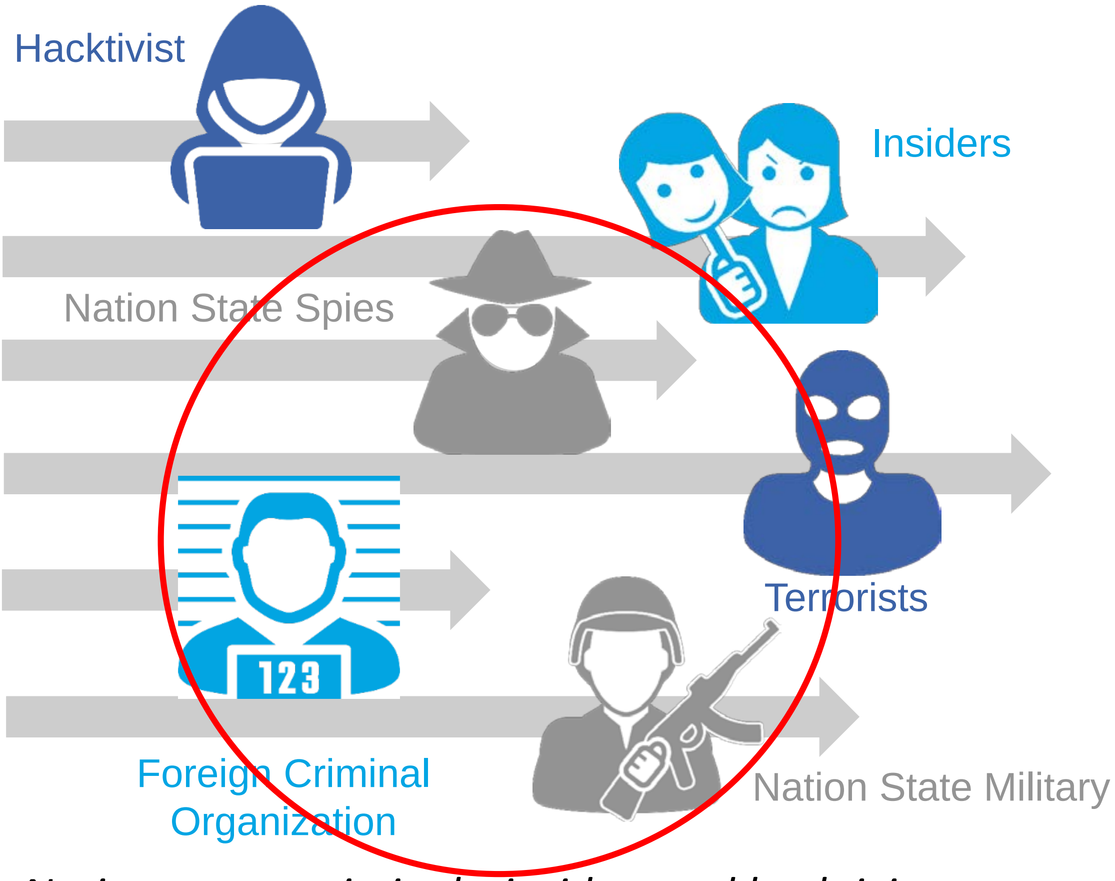
Computer Intrusions: (Foreign Based External Hacking) The average cost for lost or stolen record for health = $408. The average cost for lost or stolen record for all industries = $148. The average cost for a data breach for all industries = $3.86 million. The average cost of a healthcare breach is approximately 2.75 times all industry average or **$10.6 million**. *How much cyber insurance do you have?*

