Ransomware and Cryptojacking in Healthcare- Risk, Prevention and Response

UMA Annual Meeting – May 2019

About the Presenter

John DiMaggio, Co-Founder, CEO, 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 healthcare associations including Long Term and Post Acute Care (LTPAC), National Association for Homecare and Hospice, LeadingAge, Argentum 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.

About Blue Orange

Specialize in healthcare information privacy and security solutions.

LeadingAge CAST Commissioner

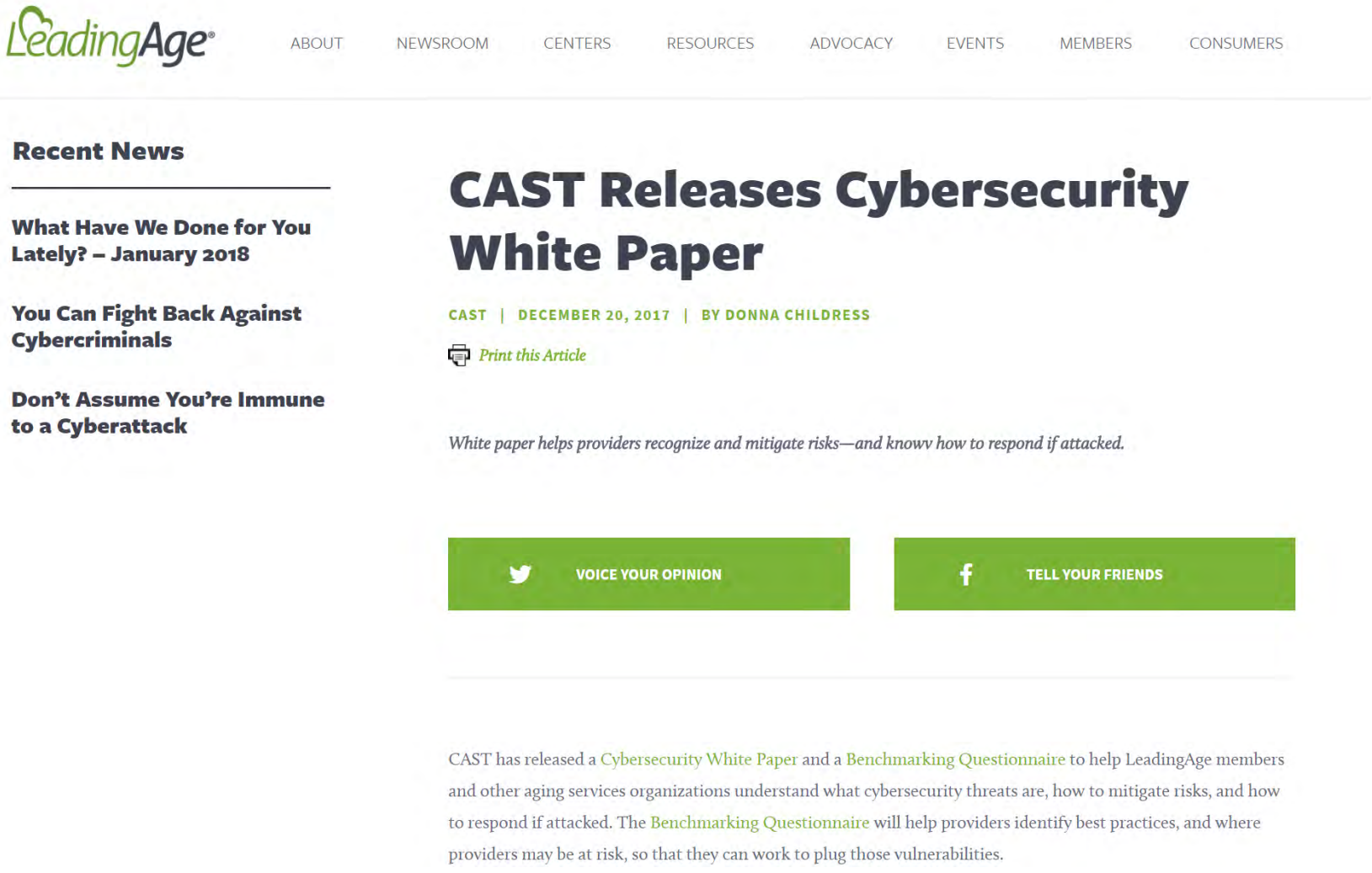
Long Term Care Expertise

National Provider

We understand that each organization is busy running its business and that human capital is limited. Our high-tech, low-touch, cost-effective approach provides continuous, maximum information and guidance and requires minimal staff time and engagement.

