

# Understanding Cybersecurity Risks in Healthcare

Presented by:  
Mac McMillan  
CEO | CynergisTek, Inc.



CynergisTek was recognized in the 2016 KLAS Security Advisory Services report for having the highest overall client satisfaction, performance and impact on security preparedness in healthcare.



CynergisTek won the 2017 Best in KLAS award for Cyber Security Advisory Services.

## Today's Presenter



- CEO & President, CynergisTek, Inc.
- Recognized as one of the top 50 Leading Health IT Experts of 2016
- Former Chair, HIMSS P&S Policy Task Force
- HIT Exchange Editorial Advisory Board
- HCPro Editorial Advisory Board
- Director of Security, DoD Agency
- Excellence in Government Fellow
- HIMSS Fellow
- U.S. Marine Intelligence Officer, Retired



**Mac McMillan**  
CEO - CynergisTek, Inc.  
[mac.mcmillan@cynergistek.com](mailto:mac.mcmillan@cynergistek.com)  
512.402.8555

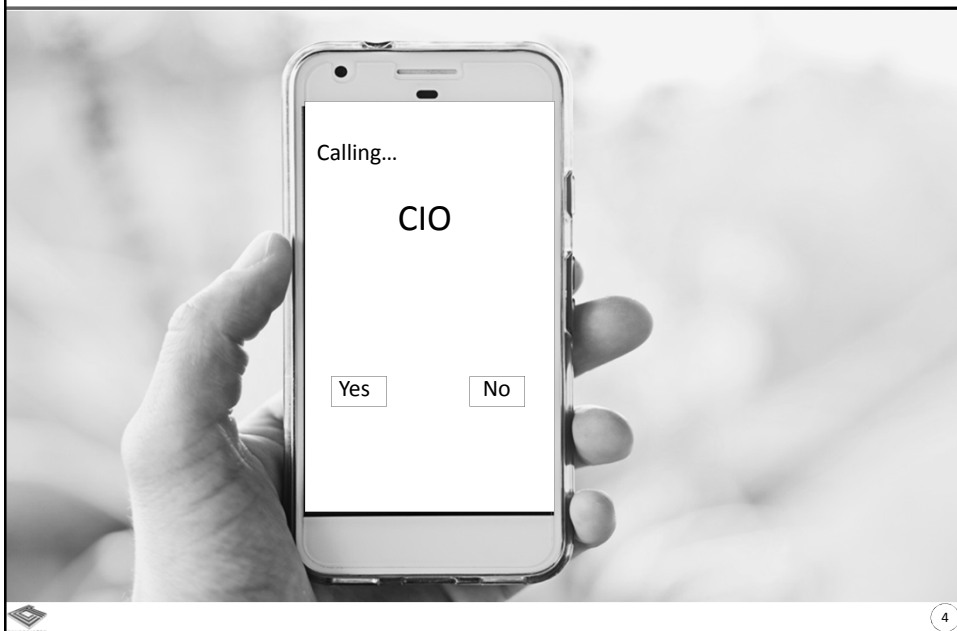


**Imagine...**



3

**After Hours...Never Good News**



4

## How Bad Could it Be...



## Pretty Bad...



9


## Changing Risk Priorities

From “Business Critical” to “Mission Critical” to “Life Critical”

