CYBERSECURITY AND PRIVACY RISKS THAT CREATE ENFORCEMENT AND OTHER EXPOSURE

TIMOTHY NOONAN, ACTING DEPUTY DIRECTOR, HEALTH INFORMATION PRIVACY DIVISION
DHHS OFFICE FOR CIVIL RIGHTS
JOAN PODLESKI, CHIEF PRIVACY OFFICER
CHILDREN'S HEALTH SYSTEM OF TEXAS
MARTI ARVIN, VP AUDIT STRATEGY
CYNERGISTEK, INC.

DISCLAIMER:

THE VIEWS EXPRESSED IN THIS PRESENTATION BELONG TO THE SPEAKERS AND DO NOT NECESSARILY REPRESENT THE VIEWS OF THEIR ORGANIZATIONS OR OTHER ORGANIZATIONS.

NOTHING IN THIS PRESENTATION CONSTITUTES LEGAL ADVICE.

2

PRESENTATION OVERVIEW

- BACKGROUND ON THE EVOLUTION OF PRIVACY AND SECURITY RISKS IN HEALTHCARE
- PRIVACY AND INFORMATION SECURITY PROGRAM MATURITY IN HEALTHCARE
- RECENT SETTLEMENTS – WHAT WENT WRONG?
- OCR PHASE II AUDITS- AN OVERVIEW OF THE FINDINGS

3

BACKGROUND

4

TOP SECURITY RISKS IN HEALTHCARE

Theft & Loss

Nearly half of all breaches involve some form of theft or loss of a device not properly protected or paper.

Insider Abuse

Breaches in healthcare continue to be carried out by knowledgeable insiders for identity theft, tax fraud, and financial fraud.

Unintentional Action

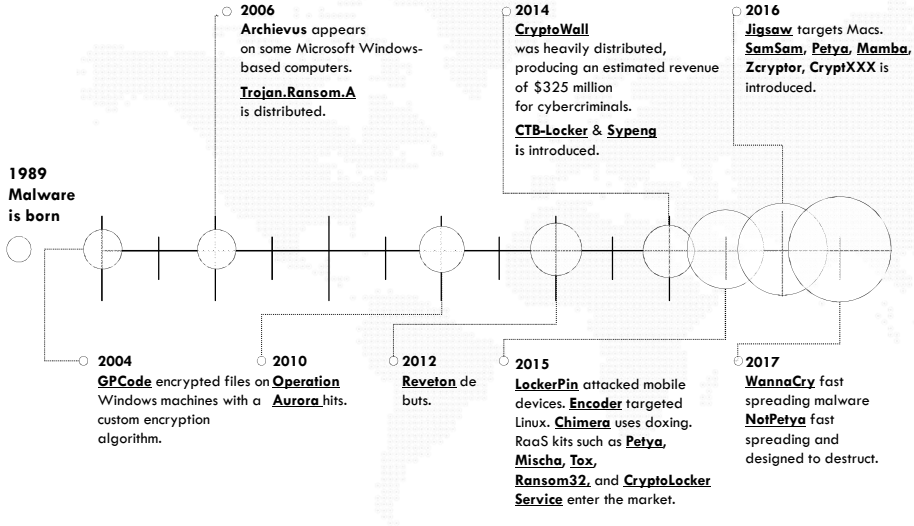
Breaches caused by mistakes or unintentional actions such as improper mailings, errant emails, or facsimiles are still prevalent.

Cyber Attacks

Majority of large breaches reported in 2017 involved some form of hacking and represented nearly 99% of the records compromised.

