CYBERSECURITY IN HEALTHCARE: WHAT YOU NEED TO KNOW TO KEEP YOUR ORGANIZATION SAFE & SECURE

PRESENTED BY

John DiMaggio
CEO
Blue Orange Compliance
John.dimaggio@blueorangecompliance.com
614-657-4109

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.

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

LEADINGAGE CAST CYBERSECURITY

BLUE ORANGE COMPLIANCE

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.

OBJECTIVES

- This session discusses the importance of not *if* an organization will have a security breach, but rather *when* and subsequent handling of the situation.

- Hear from two industry professionals as they offers guidance on:
  - protecting information
  - complying with regulations,
  - preparing for a security incident/breach,
  - responding to incidents.

AGENDA

- HealthCare Information Landscape
- Changes in Senior Living
- Security Incidents
- Cybersecurity Overview
- What's at stake
- Cybersecurity and HIPAA
- Protect
- Prepare
- Respond

2016 HEALTHCARE INDUSTRY

- FBI warns of a 600% increase in attacks to the Senior Living Industry.
- Targeted industry due to limited funding and cyber awareness and overall preparedness.
- How do we make our organizations *less of a target…*

CHANGES TO THE SENIOR LIVING LANDSCAPE

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

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

Sunday, April 15, 2018 Wang Wei

Share 7.21k Share Tweet Share

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.

Homeland Security

US-CERT United States Computer Emergency Readiness Team

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

HEALTHCARE LANDSCAPE

BLUE ORANGE COMPLIANCE

Healthcare

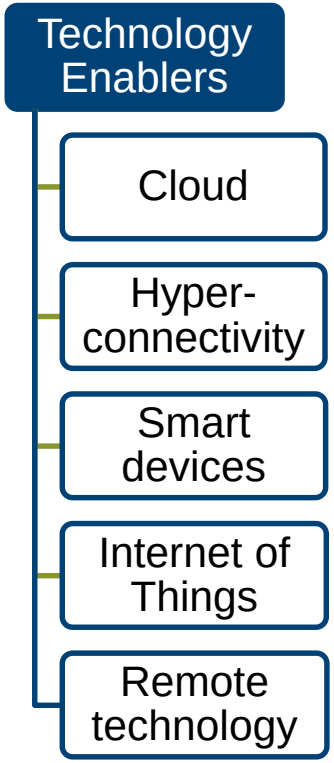
- Electronic
- Push toward interoperability
- Cost shift outside 4 walls
- Information outside 4 walls