Confidentiality	Availability	Text Integrity
<ul style="list-style-type: none"> <li>• PHI (HIPAA)</li> <li>• But also PII &amp; PCI</li> <li>• Account Information</li> <li>• Billing &amp; Payment Data</li> <li>• Intellectual Property               <ul style="list-style-type: none"> <li>• Clinical Trials</li> <li>• Research</li> <li>• Design &amp; Formularies</li> </ul> </li> <li>• Legal &amp; HR Documents</li> <li>• Identities &amp; Credentials</li> </ul>	<ul style="list-style-type: none"> <li>• Clinical Systems               <ul style="list-style-type: none"> <li>• EHR &amp; Specialty</li> <li>• Ancillary (PACS, Lab, Pharma)</li> <li>• ePrescription / EPCS</li> </ul> </li> <li>• Medical Devices               <ul style="list-style-type: none"> <li>• Availability of clinical services and results</li> </ul> </li> <li>• Business Systems               <ul style="list-style-type: none"> <li>• Email</li> <li>• Billing, Scheduling</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Critical Patient Data               <ul style="list-style-type: none"> <li>• Prescriptions, Medications</li> <li>• Dosages</li> <li>• Allergies</li> <li>• History</li> <li>• Diagnosis</li> <li>• Alarms</li> </ul> </li> <li>• Critical Technical Data               <ul style="list-style-type: none"> <li>• Calibration</li> <li>• Safety Limits</li> </ul> </li> </ul>

Patient Experience: “Patient Trust Zone”


Patient Harm Risk: “Patient Safety Zone”

 7

## The Cost of Insecurity

“Cybercrime damage costs will hit \$6 trillion annually by 2021”

CSO Dec. 2016

 8

## Cybercrime as a Business



- Cybercrime will cost businesses over \$2 trillion by 2019
- Trends in cybercrime all make cyber-criminals more effective
  - Cybercrime-as-a-service model gives less technically-savvy criminals access
  - Dark web marketplaces make “monetizing” stolen data as easy as buying on Amazon
  - Cybercriminals are adopting tactics previously only used by nation-state attackers



<https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion>



9

## Top Security Risks in Healthcare



Threat & Loss	No change. Nearly half of all breaches involve some form of theft or loss of a device not properly protected.
Insider Abuse	Breaches in healthcare continue to be carried out by knowledgeable insiders for identity theft, tax fraud, and financial fraud.
Unintentional Action	Breaches caused by mistakes or unintentional actions such as improper mailings, errant emails, or facsimiles are still prevalent.
Cyber Attacks	<b>Majority of breaches reported in 2017 so far involved some form of hacking and represented nearly 99% of the records compromised.</b>