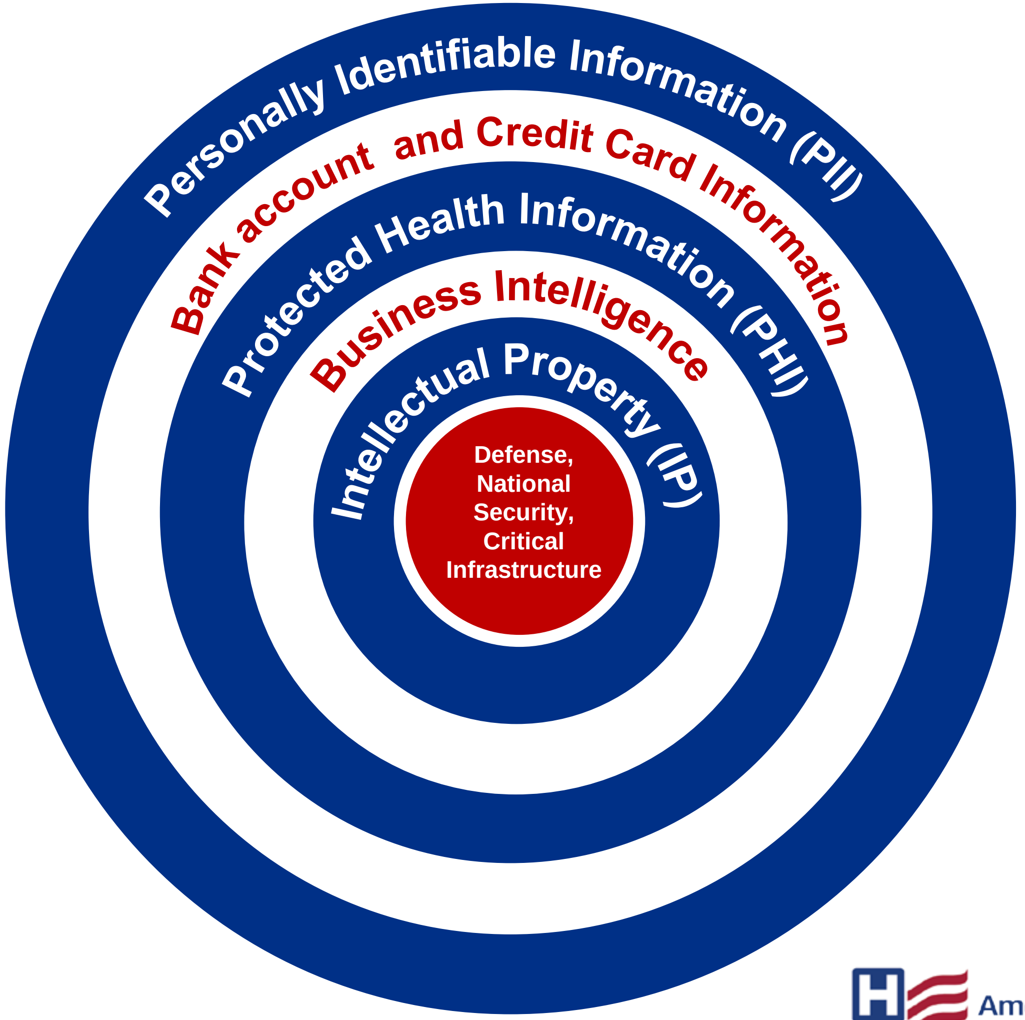
American Hospital Association™
Advancing Health in America

Sources: FBI 2018 Internet Crime Report (4/19/2019) Verizon 2018 PHI Data Breach Report; 2018 Data Breach Study: United States, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC

Data Rich Environment = Target Rich Environment

Targeted Data



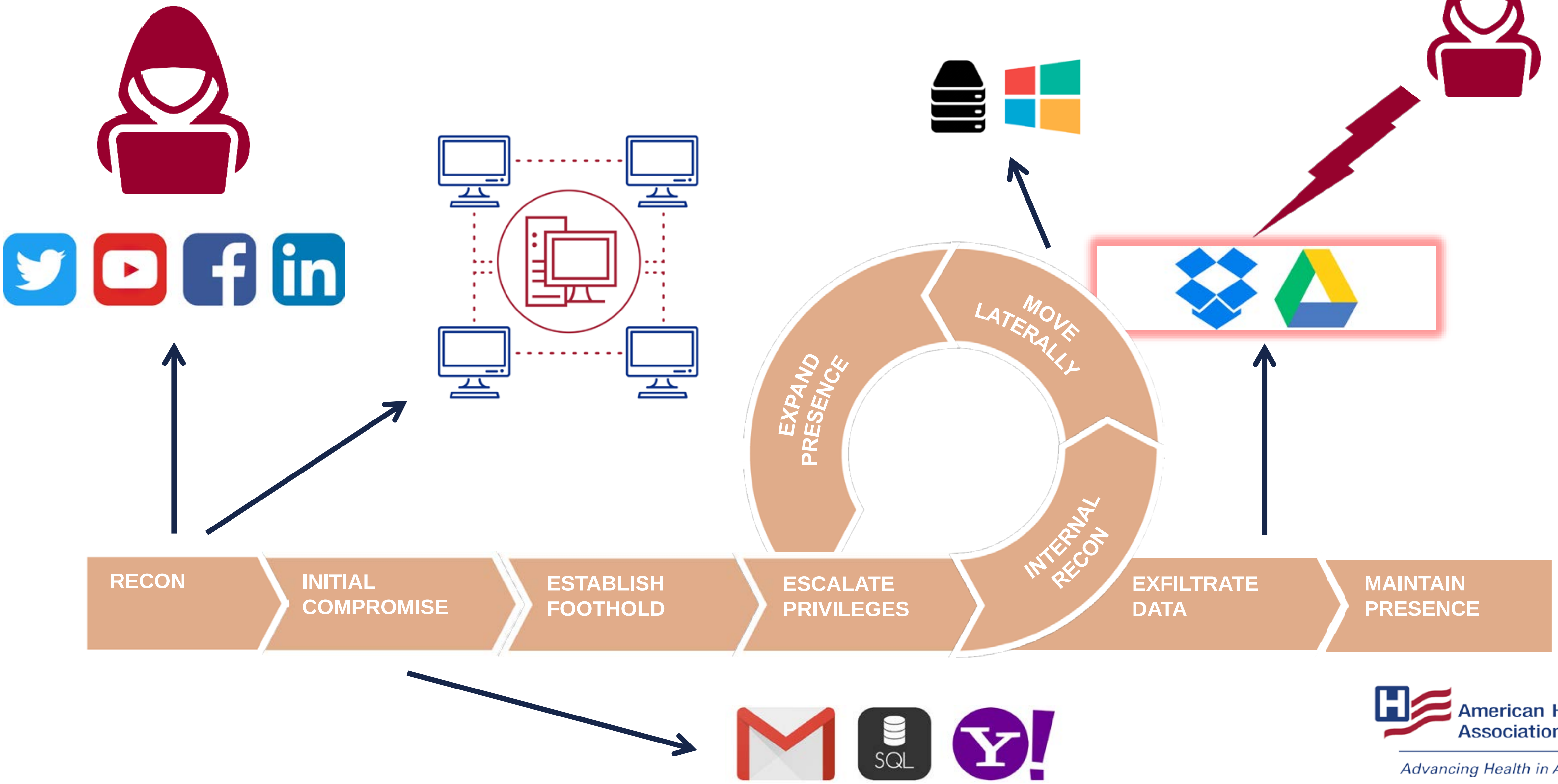


Personally Identifiable Information (PII)
Bank account and Credit Card Information
Protected Health Information (PHI)
Business Intelligence
Intellectual Property (IP)
Defense, National Security, Critical Infrastructure

Nation states, criminals, insiders and hacktivists are aggressively targeting healthcare providers to steal their valuable data. ***"One stop hacking!"***

American Hospital Association™
Advancing Health in America

Anatomy of a Hack



American Hospital Association™
Advancing Health in America

Factors Leading to Increased Cyber Risk in Healthcare

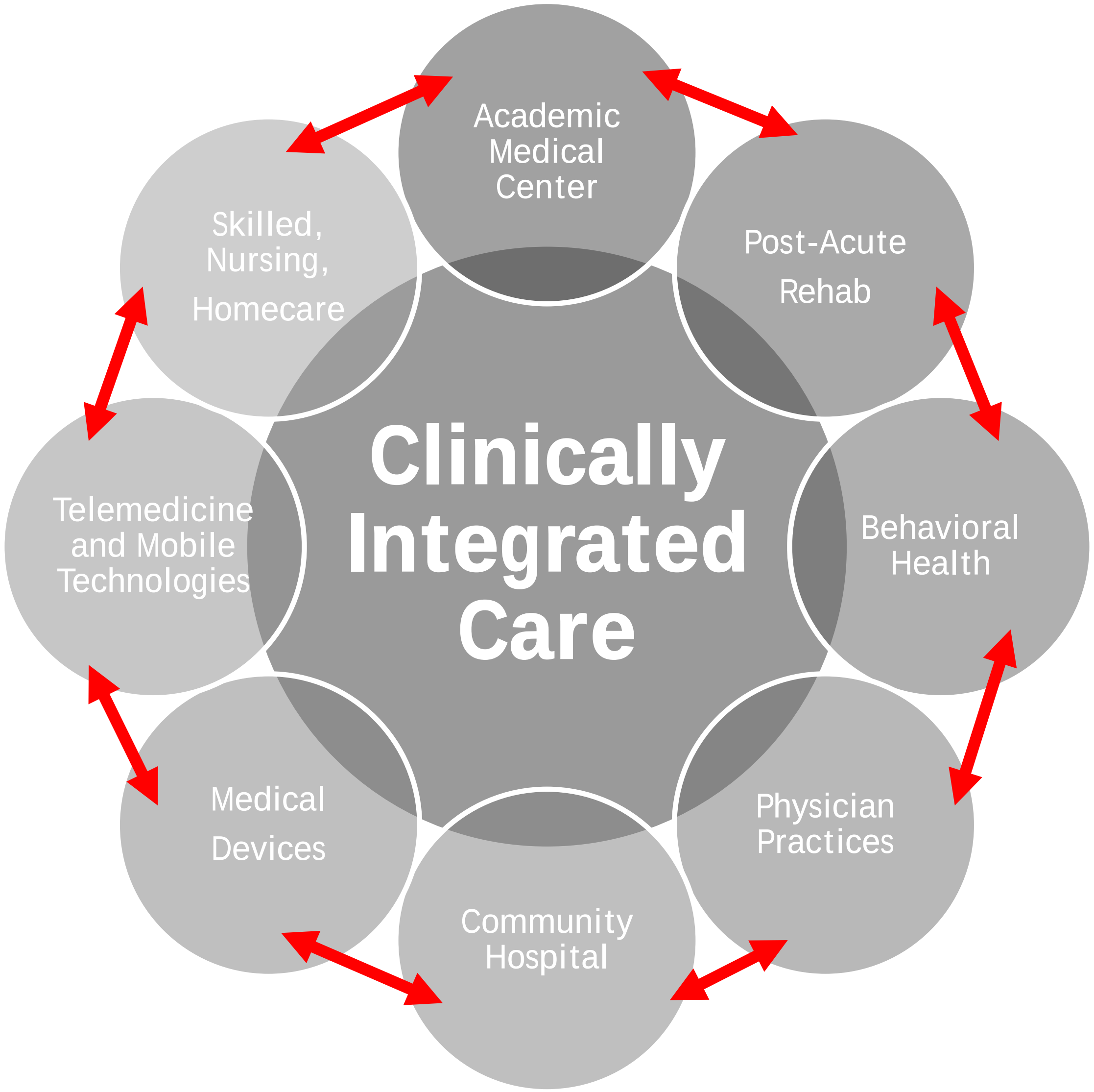
- Expanded use of network and internet connected devices including *medical devices*. ***Cyber is a patient safety issue.***
- Legacy computer systems and medical devices in hospitals. Some run “out of support” operating systems.
- Lack of cybersecurity resources – financial, technical and human.
- Accurate hardware and software inventory challenges.
- Multiple, complex and overlapping networks. Open and wireless networks.
- Mandatory transition from paper to electronic health records.
- “Bring your own device” (BYOD) policy.
- Requirement to share PHI among providers. Value based payment models.
- Only sector which stores and combines PII, PHI, PCI, **Medical Research and Intellectual Property**.