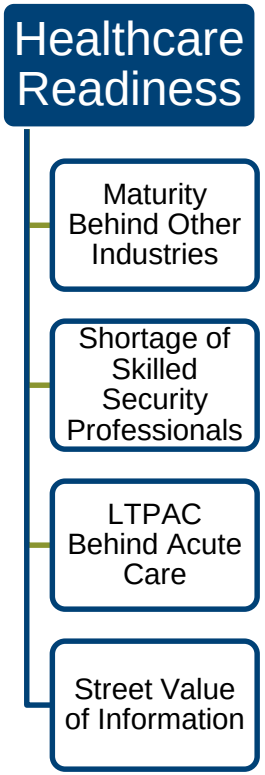
Acute Care

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

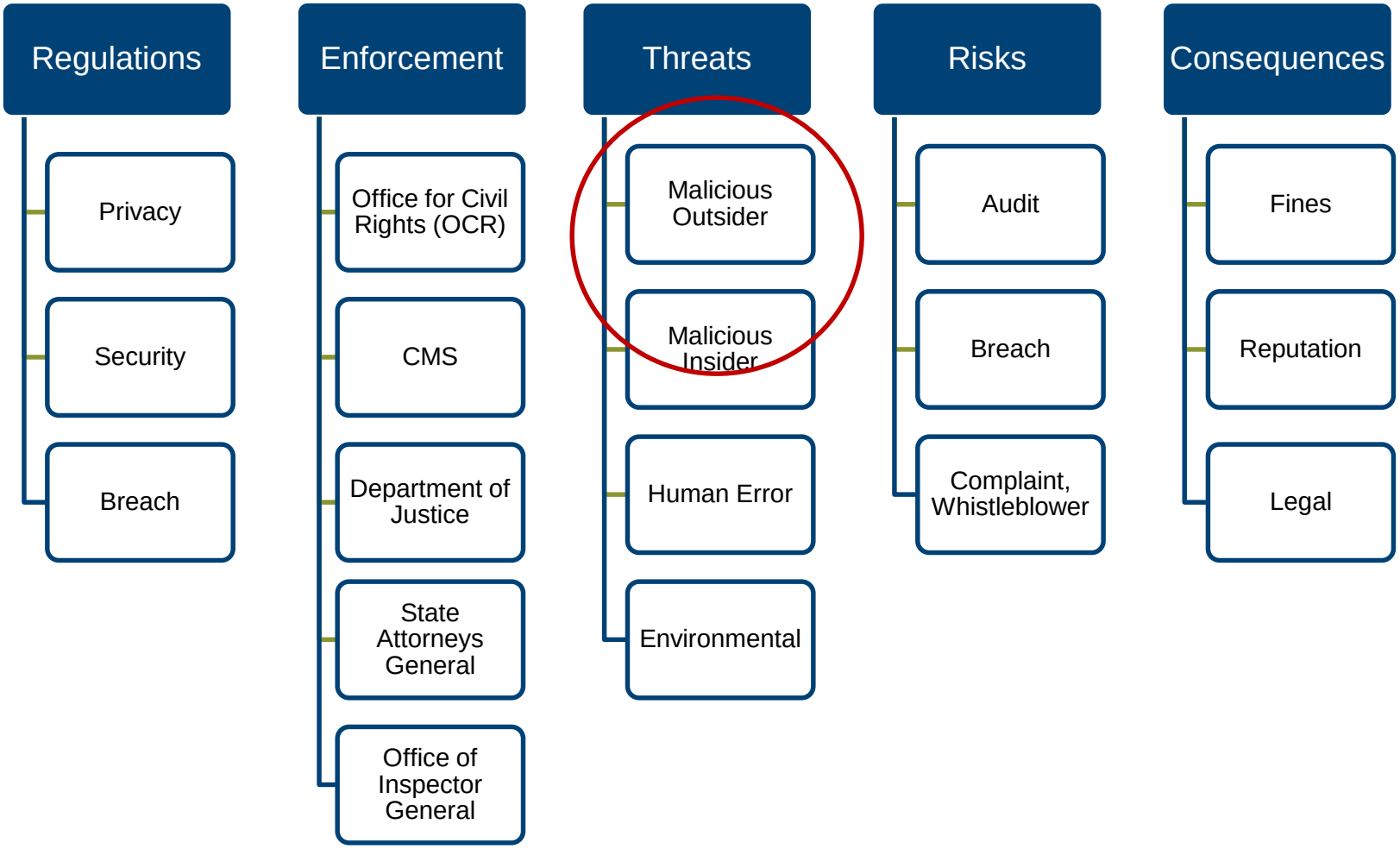
Long Term Post-Acute Care (LTPAC)

- Push toward interoperability
- Implementing EHR
- Implementing applicable technology





PRIVACY AND SECURITY



RANSOMWARE

BLUE ORANGE COMPLIANCE

- 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

BLUE ORANGE COMPLIANCE

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

LARGEST HEALTHCARE BREACHES OF 20[illegible]

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

COMMON MISCONCEPTIONS

BLUE ORANGE COMPLIANCE

- 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

AM I TOO SMALL?

BLUE ORANGE COMPLIANCE

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?

BLUE ORANGE COMPLIANCE

Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule after the theft of a CHCS mobile device compromised the protected health information (PHI) of hundreds of nursing home residents. CHCS provided management and information technology services as a business associate to six skilled nursing facilities. The total number of individuals affected by the combined breaches was 412. The settlement includes a monetary payment of $650,000 and a corrective action plan.

…..

OCR initiated its investigation on April 17, 2014, after receiving notification that CHCS had experienced a breach of PHI involving the theft of a CHCS-issued employee iPhone. The iPhone was unencrypted and was not password protected. The information on the iPhone was extensive, and included social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information. At the time of the incident, CHCS had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident; OCR also determined that CHCS had no risk analysis or risk management plan.

US Department of Health and Human Services. Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement,, July 3, 2016

AM I TOO SMALL?

BLUE ORANGE COMPLIANCE

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

WHAT TO DO?

BLUE ORANGE COMPLIANCE

Protect

- Infrastructure
- Tools
- Processes
- Recovery
- Authentication

Prepare

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

Respond

- Incident Response Plan – Table Top
- Know your Cyber Security Insurance Policy
- Have Knowledgeable Legal Resources
- Have Documentation Ready