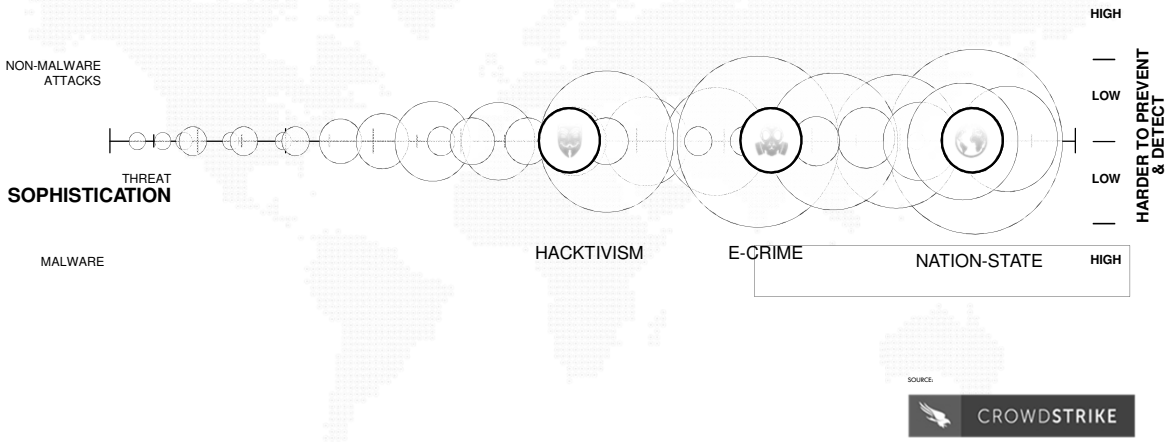
5

ATTACKS ARE GROWING IN FREQUENCY



- Every time a new smartphone is turned on, the digital attack surface grows. Every time a new device is connected to the Internet of Things (IoT), the cyber landscape becomes less secure.
  – *McKinsey & Company*
- Industry experts estimates healthcare cyberattacks rose 320% between 2015 and 2016.
- Healthcare has emerged as the most frequently targeted industry, with 164 threats detected per 1,000 host devices.
  – *Vectra Networks Industry Report 2017*
- Accordingly, healthcare cybersecurity spending is expected to reach nearly $65 billion by 2021.
  – *Cybersecurity Ventures 2017*

ATTACKS ARE GROWING IN SOPHISTICATION



SOURCE: CROWDSTRIKE

CHANGING RISK PRIORITIES

From "Business Critical" to "Mission Critical" to "Life Critical"

Confidentiality	Availability	Integrity

• PHI (HIPAA)
• But also PII & PCI
• Account Information
• Billing & Payment Data
• Intellectual Property
  - Clinical Trials
  - Research
  - Design & Formularies
• Legal & HR Documents
• Identities & Credentials
	• Clinical Systems
	  - EHR & Specialty
	  - Ancillary (PACS, Lab, Pharma)
	  - ePrescription / EPCS
	• Medical Devices
	  - Availability of clinical services and results
	• Business Systems
	  - Email
	  - Billing, Scheduling
		• Critical Patient Data
		  - Prescriptions, Medications
		  - Dosages
		  - Allergies
		  - History
		  - Diagnosis
		  - Alarms
		• Critical Technical Data
		  - Calibration
		  - Safety Limits

Patient Experience: "Patient Trust Zone"

Patient Harm: "Patient Safety Zone"

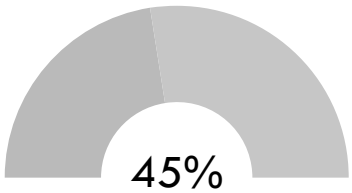
PRIVACY AND INFORMATION SECURITY PROGRAM MATURITY IN HEALTHCARE

ANNUAL REPORT OVERVIEW

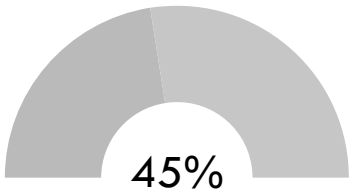
- ANALYZED THE AGGREGATED MATURITY RATINGS OF ASSESSMENTS PERFORMED IN 2017 USING THE NIST CSF AS THE BENCHMARK STANDARD
- PROPRIETARY DATA BASED ON THIRD-PARTY ANALYSIS, NOT SELF REPORTING
- SAMPLE REPRESENTS THE ENTIRE CONTINUUM OF CARE, FROM CRITICAL ACCESS HOSPITALS TO LARGE AMCS TO BUSINESS ASSOCIATES
- DISSECTED FINDINGS BY MULTIPLE CRITERIA: SIZE, REVENUE, TYPE, ETC.

