North Carolina HFMA

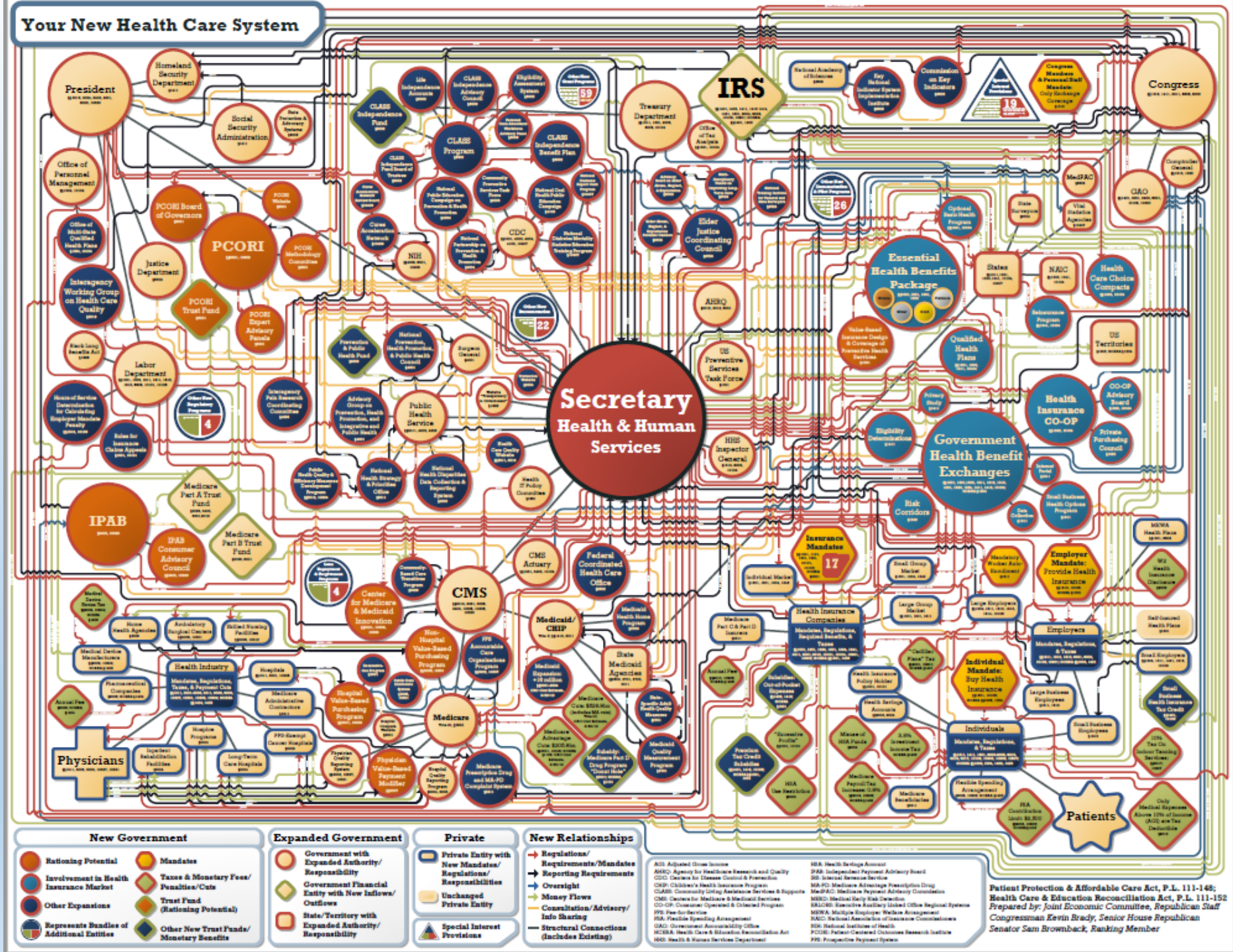
Cybersecurity and Business Operations - Notes from a Facility that worked through a Cyber Event