CYBER SECURITY: THEORY

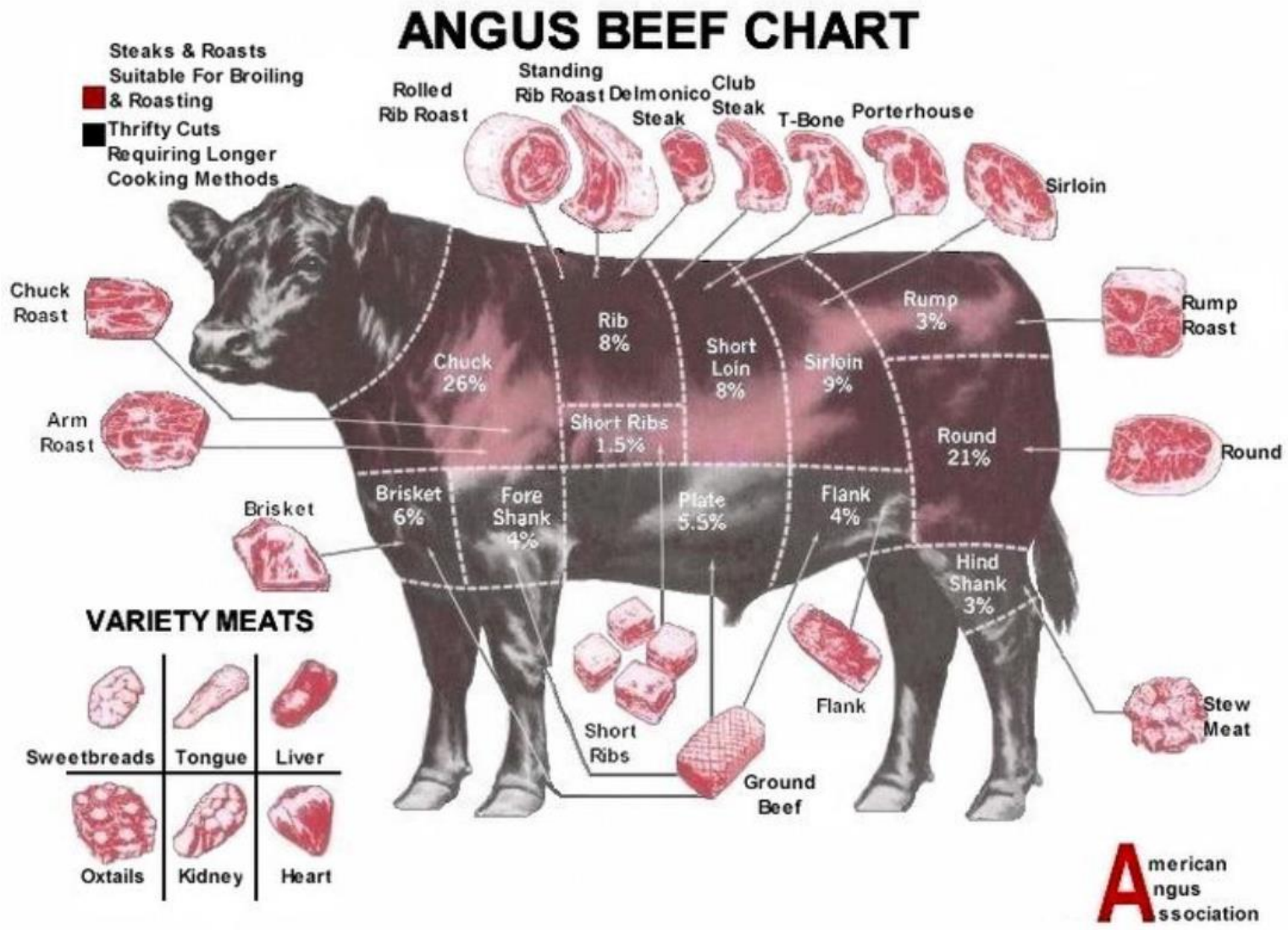
BLUE ORANGE COMPLIANCE

- 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

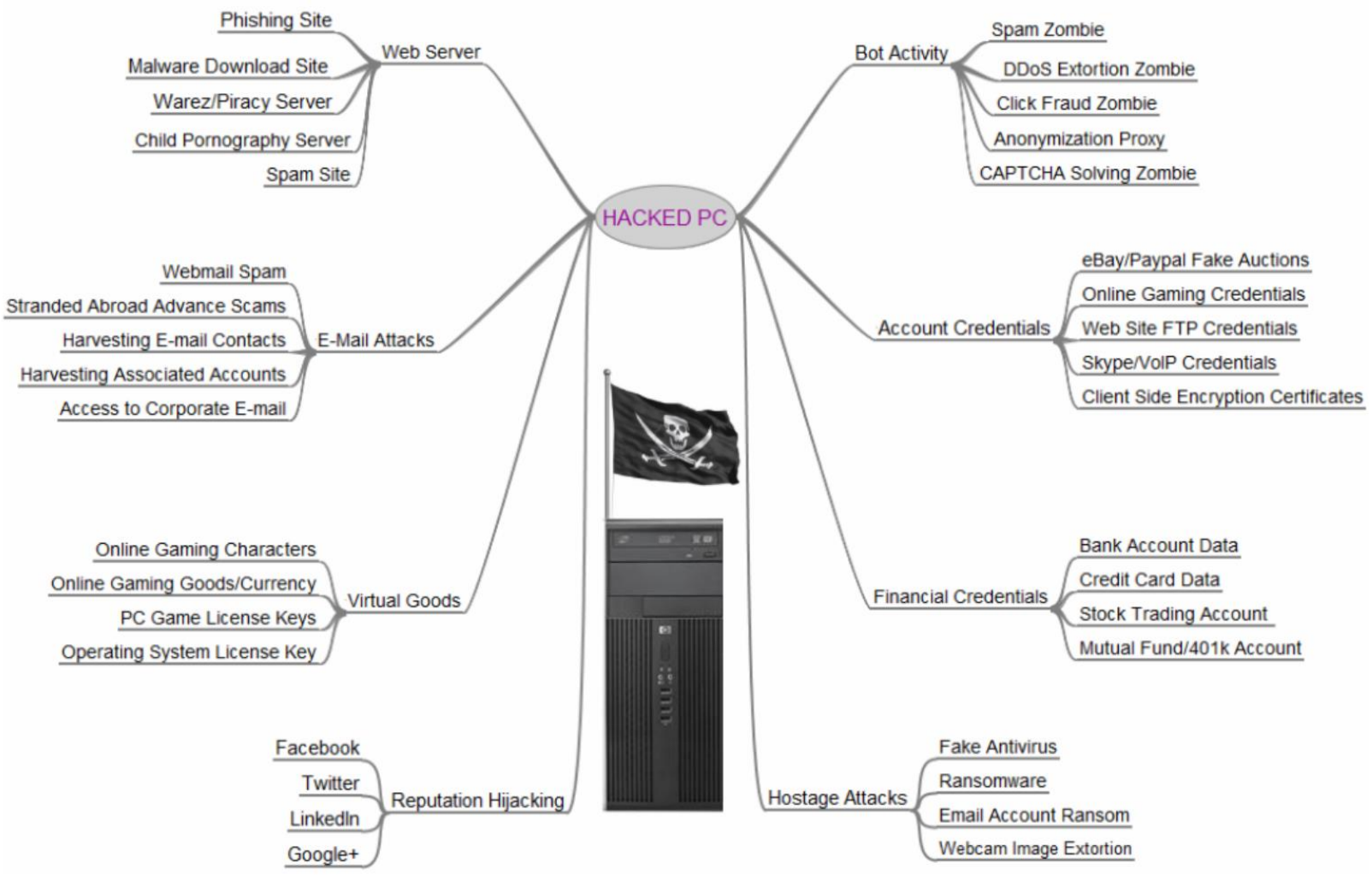
BLUE ORANGE COMPLIANCE

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



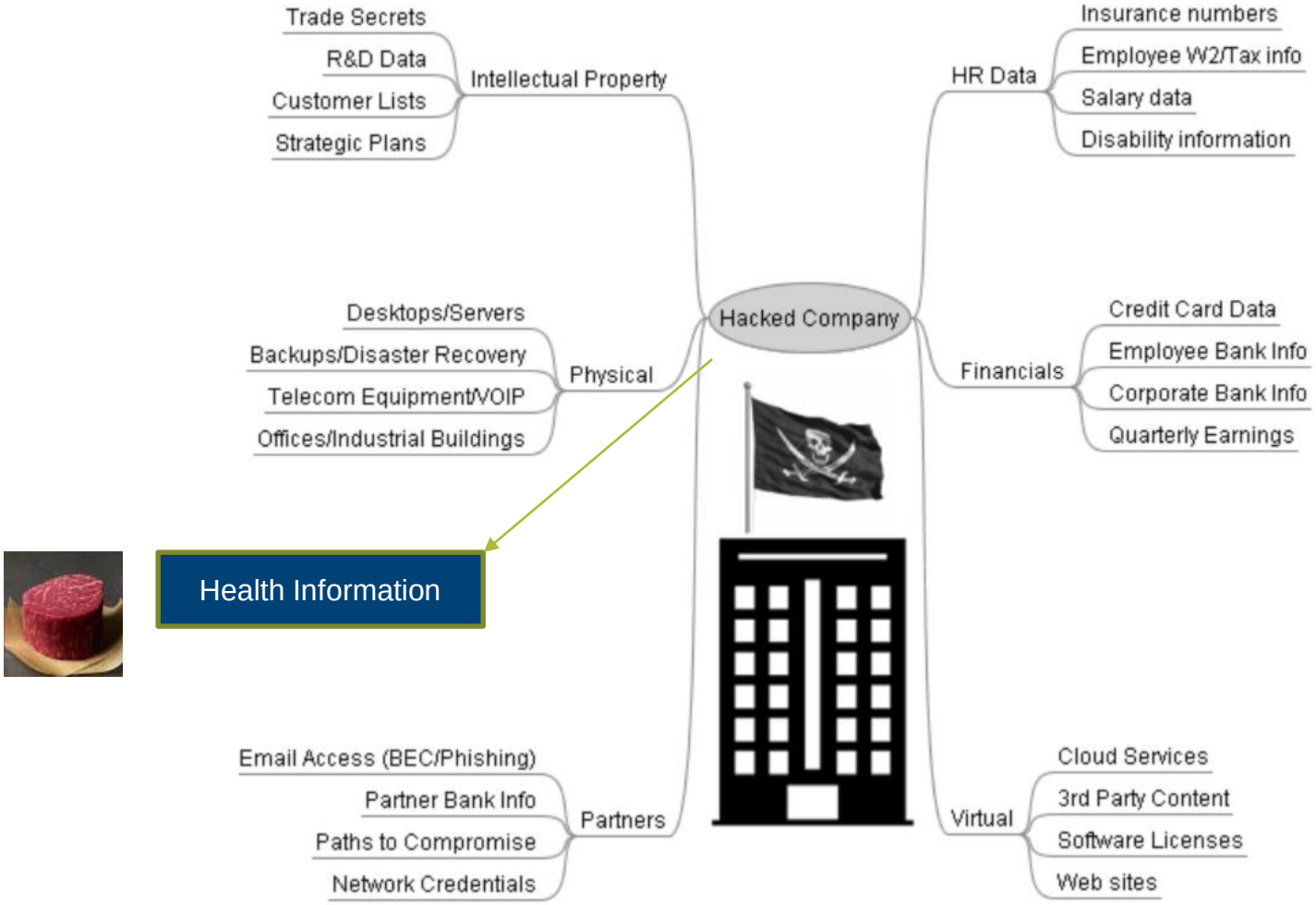
Source: American Angus Association

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

CYBER ATTACK TECHNIQUES

BLUE ORANGE COMPLIANCE

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

BLUE ORANGE COMPLIANCE

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

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

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

BLUE ORANGE COMPLIANCE

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

Countermeasures

- Security Awareness Training
- Off-line and regular backups
- Lowest system privileges
- System/Antivirus Updates

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 Entity Types
  - Covered Entity
  - Affiliated Covered Entity (ACE)
  - Hybrid
  - Organized Healthcare Arrangement (OHCA)

REGULATIONS

BLUE ORANGE COMPLIANCE

- 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

STATE REGULATION EXAMPLE

Ohio

Confidentiality	
General	Ohio Revised Code § 3721.13(10). All residents have the right to confidential treatment of personal and medical records.
