Cyber Security in Healthcare: What you need to know to protect your practice

John DiMaggio, CEO, BlueOrange Compliance

October 11, 2019

About the Presenter

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

BLUE ORANGE® COMPLIANCE

Specialize in healthcare information privacy and security solutions.

LeadingAge CAST Commissioner

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
- Mock Office for Civil Rights HIPAA Audits
- Analytics
- HITRUST Assessor
- Penetration Testing

Agenda

- HealthCare Information Landscape
- Cybersecurity in Healthcare Overview
- Ransomware Overview
- Cybersecurity and HIPAA
- Protect, Prepare, Respond

Changes to Healthcare

Internet of Things (IoT)

Mobile Access

Cloud Computing

Mergers, Acquisitions, Divestitures

Borderless Perimeter

Perfect Storm

Healthcare

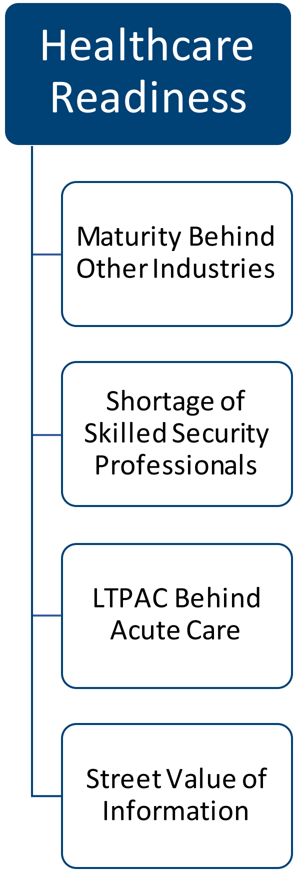
- Electronic
- Push toward interoperability
- Information outside 4 walls

Acute Care

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

Long Term Post-Acute Care (LTPAC)

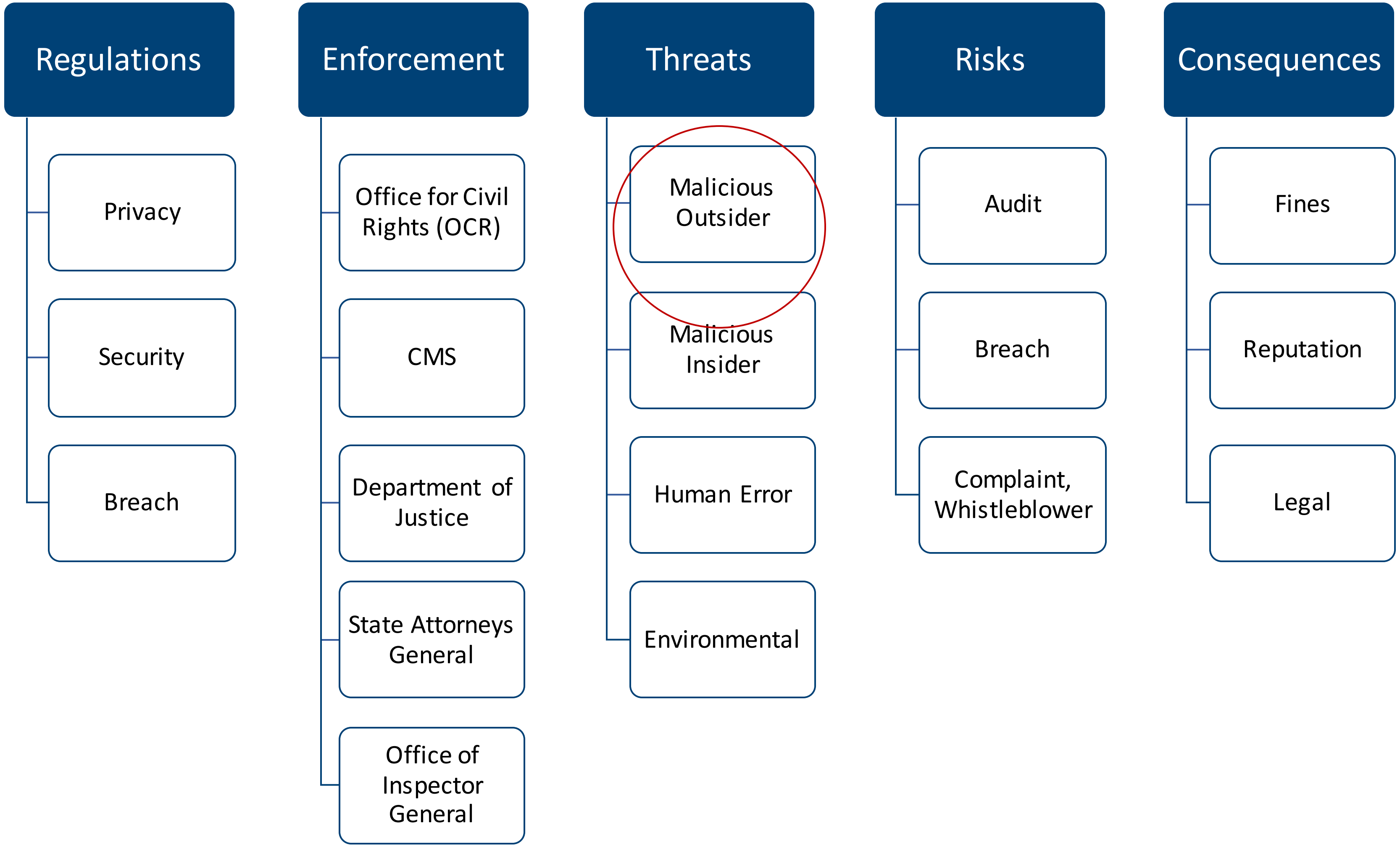
- Push toward interoperability
- Implementing EHR
- Implementing applicable technology



Healthcare Readiness

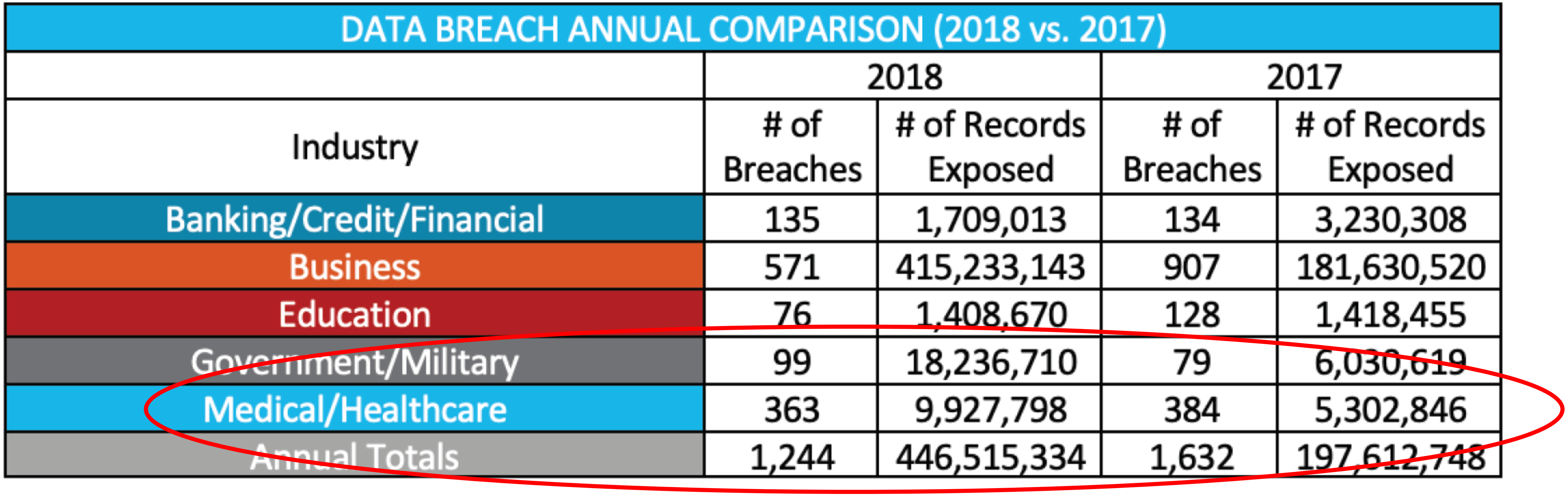
- Maturity Behind Other Industries
- Shortage of Skilled Security Professionals
- LTPAC Behind Acute Care
- Street Value of Information