Adrienne Chase, CSW, EJD, CHC, CHPC, CCEP

Compliance Executive/Leader

Agenda

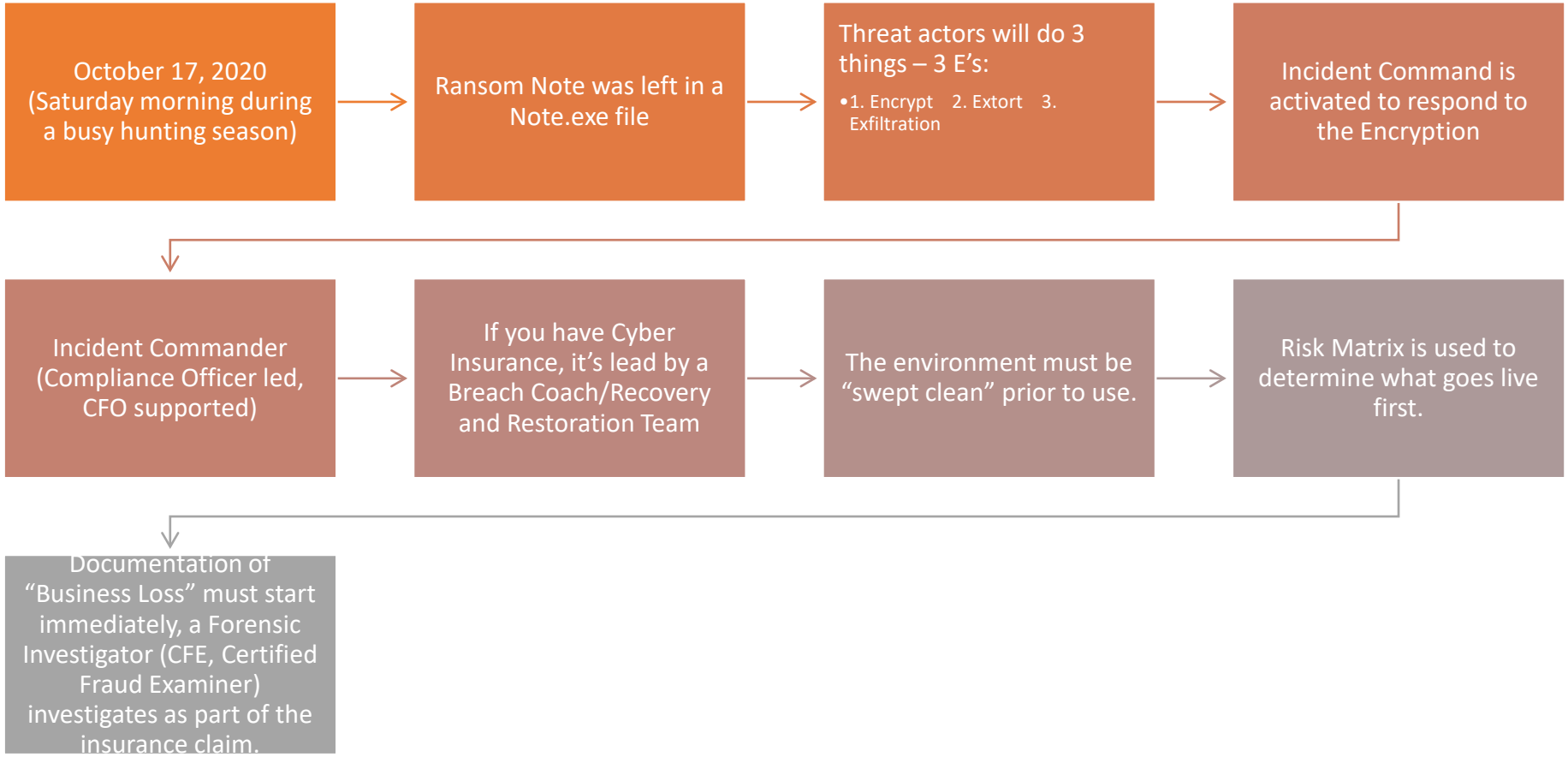
- The Regulatory Landscape in Healthcare
- Introduction and Ransomware Cyber Event Overview
- Insurance Coverage
- Documentation Tips
- Business Contingency Plans and Business Impact Assessments
- Lessons Learned
- Best Practices
- Checklist
- Resources