Patient Rights	
Access	Ohio Revised Code § 3721.13(8). Residents have the right to access all information in the resident's medical record. If the attending physician determines it is not medically advisable, then the information must be given to the resident's sponsor if the sponsor is authorized to receive such information.
Restrictions	Ohio Revised Code § 3721.13(10). Residents have the right to approve or refuse the release of medical records outside of the facility, unless certain exceptions (release in connection with transfer to another provider or as required by law, rule or third party payment contract).
Breach Notification	
Ohio Revised Code § 1349.19. Any person or entity that conducts business in Ohio and owns or licenses computerized data that contains personal information (defined as an individual's name when linked to certain data elements, including social security number, driver's license number or any account number) must disclose any unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of such personal information. Notice must be made within 45 days to the individual whose data was compromised and, if involving more than 1,000 individuals, to consumer reporting agencies.	

SECURITY SCOPE

BLUE ORANGE COMPLIANCE

Example Security Control Families

Access Control
Audit and Accountability
Certification, Accreditation, and Security Assessment
Configuration Management
Contingency Planning
Identification and Authentication
Incident Response
Maintenance
Media Protection
Physical and Environmental
Security Planning
Security Awareness and Training
Personnel Security
Risk Assessment
System and Service Acquisition
System and Communications
System and Information Integrity

WHAT'S AT RISK? PENALTIES PLUS…

BLUE ORANGE COMPLIANCE

Civil Monetary Penalties

Willful Neglect <u>not</u> corrected within 30 days	• Min. $50,000/violation • Max. $1,500,000/ calendar year
Willful Neglect corrected within 30 days	• Min. $10,000/violation • Max $50,000/violation • Max. $1,500,000/ calendar year
Reasonable Cause	• Min. $1000/violation • Max $50,000/violation • Max. $1,500,000/ calendar year
Did not Know	• Min. $100/violation • Max $50,000/violation • Max. $1,500,000/ calendar year

Other Costs

- Legal
- Accelerated Remediation
- Public Relations
- Reputation

US Department of Health and Human Services Office for Civil Rights. 45 CFR 160.404

PRIVACY AND SECURITY AND LONG TERM CARE

BLUE ORANGE COMPLIANCE

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
10. “It won’t happen to us”
11. “My I.T. guy has it covered”
12. “I invested in new networks”
13. “I Use a cloud-based EHR”