Privacy and Security



- Regulations
  - Privacy
  - Security
  - Breach
- Enforcement
  - Office for Civil Rights (OCR)
  - CMS
  - Department of Justice
  - State Attorneys General
  - Office of Inspector General
- Threats
  - Malicious Outsider
  - Malicious Insider
  - Human Error
  - Environmental
- Risks
  - Audit
  - Breach
  - Complaint, Whistleblower
- Consequences
  - Fines
  - Reputation
  - Legal

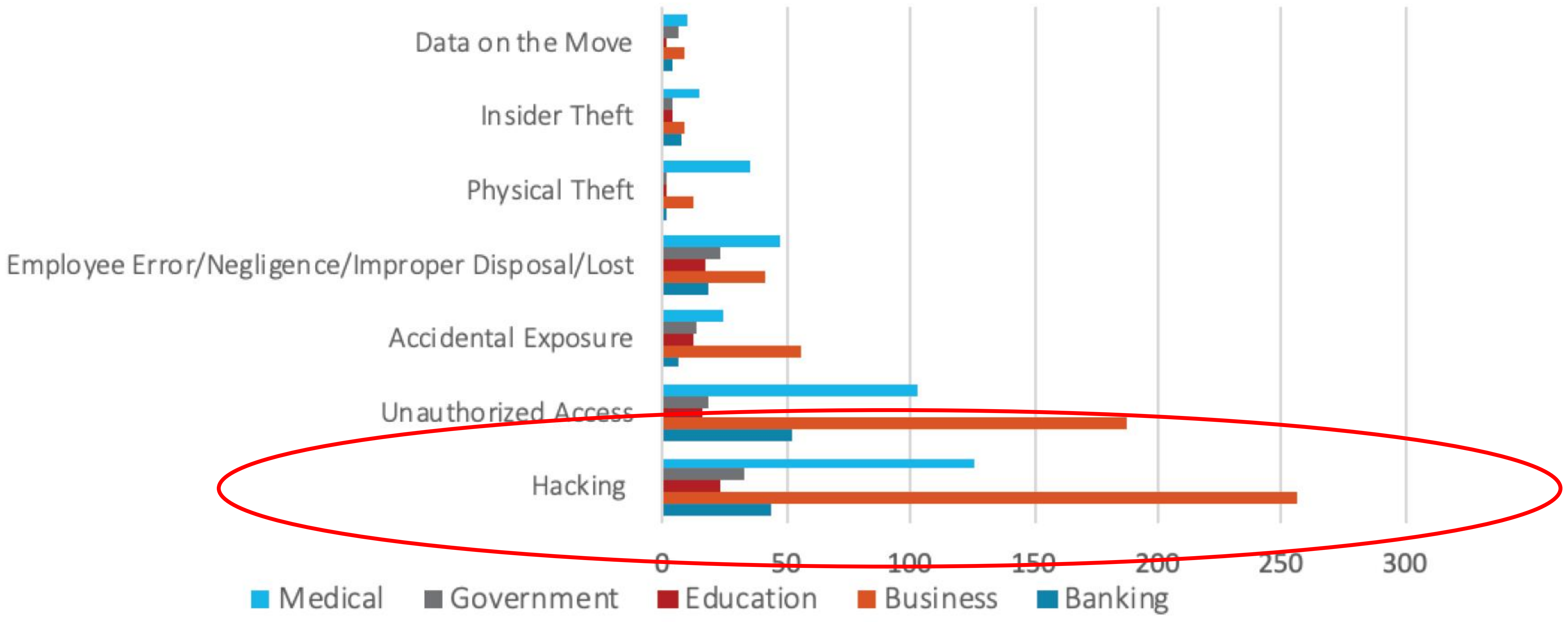
Statistics



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

2018 BREACHES BY TYPE/INDUSTRY



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

Cyber Risk in Healthcare

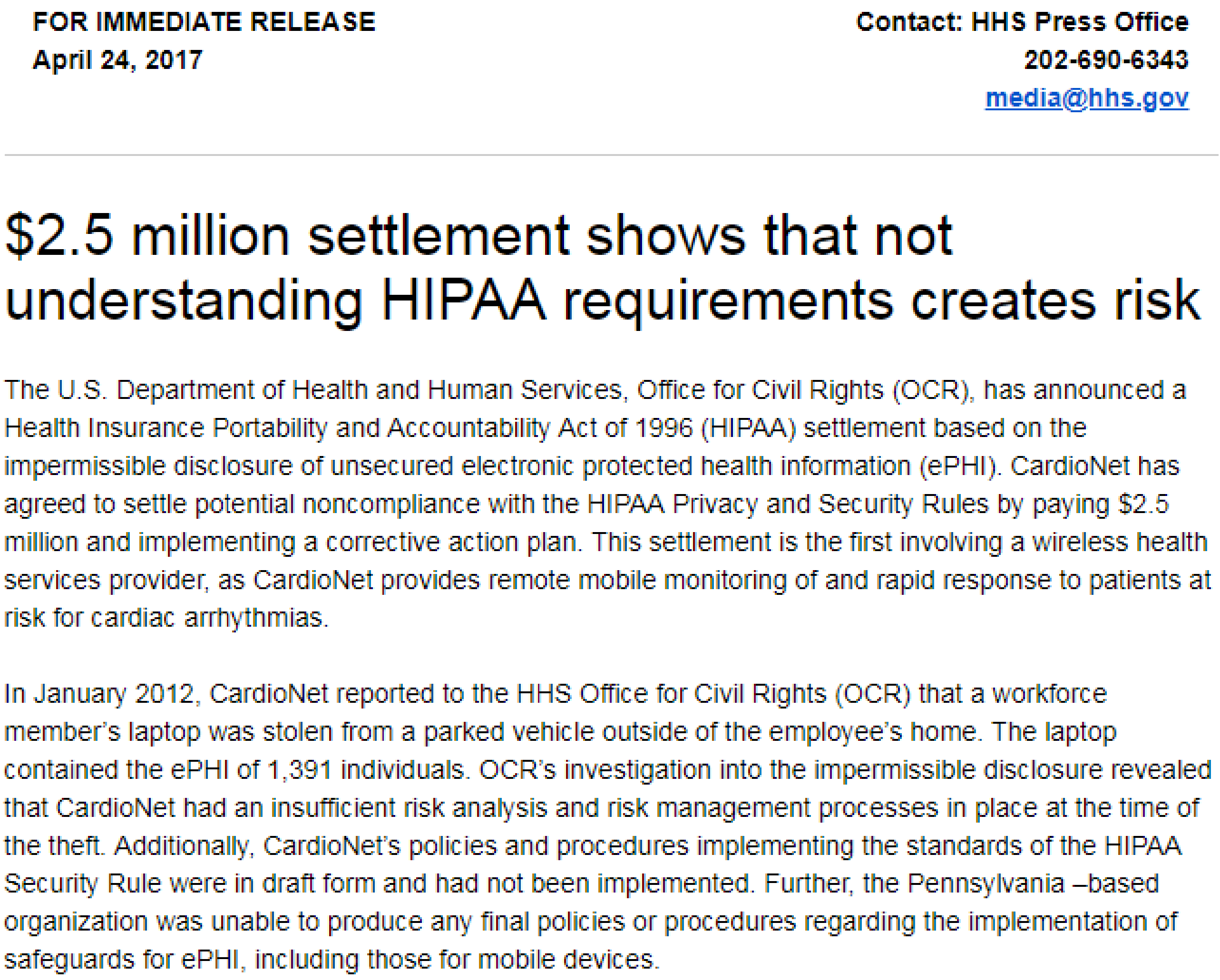
- Downtime/Business Disruption
- Office for Civil Rights HIPAA Violation (Breach)
    - Investigation
    - Fines/Penalties
    - Corrective Action Plan
- Civil Litigation
- Reputation Damage
- Individual Notification/Credit Monitoring Costs
- Legal Expenses
- Forensic/Repair