Your New Health Care System
Secretary
Health & Human Services
President
Homeland Security Department
Social Security Administration
Office of Personnel Management
Office of Multi-State Qualified Health Plans
Interagency Working Group on Health Care Quality
Justice Department
Labor Department
Black Lung Benefits Act
House of Service Determination for Calculating Employer Mandate Penalty
Rules for Insurance Claims Appeals
PCORI
PCORI Board of Governors
PCORI Trust Fund
PCORI Expert Advisory Panels
PCORI Methodology Committee
PCORI Website
Interagency Pain Research Coordinating Committee
IPAB
IPAB Consumer Advisory Council
Medicare Part A Trust Fund
Medicare Part B Trust Fund
Physicians
Medical Device Manufacturers
Pharmaceutical Companies
Annual Fee
Medical Device Excise Tax
Home Health Agencies
Ambulatory Surgical Centers
Skilled Nursing Facilities
Health Industry
Mandates, Regulations, Taxes, & Payment Cuts
Hospitals
Medicare Administrative Contractors
Hospice Programs
Injectable Rehabilitation Facilities
Long-Term Care Hospitals
PPS-Exempt Cancer Hospitals
Physician Quality Reporting System
Physician Value-Based Payment Modifier
Hospital Quality Reporting Program
Medicare Prescription Drug and MA-PD Complaint System
Hospital Value-Based Purchasing Program
Non-Hospital Value-Based Purchasing Program
Accountable Care Organizations Program
Medicare
Medicare Cuts $525 Bln (Includes MA cuts)
Medicare Advantage Cuts $202 Bln
Subsidy: Medicare Part D Drug Program "Donut Hole"
CMS
Center for Medicare & Medicaid Innovation
CMS Actuary
Medicaid/ CHIP
Medicaid Expansion +16 million
State Medicaid Agencies
State-Only Adult Health Insurance
Medicaid Quality Measurement Program
Medicaid Health Home Program
Federal Coordinated Health Care Office
Public Health Service
Public Health Quality & Improvement Program
National Health Strategy & Priorities Office
National Health Disparities Data Collection & Reporting System
Health Care Quality Website
Health IT Policy Committee
Advisory Group on Prevention, Health Promotion, and Integrative and Public Health
Prevention & Public Health Fund
National Prevention, Health Promotion, & Public Health Council
Surgeon General
CDC
National Partnership on Prevention & Health Promotion
National Diabetes Prevention Education Training Program
National Public Education Campaign on Prevention & Health Promotion
National Oral Health Public Education Campaign
Community Transformation Grants
Community Preventive Services Task Force
CLASS Program
CLASS Independence Benefit Plan
CLASS Independence Fund
CLASS Independence Advisory Council
CLASS Independence Fund Board of Trustees
Life Independence Accounts
Eligibility Assessment System
Data Protection & Advocacy System
Cures Innovation Network
NIH
Treasury Department
IRS
Office of Tax Analysis
Elder Justice Coordinating Council
AHRQ
US Preventive Services Task Force
HHS Inspector General
Essential Health Benefits Package
Value-Based Insurance Design & Coverage of Preventive Health Services
Eligibility Determinations
Risk Corridors
Government Health Benefit Exchanges
Health Insurance CO-OP
CO-OP Advisory Board
Private Purchasing Council
Small Business Health Options Program
Data Collection
Qualified Health Plans
Primary Study
Optional Basic Health Program
State Surveyors
States
NAIC
Reinsurance Program