- Security Risk Assessments and Guidance
- HIPAA Privacy and Security
- Cyber Security Services
- Penetration Testing
- Analytics
- HITRUST Assessor

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
- Cryptojacking Overview
- Ransomware, Cryptojacking 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

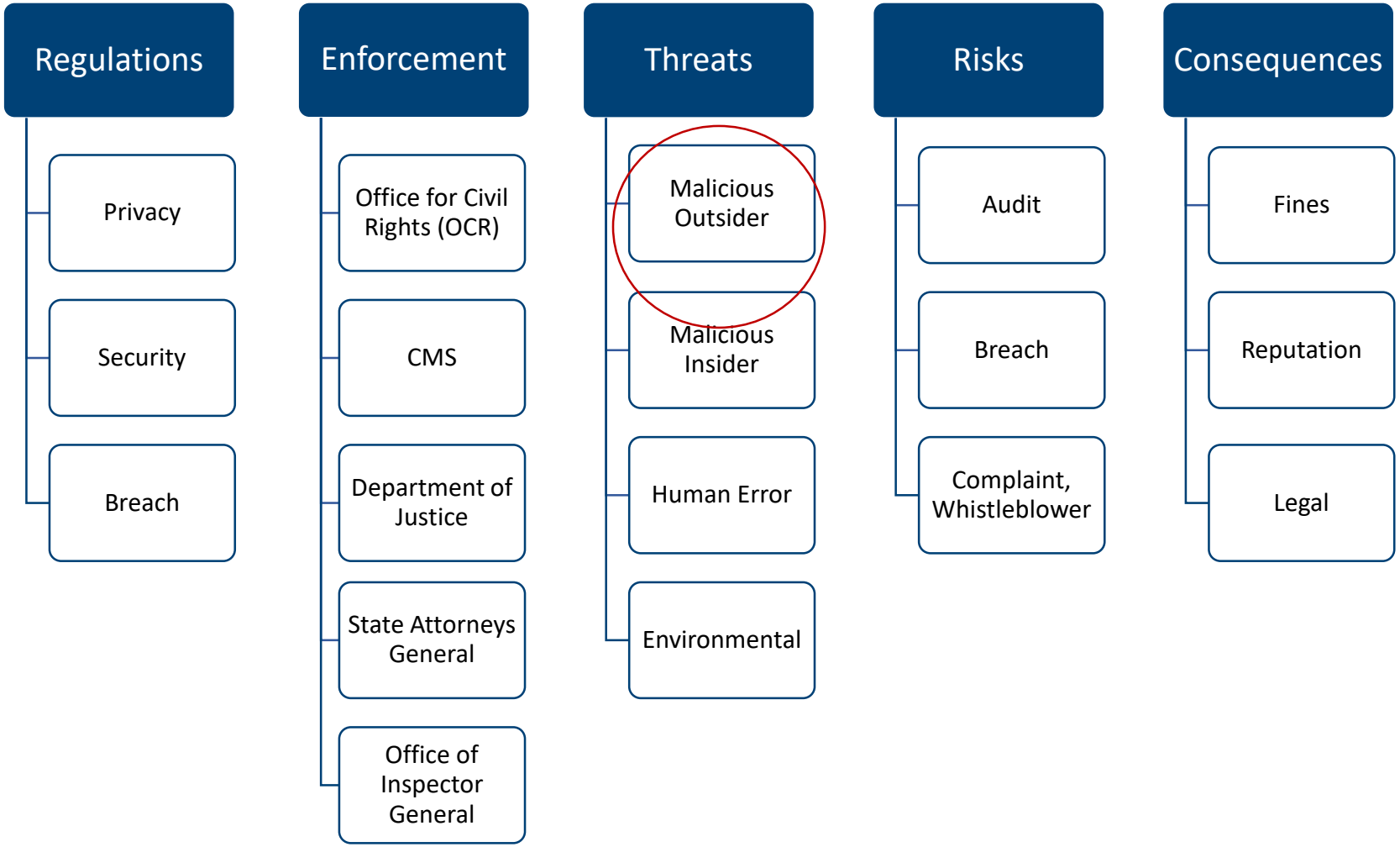
Technology Enablers

- Cloud
- Hyper-connectivity
- Smart devices
- Internet of Things
- Remote technology