Laptops and mobile devices

$2.5 million

Insufficient risk analysis

Insufficient risk management process



FOR IMMEDIATE RELEASE
April 24, 2017

Contact: HHS Press Office
202-690-6343
media@hhs.gov

$2.5 million settlement shows that not understanding HIPAA requirements creates risk

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced a Health Insurance Portability and Accountability Act of 1996 (HIPAA) settlement based on the impermissible disclosure of unsecured electronic protected health information (ePHI). CardioNet has agreed to settle potential noncompliance with the HIPAA Privacy and Security Rules by paying $2.5 million and implementing a corrective action plan. This settlement is the first involving a wireless health services provider, as CardioNet provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias.

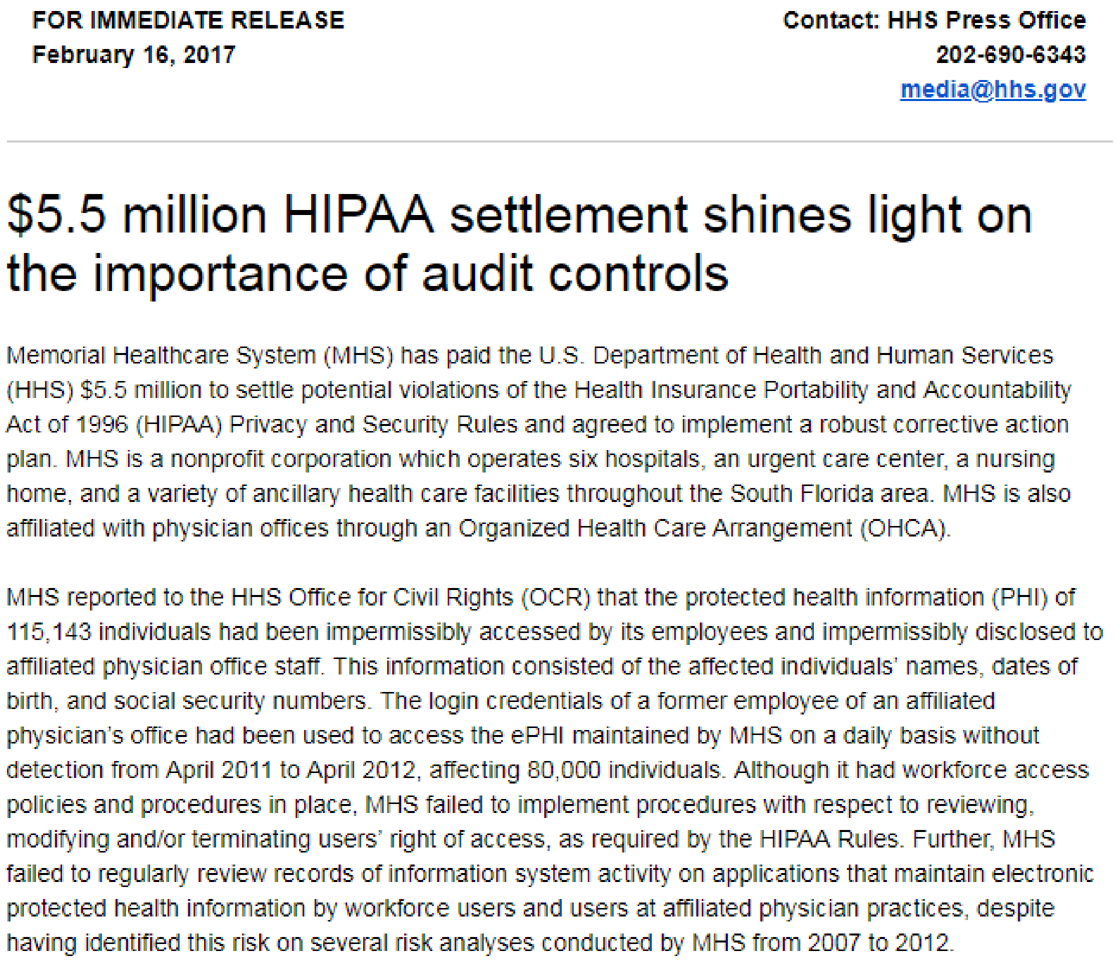
In January 2012, CardioNet reported to the HHS Office for Civil Rights (OCR) that a workforce member's laptop was stolen from a parked vehicle outside of the employee's home. The laptop contained the ePHI of 1,391 individuals. OCR's investigation into the impermissible disclosure revealed that CardioNet had an insufficient risk analysis and risk management processes in place at the time of the theft. Additionally, CardioNet's policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented. Further, the Pennsylvania –based organization was unable to produce any final policies or procedures regarding the implementation of safeguards for ePHI, including those for mobile devices.

