Cybersecurity: How to Handle a Growing Threat in Healthcare

SoCal HIMSS CIO Forum
Dec 8, 2016

With you today

Patrick Hynes

Patrick is a Principal in PwC's Cyber Crime and Breach Response practice. He and his team help clients investigate breaches and system compromise by either external parties (state sponsored; organized crime, etc.) or through insider threat. He also helps clients prepare for breaches by increasing board and executive awareness, evaluating and enhancing detect and respond capabilities, and helping clients assess the current vulnerabilities in their environment that puts them at risk for a successful attack. Patrick has helped health care organizations in both identifying threats and weaknesses on their networks caused by clinical devices, as well as led investigations into breaches and cyberattacks at hospitals and insurance companies.

Home office: Los Angeles, CA

The actors and the information they target

Adversary

What's most at risk?

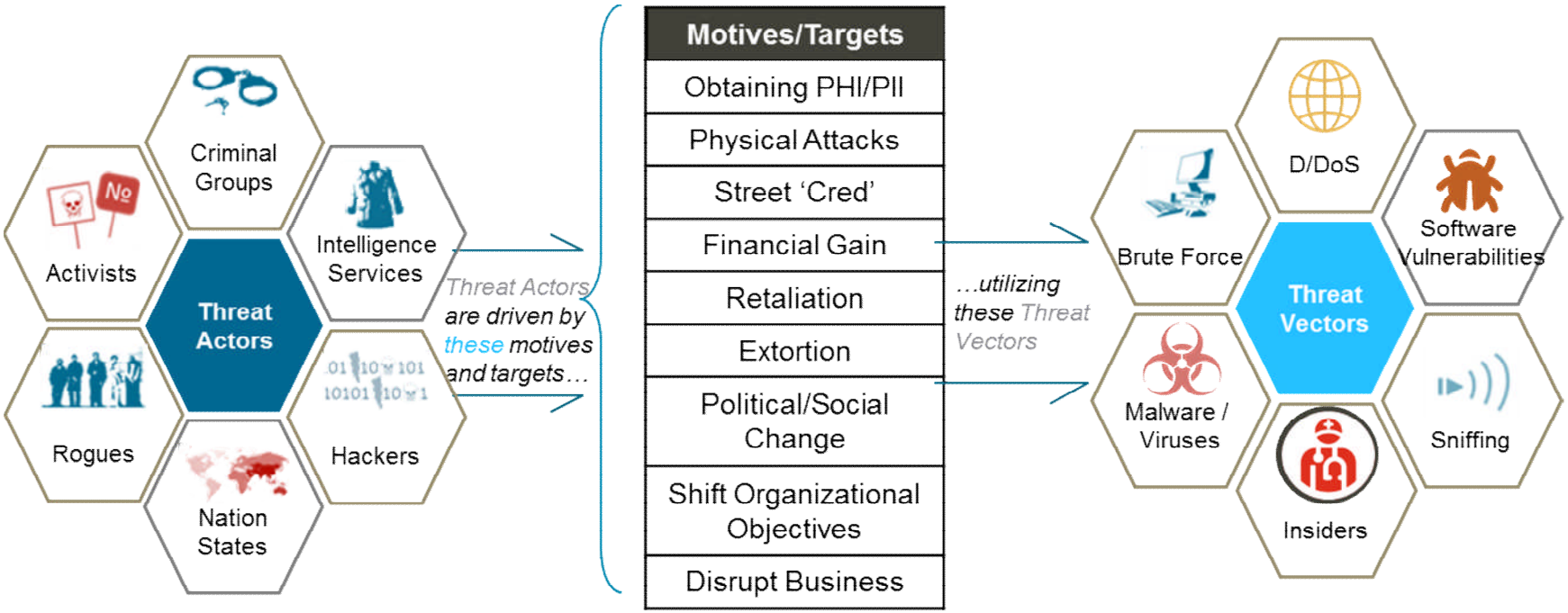
- Industrial Control Systems (SCADA)
- Emerging technologies
- Payment card and related information / financial markets
- Advanced materials and manufacturing techniques
- Energy data
- R&D and / or product design data
- Healthcare, pharmaceuticals, and related technologies
- Business deals information
- Health records and other personal data
- Information and communication technology and data