ANNUAL REPORT FINDINGS

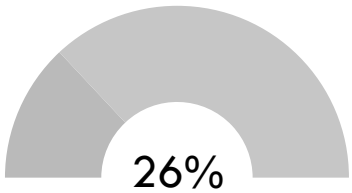
AVERAGE NIST CSF CONFORMANCE



MEDIAN NIST CSF CONFORMANCE



STANDARD DEVIATION ACROSS ALL ASSESSMENTS



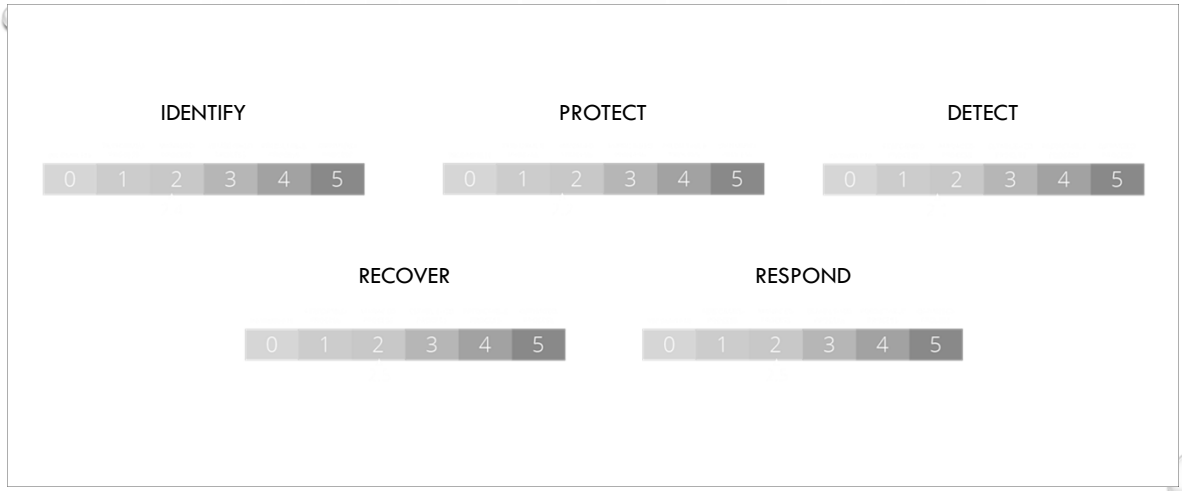
11

ANNUAL REPORT FINDINGS

- RESULTS SHOW US THAT THERE IS STILL CONSIDERABLE ROOM FOR IMPROVEMENT IN CYBERSECURITY, DESPITE OVER TEN YEARS OF REGULATION
- WE AS AN INDUSTRY ARE NOT EQUIPPED OR PREPARED TO ADDRESS CYBER THREATS OR INCIDENTS WHEN THEY OCCUR, OR EVENT IDENTIFY WHERE RISKS MAY BE
- "A CHAIN IS ONLY AS STRONG AS ITS WEAKEST LINK."