- Mergers & Acquisitions create systems compatibility and data inventory challenges. The entity being acquired may have embedded cyber risk.
- Victims are often unaware when PHI is stolen. No ability to “cancel” your healthcare records
- Third party vendors with network access.
- Healthcare records have a higher payout on the dark web (10 – 70x more than credit card numbers).
- Cybercrime displacement from financial services.
- Move toward interoperability and patient access.

American Hospital Association™

Advancing Health in America

Emerging And Embedded Cybersecurity Risk



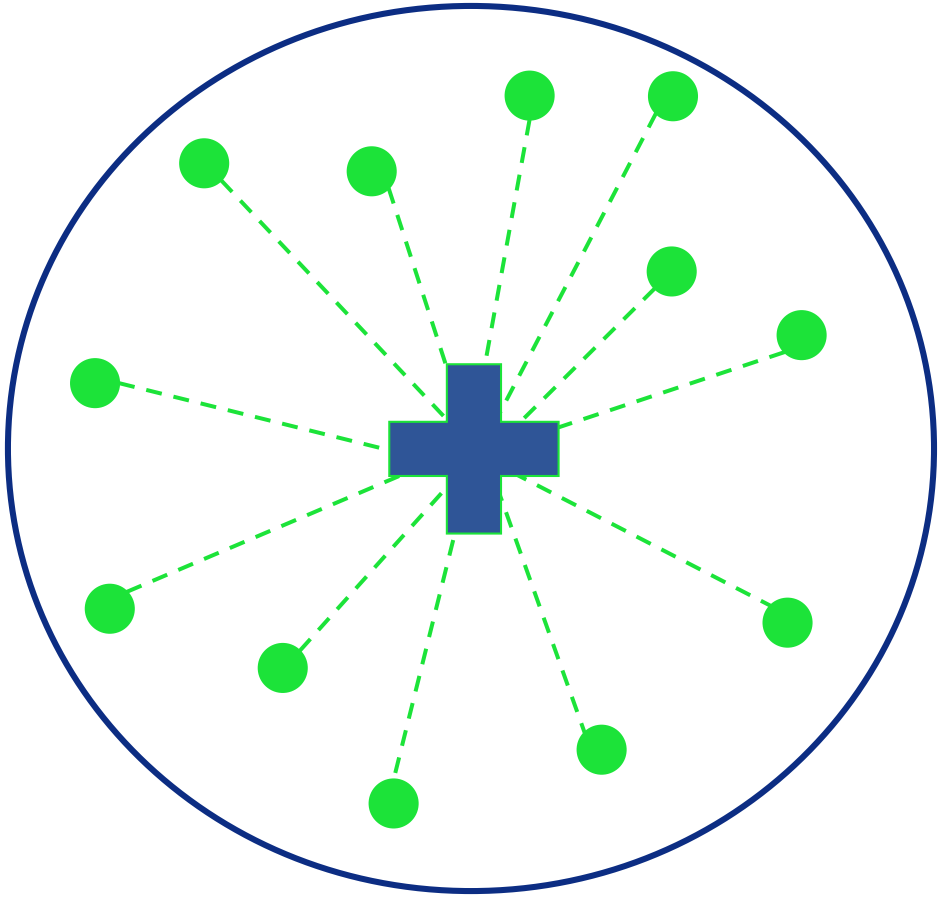
- Various forces – including the move toward payment tied to quality, clinical outcomes and episodes of care – are driving clinical integration across provider types, leading to ***new and more complex data sharing and integration requirements for providers.*** Clinical integration also includes telemedicine and mobile technologies and….

5G is coming!