Input from Office of the National Counterintelligence Executive, *Report to Congress on the Foreign Economic Collection and Industrial Espionage, 2009-2011, October 2011.*

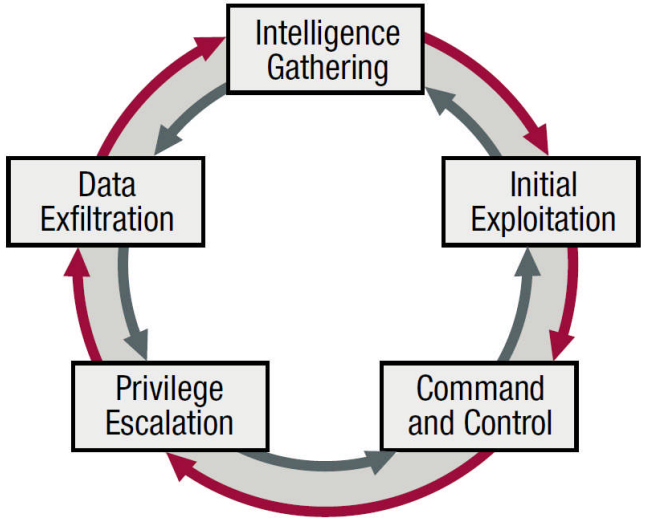
Motives and ***tactics*** evolve and what adversaries target vary depending on the organization and the products and services they provide.

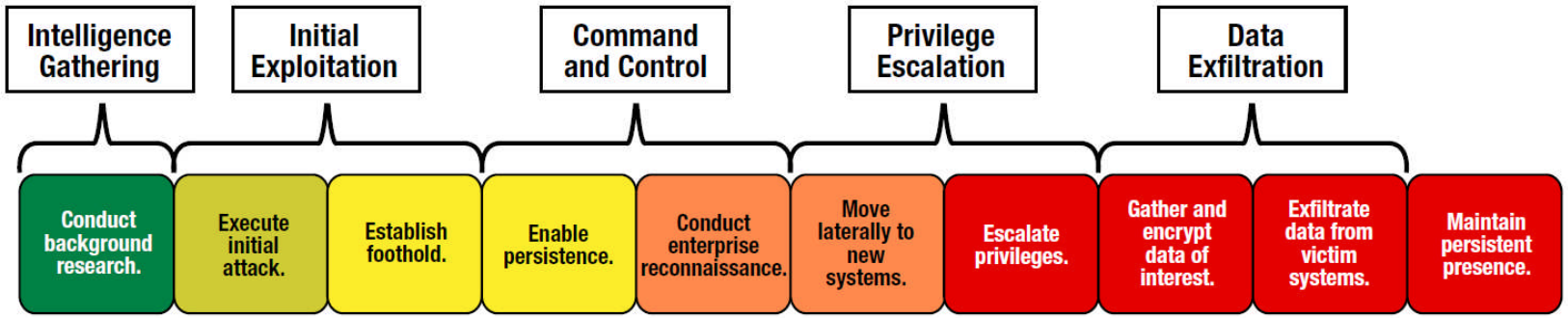
Medical Information Cyber Threat Landscape

*Many **Health Information Systems** are **vulnerable to compromise**, creating a new set of **risks** in healthcare. Threat actors are **targeting medical information** for some of the reasons listed below:*