Terminating access/audit

Failure to terminate access

Failure to review audit trails

$5.5 million



FOR IMMEDIATE RELEASE
February 16, 2017

Contact: HHS Press Office
202-690-6343
media@hhs.gov

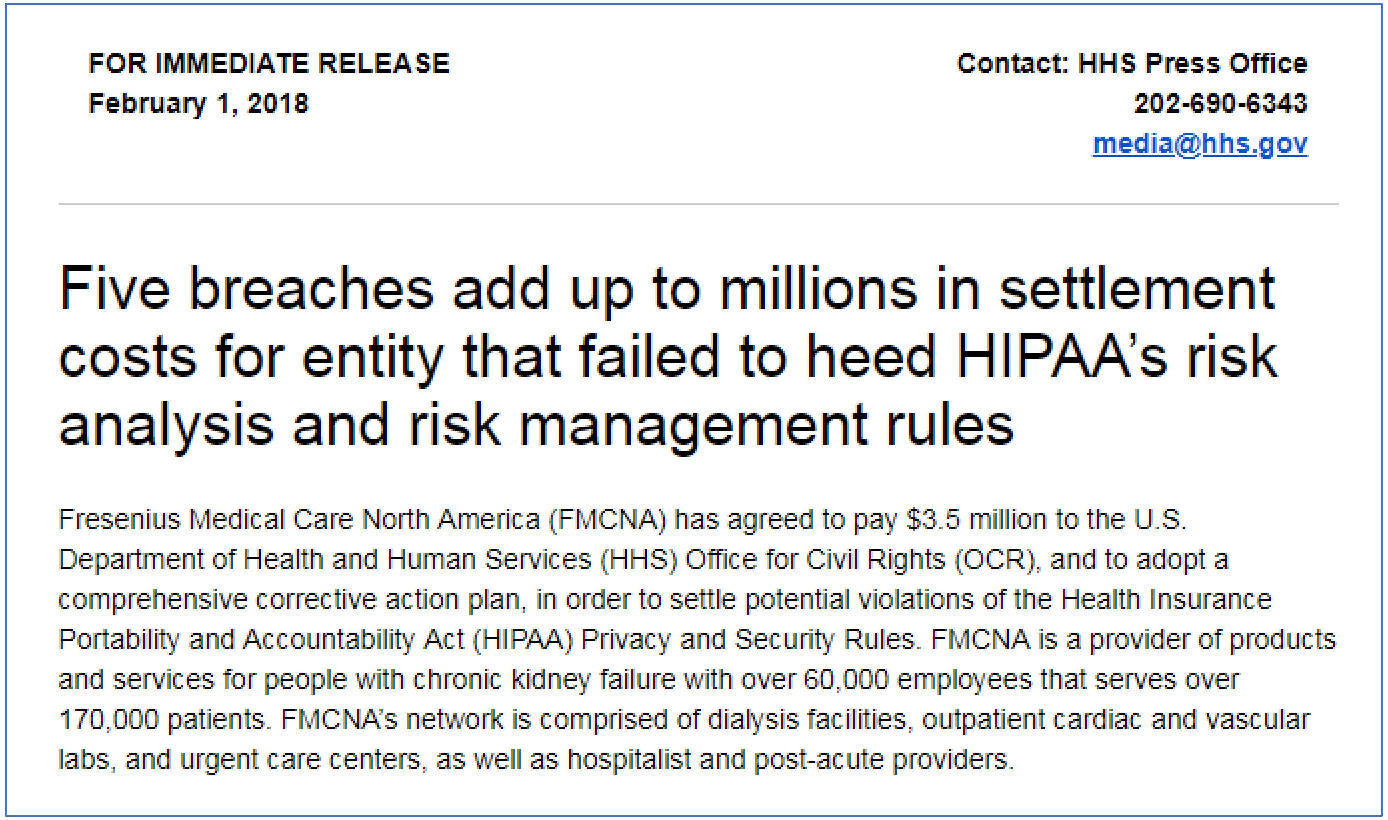
$5.5 million HIPAA settlement shines light on the importance of audit controls

Memorial Healthcare System (MHS) has paid the U.S. Department of Health and Human Services (HHS) $5.5 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and agreed to implement a robust corrective action plan. MHS is a nonprofit corporation which operates six hospitals, an urgent care center, a nursing home, and a variety of ancillary health care facilities throughout the South Florida area. MHS is also affiliated with physician offices through an Organized Health Care Arrangement (OHCA).

MHS reported to the HHS Office for Civil Rights (OCR) that the protected health information (PHI) of 115,143 individuals had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff. This information consisted of the affected individuals' names, dates of birth, and social security numbers. The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals. Although it had workforce access policies and procedures in place, MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access, as required by the HIPAA Rules. Further, MHS failed to regularly review records of information system activity on applications that maintain electronic protected health information by workforce users and users at affiliated physician practices, despite having identified this risk on several risk analyses conducted by MHS from 2007 to 2012.

Importance of policies and procedures

$3.5 million



FOR IMMEDIATE RELEASE
February 1, 2018

Contact: HHS Press Office
202-690-6343
media@hhs.gov

Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules

Fresenius Medical Care North America (FMCNA) has agreed to pay $3.5 million to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), and to adopt a comprehensive corrective action plan, in order to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. FMCNA is a provider of products and services for people with chronic kidney failure with over 60,000 employees that serves over 170,000 patients. FMCNA's network is comprised of dialysis facilities, outpatient cardiac and vascular labs, and urgent care centers, as well as hospitalist and post-acute providers.

Failure to conduct accurate and thorough risk analysis

Failure to implement policies and procedures

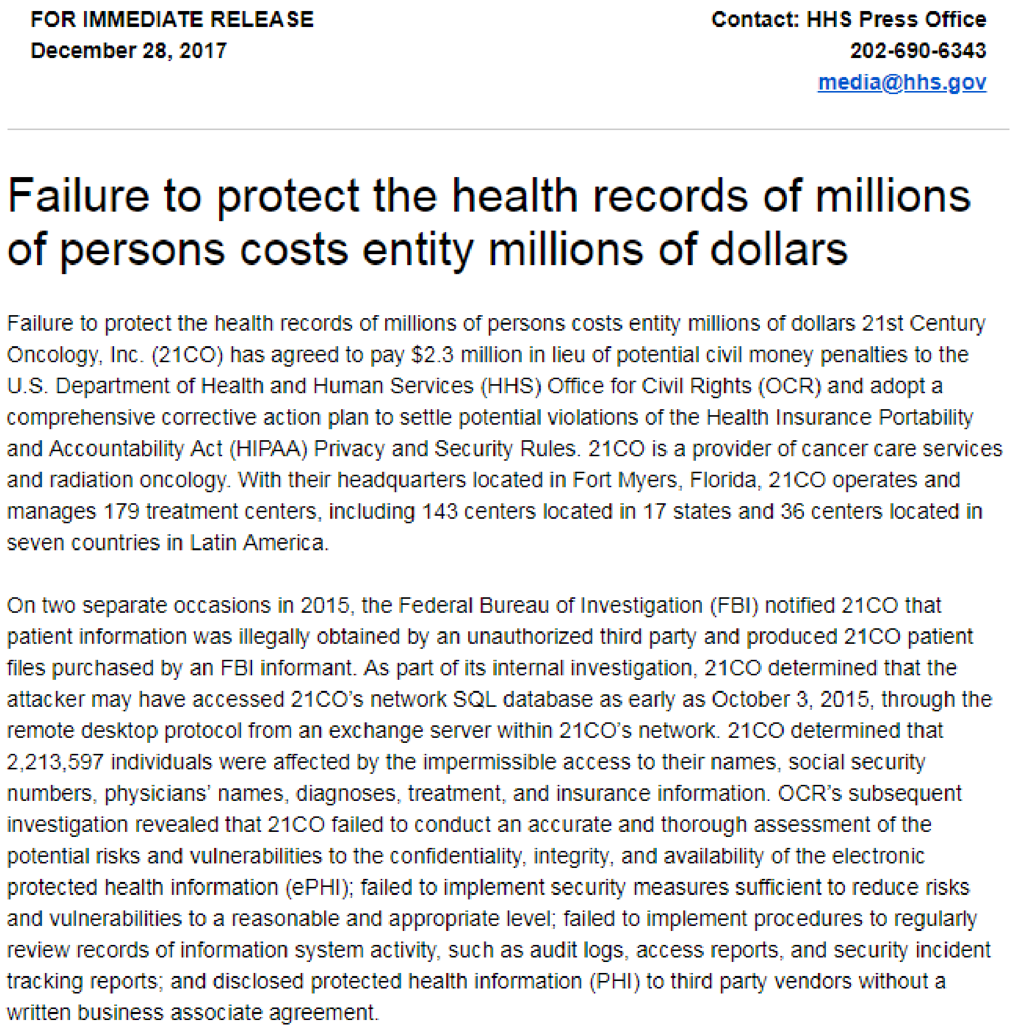
Failure to encrypt information where it was reasonable to do so

Cyber attacks

$2.3 million

Failure to review system activity

Failure to implement security measures



FOR IMMEDIATE RELEASE
December 28, 2017

Contact: HHS Press Office
202-690-6343
media@hhs.gov

Failure to protect the health records of millions of persons costs entity millions of dollars

Failure to protect the health records of millions of persons costs entity millions of dollars 21st Century Oncology, Inc. (21CO) has agreed to pay $2.3 million in lieu of potential civil money penalties to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and adopt a comprehensive corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. 21CO is a provider of cancer care services and radiation oncology. With their headquarters located in Fort Myers, Florida, 21CO operates and manages 179 treatment centers, including 143 centers located in 17 states and 36 centers located in seven countries in Latin America.