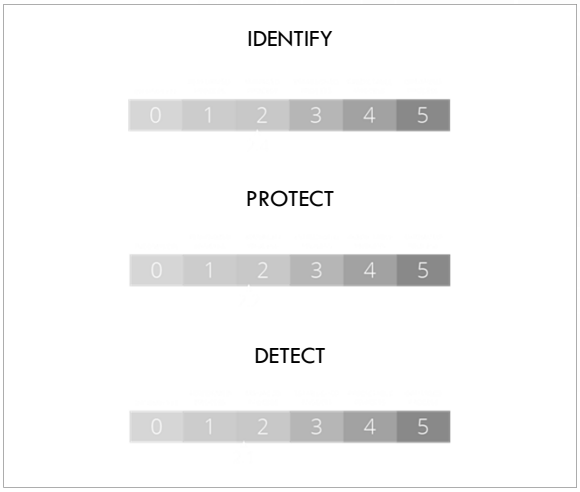
12

ANNUAL REPORT FINDINGS



13

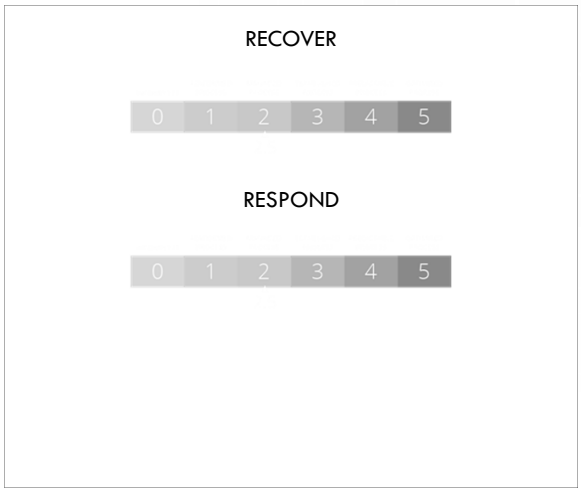
IDENTIFY, PROTECT & DETECT



- A COMPANY IS HIT WITH RANSOMWARE EVERY 40 SECONDS SOMEWHERE IN AMERICA.
- A SURVEY OF 1,300 PHYSICIANS CONDUCTED BY THE AMA AND ACCENTURE FOUND THAT FOUR OUT OF FIVE HAD EXPERIENCED SOME FORM OF A CYBERATTACK
- HEALTHCARE ORGANIZATIONS AND VENDORS HANDLING INFORMATION PROTECTED BY THE HIPAA RULES REPORTED 178 BREACHES IN 2017 WERE DUE TO A CYBERSECURITY INCIDENT.

14

RESPOND & RECOVER



- BETWEEN LOST CHARGE CAPTURE, UNFORESEEN OVERTIME, AND PAYMENT DELAYS PROVIDERS CAN END UP AS MUCH AS $10M - $50M IN THE RED QUICKLY
- "IF YOU FAIL TO PLAN, YOU ARE PLANNING TO FAIL!" B. FRANKLIN

15

RECENT SETTLEMENTS – WHAT WENT WRONG?

16

FOCUS ON RISK ASSESSMENTS

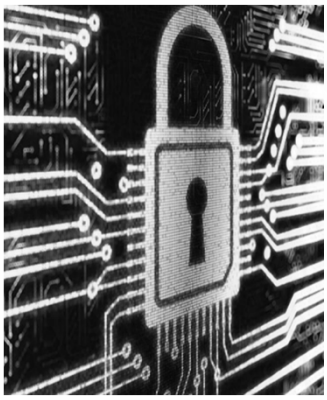
WHAT WENT WRONG?

- FAILURE TO ADDRESS OR FULLY REMEDIATE RISKS IDENTIFIED AND DOCUMENTED PRIOR TO INCIDENTS HAVE RESULTED IN RECENT FINES OF **$3.2M** AND **$5.5M**
  - ACCESS CONTROLS TO EPHI – FORMER EMPLOYEE ID
  - ENCRYPTION OF MOBILE DEVICES

WHAT WENT WRONG?

- **$5.5MILLION** FOR FAILURE TO:
  - CONDUCT A THOROUGH RISK ASSESSMENT FOR ALL THEIR EPHI (NOT JUST THE EMR);
  - HAVE SUFFICIENT PHYSICAL CONTROLS TO DATA CENTERS;
  - OBTAIN ASSURANCES FROM BUSINESS ASSOCIATES ON SAFEGUARDING EPHI;
  - PROTECT AN UNENCRYPTED LAPTOP.

WHAT WENT WRONG?



- **$2.7MILLION FOR FAILURE TO**:
  - PERFORM A FULL RISK ASSESSMENT FOR ALL EPHI;
  - STORE EPHI WITH A CLOUD PROVIDER WITHOUT A BAA;
  - MAINTAIN EPHI ONLY ON ENCRYPTED DEVICES.

WHAT WENT WRONG?

- **$2.5MILLION** FINE - STOLEN LAPTOP WITH EPHI OF 1391 INDIVIDUALS
- NO RISK ASSESSMENT OR RISK MANAGEMENT PROCESSES IN PLACE
- NO POLICIES OR PROCEDURES FOR MOBILE DEVICES
- SECURITY RULE POLICIES ALL IN DRAFT FORM!