US Territories
Health Care Choice Compacts
MedPAC
Vital Statistics Agencies
GAO
Comptroller General
Congress
Congress Members & Personal Staff Mandate: Only Exchange Coverage
Commission on Key Indicators
National Academy of Sciences
Key National Indicator System Implementation Institute
Insurance Mandates
Health Insurance Companies
Mandates, Regulations, Required Benefits, & Taxes
Medicare Part C & Part D Insurers
Annual Fee
Individual Market
Small Group Market
Large Group Market
Mandatory Worker Auto-Enrollment
Employer Mandate: Provide Health Insurance
Employers
Mandates, Regulations, & Taxes
Large Employers
Small Employers
Self-Insured Health Plans
MEWA Health Plans
W2 Health Insurance Disclosure
Small Business Health Insurance Tax Credit
Large Business Employers
Small Business Employers
Individual Mandate: Buy Health Insurance
Individuals
Mandates, Regulations, & Taxes
Health Insurance Policy Holder
Health Savings Accounts
Waiver of HSA Funds
Medicare Payroll Tax Increase: 0.9%
3.8% Investment Income Tax
Flexible Spending Arrangement
HSA Contribution Limit: $3,300
Medicare Beneficiaries
"Cadillac" Plans" Tax
"Excessive Profits"
HSA Use Restriction
Premium Tax Credit Subsidies
Individual Out-of-Pocket Expenses
10% Tax On Indoor Tanning Services
Only Medical Expenses Above 10% of Income (AGI) are Tax Deductible
Patients
New Government
Rationing Potential
Involvement in Health Insurance Market
Other Expansions
Represents Bundles of Additional Entities
Mandates
Taxes & Monetary Fees/ Penalties/Cuts
Trust Fund (Rationing Potential)
Other New Trust Funds/ Monetary Benefits
Expanded Government
Government with Expanded Authority/ Responsibility
Government Financial Entity with New Inflows/ Outflows
State/Territory with Expanded Authority/ Responsibility
Private
Private Entity with New Mandates/ Regulations/ Responsibilities
Unchanged Private Entity
Special Interest Provisions
New Relationships
Regulations/ Requirements/Mandates
Reporting Requirements
Oversight
Money Flows
Consultation/Advisory/ Info Sharing
Structural Connections (Includes Existing)
AGI: Adjusted Gross Income
AHRQ: Agency for Healthcare Research and Quality
CDC: Centers for Disease Control & Prevention
CHIP: Children's Health Insurance Program
CLASS: Community Living Assistance Services & Supports
CMS: Centers for Medicare & Medicaid Services
CO-OP: Consumer Operated & Oriented Program
FFS: Fee-for-Service
FSA: Flexible Spending Arrangement
GAO: Government Accountability Office
HCERA: Health Care & Education Reconciliation Act
HHS: Health & Human Services Department
HSA: Health Savings Account
IPAB: Independent Payment Advisory Board
IRS: Internal Revenue Service
MA-PD: Medicare Advantage Prescription Drug
MedPAC: Medicare Payment Advisory Commission
MSEO: Medical Early Risk Detection
SNAC/EO: Executive Auxiliary United Office Regional Systems
MEWA: Multiple Employer Welfare Arrangement
NAIC: National Association of Insurance Commissioners
NIH: National Institutes of Health
PCORI: Patient-Centered Outcomes Research Institute
PPS: Prospective Payment System
Patient Protection & Affordable Care Act, P.L. 111-148;
Health Care & Education Reconciliation Act, P.L. 111-152
Prepared by: Joint Economic Committee, Republican Staff
Congressman Kevin Brady, Senior House Republican
Senator Sam Brownback, Ranking Member