On two separate occasions in 2015, the Federal Bureau of Investigation (FBI) notified 21CO that patient information was illegally obtained by an unauthorized third party and produced 21CO patient files purchased by an FBI informant. As part of its internal investigation, 21CO determined that the attacker may have accessed 21CO's network SQL database as early as October 3, 2015, through the remote desktop protocol from an exchange server within 21CO's network. 21CO determined that 2,213,597 individuals were affected by the impermissible access to their names, social security numbers, physicians' names, diagnoses, treatment, and insurance information. OCR's subsequent investigation revealed that 21CO failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information (ePHI); failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and disclosed protected health information (PHI) to third party vendors without a written business associate agreement.

Am I Too Small?

Dermatology practice settles potential HIPAA violations

Adult & Pediatric Dermatology, P.C., of Concord, Mass., (APDerm) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules with the Department of Health and Human Services, agreeing to a $150,000 payment. APDerm will also be required to implement a corrective action plan to correct deficiencies in its HIPAA compliance program. APDerm is a private practice that delivers dermatology services in four locations in Massachusetts and two in New Hampshire. This case marks the first settlement with a covered entity for not having policies and procedures in place to address the breach notification provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

The HHS Office for Civil Rights (OCR) opened an investigation of APDerm upon receiving a report that an unencrypted thumb drive containing the electronic protected health information (ePHI) of approximately 2,200 individuals was stolen from a vehicle of one its staff members. The thumb drive was never recovered. The investigation revealed that APDerm had not conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process. Further, APDerm did not fully comply with requirements of the Breach Notification Rule to have in place written policies and procedures and train workforce members.

“As we say in health care, an ounce of prevention is worth a pound of cure,” said OCR Director Leon Rodriguez. “That is what a good risk management process is all about – identifying and mitigating the risk before a bad thing happens. Covered entities of all sizes need to give priority to securing electronic protected health information.”

In addition to a $150,000 resolution amount, the settlement includes a corrective action plan requiring AP Derm to develop a risk analysis and risk management plan to address and mitigate any security risks and vulnerabilities, as well as to provide an implementation report to OCR.

US Department of Health and Human Services. Dermatology practice settles potential HIPAA violations,, December 26, 2013

Am I Too Small?

HHS announces first HIPAA breach settlement involving less than 500 patients

Hospice of North Idaho settles HIPAA security case for $50,000

The Hospice of North Idaho (HONI) has agreed to pay the U.S. Department of Health and Human Services' (HHS) $50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This is the first settlement involving a breach of unsecured electronic protected health information (ePHI) affecting fewer than 500 individuals.

The HHS Office for Civil Rights (OCR) began its investigation after HONI reported to HHS that an unencrypted laptop computer containing the electronic protected health information (ePHI) of 441 patients had been stolen in June 2010. Laptops containing ePHI are regularly used by the organization as part of their field work. Over the course of the investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI. Further, HONI did not have in place policies or procedures to address mobile device security as required by the HIPAA Security Rule. Since the June 2010 theft, HONI has taken extensive additional steps to improve their HIPAA Privacy and Security compliance program.

"This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information." said OCR Director Leon Rodriguez. "Encryption is an easy method for making lost information unusable, unreadable and undecipherable."

US Department of Health and Human Services. HHS announces first HIPAA breach settlement involving less than 500 patients,, January 2, 2013

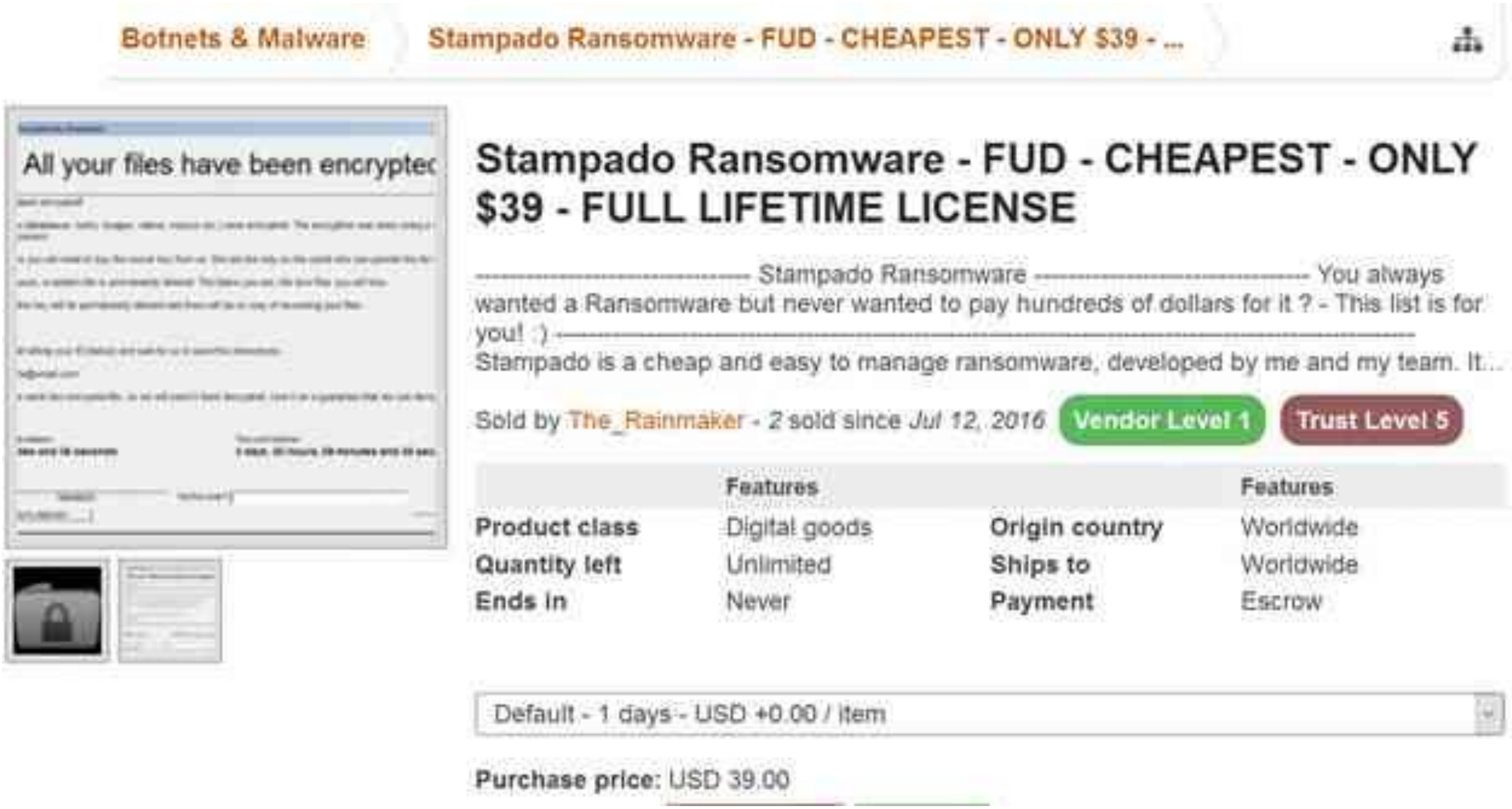
Hackers Marketplace

RANSOMWARE AS A SERVICE (WITH WARRANTY)

COMPROMISED SERVERS FOR RENT

FREE HACKING TOOLS READILY AVAILABLE

RANSOMWARE-AS-A-SERVICE (RAAS)



Botnets & Malware › Stampado Ransomware - FUD - CHEAPEST - ONLY $39 - ...