WHAT WENT WRONG

ANTHEM, INC. - $16,000,000

- 78.8M INDIVIDUALS AFFECTED
  - LARGEST HEALTH DATA BREACH IN U.S.
- GAINED ACCESS THROUGH SPEAR FISHING IN FEB. 2014
- DATA EXTRACTED FROM DEC. 2014 TO JAN. 2015
  - INCLUDED NAMES, ADDRESSES, DATES OF BIRTH, EMAIL ADDRESSES, SSNS, MEDICAL ID NUMBERS AND EMPLOYMENT INFORMATION
- ISSUES WITH RISK ANALYSIS, INFORMATION SYSTEM ACTIVITY REVIEW, SECURITY INCIDENT RESPONSE AND REPORTING, AND ACCESS CONTROLS
- 2 OTHER SETTLEMENTS –
  - NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS (DECEMBER 2016)
  - CLASS ACTION (AUGUST 2018)

22

FOCUS ON ENCRYPTION & SAFEGUARDS

WHAT WENT WRONG?

$2,140,500 SETTLEMENT

- EPHI OF 31,800 PEOPLE LEFT OPEN TO THE INTERNET FOR A LITTLE OVER A YEAR
- FAILURE TO RECOGNIZE THE RISK OF A NEW SERVER
- NO ENTERPRISE-WIDE RISK ASSESSMENT

WHAT WENT WRONG?

- A FIREWALL IS OF LITTLE VALUE IF EVERYTHING ISN'T BEHIND IT.
- A HEALTH PLAN PAID **$1.7MILLION** IN FINES BECAUSE A WEAKNESS IN 1 PROGRAM LEFT THEIR NETWORK AND THE EPHI OF OVER 600,000 INDIVIDUALS OPEN TO THE INTERNET!

WHAT WENT WRONG?

- A PHYSICIAN ATTEMPTED TO DEACTIVATE A PERSONALLY OWNED COMPUTER WHICH OPENED UP A COVERED ENTITY'S NETWORK FIREWALL, ALLOWING INTERNET ACCESS TO PHI
- A UNIVERSITY & ITS AFFILIATED HOSPITAL PAID **$4.8MILLION** FOR THAT FAILURE

WHAT WENT WRONG?

- WHAT'S THE COST OF A LOST OR STOLEN LAPTOP?
- ENCRYPTED: $0 IN FINES
- UNENCRYPTED: **$3.9MILLION** PAID WHEN 1 LAPTOP WITH INFORMATION ON 13,000 RESEARCH PATIENTS WAS STOLEN

WHAT WENT WRONG?

- $5.5MILLION FOR FAILURE TO PROVIDE REASONABLE ACCESS CONTROLS RESULTING IN IMPERMISSIBLE ACCESS TO PHI OF OVER 115,000 INDIVIDUALS:
  - DID NOT TURN OFF ACCESS FOR A FORMER EMPLOYEE OF AN AFFILIATED PHYSICIAN PRACTICE
  - DID NOT MONITOR ACCESS TO EPHI

WHAT WENT WRONG

ABC Cases $999,000

- BOSTON MEDICAL CENTER - $100,000
- BRIGHAM AND WOMEN'S HOSPITAL - $384,000
- MASSACHUSETTS GENERAL HOSPITAL - $515,00
  - BWH AND MGH ARE MEMBERS OF PARTNERS HEALTHCARE - AN INTEGRATED HEALTH CARE DELIVERY SYSTEM THAT INCLUDES COMMUNITY HOSPITALS, PRIMARY CARE AND SPECIALTY PHYSICIANS, SPECIALTY FACILITIES, COMMUNITY HEALTH CENTERS AND OTHER HEALTH-RELATED ENTITIES
- ALL THREE INVOLVED FILMING FOR "SAVE MY LIFE: BOSTON TRAUMA"
- SIMILAR TO ANOTHER ABC TV SHOW – "NY MED"
  - "NY MED" RESULTED IN A 2016 SETTLEMENT WITH NY PRESBYTERIAN FOR $2.2M
- OCR FILMING GUIDANCE - HTTPS://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/FAQ/2023/FILM-AND-MEDIA/INDEX.HTML

38

AND IT'S NOT JUST HIPAA …..