10

## The Cyber Threat Spectrum



11

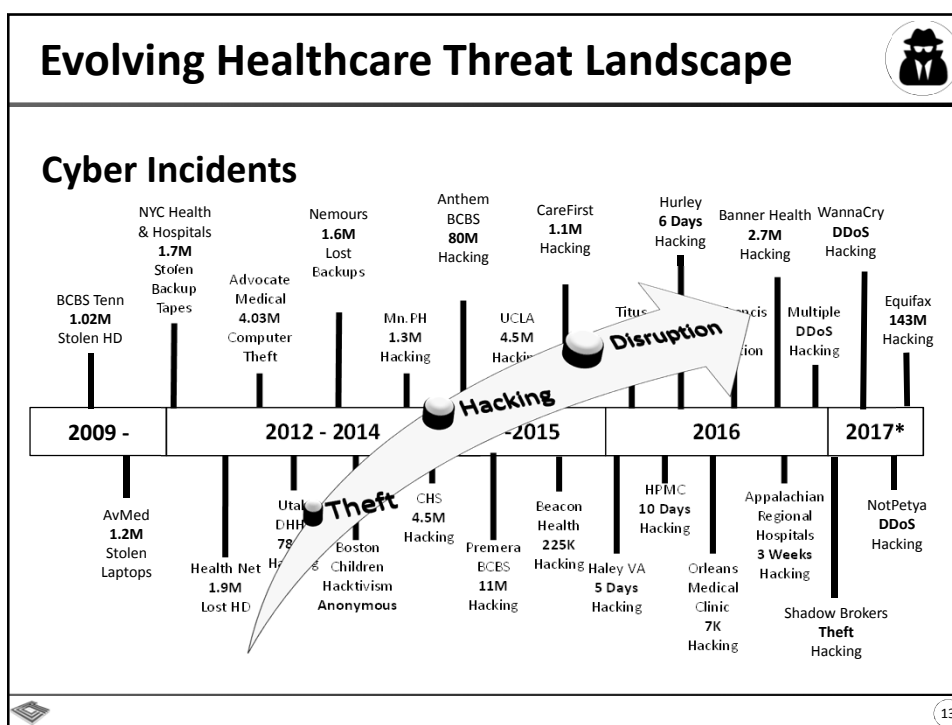
## Convergence = Opportunity



- In 2017, less than 1 in 10 providers had not adopted an EHR system, compared to the inverse in 2003
- Hacking has increase several hundred percent since 2015
- Ransomware attacks have soared to 80,000 per hour
- Breaches in 2017 are more about disruption and destruction than simple theft of data or extortion
- And the new concern is data corruption, the silent attacker



12



## Breach Statistics (2015 – 2017)

- 58% of incidents involve insiders – healthcare has the highest percentage of incidents involving internal actors
- Medical device hacking creates media hype and presents greatest patient safety issue, but its still databases and documents most often involved
- Ransomware is the top malware attack by a wide margin, 70% of attacks of malicious code were ransomware
- Basic security measures are still not be implemented, data still not being encrypted, access not controlled

Verizon 2018 PHI Data Breach Investigations Report

## Motive



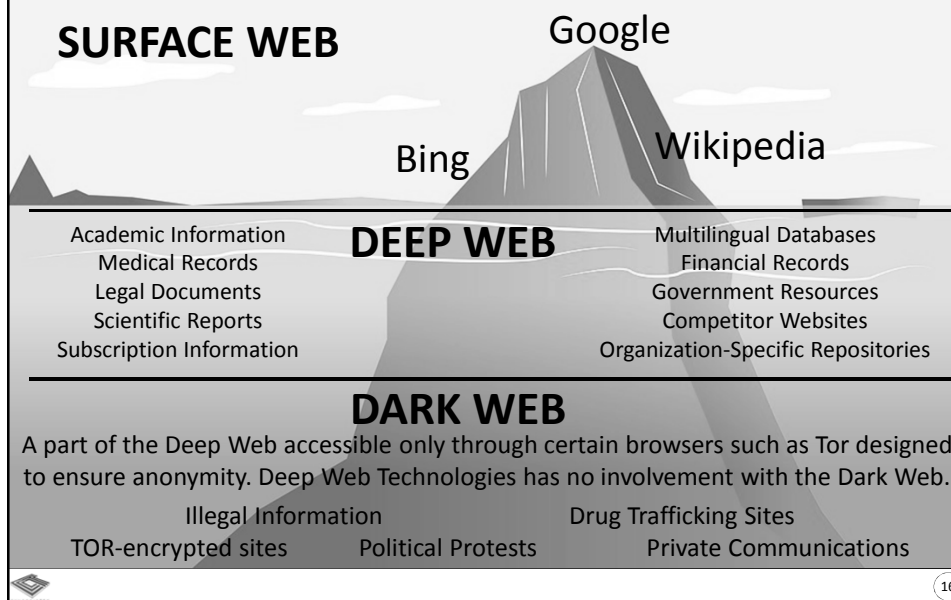
*“When there is an observable motive for a data breach, regardless of ‘whodunit,’ it’s most often money. The access that healthcare workers have presents many opportunities for identity theft and fraud such as tax fraud, establishing lines of credit, etc.”*

Verizon PHIBR 2018



15

## The Ascent into Darkness



16



## Dark Web Marketplace



A little initiative, a curious nature, a deviant behavior, a Bitcoin wallet, PGP for encrypted communication, and a TOR browser and you are in business...



