Ransomware in Healthcare – Risk, Prevention and Response

Free registration sponsored by

Disclaimer

Conference presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the participants individually and, unless expressly stated to the contrary, are not the opinion or position of the Workgroup for Electronic Data Interchange, its cosponsors, or its committees. The Workgroup for Electronic Data Interchange does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

About the Presenter

John DiMaggio, Chief Executive Officer, Blue Orange Compliance

John DiMaggio is the co-founder and CEO of Blue Orange Compliance, a firm dedicated to helping health care providers and business associates navigate the required HIPAA and HITECH Privacy and Security regulations. John is a recognized healthcare information compliance speaker to state bar associations, HIMSS, Health Care Compliance Association (HCCA) and long term care associations including Long Term and Post Acute Care (LTPAC), NAHC, LeadingAge, ALFA and many state Healthcare Associations. John is also a LeadingAge CAST Commissioner.

John's extensive healthcare experience includes Chief Information Officer with NCS Healthcare and Omnicare; senior operations roles with NeighborCare, and general consulting to the industry. John began his career as a key expert in Price Waterhouse's Advanced Technologies Group and served on several national and international standards organizations including the American National Standards Institute (ANSI) and the International Standards Organization (ISO).

John is the named inventor for multiple healthcare technology and process patents. He holds an MBA in Finance from Katz Graduate School of Business and a BS in Computer Science from the University of Pittsburgh.

LeadingAge CAST Cybersecurity

LeadingAge ABOUT NEWSROOM CENTERS RESOURCES ADVOCACY EVENTS MEMBERS CONSUMERS

Recent News

What Have We Done for You Lately? – January 2018

You Can Fight Back Against Cybercriminals

Don't Assume You're Immune to a Cyberattack

CAST Releases Cybersecurity White Paper

CAST | DECEMBER 20, 2017 | BY DONNA CHILDRESS

Print this Article

White paper helps providers recognize and mitigate risks—and knowv how to respond if attacked.

VOICE YOUR OPINION

TELL YOUR FRIENDS

CAST has released a Cybersecurity White Paper and a Benchmarking Questionnaire to help LeadingAge members and other aging services organizations understand what cybersecurity threats are, how to mitigate risks, and how to respond if attacked. The Benchmarking Questionnaire will help providers identify best practices, and where providers may be at risk, so that they can work to plug those vulnerabilities.

Agenda

- HealthCare Information Landscape
- Cybersecurity in Healthcare Overview
- Ransomware Overview
- Encryption Methods & Architecture
- Ransomware and HIPAA
- Protect, Prepare, Respond
- Ransomware Case Study – Erie County Medical Center

Changes to Healthcare

- Internet of Things (IoT)
- Mobile Access
- Cloud Computing
- Mergers, Acquisitions, Divestitures
- Borderless Perimeter

Healthcare Landscape

Healthcare

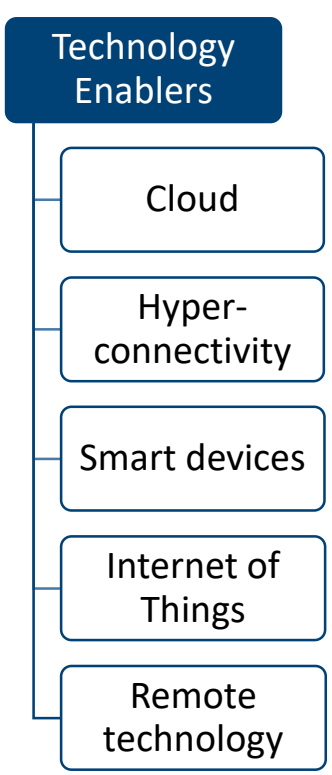
- Electronic
- Push toward interoperability
- Cost shift outside 4 walls
- Information outside 4 walls

Acute Care

- EHR start since 2010
- Meaningful Use Stages
- Receiving incentives

Long Term Post-Acute Care (LTPAC)

- Push toward interoperability
- Implementing EHR
- Implementing applicable technology