American Hospital Association™
Advancing Health in America

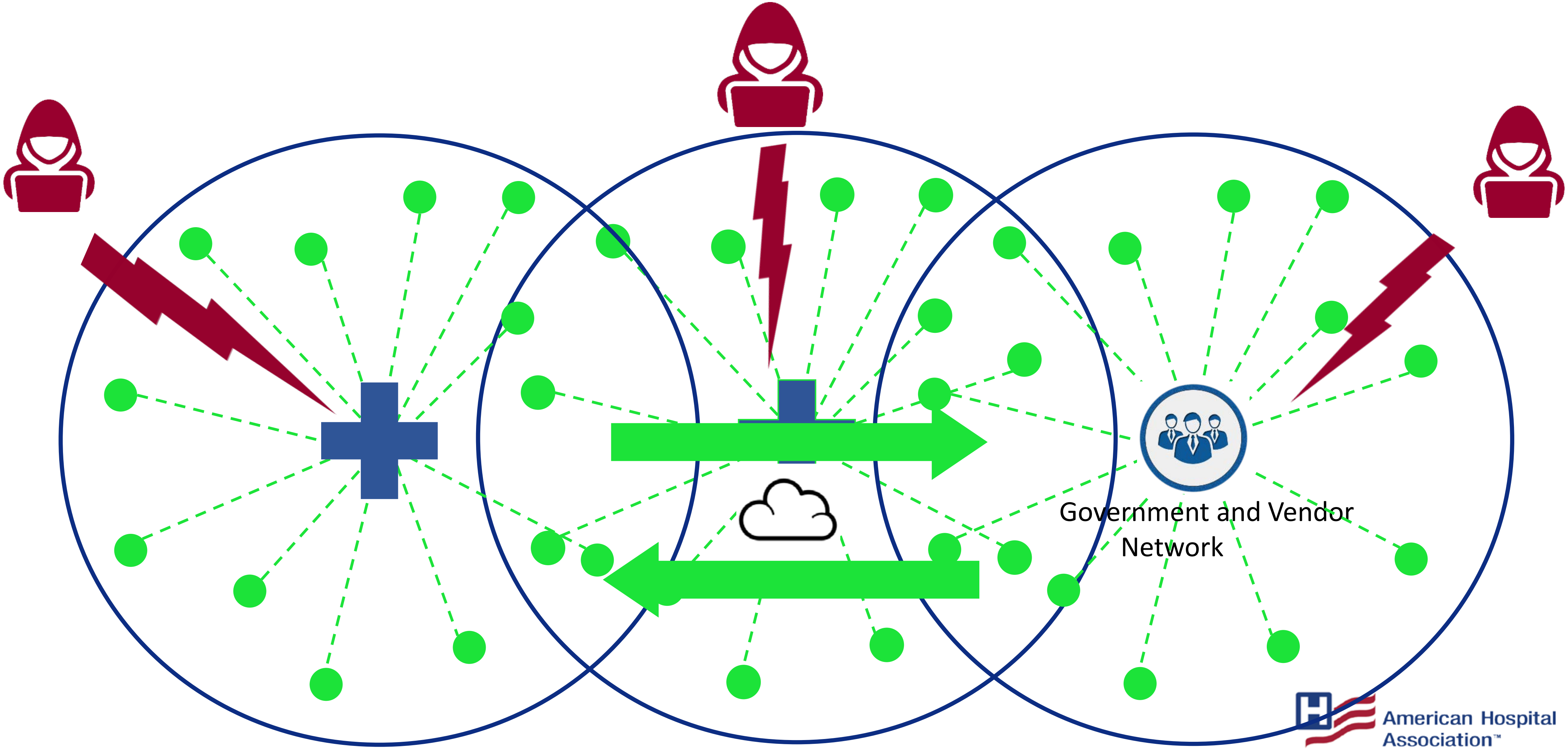
Cyber Risk and State Hospital Associations