**1.5 billion documents accessible on the web**

Digital Shadows



17

## Motivated, Persistent & Disruptive



- Cyber extortion
- Cyber espionage
- Hacktivism
- Targeted attacks
- Cyber terrorism
- APTs & malware
- Partners & insiders



18

## Shadow Broker Hackers



- In 2017 the “Shadow Brokers” leaked a gigabyte worth of NSA weaponized software exploits.
- Multiple zero-day attacks were included in these files.
- These tools can be used by anyone - complete, unredacted computer code.
- ***Still seeing new malware attacks today using this source code...***



19

## Cyber Espionage: Intelligence



Cyber espionage is being carried out by nation-state actors

- Large breaches such as Anthem, Premera, Community Health Systems, UCLA are suspected cases of espionage
- A case example is the OPM intrusion presumed by a Chinese group that captured security clearance documents
- But...they are also targeting industrial control systems that control and manage critical infrastructure



20

## Hacktivism: A Mixed Bag



Attacking for a cause

- 2003 started with 15 year old in his bedroom in NY
- 2008 Anonymous launches attack against Scientology
- 2011 Anonymous dumps StratFor emails, they never recover
- 2012 Anons attack WikiLeaks and ther China
- 2014 Anonymous hacked Boston Children's protesting removal of child
- 2016 Anonymous attacks Hurley Medical Center over water issue
- 2017 Anonymous joins fight against ISIS



21

## Targeted Attacks: Multiple Motivations





Typically nation-state attack groups

- "APTs are known for being highly sophisticated, using multiple vectors to attack a target network, and having unrelenting tenacity"
- Many attacks go undetected for considerable periods of time – estimated 314 days on average
- Phishing, ransomware, cryptomining have increased dramatically
- Newer disruptive attacks replacing traditional data attacks



22

**FBI Alert for Anon. FTP**



**Private Industry Notification**  
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

**22 March 2017**  
PIN Number  
**170322-001**

**Cyber Criminals Targeting FTP Servers to  
Compromise Protected Health Information**



**I See You...**



 **SHODAN**

- Google for Hackers
- Security Researchers
- Criminals





## Complacency is NOT an Option



Security protocols in WiFi have a "serious weakness" that could be exploited by in-range attackers to forcibly reinstall keys on the device, route around HTTPS and encryption, and eavesdrop on all communications and potentially manipulate data or inject malware.



OCR requires healthcare entities to use WPA2 to meet requirements for protecting PHI.



## Cyber Extortion



- Two forms: Crypto ransomware (data) and Locker ransomware (system)
- Today multiple variants of malware using sophisticated encryption, crypto currency, TOR networks, etc.
- No longer indifferent – everyone is a target, employ destructive threat as incentive
- Fast becoming webs most profitable attacks
- 100% profitable as thieves use your resources and electricity
- High % of payees, lowering data prices and mining values rising



***The United States is the largest target worldwide by a huge margin.  
"nearly 70% of victims report paying ransom"***



## Ubiquitous Is The New Paradigm



*20B networked IoT devices expected by 2020*

- Smart phones
- IoT
- Social media
- POS systems
- Medical devices
- Removable media (USBs)
- SPAM & email
- Applications
- Smart TVs
- CCTV cameras
- Environmental systems
- Downloads
- Attachments
- Browsers
- Wearables
- Telehealth



**56% don't inventory IoT**  
**Less than 20% can ID**  
**70% consider IoT a high threat**  
**Only 29% monitor IoT for threats**  
**21% hacked by IoT**

*Ponemon Institute*

*Who's watching your house?*



27

## Healthcare as a Critical Infrastructure



Attacks against nation states (WannaCry/Petya), attacks against communications (Mirai) and attacks against power (gas pipeline firms in U.S.) all designed to disrupt critical infrastructure and the businesses and services they support. Healthcare is a collateral target, but could be the "target".



28

## Are We Ready?



60% of IT security experts who responded to the Black Hat Attendee Survey believe that a successful attack on U.S. critical infrastructure will happen within two years. Also, only 26% of respondents believe that the country is prepared to handle such an attack.