OFFICE FOR CIVIL RIGHTS INVESTIGATIONS

BLUE ORANGE COMPLIANCE

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

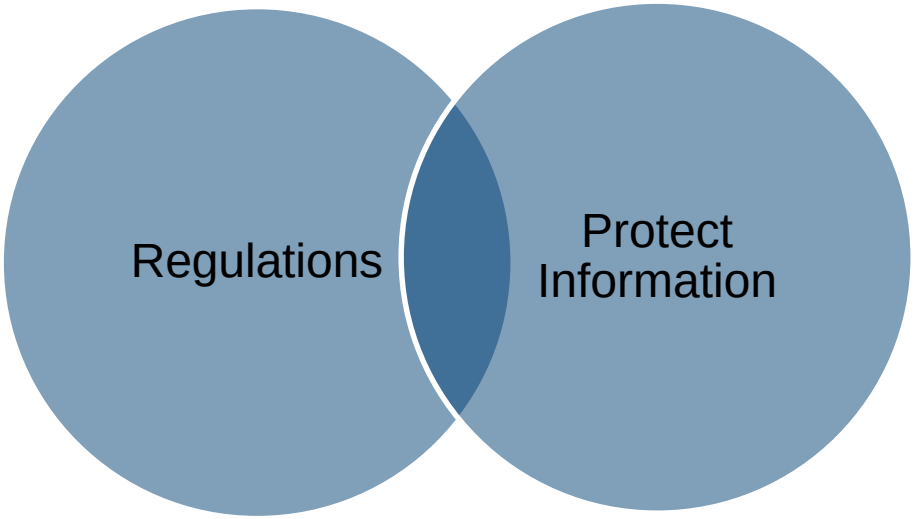
Possible Outcomes

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

WHAT SHOULD YOU DO?

BLUE ORANGE COMPLIANCE

1. Protect Information
2. Meet Regulations



WHAT TO DO?

BLUE ORANGE COMPLIANCE

Protect

- Infrastructure
- Tools
- Processes
- Recovery
- Authentication

Prepare

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

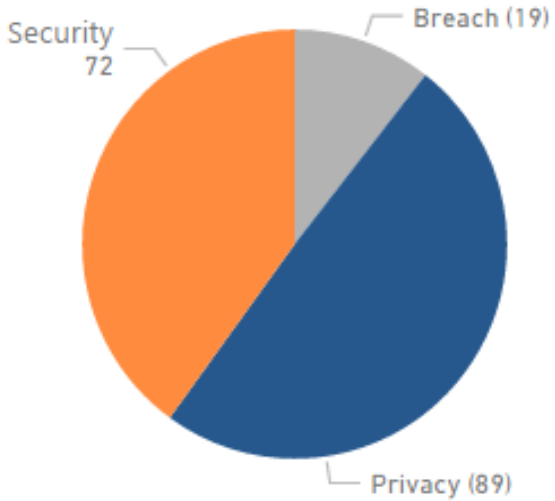
Respond

- Incident Response Plan – Table Top
- Know your Cyber Security Insurance Policy
- Have Knowledgeable Legal Resources
- Have Documentation Ready

OFFICE FOR CIVIL RIGHTS HIPAA AUDIT PROTOCOL

BLUE ORANGE COMPLIANCE

180 Audit Items



General Item Structure

1. Do Policies and procedures exist for the item?
2. Does the entity perform the necessary requirements for 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 HIPAA AUDIT PROTOCOL WALKTHROUGH
SECURITY EXAMPLE

BLUE ORANGE COMPLIANCE

Audit Type	Section	Key Activity	Established Performance Criteria	Audit Inquiry
Security	§164.308(a)(1)(ii)(A)	Security Management Process -- Risk Analysis	§164.308(a)(1)(ii)(A): 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.	Does the entity have policies and procedures in place to conduct an accurate and thorough assessment o the confidentiality, integrity, and availability of all the electronic protected health information (ePHI) it creat Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities t availability of all the ePHI it creates, receives, maintains, or transmits? Determine how the entity has implemented the requirements. Obtain and review risk analysis policies and procedures. Evaluate and determine if written policies and pr the purpose and scope of the risk analysis, workforce member roles and responsibilities, management inv frequently the risk analysis will be reviewed and updated. Obtain and review the written risk analysis or other record(s) that documents that an accurate and thorou vulnerabilities to the confidentiality, integrity, and availability of all ePHI was been conducted. Evaluate an other documentation contains: • A defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI • Details of identified threats and vulnerabilities • Assessment of current security measures • Impact and likelihood analysis • Risk rating Obtain and review documentation regarding the written risk analysis or other documentation that immedia or other record, if any. Evaluate and determine if the risk analysis has been reviewed and updated on a pe the environment and/or operations, security incidents, or occurrence of a significant event.
Security	§164.308(a)(1)(ii)(B)	Security Management Process -- Risk Management	§164.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Does the entity have policies and procedures in place regarding a risk management process sufficient to r reasonable and appropriate level? Has the entity implemented security measures sufficient to reduce risks and vulnerabilities to a reasonabl Obtain and review policies and procedure related to risk management. Evaluate and determine if the docu what is considered an acceptable level of risk based on management approval, the frequency of reviewing members' roles in the risk management process. Obtain and review documentation demonstrating the security measures implemented and/or in the proces
Security	§164.308(a)(1)(ii)(C)	Security Management Process – Sanction Policy	§164.308(a)(1)(ii)(C): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Does the entity have policies and procedures in place regarding sanctions to apply to workforce members security policies and procedures? Does the entity apply appropriate sanctions against workforce members who fail to comply with its securi Obtain and review documentation of the sanction policies and procedures (which could be an aspect of a contain a reasonable and appropriate process to sanction workforce members for failures to comply with t