State Hospital Association



American Hospital Association™
Advancing Health in America

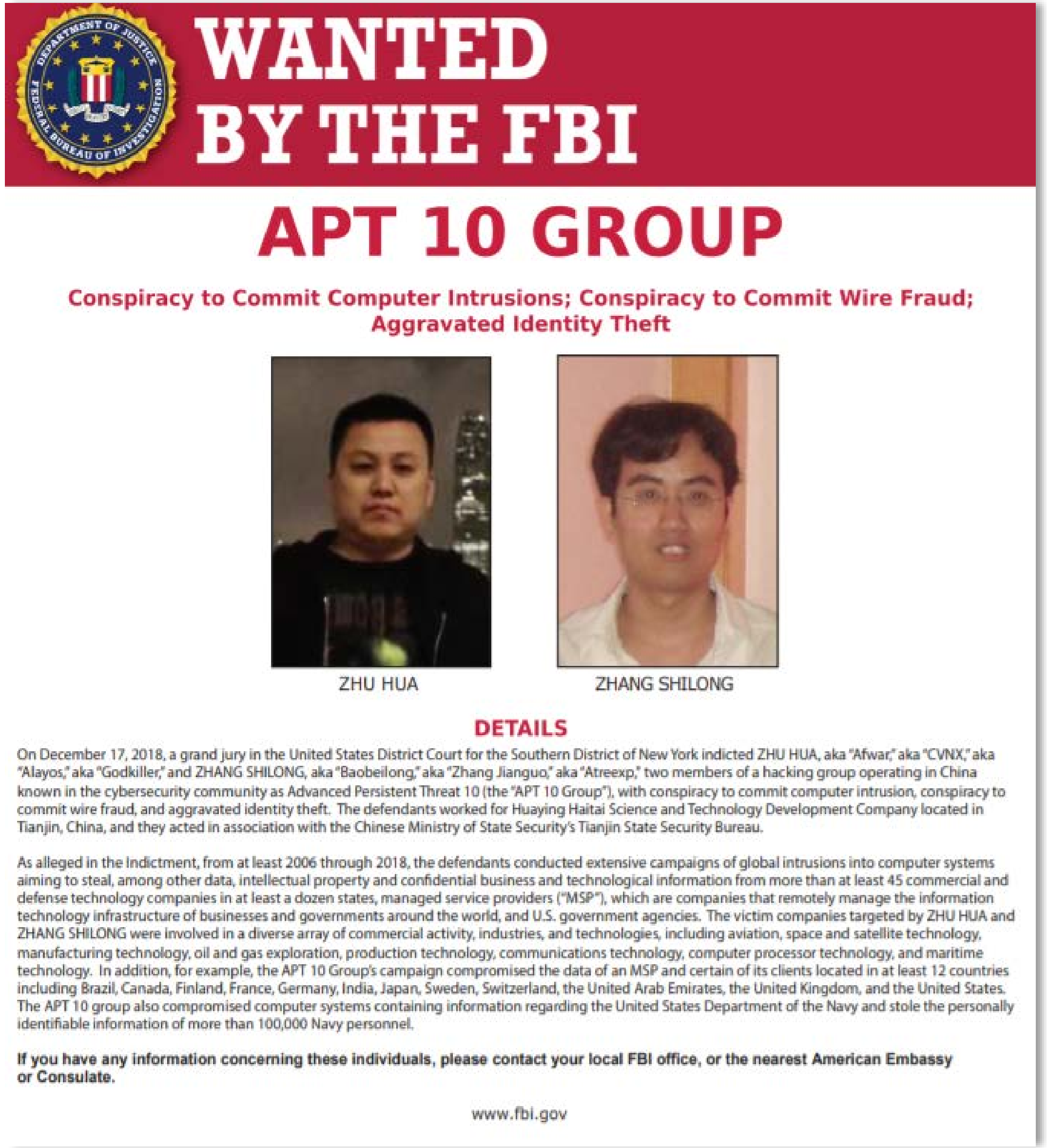
Network Mapping - The Hackers Point of View