Largest Healthcare Breaches of 2017

Position	Breached Entity	Entity Type	Records Exposed	Cause of Breach
1	Commonwealth Health Corporation	Healthcare Provider	697,800	Theft
2	Airway Oxygen, Inc.	Healthcare Provider	500,000	Hacking/IT Incident
3	Women's Health Care Group of PA, LLC	Healthcare Provider	300,000	Hacking/IT Incident
4	Urology Austin, PLLC	Healthcare Provider	279,663	Hacking/IT Incident
5	Pacific Alliance Medical Center	Healthcare Provider	266,123	Hacking/IT Incident
6	Peachtree Neurological Clinic, P.C.	Healthcare Provider	176,295	Hacking/IT Incident
7	Arkansas Oral & Facial Surgery Center	Healthcare Provider	128,000	Hacking/IT Incident
8	McLaren Medical Group, Mid-Michigan Physicians Imaging Center	Healthcare Provider	106,008	Hacking/IT Incident
9	Harrisburg Gastroenterology Ltd	Healthcare Provider	93,323	Hacking/IT Incident
10	VisionQuest Eyecare	Healthcare Provider	85,995	Hacking/IT Incident
11	Washington University School of Medicine	Healthcare Provider	80,270	Hacking/IT Incident
12	Emory Healthcare	Healthcare Provider	79,930	Hacking/IT Incident
13	Salina Family Healthcare Center	Healthcare Provider	77,337	Hacking/IT Incident
14	Stephenville Medical & Surgical Clinic	Healthcare Provider	75,000	Unauthorized Access/Disclosure
15	Morehead Memorial Hospital	Healthcare Provider	66,000	Hacking/IT Incident
16	Primary Care Specialists, Inc.	Healthcare Provider	65,000	Hacking/IT Incident
17	Enterprise Services LLC	Business Associate	56,075	Unauthorized Access/Disclosure
18	ABCD Pediatrics, P.A.	Healthcare Provider	55,447	Hacking/IT Incident
19	Network Health	Health Plan	51,232	Hacking/IT Incident
20	Oklahoma Department of Human Services	Health Plan	47,000	Hacking/IT Incident

Cyber Security: Theory

- If something is connected it to the Internet, someone will try to hack it.
- If what you put on the Internet has any value, someone will invest time and effort to steal it and market it.
- Whatever the price paid for the information is much less than the value of the information to the owner
- If you don't invest in protecting the information, it will be stolen

Cyber Risk in Healthcare

1. Downtime/Business Disruption
2. Office for Civil Rights HIPAA Violation (Breach)
    - Investigation
    - Fines/Penalties
    - Corrective Action Plan
3. Civil Litigation
4. Reputation Damage
5. Individual Notification/Credit Monitoring Costs
6. Legal Expenses
7. Forensic/Repair

Cyber Attack Techniques

Motivators

1. Money
2. Fun
3. Social/Political Cause
4. Information

Best Practice Stages

1. Reconnaissance
2. Scan
3. Gain Access
4. Maintain Access
5. Clear Tracks

Attack Stages - Analogy

Stage	Burglar - Your House	Hacker - Your Organization
Reconnaissance	• Drive by - schedule • Look at county auditor site • Facebook	• LinkedIn • Google • SEC Filings • Website
Scanning	• Check doors, windows • Try garage codes	• Scan ports • Phone calls • Physical visit
Gain Access	• Enter through window	• Phishing • Malware • Social
Maintain Access	• Add garage code • Find spare key	• Create back door • Create user
Clear Tracks	• Leave house as was • Remove fingerprints	• Clear audit logs

Common Misconceptions

- It will never happen to me
- Our network is secure
- We are not a big company
- We don’t have personal information, so we aren’t a target
- We have never been attacked
- I have Cyber-Insurance

Healthcare has largest number of records breached by industry

Stolen health record worth 10x stolen credit card number

Ransomware

- Malware
- Enters through infected Ads, files, network weaknesses
- Encrypts files
- Ransom demanded for key
- Usually no data is stolen

Ransomware Business

- 500% Increase over past 2 years
- 3500% Increase in domains hosting ransomware
- 39% of organizations estimate they would be down for multiple days in event of an attack
- $1 Billion - Total Cost of Ransomware in 2016

Cybersecurity Insiders: https://www.cybersecurity-insiders.com/portfolio/2017-ransomware-report/)

Hackers Marketplace

- Ransomware as a Service (with warranty)
- Compromised servers for rent
- Free hacking tools readily available

Cyber Statistics

Cyber criminal attacks (hacking) as root cause of breaches:

- Breaches experienced in last 2 years: 50%
- 2015: 45%
- 2011: 20%

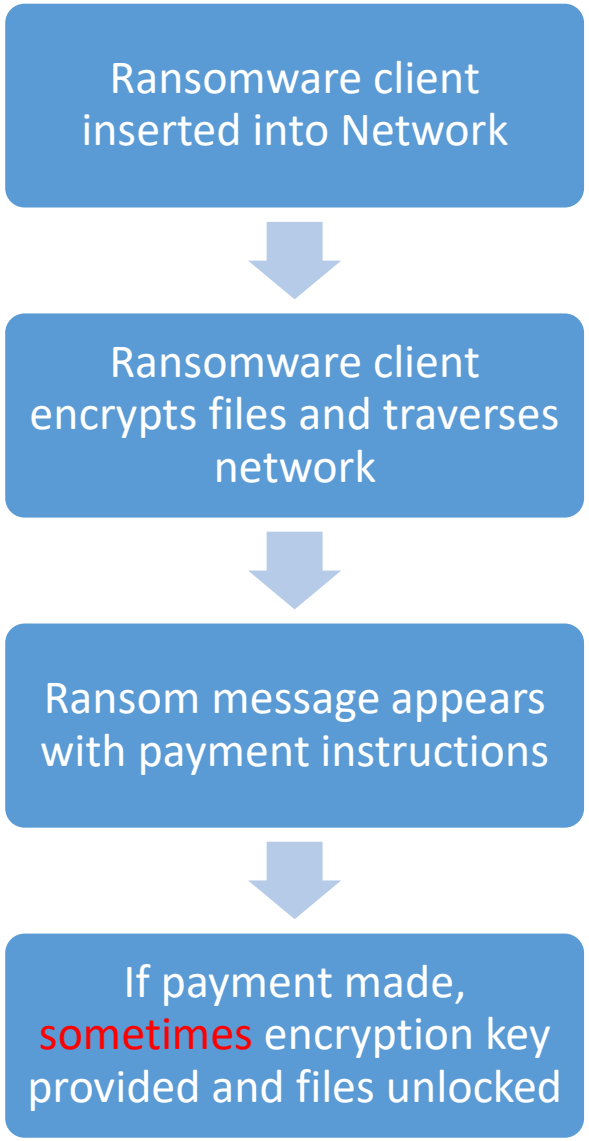
Next leading cause: Error by 3rd party partner (Business Associate)

Average number of days before a breach is detected: 201 days

Source: Ponemon Institute: Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data

Ransomware Components

- Encryption Client/Script
- Encryption Algorithm
- Encryption Key
- Ransom Message
- Optional Command and Control Server (CCS)
- Bitcoin Wallet Id
- Price



Ransomware Strains

- Apocalypse
- Cerber
- CryptoWall
- CTB Locker
- Jigsaw
- Locky
- Petya
- TeslaCrypt
- TorrentLocker
- Unlock92
- SamSam

Ransomware Types

- Malicious
- Financial-Based
  - Amateur
  - Business Grade – Reputable??
- Techniques
  - Spray
  - Targeted

Ransomware Entry Points

- Network Configuration
  - Exposed Server Message Block (SMB)
  - Remote Desktop Protocol (RDP)
- Unpatched Software
- Malicious Website
- Phishing email link or attachment
- USB Drive
- Weak passwords
- …

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

Sunday, April 15, 2018 Wang Wei

Internet-connected technology, also known as the Internet of Things (IoT), is now part of daily life, with smart assistants like Siri and Alexa to cars, watches, toasters, fridges, thermostats, lights, and the list goes on and on.

But of much greater concern, enterprises are unable to secure each and every device on their network, giving cybercriminals hold on their network hostage with just one insecure device.

Since IoT is a double-edged sword, it not only poses huge risks to enterprises worldwide but also has the potential to severely disrupt other organisations, or the Internet itself.

National Cyber Awareness System:

TA18-106A: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices

04/16/2018 01:25 PM EDT

Original release date: April 16, 2018

Systems Affected

- Generic Routing Encapsulation (GRE) Enabled Devices
- Cisco Smart Install (SMI) Enabled Devices
- Simple Network Management Protocol (SNMP) Enabled Network Devices

Overview

Ransomware – How it Spreads

- Network File shares
- Local or Domain Admin Rights on Accessed Computer/User

What to do?