Healthcare Readiness

- Maturity Behind Other Industries
- Shortage of Skilled Security Professionals
- LTPAC Behind Acute Care
- Street Value of Information

Privacy and Security

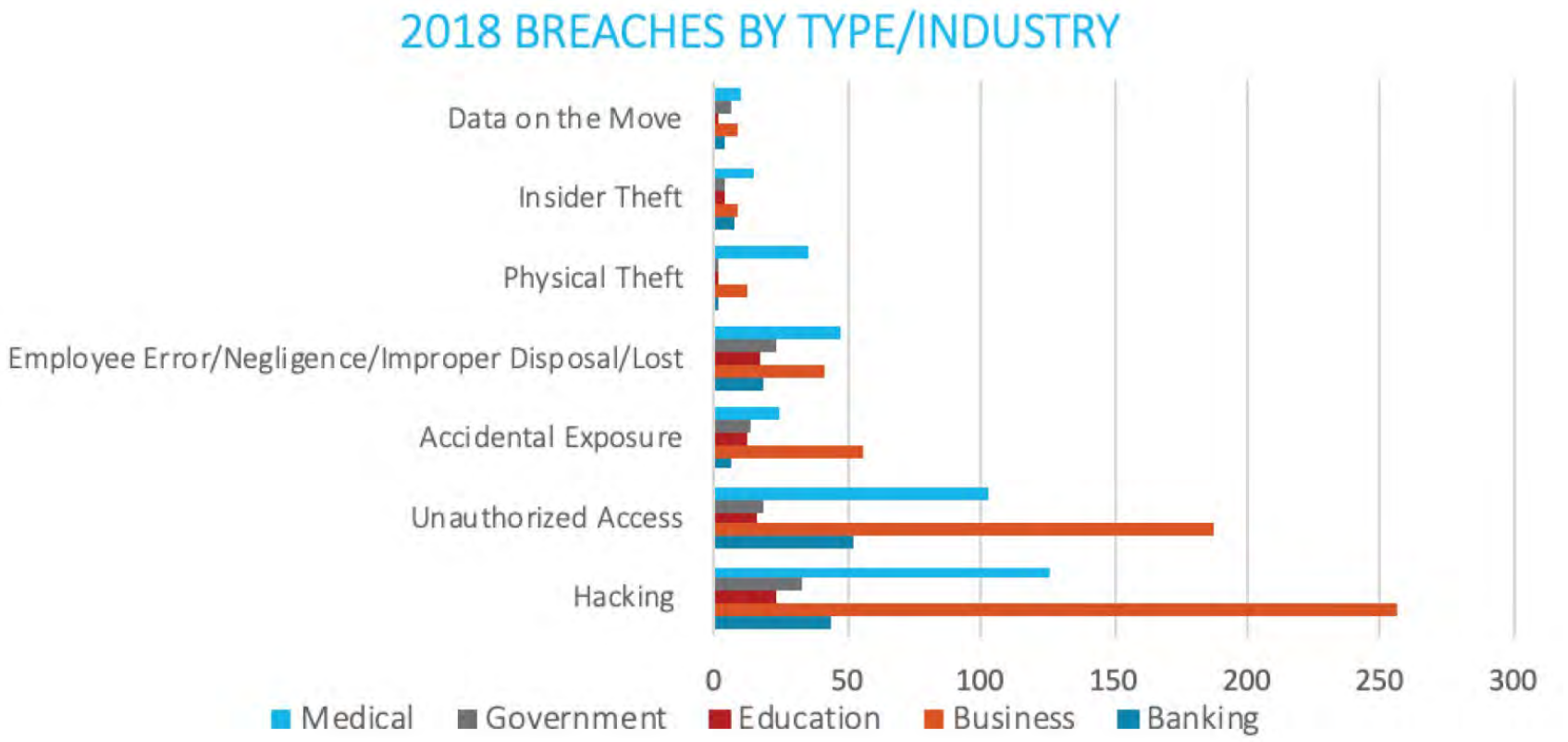


Statistics

DATA BREACH ANNUAL COMPARISON (2018 vs. 2017)				
	2018		2017	
Industry	# of Breaches	# of Records Exposed	# of Breaches	# of Records Exposed
Banking/Credit/Financial	135	1,709,013	134	3,230,308
Business	571	415,233,143	907	181,630,520
Education	76	1,408,670	128	1,418,455
Government/Military	99	18,236,710	79	6,030,619
Medical/Healthcare	363	9,927,798	384	5,302,846
Annual Totals	1,244	446,515,334	1,632	197,612,748

Source: IRTC 2018 END-OF-YEAR DATA BREACH REPORT

Statistics



Source: IRTC 2018 END-OF-YEAR DATA BREACH REPORT

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

Hackers Marketplace

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

Privacy and Security and Senior Living

1. Combination of HIPAA Covered/Non-Covered Entities
2. Usually residents, employees and information move across the Entities
3. CMS Regulations also apply
4. Have protected health information (PHI) and sensitive resident financial information
5. Demonstrate to current and prospective families/residents
6. Financial resources limited
7. I.T. focused on “lights-on” activities
8. Limited in-house privacy and security knowledge
9. Current resources busy running business

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
- The senior living industry is to small to be noticed

Healthcare has largest number of records breached by industry

Stolen health record worth 10x stolen credit card number