- ALL 50 STATES NOW HAVE SOME TYPE OF DATA BREACH NOTIFICATION STATUTE
  - ALABAMA ADDED IN APRIL 2018
  - ALL BUT 8 CONCERN ELECTRONIC DATA ONLY
- IN JUNE, NEW JERSEY AG ANNOUNCED FORMATION OF A NEW DATA PRIVACY & CYBERSECURITY SECTION
- ALSO IN JUNE, THE NEW CALIFORNIA CONSUMER PRIVACY ACT WAS PASSED
- IN SEPTEMBER, THE MASSACHUSETTS AG SIGNED A $250,000 SETTLEMENT AGREEMENT WITH UMASS MEMORIAL MEDICAL CENTER FOR A PRIVACY VIOLATION
- AND LET'S NOT FORGET ABOUT GDPR!

30

OCR PHASE II AUDITS- AN OVERVIEW OF THE FINDINGS

31

AUDIT PROGRAM PURPOSE & STATUS

- SUPPORT IMPROVED COMPLIANCE
- IDENTIFY BEST PRACTICES; UNCOVER RISKS & VULNERABILITIES; DETECT AREAS FOR TECHNICAL ASSISTANCE; ENCOURAGE CONSISTENT ATTENTION TO COMPLIANCE
- DEVELOP TOOLS AND GUIDANCE FOR INDUSTRY SELF-EVALUATION AND BREACH PREVENTION
- DESK AUDITS OF COVERED ENTITIES COMPLETED – SEPT 2017
- DESK AUDITS OF BUSINESS ASSOCIATES COMPLETED – DEC 2017
- WEBSITE UPDATES WITH SUMMARY FINDINGS – TO BE PUBLISHED

PHASE 2 - AUDIT PROVISIONS

- FOR COVERED ENTITIES (166):
  - SECURITY RULE (63): RISK ANALYSIS AND RISK MANAGEMENT;
  - BREACH NOTIFICATION RULE: CONTENT AND TIMELINESS OF NOTIFICATIONS; **OR**
  - PRIVACY RULE: NPP AND INDIVIDUAL ACCESS RIGHT
- FOR BUSINESS ASSOCIATES (41):
  - SECURITY RULE: RISK ANALYSIS AND RISK MANAGEMENT **AND**
  - BREACH NOTIFICATION RULE: REPORTING TO COVERED ENTITY
- SEE AUDITEE PROTOCOL GUIDANCE FOR MORE DETAILS:
  HTTP://WWW.HHS.GOV/SITES/DEFAULT/FILES/2016HIPAADESKAUDITAUDITEEGUIDANCE.PDF

CE DESK AUDIT RATINGS

		Rating					
Element #	Provision	1	2	3	4	5	N/A
P55	Notice	2	34	40	11	16	0
P58	eNotice	59	16	4	6	15	3
P65	Access	1	10	27	54	11	0
BNR 12	Timeliness	67	6	2	9	12	7
BNR13	Content	14	15	24	38	7	5
S2	Risk Analysis	0	9	20	21	13	0
S3	Risk Management	2	2	15	28	16	0

BA DESK AUDIT RATINGS

		Rating					
Element #	Provision	1	2	3	4	5	N/A
BNR17	Notice to CEs	0	2	4	3	0	32
S2	Risk Analysis	3	4	16	12	6	0
S3	Risk Management	0	5	8	21	7	0

INITIAL TAKE-AWAYS

Best Outcomes

- Providing timely notice of breach
- Posting of NPP on website
- Providing required NPP content

OCR will examine entity practices for lessons learned that can be shared in technical assistance

Most Room for Improvement

- Risk Management
- Risk Analysis
- Enabling Individual Access

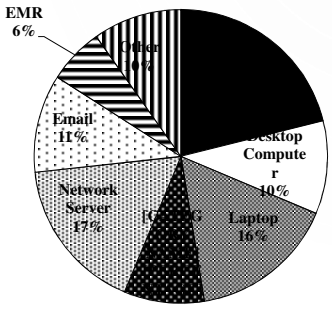
Review OCR guidance and technical assistance