- Protect
- Prepare
- Respond

Ransomware – Protect

- Make sure networks are configured correctly
- Implement “Least Privileged” to ensure users have minimal access and rights to do their jobs
- Limit file shares to only users that require the information
- Make sure systems are patched – run regular internal and external vulnerability scans
- Make sure backups are not on-line or accessible from user accounts
- Constantly educate your staff

Ransomware – Prepare

- Know your backup recovery times (RTO) and recovery points (RPO)
- Know your cyber insurance policy and process/cost/coverage to trigger
- Know your local FBI/law enforcement contacts
- Know your healthcare/cyber expertise legal counsel
- Have a good PR/Messaging to employees, public
- Research how to pay a ransom (bitcoin)
- Have polices and procedures, regulatory components in case of investigation or litigation
- Have cyber incident/ransomware plan in place and practiced
- Have ransomware identify tools available – identify strain

Ransomware – Respond

- Implement your plan
- Contact law enforcement
- Communicate to all stakeholders
- If recovered from backup, enter data generated or modified since your last backup recovery point

The after-party

- Perform HIPAA Breach Risk Assessment
- Check integrity of data

So…You Received the Ransomware Note

- Shutdown Systems?
- Identify Strain to determine if public key is available
- Revert to Paper?
- Pay the Ransom?
  - Approximately 75%
  - Price
  - Recovery Time
- Contact Cyber Insurance Company?
- Contact Law Enforcement?
- Contact Legal?
- Implement your ransomware plan!!!

Test Scenario

- Simulate user opening an infected email
- Helpdesk reports multiple calls of slow systems and limited access to files. Other departments follow.
- Ransom message appears

HIPAA – Who needs to comply?

- Covered Entity (CE):
  - Health Plans
  - Health Care Providers: Any provider who electronically transmits health information in connection with standardized transactions regulated by HIPAA (e.g., claims transactions, benefit eligibility inquires, etc.).
  - Health Care Clearinghouses: Entities that process nonstandard information they receive from one entity into a standard format (or vice versa).
- Business Associate (BA):
  - A person or organization (other than a member of the CE's workforce) that performs certain functions or activities on behalf of the CE that involves the use or disclosure of protected information.