The life cycle of a typical breach

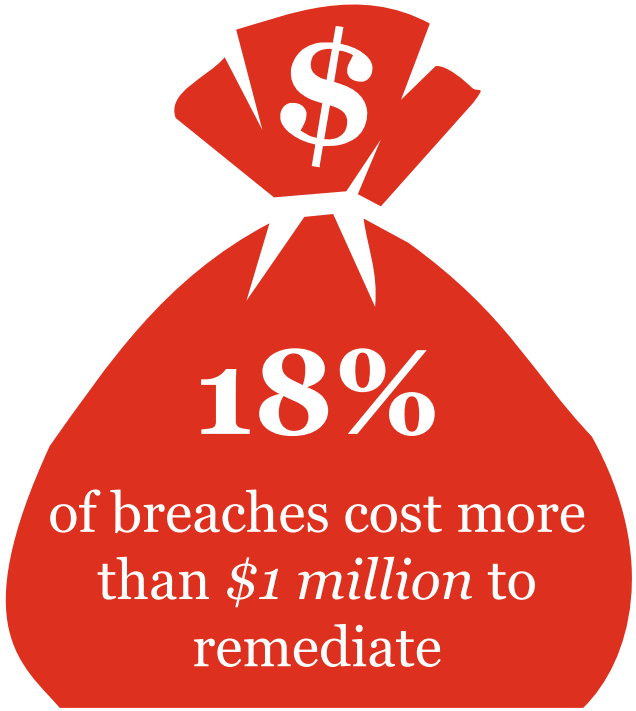




Source: ISACA – Responding to Targeted Cyberattacks

The cost of breaches.

Cybersecurity breaches are common and costly



Customers value Security over Utility!

"When using medical devices or healthcare mobile apps, I most value…"

…functionality and ease of use

…knowing my health data is secure

PwC HRI Consumer Survey 2015

Over the years, health information systems and medical devices have seen dramatic technological advances, transforming how and where information can be accessed…

Before

Devices are connected to patients physically

Data obtained from devices are stored on paper or locally

Devices are physical products

Care is hand-administered at a health care location

Physical access is needed to view health data

Now

Devices are connected wirelessly to patients and other devices

Data obtained from devices are stored in the cloud

Devices include software and even databases of health information

Care is available to patients in the palm of their hand through apps and sensors

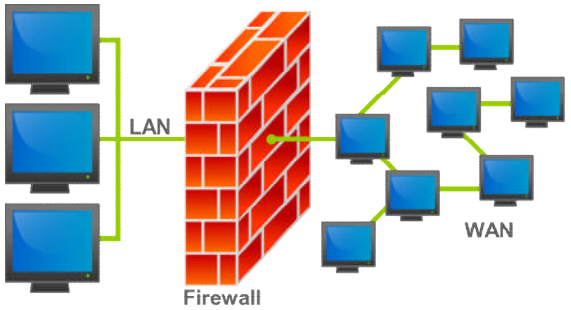
Health data can be accessed anywhere on earth

Governance of networked clinical systems– key questions

- Who is in charge of securing networked clinical systems?
- Do we know how many systems do we have and where they are?
- Do we know how much PHI/HIPAA sensitive information is stored on each, and for how long?
- Do we have enough staffing focused on secure management of these systems?
- Do we have a procedure to “harden” new systems before they are put on the network?
- Do we segregate the devices from the rest of the network or limit where they can talk?
- Can we detect if new unmanaged / “rogue” hosts have been placed on the network?
- How are vendors remotely supporting these devices?
- Do we have a way to monitor where these devices are talking and/or if they are still compliance with our standards?

Manage / monitor what is on the network

- Network restrictions
  - **Discover / map**: Determine list of clinical devices
  - **Group**: Place into one or more groups at firewall / routers / other network control devices



  - **Restrict**: Restrict from accessing Internet and/or restrict to strict list of Internet sites (i.e. for patching / software upgrades)
- Network monitoring
  - **Beaconing**: Infected device "phoning home"
  - **Data Transfer**: Large transfers of data to external sites
  - **Internal connection patterns**: Internal workstation connecting to multiple devices from unusual location or at unusual times
  - **Participation in DDoS attacks**: Your organization may be attacking others!

Health Network and Medical Device Cybersecurity Framework

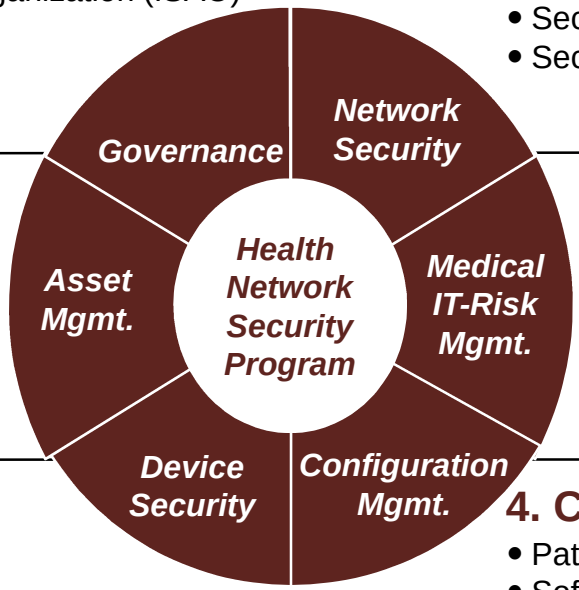
The following diagram outlines the key components of the Health Network Cybersecurity Framework, including roles and responsibilities for management of security risks:

1. Medical IoT Governance

- Development of Governance Model with clearly established roles, responsibilities, and FTE
- Information Sharing and Analysis Organization (ISAO)
- Security Strategy, Risk Mgt Policy
- Minimum Security Baseline

2. Network Security

- Network Segmentation and Access Control
- Logging and Monitoring for Malicious Activity
- Forensic Toolkit for Intrusion Analysis
- Secure Remote Access
- Secure Medical IoT Device Network



3. Medical IT Risk Management

- Vendor Risk
- Risk Profiling
- Control Profile Development
- Secure Disposal Processes
- Physical Host Security
- Device Risk Assessment Process

6. Asset Management

- Host Inventory
- Host Attribute Collection
- Asset Management
- Secure Device Procurement Processes

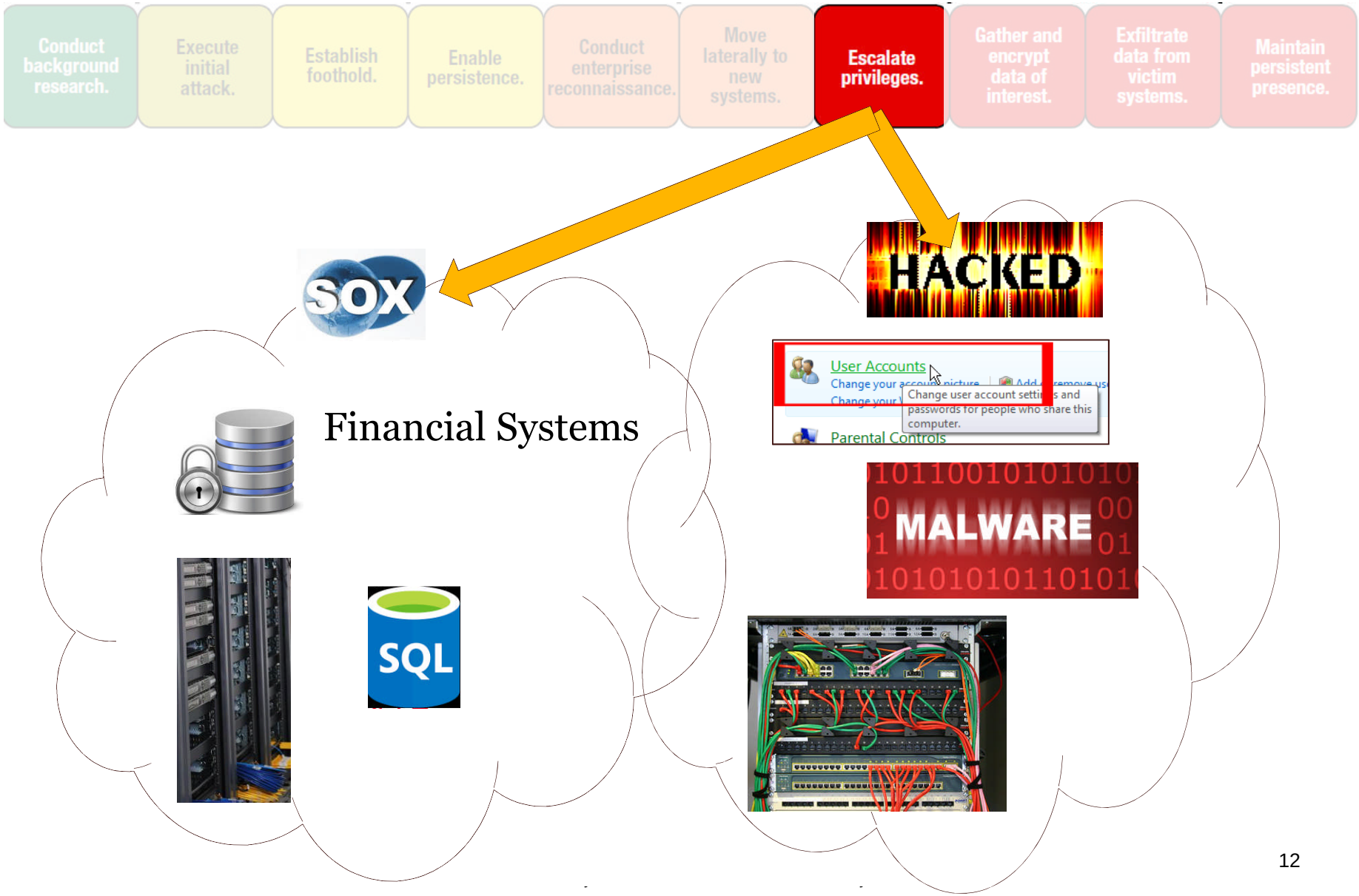
5. Host Security

- Host / Data Encryption
- Access Control and Authentication
- Wireless Security Controls

4. Configuration Management

- Patch Management Processes
- Software Version Control Processes
- Change Management Processes
- Logging and Monitoring for configuration changes

Other Considerations:
Crossover of breach into SOX and financial reporting controls



Before the breach I wish I …

People

- …knew who to call for help
- …had grabbed senior management's ear more about privacy and security initiatives
- …had an incident response team that met regularly
- …had held regular training
- …had my outside team on retainer (forensic experts, privacy counsel, and communications firm)
- …had paid closer attention to breaches in the news to observe how the market reacts to different messages
- …had considered law enforcement assistance

Process

- …knew what sensitive data I have to protect.
- …knew where my sensitive data was
- …had gone through table top exercises or hypothetical breach scenarios with the team
- …knew what applications each employee had access to
- …had considered the privacy implications of our global locations
- …was more aware of our regulatory reporting obligations

Technology

- …had network logging enabled with sufficient size allocated
- …had servers backed up and backups under control
- …had enforced records management and gotten rid of old data – especially online
- …had full disk encryption on my laptops
- …had better security measures (password standards / account management standards)
- …had DLP in place to monitor the perimeter
- …had more effectively managed security integration from acquisitions

During the breach I wish I …

People

- …had kept the circle of "people in the know" small
- …had engaged forensic experts, a Communications team, and privacy counsel from the start