All your files have been encrypted

Stampado Ransomware - FUD - CHEAPEST - ONLY $39 - FULL LIFETIME LICENSE

------------------------------------ Stampado Ransomware ------------------------------------ You always wanted a Ransomware but never wanted to pay hundreds of dollars for it ? - This list is for you! :) --
Stampado is a cheap and easy to manage ransomware, developed by me and my team. It...

Sold by The_Rainmaker - 2 sold since *Jul 12, 2016* Vendor Level 1 Trust Level 5

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 39.00

Image: TrendMicro

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

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

Money

Fun

Social/Political Cause

Information

Best Practice Stages

Reconnaissance

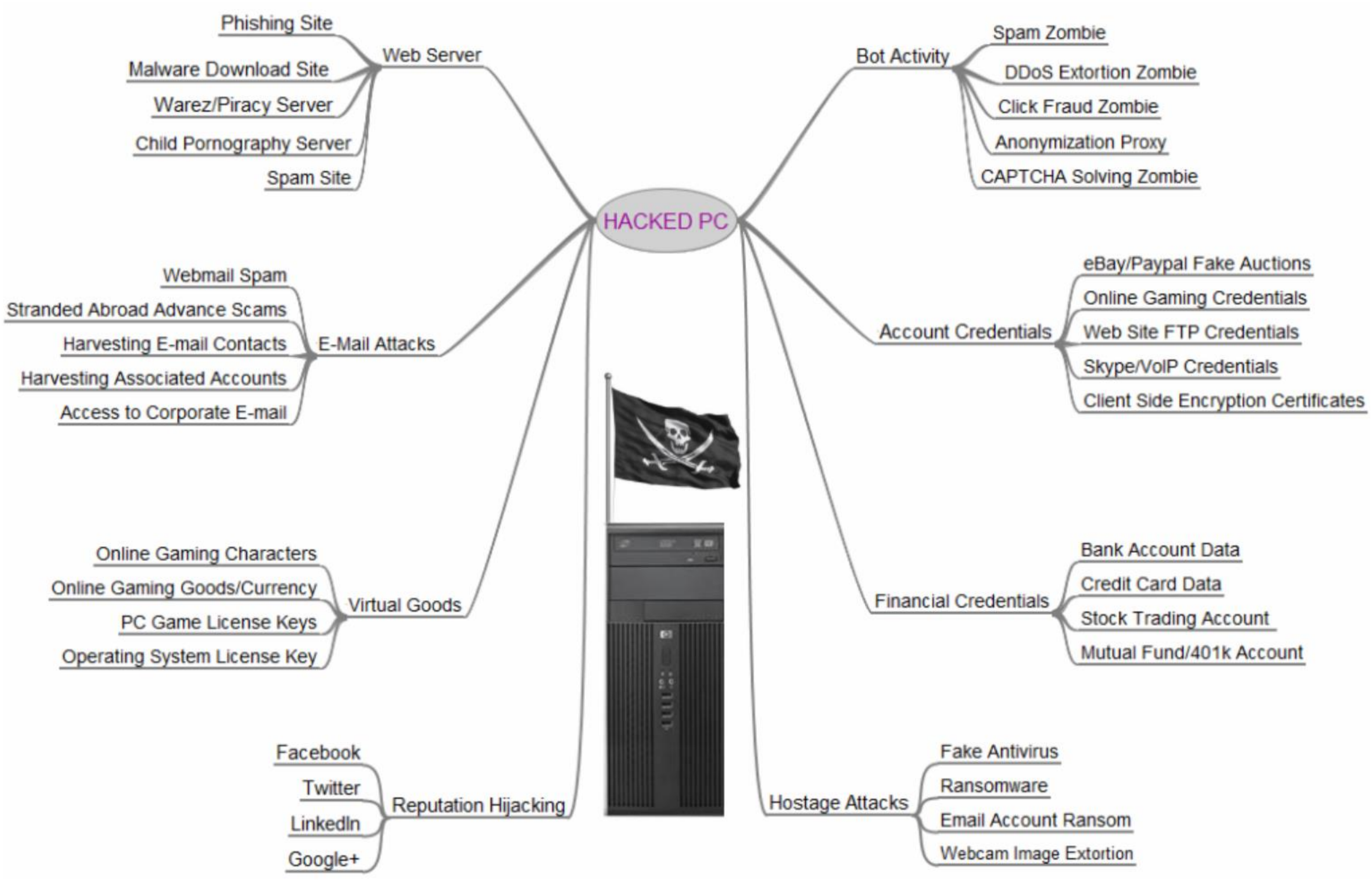
Scan

Gain Access

Maintain Access

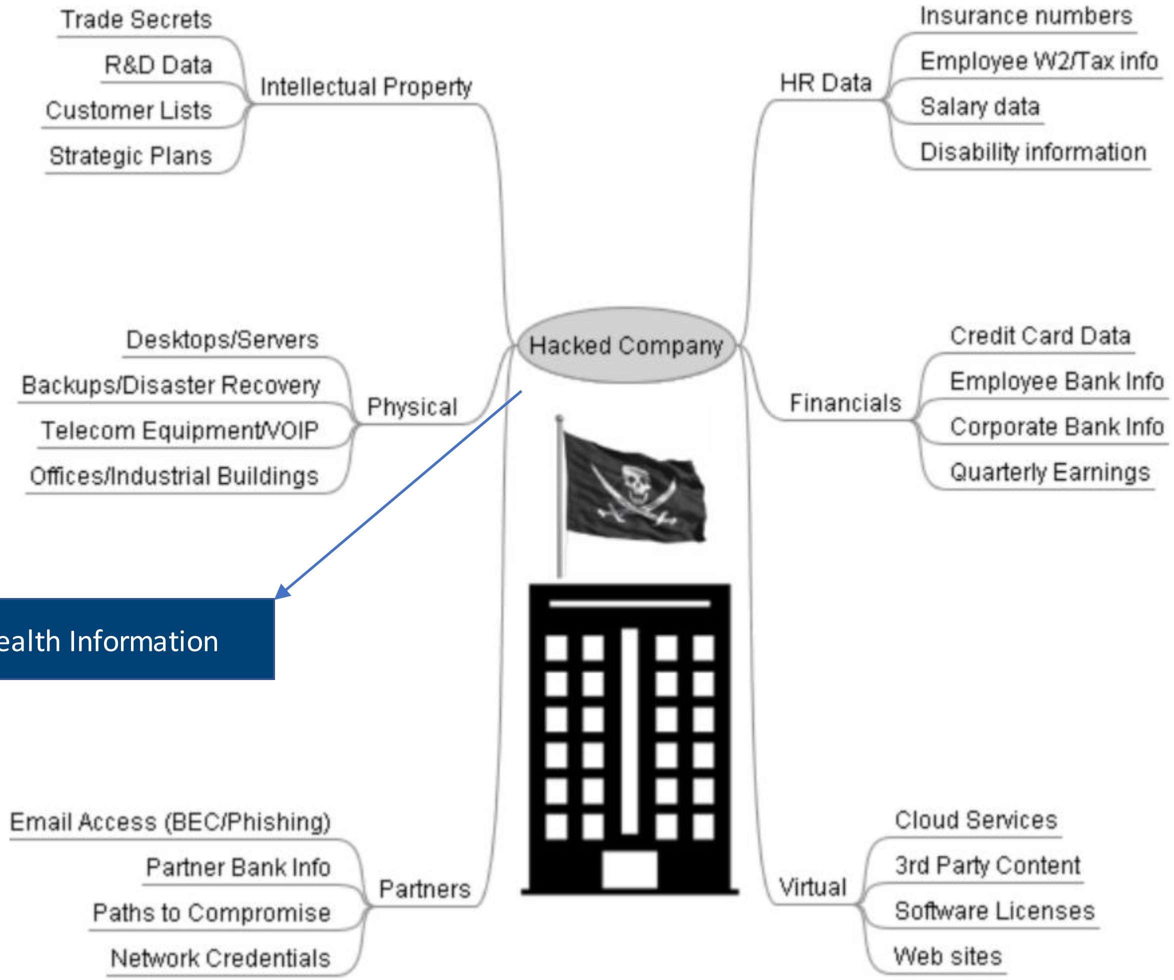
Clear Tracks

Value of a Hacked PC



Krebs on Security – Value of Hacked PC

Value of a Hacked Company



Health Information

Krebs on Security – Value of Hacked Company 2016

Attack Stages Analogy

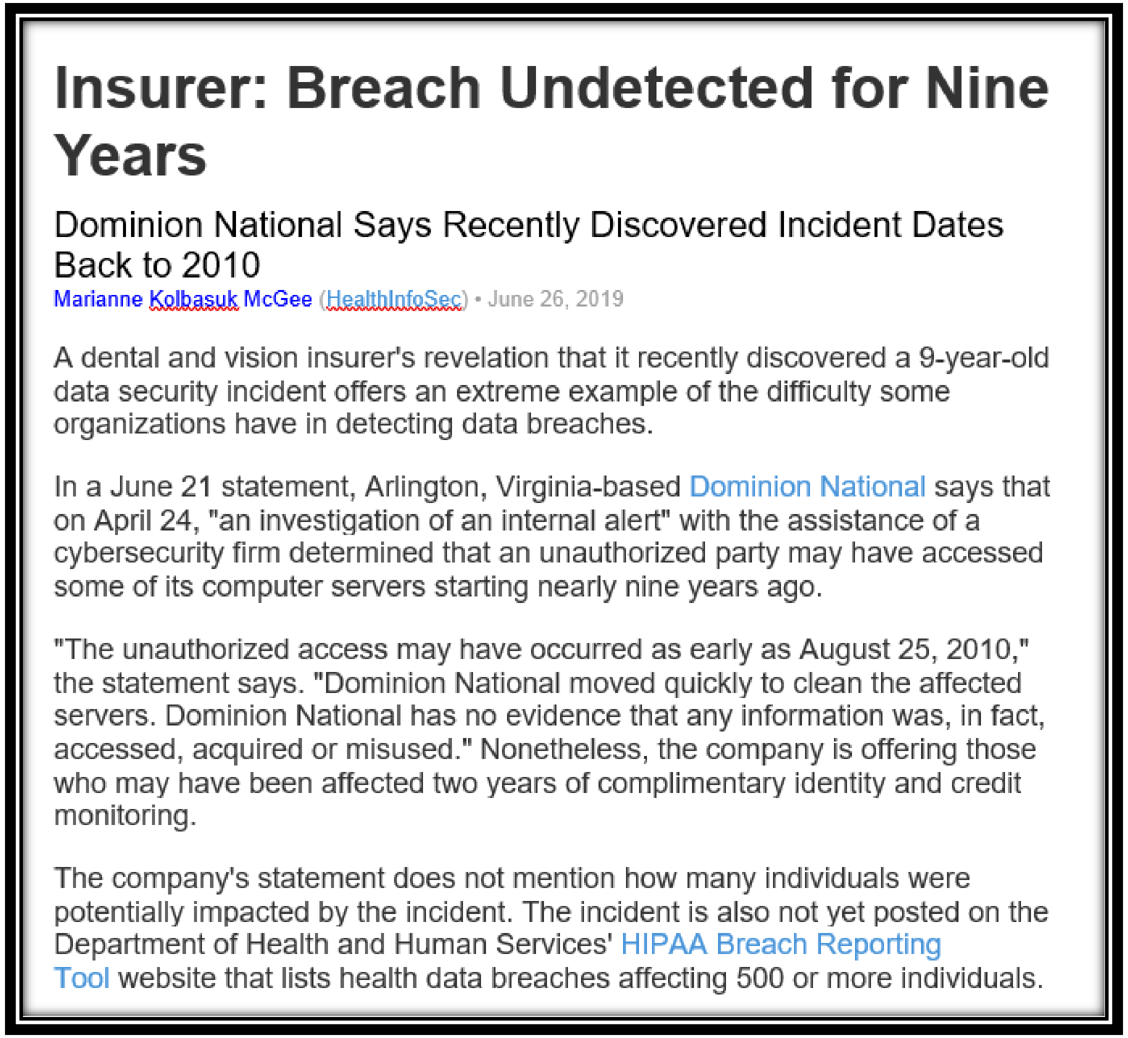
Stage	Burglar Your House	Hacker Your Organization
Reconnaissance	• Drive by - schedule • Look at county auditor site • Facebook	• LinkedIn • Google • SEC Filings • Website
Scanning	• Check doors, windows • Try garage codes	• Scan ports • Phone calls • Physical visit
Gain Access	• Enter through window	• 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: 197 days

Source: Ponemon Institute: Cost of a Data Breach Study, July 2018