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 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

Cyber Statistics

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

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

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

Penetration Test Stats

- 15-25% of your workforce fall for phishing
- 15-20 minutes – Access to System - very weak passwords
- 3 hours to get control
- Another 30-60 minutes to get your PHI

Ransomware

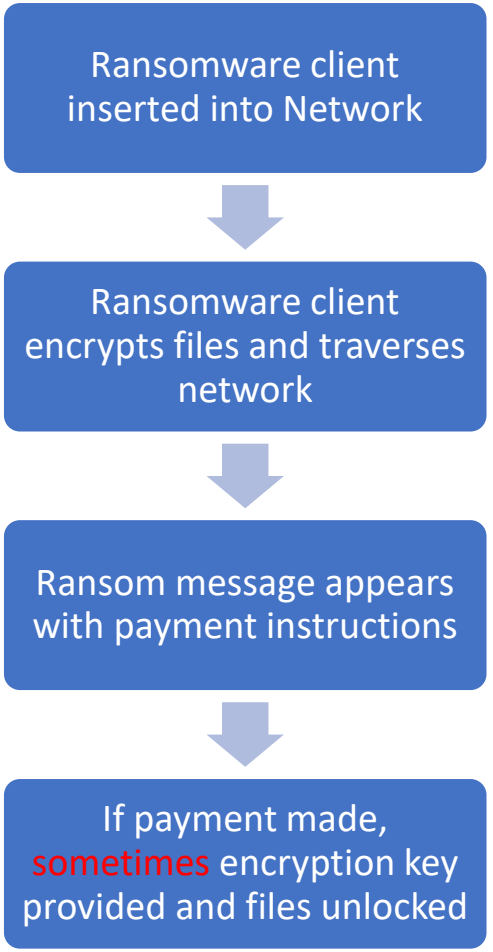
- Malware
- Enters through infected Ads or files
- Encrypts files
- Ransom demanded for key
- Usually no data is stolen

Ransomware statistics

- A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021. (Source: Cyber Security Ventures)
- 1.5 million new phishing sites are created every month. (Source: webroot.com)
- Ransomware attacks have increased over 97 percent in the past two years. (Source: Phishme)
- A total of 850.97 million ransomware infections were detected by the institute in 2018.
- 34% of businesses hit with malware took a week or more to regain access to their data. (Source: Kaspersky)
- In 2019 ransomware from phishing emails increased 109 percent over 2017. (Source: PhishMe)

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
- …

Ransomware – How it Spreads

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

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 logs stored and managed
- Have cyber incident/ransomware plan in place and practiced
- Have ransomware identify tools available – identify strain
- Perform table top exercises
- Have a plan (playbook)

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!!!