American Hospital Association™

Advancing Health in America

December 17, 2018 - Indictment and FBI FLASH issued



WANTED BY THE FBI

APT 10 GROUP

Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

ZHU HUA

ZHANG SHILONG

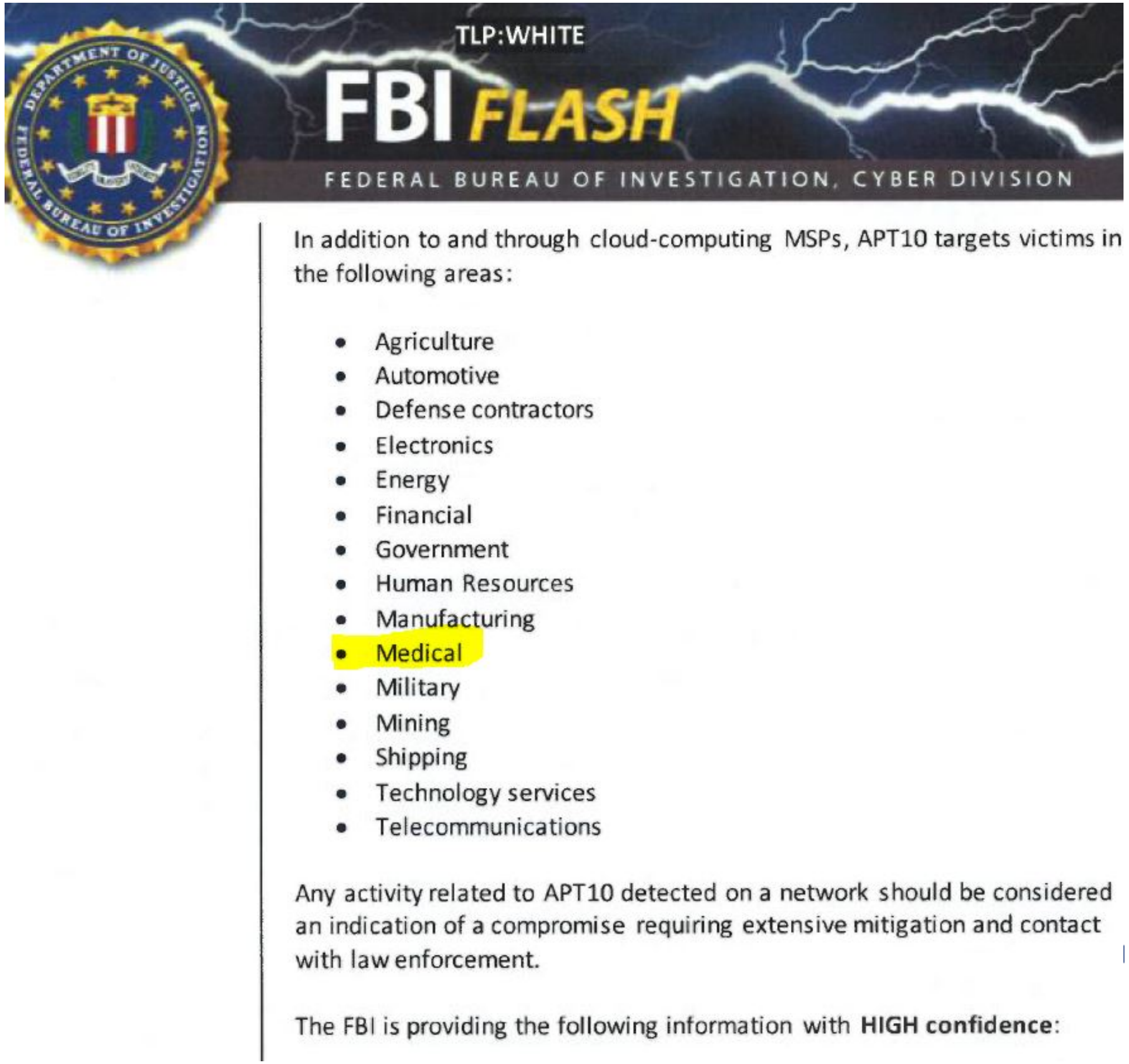
DETAILS

On December 17, 2018, a grand jury in the United States District Court for the Southern District of New York indicted ZHU HUA, aka "Afwar," aka "CVNX," aka "Alayos," aka "Godkiller," and ZHANG SHILONG, aka "Baobeilong," aka "Zhang Jianguo," aka "Atreexp," two members of a hacking group operating in China known in the cybersecurity community as Advanced Persistent Threat 10 (the "APT 10 Group"), with conspiracy to commit computer intrusion, conspiracy to commit wire fraud, and aggravated identity theft. The defendants worked for Huaying Haitai Science and Technology Development Company located in Tianjin, China, and they acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

As alleged in the Indictment, from at least 2006 through 2018, the defendants conducted extensive campaigns of global intrusions into computer systems aiming to steal, among other data, intellectual property and confidential business and technological information from more than at least 45 commercial and defense technology companies in at least a dozen states, managed service providers ("MSP"), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, and U.S. government agencies. The victim companies targeted by ZHU HUA and ZHANG SHILONG were involved in a diverse array of commercial activity, industries, and technologies, including aviation, space and satellite technology, manufacturing technology, oil and gas exploration, production technology, communications technology, computer processor technology, and maritime technology. In addition, for example, the APT 10 Group's campaign compromised the data of an MSP and certain of its clients located in at least 12 countries including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The APT 10 group also compromised computer systems containing information regarding the United States Department of the Navy and stole the personally identifiable information of more than 100,000 Navy personnel.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov



TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

In addition to and through cloud-computing MSPs, APT10 targets victims in the following areas:

- Agriculture
- Automotive
- Defense contractors
- Electronics
- Energy
- Financial
- Government
- Human Resources
- Manufacturing
- Medical
- Military
- Mining
- Shipping
- Technology services
- Telecommunications

Any activity related to APT10 detected on a network should be considered an indication of a compromise requiring extensive mitigation and contact with law enforcement.

The FBI is providing the following information with **HIGH confidence**:

Top 12 Risk Considerations for Leadership

Patient Safety & Mission Critical Systems

- ***Mission-critical systems, devices and networks related to patient safety and care delivery - first and always!***
- Cyberattack vulnerability?

#1

Strategic Cyber-Risk Profile

- Strategic cyber-risk profile, from the adversaries' perspective.
- Main cyber adversaries based upon patients, data sets and network connections.
- ***Who is coming after us?***

#2

Tactical Cyber- Risk Profile

- Current state tactical cyber-risk profile based on our latest risk assessments and vulnerability and penetration testing?
- ***Polices, procedures risk assessment vs. technical risk assessment***

#3

Prioritization

- Prioritization of cybersecurity policies, procedures, controls and technical risks - ***patient safety and care delivery first, data protection second, business operations third?***

#4

Capabilities

- Sufficient and capable human and technical resources?
- Sufficient budget devoted to our information-security program?
- ***CISO reporting structure***

#5

Vendor Risk-Management Program

- Recent in-depth technical, legal, policy and procedural, review
- Vendor cyber risk exposure – access to networks, data and ***concentration of risk and mission criticality***

#6

Top 12 Risk Considerations for Leadership

Cybersecurity Culture

- Compliance based or pro-active, top down, team approach?
- Empowerment of staff
- Protection of patient safety and data

#7

Risk Mitigation Strategy

- Based upon cyber risk profile
- Integration into an overall multidisciplinary, ERM program and governance structure
- CTO, CMO, CIO & CISO interaction
- Framework?