Insurer: Breach Undetected for Nine Years

Dominion National Says Recently Discovered Incident Dates Back to 2010

Marianne Kolbasuk McGee (HealthInfoSec) • June 26, 2019

A dental and vision insurer's revelation that it recently discovered a 9-year-old data security incident offers an extreme example of the difficulty some organizations have in detecting data breaches.

In a June 21 statement, Arlington, Virginia-based Dominion National says that on April 24, "an investigation of an internal alert" with the assistance of a cybersecurity firm determined that an unauthorized party may have accessed some of its computer servers starting nearly nine years ago.

"The unauthorized access may have occurred as early as August 25, 2010," the statement says. "Dominion National moved quickly to clean the affected servers. Dominion National has no evidence that any information was, in fact, accessed, acquired or misused." Nonetheless, the company is offering those who may have been affected two years of complimentary identity and credit monitoring.

The company's statement does not mention how many individuals were potentially impacted by the incident. The incident is also not yet posted on the Department of Health and Human Services' HIPAA Breach Reporting Tool website that lists health data breaches affecting 500 or more individuals.

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)

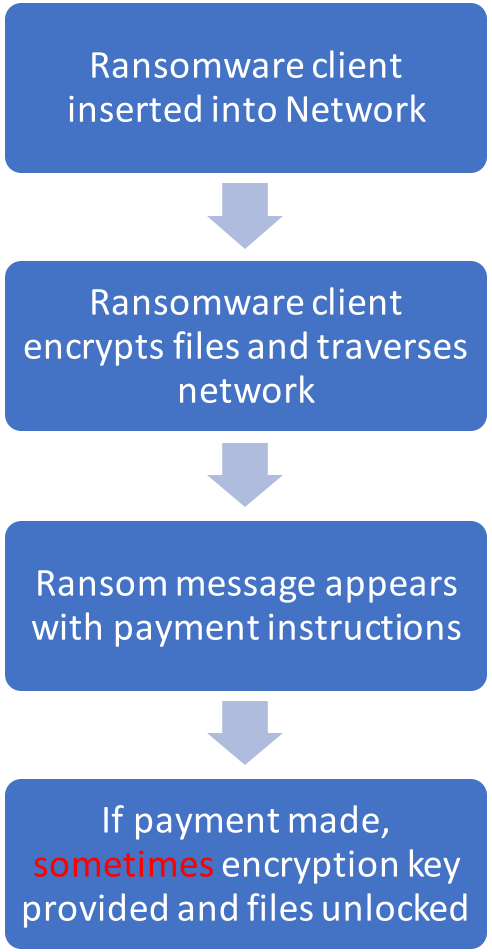
A total of 850.97 million ransomware infections were detected by the institute in 2018.