*Dark Reading, July 10, 2017*



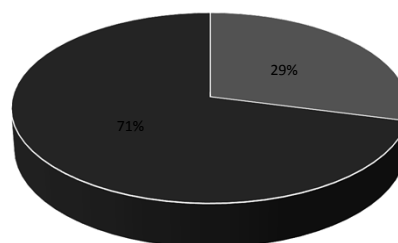
29

## Human Nature WILL NOT Change



- Insider threats have continued to grow year over year since 2010
- Many CIOs recognize people with elevated privileges are a big risk
- Contractors/service providers have become a big concern
- Most pharmacy data thefts and fraud are the work of insider
- Most feel awareness training is failing
- Traditional compliance/rule based auditing is failing

**Insiders are Responsible for 90% of Security Incidents**



■ Malicious ■ Unintentional



30

## Supply Chain Risks



- **Printers** returned to leasing company compromise thousands of patient records
- 400 hospitals billings delayed as clearinghouse hit with **ransomware**
- **Failure to apply fix** to router results in compromise and loss of 4.5M records
- Mistake during **software upgrade test** results in 8,000 letters mailed
- Three hospital networks compromised by **medical device hack** called MedJack
- 450,000 medical records exposed when vendor's software engineer sets up **unauthorized GitHub database** without security
- Hospital network taken offline by **ransomware attack** for more than week due to two Citrix servers left vulnerable by vendor
- Hospitals lose critical EHR when hosted SaaS site compromised by **IoT attack**
- Hospital suffers over 680 assets encrypted by **ransomware** in less than two hours because contractor installs auto-deploy software on network remotely
- Hospitals lose dictation/transcription capability when vendor hit with **ransomware attack**
- NJ hospital fined by state because vendor makes **unauthorized change** to cloud hosted database exposing PHI
- And, on and on it goes...



31

## Emerging Threats



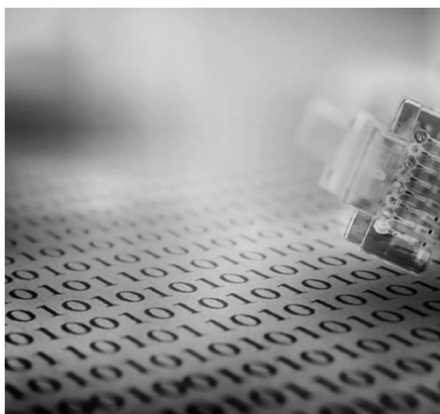
- Artificial intelligence and machine learning
  - Not from the detection and protection side . . .
  - from cyber criminals
- File-less and file-light malware
- Supply chain



32



## Security Challenges are Persistent



- Configuration management
- Securing end points
- Encryption of data
- Prevention of leakage
- Log management
- Establishing identity
- Monitoring system activity
- Accounting for access
- Ensuring minimal necessary
- Technical testing
- Data search/control
- Asset management



33

## Mitigating The Threat



- ☐ Keep up with Threat intelligence
- ☐ Maintain a current and accurate asset inventory
- ☐ Have an enterprise wide patching solution
- ☐ Implement effective mitigating controls
- ☐ Equip your enterprise with effective detection
- ☐ Develop and practice a broad incident response plan



34

## Where We Are Today



Top CISO concerns for 2018

**70%: lack of competent in-house staff**

**67%: data breach**

**59%: cyberattack**

**54%: inability to reduce employee negligence**

**48%: ransomware**

*Source: Ponemon Institute Survey and Opus*

**84% of HCOs do not have a cybersecurity leader**

**Only 15% of organizations have a CISO currently in charge**

**Over 50% of all respondents said they do not conduct regular risk assessments**

**92% of C-suite said data breach and cyber still not a key area of focus for the board**

*Q4 2017 Black Book survey (323 strategic decision makers in US HCOs – provider and payer)*



35

## Priorities



**89% of respondents said their 2018 budgets were dedicated to business functions**

- **"Only a small fraction" was being saved for cybersecurity**

*Q4 2017 Black Book survey (323 strategic decision makers in US HCOs – provider and payer)*



36

## Cybersecurity Reality



“Executives need to recognize that compliance does not equal security and checking the box is no longer sufficient.”



37

## Questions?



Questions?

**Mac McMillan, FHIMSS, CISM**  
**President & CEO**  
mac.mcmillan@cynergistek.com  
512.402.8555



38