#8

Risk Mitigation Implementation Plan

- Cyber-risk mitigation strategy implementation road map
- Cost/Risk reduction impact analysis for each objective

#9

Incident Response Plan

- Representatives from all functions
- Roles and responsibilities defined
- Last updated and tested?
- Downtime procedures, backups tested
- Ransomware scenario

#10

Cyber Insurance

- Analysis and policy integration
- Adequate coverage and current to cover all breach costs?
- Incident response plan integration

#11

Independent Review

- Independent and objective outside expert review of:
  - Risk profile
  - Gaps and mitigation strategy
  - Validation of processes
  - Recommendations

#12

American Hospital Association®

Cybersecurity and Risk Advisory Services

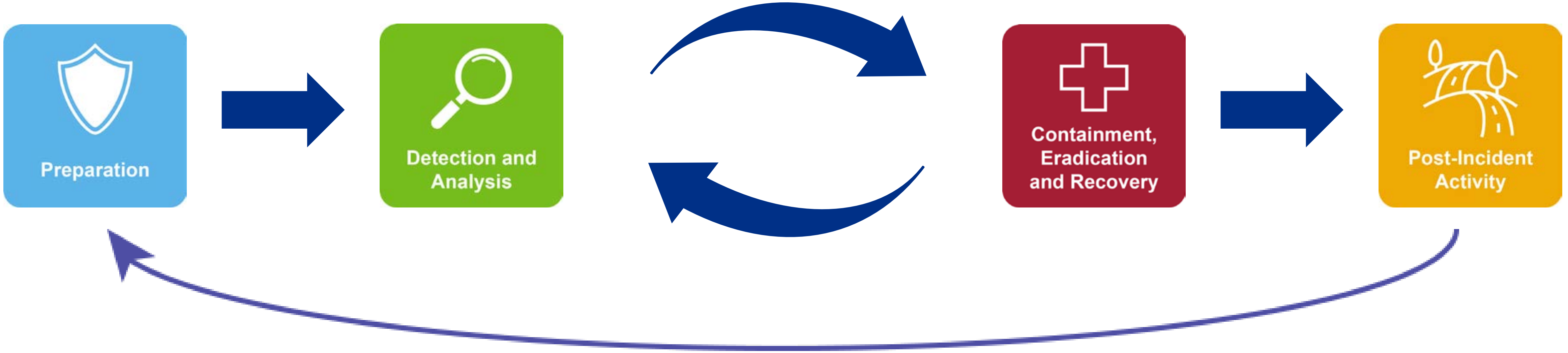
- STRATEGIC CYBERSECURITY AND RISK ADVISORY SERVICES
- HOSPITAL LEADERSHIP CYBERSECURITY EDUCATION AND AWARENESS
- CYBER AND RISK INCIDENT RESPONSE STRATEGY AND ADVISORY SERVICES
- LAW ENFORCEMENT AND NATIONAL SECURITY RELATIONS

American Hospital Association™
Advancing Health in America

Tabletop Exercise – Example Overview and Objectives

- The goal of the tabletop exercise is to employ knowledge provided in the previous sessions and to increase situational awareness for hospital leadership in dealing with a major cyber incident. The target time range for the exercise is 90 minutes followed by discussion.

- The exercise has complex elements which will be covered in a compressed timeline. There are no absolute correct or incorrect responses, we hope to learn as a group based upon our collective knowledge and experience. The exercise combines multiple real world scenarios in an effort to provoke discussion and thought on how the multiple facets of incident response are employed in combination with patient care and non-technical priority issues which arise as a result of the incident.



Questions? For further information contact:

John Riggi, Senior Advisor for Cybersecurity and Risk

jriggi@aha.org

(O) +1 202-626-2272

(M) +1 202-640-9159 (**24 hours**)

800 10th Street N.W. Suite 400

Washington, D.C. 20001

- John Riggi, having spent nearly 30 years as a highly decorated veteran of the FBI, serves as the Senior Advisor for Cybersecurity and Risk for the American Hospital Association (AHA) and their 5000+ member hospitals. In this role, John serves as a resource nationally to assist members identify and combat cyber and other sources of risk to their organizations. Additionally, John will support the AHA's policy efforts and Federal agency relations on cyber and other risk related issues. Previously, John led BDO Advisory's Cybersecurity and Financial Crimes Practice.
- While at the FBI, John served as a representative to the White House Cyber Response Group. He also led the FBI Cyber national program to develop mission critical partnerships with the healthcare and other critical infrastructure sectors for the investigation and exchange of information related to national security and criminal-related cyber threats.
- John held a national strategic role in the FBI investigation of the largest cyber-attacks targeting healthcare, energy, entertainment, technology, financial services, government and other sectors. John led BDO's exclusive engagement with the AHA to provide cybersecurity training for their 5000+ member hospital CEOs.
- Co-lead on the national HHS/Health Care Sector Coordinating Council Task Group to develop cyber enterprise risk resources for the field.
- In addition, he serves as an official private sector validator for the White House's Presidential Policy Directive (PPD)-41 on U.S. Cyber Incident Coordination. The PPD is designed to foster an improved working relationship between the public and private sector.
- He also served as a senior FBI representative to the CIA's Counterterrorism Center. John is the recipient of the FBI Director's Award for leading a highly successful classified terrorism financing interdiction program and the recipient of the CIA George H.W. Bush Award for Excellence in Counterterrorism, the CIA's highest counterterrorism award. John presents extensively on cybersecurity topics and is frequently interviewed by the media on cybersecurity issues.

American Hospital Association™

Advancing Health in America