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 client inserted into Network

Ransomware client encrypts files and traverses network

Ransom message appears with payment instructions

If payment made, sometimes encryption key provided and files unlocked

Ransomware Types

Malicious

Financial-Based

Amateur

Business Grade – Reputable??

Ransomware Techniques

Spray

Targeted

Ransomware Entry Points

- Network Configuration
- 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

What questions would you have?

- How long until we’re back up?
- How much is the ransom?
- Can we completely recover from backup if we don’t pay the ransom?
- How long would it take to recover?
- How much data would we lose if we recover?
- How much does it cost per hour to be down (without computers)?
- Did we call law enforcement? What did they say?
- Who do we call to help?
- Will cyber insurance cover this? Is there a deductible? How much?

Cyber Security Vulnerabilities

Technical

- Software Patches
- Open Ports
- Wireless
- Anti-virus/malware
- Weak passwords
- Unmanaged accounts
- Email
- Encryption
- Non-secure web-facing application
- Default accounts
- Mobile devices

Human

- Password sharing
- Phone skills
- Links

Physical

- Wired ports
- Visitor management

Mobile Devices

- Policies and Procedures
- BYOD
- Encryption
- Email/Text
- Management
- Access

Regulations

HIPAA
The Health Insurance Portability and Accountability Act of 1996

- 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 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 Agreement
  - Fines
  - Corrective Action Plan

The After-Party- 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."

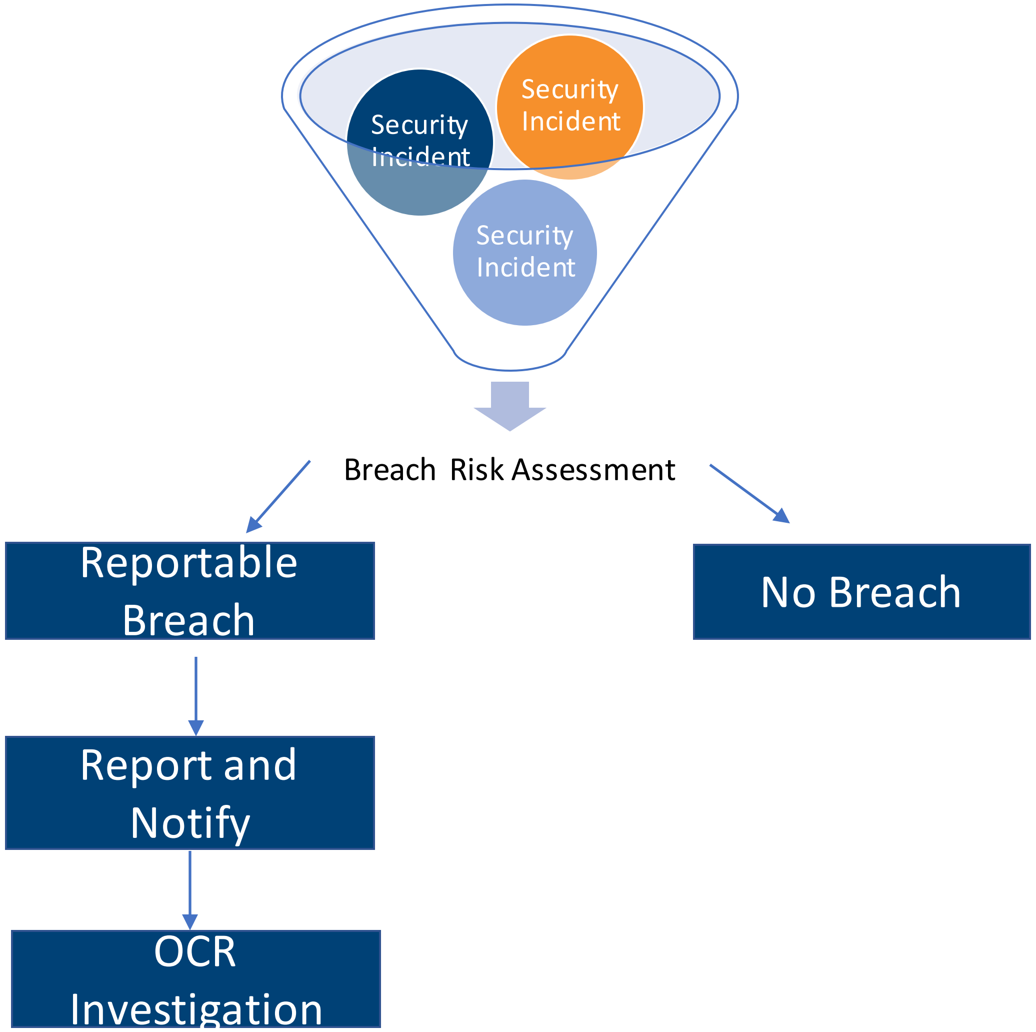
Breach Risk Assessment

OCR Investigation

Management/Board Level Discussion Items

- When was the last time we practiced our cyber incident response capability?
- If an incident happened right now could we continue operations?
- Short Term vs Long Term Incident
- Do we have retainers in place for Legal, PR, and Cyber Security
- Do we have cyber insurance to cover this? What does it cover?

Breach Analysis and Process



Security Incident

Security Incident

Security Incident

Breach Risk Assessment

Reportable Breach

No Breach

Report and Notify

OCR Investigation

Breach Process Overview

- Contact cyber insurance carrier if applicable
  - May require certain legal, forensics firms, policy limitations
- Recommend contact attorney for attorney client privilege
- Response team - get on top of it
- Internal policies – then follow
- Investigation internally – do not call it a breach until you know
- Only look at compromised systems with proper experts
- Do not ignore dark web communications
- Determine individuals affected
- > 500 notify individuals, media, HHS
- 60 days from discovery
- Press release

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)

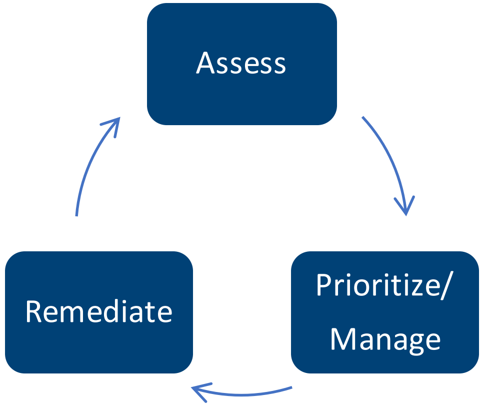
- Letter including request for information
- 30 days to produce information requested
  - Information has to exist prior to letter or when specified
- Communication Exchange

Possible Outcomes

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

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. Develop Privacy and Security Governance
7. Workforce security reminders



Additional Information

- LeadingAge CAST Cyber Security Whitepaper and Benchmarking tool
- https://www.leadingage.org/cast/cast-releases-cybersecurity-white-paper

- Download Cyber Security E Book
- Download VcD and Listening Devices

- www.blueorangecompliance.com

- 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