- …had informed the executive leadership group / Board sooner
- …had better Project Management of the incident response process
- …had regularly met as an incident response tiger team
- …had anticipated the myriad threats from inside and out
- …thought about the impact of/from my third parties

Process

- …had acted immediately to remediate vulnerabilities
- …had not reached out to the public too soon
- …started to quantify broader exposure sooner
- …had cast the data mining net broader
- … had better documentation of actions taken
- …held standing updates with the investigative team
- …had not communicated preliminary numbers to anyone
- …had considered the business impact/risk of each new finding as we went
- … remembered that bad news doesn't get better with age

Technology

- …had taken live memory dumps before shutting down servers
- …had insisted on full forensic images of servers and laptops
- …had imaged more servers and laptops from the start
- …had pulled network logs immediately and increased log capacity
- …had pulled oldest available backups from the start
- …had reset passwords more quickly
- …had been more careful with evidence handling

After the breach I wish I …

People

- …had used the exposure to the Board to enhance my security program while I had their attention
- …had used the opportunity to revisit our governance structure - security, legal and risk management relationships
- …had prepared the employee base with a transparent, consistent message
- …had used this as an opportunity to roll out privacy training
- …had engaged my experts under privilege

Process

- …had not assumed it was over when it seemed so
- …had used this as an opportunity to build and expand my privacy and security programs
- …had documented lessons learned / done an aftermath review
- …had not over-communicated or revised numbers
- …had anticipated long term regulatory scrutiny
- …had used this as an opportunity to build privacy and security risk assessments into new initiatives
- …had used this experience to build a playbook

Technology

- …had developed a remediation plan with technology enhancements, security program improvements, data reduction
- …had tested my remediation actions
- …had considered global improvements
- …had preserved investigative evidence more effectively
- …had changed encryption, external media, USB, email policies
- …had reconsidered by cloud and third party technology providers preparedness

Thank You!

Patrick Hynes
Principal, Cyber Crime & Breach Response
T: +1-213-217-3776
E: patrick.hynes@pwc.com