U.S. Dept of Health and Human Services. Retrieved from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/

HIPAA BREACH DEFINITION

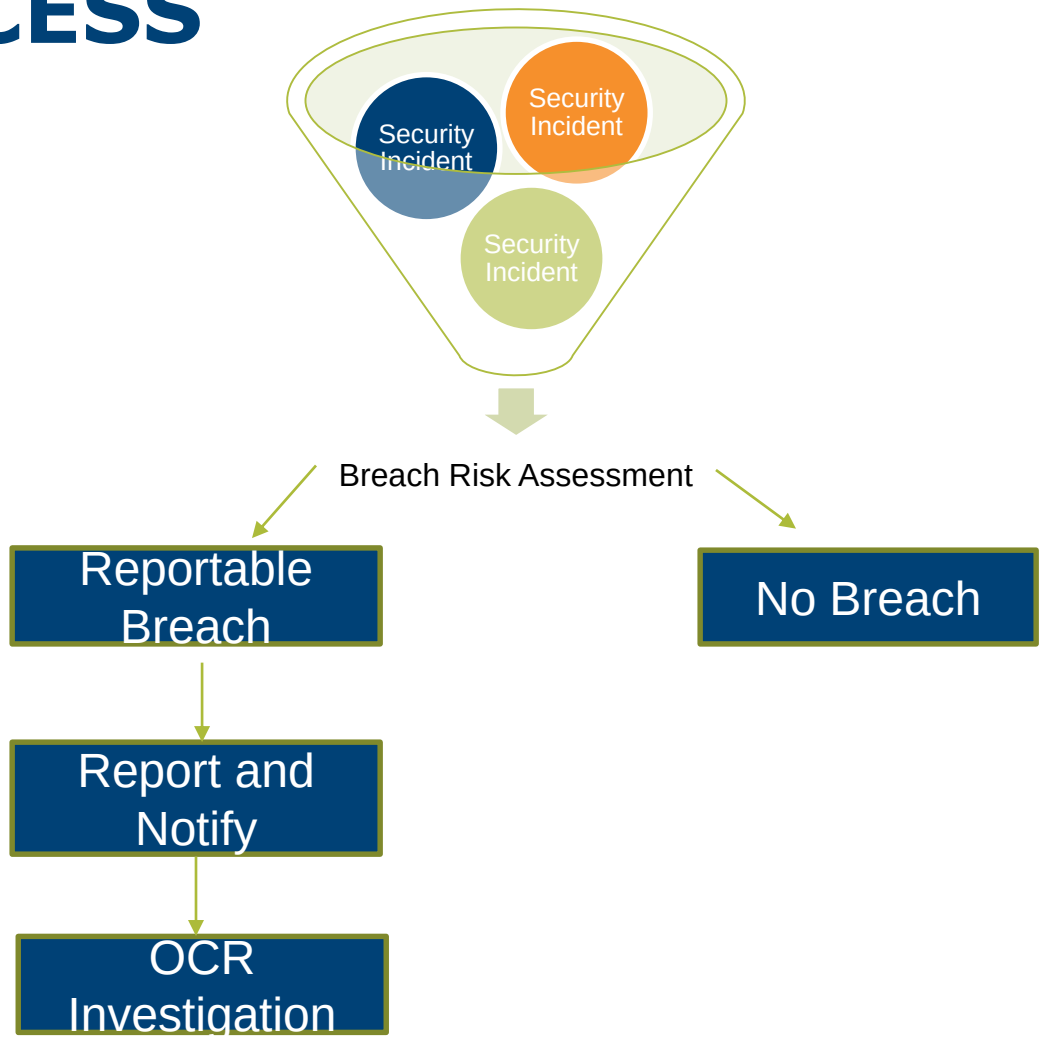
BLUE ORANGE COMPLIANCE

"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

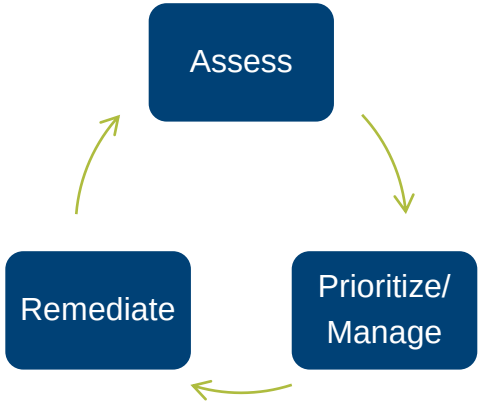


BREACH PROCESS OVERVIEW

- 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



HIPAA SECURITY RISK ANALYSIS

- Required by HIPAA Regulations
- Thorough and Accurate – Assess all requires areas
- Perform Regularly

RESPOND

1. Incident Response Plan - Drill
2. Know your Cyber Security Insurance Policy
3. Have Knowledgeable Legal Resources
4. Have Documentation Ready

CYBER INSURANCE

BLUE ORANGE COMPLIANCE

Information Security Policies

1. Has the **Applicant** implemented a formal information security policy which is applicable to a the **Applicant's** business units?

   If "Yes",

   (a) Does the **Applicant** test the security required by the security policy at least annually?

   (b) Does the **Applicant** regularly identify and assess new threats and adjust the security p to address the new threats?

   (c) Does the **Applicant's** information security policy include policies for the use and storag personally identifiable or other confidential information on laptops?

Web Server Security

1. Does the **Applicant** store personally identifiable or other confidential information on their servers?
2. Do the **Applicant's** web servers have direct access to personally identifiable or other confide information?
3. Does the **Applicant** have firewalls that filter both inbound and outbound traffic?

Virus Prevention, Intrusion Detection & Penetration Testing

1. Are anti-virus programs installed on all of the **Applicant's** PC's and network systems?

   If "Yes", how frequently are the virus detection signatures updated?

2. Does the **Applicant** employ intrusion detection or intrusion protection devices on their netw or IDS or IPS software on the **Applicant's** hosts?

   If "Yes", how frequently are logs reviewed? _____

3. Does the **Applicant** run penetration tests against all parts of their network?

   If "Yes", how often are the tests run? _____

4. Has the **Applicant** been the target of any computer or network attacks (including virus attack the past 2 years?

   If "Yes", did the number of attacks increase?

Mobile Device Security