Introduction

- Compliance and Privacy Professional with a Social Work and Law background.
- Started a career in social work and clinical case management (direct patient care).
- Obtained a law degree specializing in Healthcare Compliance and sought credentials for Ethics, Privacy, and Compliance.
- Served as a Compliance Professional for 12 years and never imagined living through a “cyber event” for 11 weeks.
- Participated in numerous Table Top Exercise (TTX) events throughout my career which assisted in “what to do” when an event actually happens (aka: preparedness).

“The Incident”



Incident Command and Emergency Preparedness

THE INCIDENT RUNS 24/7 AND IT STAFF WORK AROUND THE CLOCK TO CLEAN AND SANITIZE THE ENVIRONMENT IN ORDER FOR SYSTEMS TO BE UTILIZED IN A SAFE WAY.

KEEP A LOG BOOK OF THE INCIDENT BY THE INCIDENT COMMANDER, WE CALLED OURS “TECHNICAL DIFFICULTIES”

IDEALLY THE BUSINESS IMPACT ASSESSMENTS AND BUSINESS CONTINGENCY PLANS WOULD BE UTILIZED, IF YOU HAVE THEM PREPARED AND UPDATED.

PLAN FOR STAFF TO BE UTILIZED IN AN INCREASED CAPACITY.

DOCUMENT, DOCUMENT, DOCUMENT – FOR BUSINESS/FINANCIAL LOSS

Insurance Coverage – Cyber Liability

Some organizations choose not to obtain coverage.

The coverage requirements are increasingly asking for more information about the information security program.

Ensure that you share those requirements in a secured fashion, threat actors could use that information if it were compromised to gain access into your environment.

Ensure you have a good relationship with your broker who can advocate for the company and rates.

The coverage requirements are very similar to industry standard information security components (i.e. MFA, Network segmentation, etc.).

Business Interruptions / Loss Coverage

What should we document for Business Interruption/Loss?

CHOOSE A WELL VERSED PROFESSIONAL THAT KNOWS THE SERVICE LINES/OPERATIONS AND EXPENSES TO DOCUMENT.

OUTSOURCED SERVICES IN RESPONSE TO THE CYBER INCIDENT (I.E. EXTRA IT STAFF, EXTRA STAFF TO HELP WITH MEDICAL RECORD RECONCILIATION)

OVERTIME AND EXTRA HOURS PUT IN DUE TO THE CYBER INCIDENT.

SERVICE LINES AFFECTED (THERE COULD BE PARTIAL SHUT DOWNS).

PATIENTS THAT WERE RESCHEDULED OR CANCELLED APPOINTMENTS.

Business Contingency Plans and Business Impact Assessments

Integrate this into the overall Emergency Preparedness Process

Enterprise Risk engagement from an overall perspective with all of the Risk Domains: Technology Domain, Patient Safety Domain, etc.

Key highlights that should be in the plans: Top 3-5 digital systems that could be out of service (Human Capital platform, payroll, EMR, Imaging, etc).

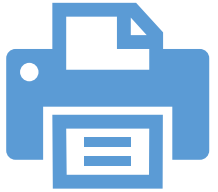
Samples and Templates are available online through reputable companies/vendors.

Lessons Learned

Nothing will ever really prepare you for a cyber attack, it's essentially like a break in, but electronically.

Know your insurance broker and practice (and practice, practice, practice) with them regarding incident management, even the smaller incidents.

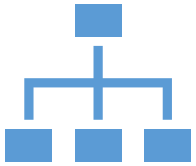
Threat actor targeting specific credentials – Finance and IT Administrators



Think about not being able to use the phone system, faxing, printers and what would you do if you didn't have those.

Best Practices

Involve yourself with the Emergency Preparedness process in the case there is a downtime.



Communicate with your Finance teams to better understand what are your critical systems (critical is defined differently depending on who is evaluating the system).

Get to know your Information Security Official and Privacy Official. Participate in the Table Top Exercise (TTX) to be able to practice, practice, practice.

In Healthcare – it's not just HIPAA/OCR implications and regulations/statutes/laws, it could be international regulators, state regulators, accreditation bodies, CMS, FTC, etc.

Checklist For You

- Insurance Broker and Cyber Carrier: Do you know them and how available are they in an imminent situations?
- Business Impact Assessment (BIA) and Business Contingency Plan (BCP) – these won't be perfect, but start with the critical systems.
- Ensure you have a document prepared in the case Finance has to collect the "damages" from a cyber attack.
- Engage and Collaborate with Enterprise Risk, Privacy Official, and Information Security Official.
- Participate in Table Top Exercises, Finance is a key role.
- Leave you with the 3 E's: Educate, Engage, Effective

Resources

- American Society of Healthcare Risk Management (ASHRM)
- *State associations
- Center for Internet Security Administration (CISA)
- *State CISA contacts
- American Hospital Association (AHA) National Cyber Risk Advisor
- *State Hospital Associations
- HIPAA COW (Collaborative of Wisconsin) and neighboring states
- OCR (Office for Civil Rights)
- FTC (Federal Trade Commission) Identity Theft Resources

Questions and Contact Information

Questions or Commentary

Adrienne Chase

(906)364-4764, LinkedIn Profile available.