Incident Response – Table Top

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

Crypto Currency

- Type of currency
- De-centralized
- Anonymous
- Utilize block-chain
- Different Types
  - Bitcoin
  - 4000+ others

Crypto-Mining

- Crypto Mining
- Process of using computing power to solve complex problems to authorize transactions
- Miners get crypto currency for processing transactions
- Requires computing power and electricity

Cryptojacking

- Unauthorized use of someone else's computer to mine cryptocurrency
- Cheaper and more profitable than ransomware
- Recurring revenue
- Website
  - Coinhive
  - Cryptoloot
- Windows Servers
- Botnets

Crypto-Jacking – Entry Points

- Click on bad link – runs on your computer or servers
- Injects code into a website or ad delivered to multiple websites
- Code executes, results sent to hackers computers

- No damage to computers
- Slows computers
  - Affect productivity
  - Consume helpdesk time to respond/eradicate

Crypto-Jacking – Examples

- BadShell – Uses Windows processes to mine
- Insider
- GitHub
- Facexworm - Chrome extension – infected facebook accounts
- WinstarNssmMiner – crashes computer if removed

Crypto-Jacking – Prevention

- Training
- Ad blocking
- Endpoint protection (antivirus/firewall)
- Web filtering
- Mobile device management

Crypto-Jacking – Detection & Response

- I.T. Team
  - Helpdesk training
  - Look for high CPU
- Response
  - Kill scripts
  - Update browser extensions
  - Breach Risk Assessment

What to do?

Protect

- Infrastructure
- Tools
- Processes
- Policies and Procedures
- Recovery
- Training
- Authentication
- Configuration
- Patching

Prepare

- Assessments
- Policies and Procedures
- Documentation
- Incident Response
- Cyber Insurance
- Evidence
- OCR Audit Protocol (Security, Privacy, Breach)
- Training

Respond

- Incident Response Plan – Table Top/Runbook
- Know your Cyber Security Insurance Policy
- Have Knowledgeable Legal Resources
- Have Documentation Ready
- Policies and Procedures
- Training

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 SECURITY REGULATION: § 164.308 Administrative safeguards:

A covered entity or business associate must, in accordance with § 164.306: (1)(i) *Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations. (ii) Implementation specifications: *(A) RISK ANALYSIS* (REQUIRED). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

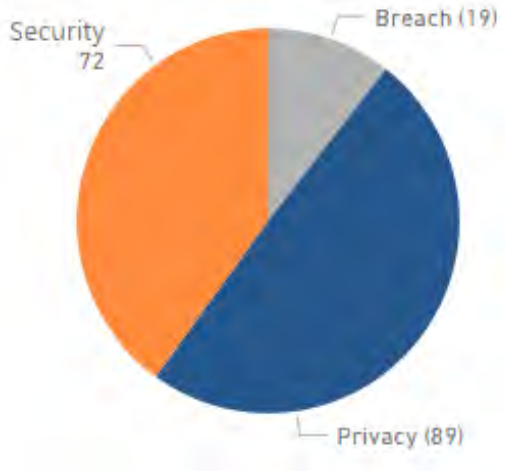
Regulations

- HIPAA (Federal floor)
  - 45 CFR 164 Subpart C - **SECURITY** STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION
  - 45 CFR 164 Subpart E - **PRIVACY** OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION
  - 45 CFR 164 Subpart D - NOTIFICATION IN THE CASE OF **BREACH** OF UNSECURED PROTECTED HEALTH INFORMATION

- State and Other Regulations
  - Confidentiality
  - Patient Rights
  - Breach

Office for Civil Rights HIPAA Audit Protocol

180 Audit Items



General Item Structure

1. Do Policies and procedures exist for the item?
2. Does the entity perform the necessary requirements if the item?
3. Obtain and review policies and procedures for the item and ensure they have required elements
4. Obtain and review documentation demonstrating the item is being performed in accordance with policies and procedures

Office for Civil Rights Investigations

Investigation Triggers

- Random Audit
- Whistleblower
- Complaint for resident or family member
- Breach (most likely)

Sample Items Requested Items

- Policies and Procedures and implementation history
- Breach Documentation (if applicable)
- List/documentation & processes for complaints
- Notice of Privacy Practices
- Designated Privacy and Security Officer
- Training documentation
- Security Risk Analyses
- Compliance documentation