1. Does the **Applicant** store personally identifiable or other confidential information on mo devices?

   If "Yes", does the **Applicant** encrypt such information?

Business Continuity

1. Does the **Applicant** have a Business Continuity Plan [BCP] specifically designed to address a network related denial-of-service attack? ☐ Yes ☐ No

Security Assessments

1. Has an external system security assessment, other than vulnerability scans or penetration tests, been conducted within the past 12 months? ☐ Yes ☐ No

   If "Yes", please indicate who conducted the assessment, attach copies of the result, and indicate whether all critical recommendations been corrected or complied with.

   If "No", please attach explanation.

Backup & Archiving

1. How frequently does the **Applicant** back up electronic data? _____
2. Does the **Applicant** store back up electronic data with a third party service provider? ☐ Yes ☐ No

   (a) If "Yes", does the **Applicant** have a written contract with the respective service provider(s)? ☐ Yes ☐ No

   (b) If "Yes" to 2(a), does the **Applicant's** contract with the service provider(s) state that the service provider:

   i) Has primary responsibility for the security of the **Applicant's** information? ☐ Yes ☐ No

   ii) Have a contractual responsibility for any losses or expenses associated with any failure to safeguard the **Applicant's** electronic data? ☐ Yes ☐ No

   iii) Does the **Applicant** review their most recent information security audit (i.e. SAS 70)? ☐ Yes ☐ No

Service Providers

1. Does the **Applicant** use third-party technology service providers? ☐ Yes ☐ No

   (a) If "Yes", does the **Applicant** have a written contract with the respective service provider(s)? ☐ Yes ☐ No

   (b) If "Yes" to 1(a), does the **Applicant's** contract with the service provider(s) state that the service provider:

   i) Has primary responsibility for the security of the **Applicant's** information? ☐ Yes ☐ No

   ii) Have a contractual responsibility for any losses or expenses associated with any failure to safeguard the **Applicant's** electronic data? ☐ Yes ☐ No

   iii) Does the **Applicant** review their most recent information security audit (i.e. SAS 70)? ☐ Yes ☐ No

Incident Response Plans

1. Does the **Applicant** have a formal incident response plan that addresses network security incidents or threats? ☐ Yes ☐ No

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