OCR BREACH STATISTICS

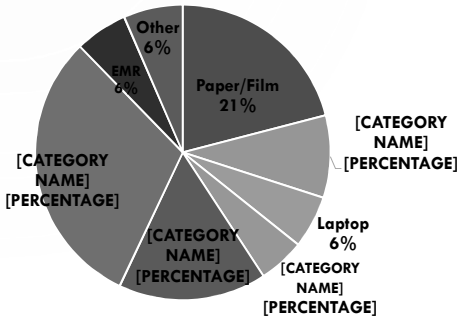
37

500+ Breaches by Location

September 23, 2009 through December 31, 2017



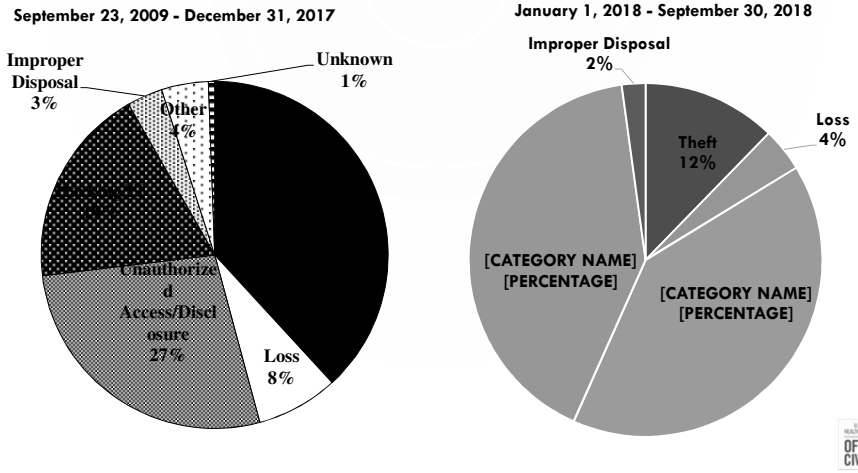
January 1, 2018 through September 30, 2018



38

21

500+ Breaches by Type



OFFICE FOR CIVIL RIGHTS

39

QUESTIONS?

40

CONTACT INFORMATION

- MARTI ARVIN, VP AUDIT STRATEGY, CYNERGISTEK, MARTI.ARVIN@CYNERGISTEK.COM
- TIMOTHY NOONAN, ACTING DEPUTY DIRECTOR, HEALTH INFORMATION PRIVACY DIVISION, TIMOTHY.NOONAN@HHS.GOV
- DHHS OFFICE FOR CIVIL RIGHTS JOAN PODLESKI, CHIEF PRIVACY OFFICER, CHILDREN'S HEALTH SYSTEM OF TEXAS, JOAN.PODLESKI@CHILDRENS.COM

41

RESOURCE MATERIAL

- OCTOBER 5, 2018, JAMA ARTICLE ON HOSPITAL COMPLIANCE WITH MEDICAL RECORDS REQUEST HTTPS://JAMANETWORK.COM/JOURNALS/JAMANETWORKOPEN/FULLARTICLE/2705850
- MASSACHUSETTS GENERAL PRESS RELEASE REGARDING JAMA RESEARCH LETTER HTTPS://WWW.MASSGENERAL.ORG/NEWS/PRESSRELEASE.ASPX?ID=2293
- SEPTEMBER 25, 2018 JAMA RESEARCH LETTER "TEMPORAL TRENDS AND CHARACTERISTICS OF REPORTABLE HEALTH DATA BREACHES, 2010-2017 HTTPS://JAMANETWORK.COM/JOURNALS/JAMA/ISSUE/320/12 (FEE FOR ACCESS)
- BLOOMBERG ARTICLE ON CHINA'S USE OF A TINY CHIP TO INFILTRATE U.S. COMPANIES HTTPS://NA01.SAFELINKS.PROTECTION.OUTLOOK.COM/?URL=HTTPS%3A%2F%2FWWW.BLOOMBERG.COM%2FNEWS%2FFEATURES%2F2018-10-04%2FTHE-BIG-HACK-HOW-CHINA-USED-A-TINY-CHIP-TO-INFILTRATE-AMERICA-S-TOP-COMPANIES&DATA=02%7C01%7CMARTI.ARVIN%40CYNERGISTEK.COM%7C8806D372901042C9A17B08D6307E7B90%7CFC7D3760178742129F7515E4F98738E9%7C0%7C0%7C636749717140131032&SDATA=I1VIDGQYAZRFM%2BOYEVODA%2F%2BN8AHVEFBQMND9RAYQIBE%3D&RESERVED=0

42