Office for Civil Rights Investigation Process (Compliance Reviews)

- Letter including request for information
- 30 days to produce information requested
  - Information has to exist prior to letter or when specified
- Communication Exchange

Possible Outcomes

- Positive
- Negative – Settlement Agreemeent
  - Fines
  - Corrective Action Plan

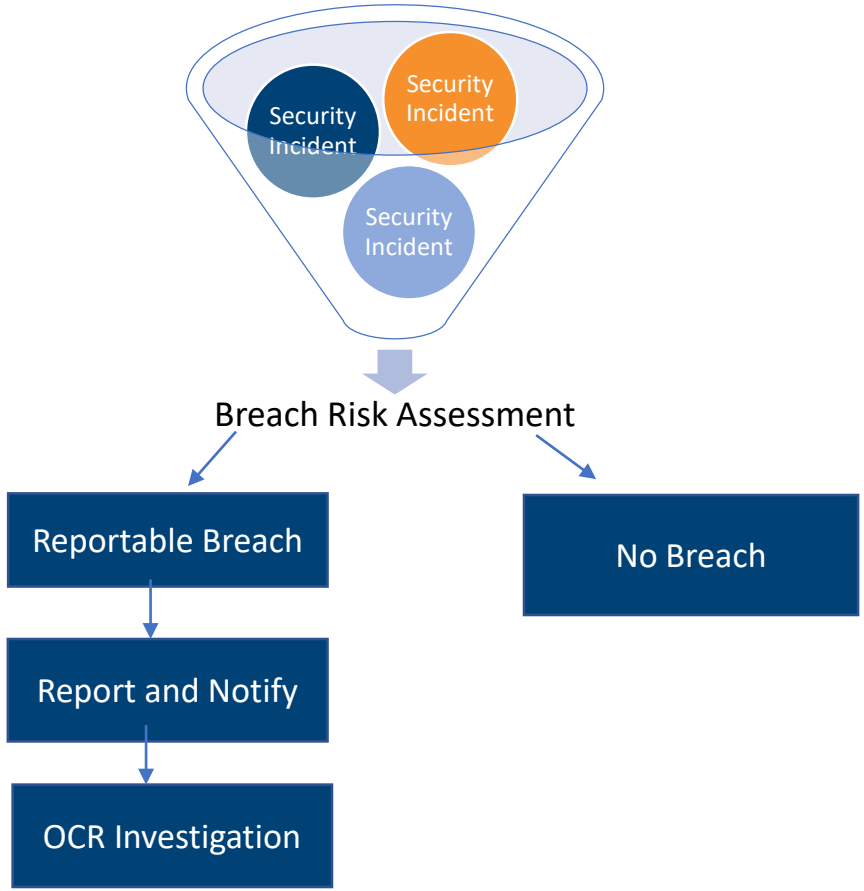
HIPAA Breach Definition

- “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

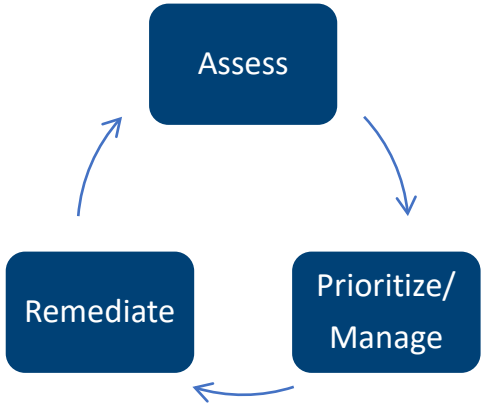


Breach Process Overview

- 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

Protect and Prepare
"It's not if, it's when"

1. **Designate Privacy and Security Officers**
2. **Perform HIPAA Security Risk Analysis**
3. **Develop and Manage Security Management Plan**
4. **Privacy, Security and Breach Policies and Procedures**
   a. Implemented
   b. Trained
   c. Supporting Documentation
5. Perform Technical Testing
   a. Vulnerability Scans
   b. Penetration Testing
6. Review OCR HIPAA Audit Protocol
7. Develop Privacy and Security Governance



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

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