




1

Agenda

- Cyber Crime
- Types of Data Being Targeted
- Cyber Crime Networks
- Security Risks
- Responding to an Event
 - Cyber Response
 - Business Continuity Response
- Discussion, Questions & Answers


 An image showing a person's hands typing on a laptop keyboard. The background of the image is a dark, abstract pattern of binary code (0s and 1s) in a light blue/green color.

2

Right from the Headlines...

- *UW Medicine mistakenly exposed information on nearly 1 million patients*
- *326,000 Patients Impacted in UConn Health Phishing Attack*
- *Third-Party Vendor Breach Impacts 45,000 Rush University Patients*
- *Emerson Hospital Reports Third-Party Vendor Breach from May 2018*
- *277,000 Patients Impacted in Medical Device Vendor Breach*
- *UCLS Health Reaches \$7.5M Settlement over 2015 Breach of 4.5M*
- *Month-Long Email Hack on Ohio Dental Insurer Impacts Patient Data*
- *42,000 AdventHealth Patients Impacted in Yearlong Data Breach*

3

Cyber Crime

A Growth Industry

- Data breaches involving health plans account for 63% of breached records between 2010 and 2017
- The majority of breaches are of health care providers – although the majority of records breached are from health plans



4

How it Works

Cyber crime networks use Crime-as-a-Service model

- Recruit technical specialists
- Develop or lease access to malware from a developer
- Spam using phishing
- Just wait to collect



5

GozNym Criminal Network



6

Target Rich Environment

- Nature of health care requires organizations within this sector to keep highly sensitive patient data
 - For doctors to make informed decisions
 - To share information within the healthcare network
 - For post care activities
 - For billing
- Housing this information poses a severe risk
- Need to be prepared with a cyber resilience strategy

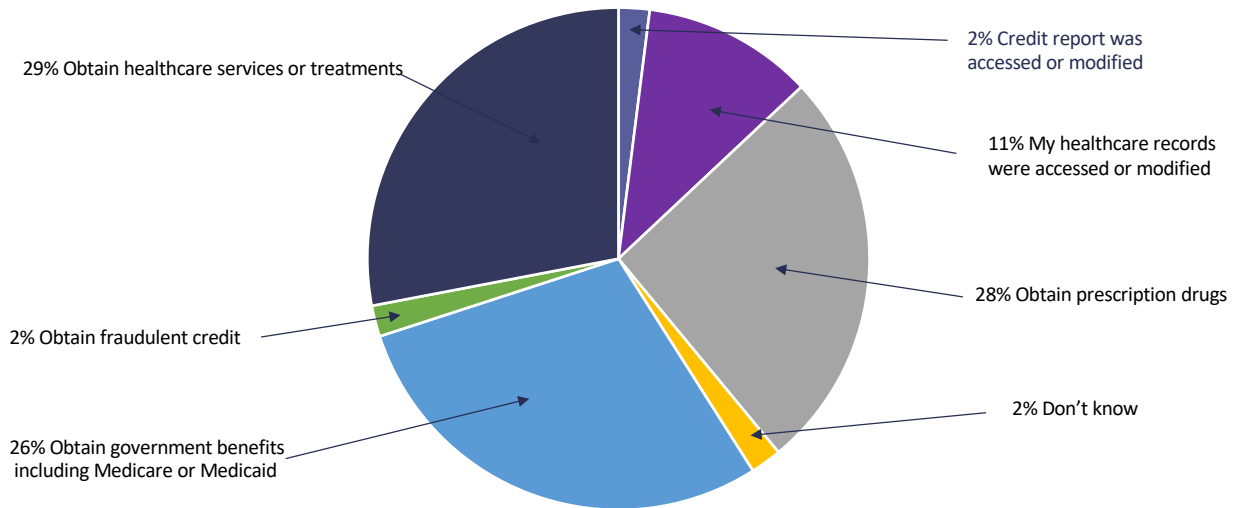
7

Target Rich...Why?