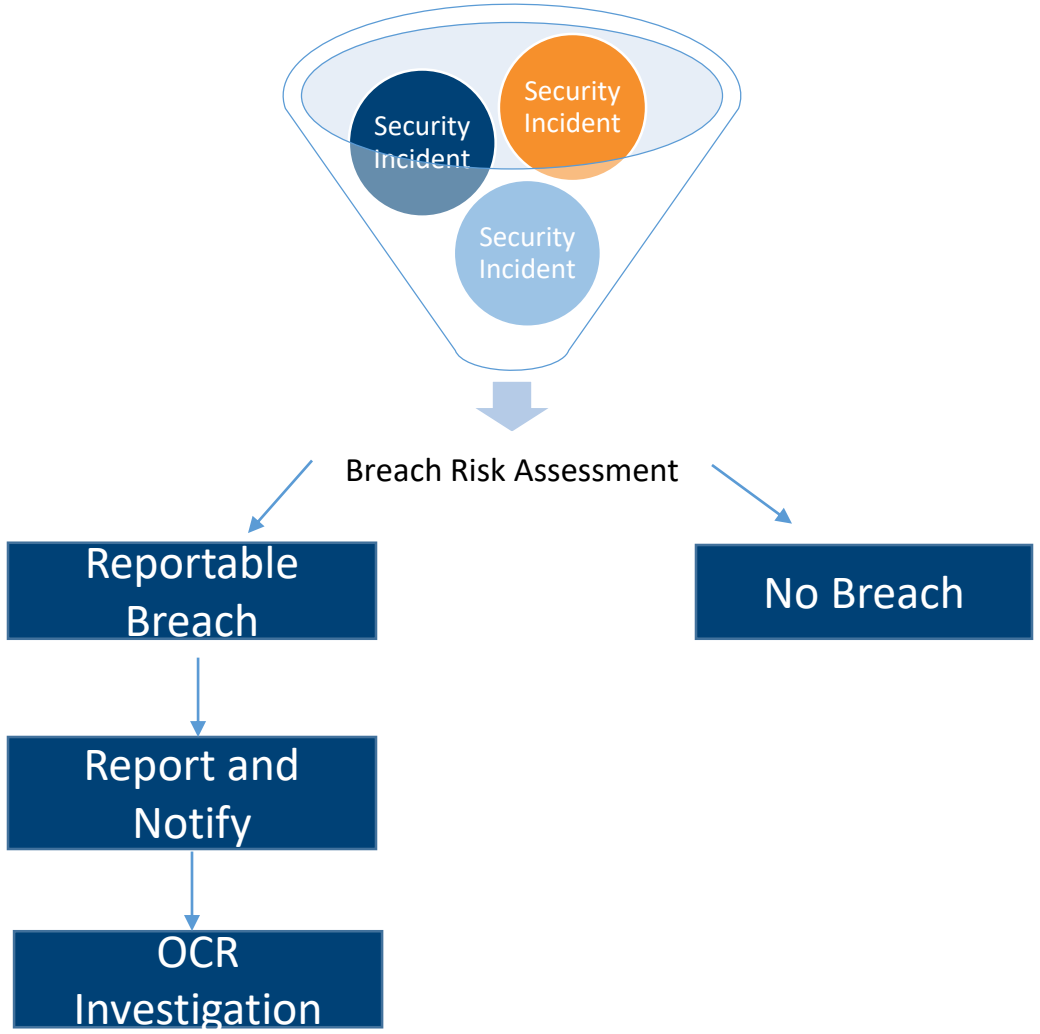
HIPAA Breach Definition

"The acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E ("HIPAA") which compromises the security or privacy of the protected health information."

Breach Causes:

- Social Engineering
  - Phishing
  - Spear Phishing
- Wireless
- Stolen Passwords
- External Perimeter
- Attack web application
- Vendors
- Human Error

Breach Analysis and Process



Breach Process Overview

- Contact cyber insurance carrier if applicable
  - May require certain legal, forensics firms
- Recommend contact attorney for attorney client privilege
- Determine individuals affected
- > 500 notify individuals, media, HHS
- 60 days from discovery
- Press release

Erie County Medical Center – Case Study

- 602 Bed Hospital in Buffalo, NY
- Level 1 Trauma Center

- Incident Stats
  - Total Cost $10M
    - $5M incident response and cleanup
    - $5M in damages/O.T., etc
  - Full recover took over 30 days

Erie County Medical Center – Timeline

- **April 2, 2017** – Initial system compromise
- **Day 0 - April 9** – Ransom note appears, decision to shut all systems down, plan organized to wipe all systems, recover from backup and revert to paper
- **Day 2 - April 10** – Decision not to pay ransom and begin recovery. Wiping and recovery begins
- **Day 10 - April 19** – First of 6,000 affected computers are brought back on-line, ER and ICU given priority
- **Day 15 - April 24** – EHR available in read-only mode, electronic patient registration restored for high priority areas, financial systems partial, temporary employee email, electronic communication with labs, etc. begins
- **Day 26 – May 5** –Staff can update EHR, paper used during outage entered into system
- **Day 29 – May 8** – Physicians can communicate with lab, radiology and other departments
- **Day 33 – May 12** – Electronic prescribing restored

Erie County Medical Center – Bright Spots

- Erie County Medical Center – New Use for HIE
  - HEALTHeLINK HIE
  - Assisted in providing access to HIE data during outage for medical record access stored by the HIE
- Prior to attack, cyber insurance increased from $2M to $10M

Erie County Medical Center – Key Points

- System Compromise
  - Attackers identified open port 3389 and Remote Desktop Protocol (RDP) exposed to the internet
  - Attacker cracked a weak password by password spray or other means
  - Attackers used windows utility to manually deploy ransomware client on multiple machines
- Ransomware Note, Price and Decision
  - Note indicated files are encrypted and demand 24 bit coins ($30,000 at the time)
  - Decision made to not pay ransom, wipe all computer and restore from backup
- Implemented Response Plan
  - Plan based on power outage scenario

Additional Information

LeadingAge CAST Cyber Security Whitepaper and Benchmarking tool

https://www.leadingage.org/cast/cast-releases-cybersecurity-white-paper

Download OCR Audit E Book

www.blueorangecompliance.com

Download Cyber Security E Book

www.blueorangecompliance.com

OCR Cyber Guidance

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

OCR Audit Protocol

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

HHS Breach “Wall of Shame”

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Thank You

Contact Info and Additional Information

John DiMaggio, CEO
Blue Orange Compliance
john.dimaggio@blueorangecompliance.com
614.567.4109

Thank You

Thank you to

For sponsoring this webinar