- 50 : 1
 - The street cost of stolen medical information is \$50 vs \$1 for a stolen Social Security number
- 10 : 1
 - The average payout for medical identity theft is \$20,000 compared to \$2,000 for regular identify theft
- Hard to detect
 - Medical identity theft takes more than twice as long to identify as compared to regular identity theft

8

The Value of PHI



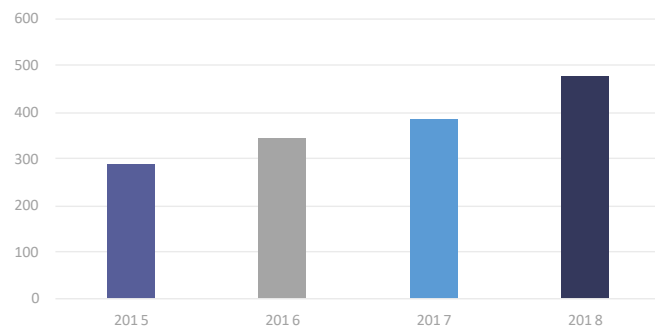
9

Attacks Increasing

Location of Breached Information:

- Provider
- Health Plan
- Business Associate

Number of Breaches Reported to HHS



10

Financial Implications

Date	Name	Amount	Date	Name	Amount
January, 2018	FileFax, Inc	\$100,000 (settlement)	September, 2018	Advance Care Hospitalists	\$500,000 (settlement)
January, 2018	Fresenius Medical Care	\$3,500,000 (judgment)	October, 2018	Allergy Associates	\$125,000 (settlement)
June, 2018	MD Anderson	\$4,384,000 (judgment)	October, 2018	Anthem, Inc	\$16,000,000 (settlement)
August, 2018	Boston Medical Center	\$100,000 (settlement)	November, 2018	Pagosa Springs	\$111,400 (settlement)
September, 2018	Brigham & Women's	\$384,000 (settlement)	December, 2018	Cottage Health	\$3,000,000 (settlement)
September, 2018	Mass General	\$515,000 (settlement)	Total		\$28,683,400

11

Implications of a Cyber Event

Subtitle goes here

12

Impacts

- A cyber event will impact their ability to:
 - Process and pay claims
 - Provide service to members
 - Transmit electronic files to PBM or other critical vendors
- A cyber event will involve
 - The state attorney general's office
 - Department of Health and Human Services, Office of Civil Rights
 - The board of directors
 - The executive leadership and legal
 - Employees

13

What Do You Need to Do?

- Collaborate with CISO on Cyber Resiliency
- Integrate Cyber Security into BCM
 - Governance
 - Executive Sponsor
 - Cyber Response Plan roles
 - Cyber Response Plan Owners
 - Cyber Response Plan Executive Team
 - Cyber Response Communications Team
 - Cyber Response Data Analysis Team
 - Cyber Response Insurance Team
 - Cyber Response Legal Team

14

P D C A

Unify BCM and Cyber Security

- Plan -
 - Identify the “crown jewels” of information assets
 - Collaborate with IT
 - Perform a cyber risk assessment
 - Identify any operational control gaps



15

P D C A

BCM and Cyber Security
Planners

- Do -
 - Integrate Cyber into BCM
 - Formalize escalation process
 - Engage with a forensics organization
 - Preserve evidence



16

P D C A

Unify BCM and Cyber Security

- Check -
 - Make sure appropriate security resources are included in the BCM program
 - Is there appropriate physical security?
 - Is there appropriate data security in place?



17

P D C A

Unify BCM and Cyber Security

- ACT –
 - Exercise your plan vigorously
 - Contain
 - Investigate
 - Remediate
 - Recover
 - Report



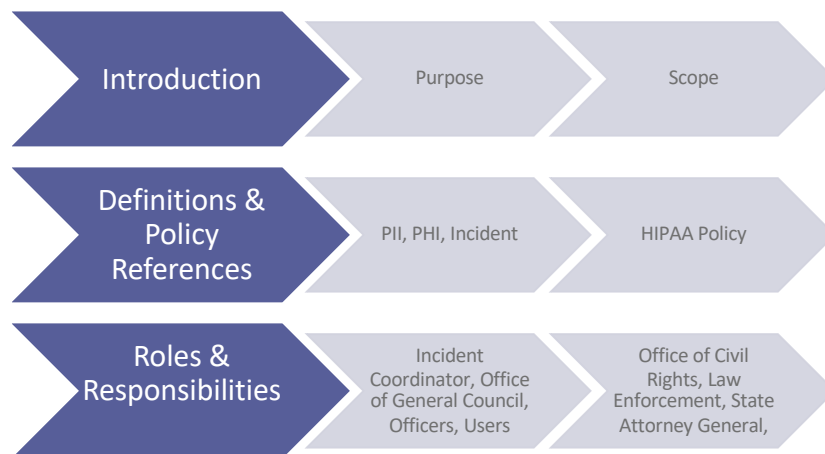
18

What Should You Include in Your Plan?

Subtitle goes here

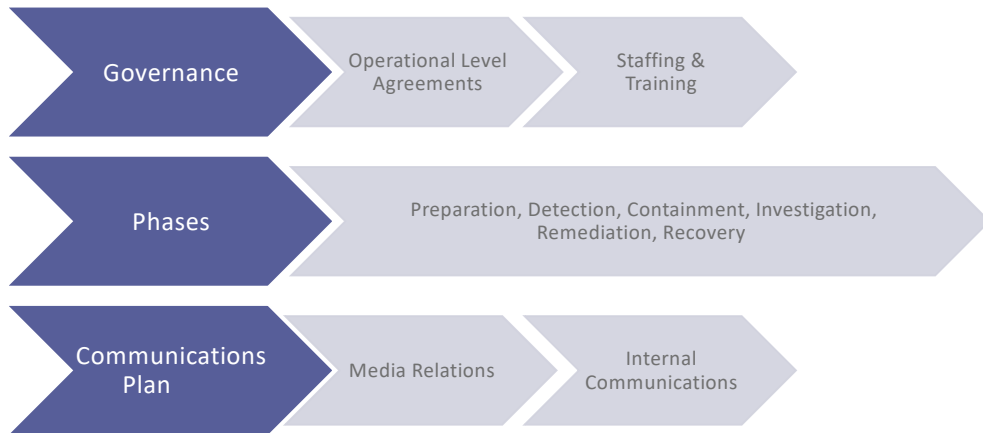
19

Plan Contents



20

Plan Contents



21

What Can You Do?



22

Security Risk Assessment

ID Data Sources

- Inventory ePHI
- Identify other data sources
- Inventory critical Apps
- Inventory what comprises the system
- Determine data flows

Classify Data

- By sensitivity
- By type
- By criticality
- Data protection policy
- Data classification policy

Assign Data Owners

- Data asset inventory and maintenance
- Ensure data is protected
- Review access to data
- Regularly review the program

Review Safeguards

- Administrative
- Policies & Procedures
- Technical
- Access Controls
- Technical Controls
- Physical

23

Cyber Security Lifecycle



24

A Parting Thought...

- Cyber-risk management needs to look beyond the internal information technology (IT) enterprise to other aggregations of risk, such as outsourcing and contractual agreements, supply chain, upstream infrastructure, and external shocks.
- So... let me ask you – is cyber crime a business continuity event?



YES

25

Thank you



26

Sources

- *DRI2018*: BC/DR Opportunities.
- *DHHS; 2018 OCR HIPAA Summary*: Settlements and Judgments.
- *HealthDay*: Health Insurance Companies are Prime Targets for Hackers.
- *The Washington Post*: A cyberattack swept across the globe last week. We should be ready for more.
- *Risk Nexus*: Beyond data breaches: global interconnections of cyber risk. Zurich / Atlantic Council May 2014
- *RSA*: Cybercrime and the Healthcare Industry.
- *Security*: Five Business Continuity Challenges for 2019
- *Security*: How Healthcare is a Major Target for Cybercriminals.
- *SecureWorld*: Inside a Cybercrime Network.