# CYBERSECURITY AND HEALTHCARE: HOW TO PREPARE BEFORE AND STEPS TO TAKE AFTER A CYBER EVENT.

February 3, 2022 for the Health Law Bar Section

Jonathan Wheatley
jwheatley@hawleytroxell.com
208.388.4914

HAWLEY TROXELL
ATTORNEYS AND COUNSELORS

1

## RECENT EVENTS

npr

### Cyberattack on Red Cross compromised sensitive data on over 515,000 vulnerable people

January 20, 2022 · 12:57 PM ET

JENNA MCLAUGHLIN

The International Committee of the Red Cross has revealed that hackers have stolen data on over 515,000 "highly vulnerable people," recipients of aid and services from at least 60 affiliates of the charitable organization worldwide.

HAWLEY TROXELL
ATTORNEYS AND COUNSELORS

2

## RECENT EVENTS

The San Diego Union-Tribune

### Scripps begins notifying more than 147,000 people of ransomware records breach

Health system says data thieves did not penetrate main Epic records system

BY PAUL SISSON

JUNE 1, 2021 1:59 PM PT

Scripps Health announced Tuesday that it has begun notifying nearly 150,000 individuals that their personal information was stolen by hackers during the ransomware attack that hit the local health care giant on May 1.

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

3

## BECOMING COMMON PLACE

**KY Hospital Systems Down During Cybersecurity Incident Investigation**

January 27, 2022 by Jill McKeon

Healthcare organizations notified victims of data breaches resulting from cyberattacks, server misconfigurations, and burglaries this week. As a result, the protected health information (PHI) of many patients could be in jeopardy. KY...

**MD Department of Health Systems Down 1 Month After Ransomware Attack**

January 13, 2022 by Jill McKeon

The Maryland Department of Health (MDH) is still trying to recover from a December 4 cyberattack that disabled multiple network infrastructure systems. The cyberattack has impacted state health workers' ability to access shared...

**Data Breaches Hit Saltzer Health, Loyola University Medical Center**

January 10, 2022 by Jill McKeon

Hospitals and outpatient facilities, both large and small, continue to be the targets of healthcare data breaches, placing additional strain on an already overworked sector. The new year began with the announcement of a protected health...

**Business Associate Data Breach Impacts 32 Healthcare Organizations**

January 06, 2022 by Jill McKeon

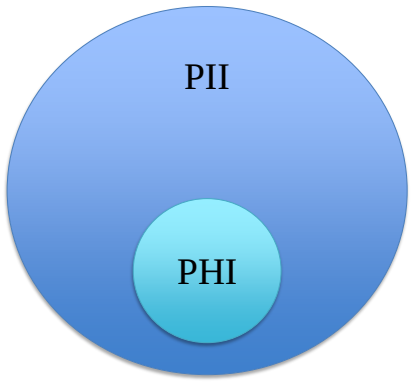
More than 30 healthcare organizations were impacted by a business associate data breach targeted at Ciox Health, a clinical data technology company. An unauthorized third party accessed one Ciox employee's email account between

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

4

## PII AND PHI

- Personally Identifiable Information
- Protected Health Information




HAWLEY TROXELL
ATTORNEYS AND COUNSELORS

5

## IBM REPORT

A recent report prepared by IBM contains some startling statistics on data breach costs:

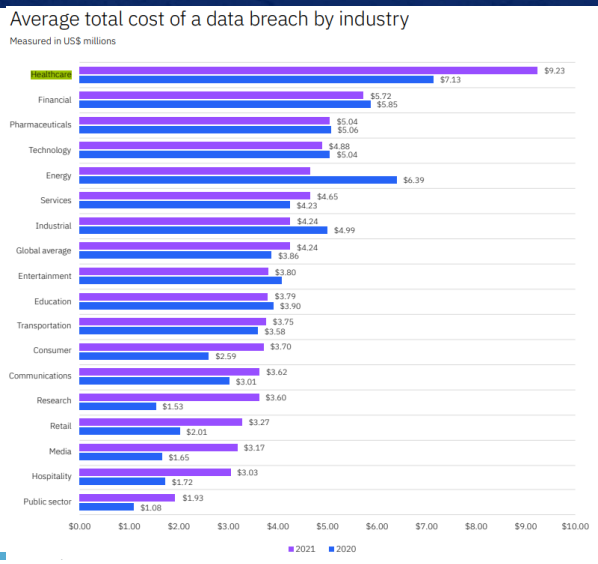
- Average total data breach costs rose from $3.86 million to $4.24 million in 2021.
- The average cost was $1.07 million higher in breaches where remote work was a factor in causing the breach.
- Healthcare data breach costs increased from an average total cost of $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase.
- Customer PII was the costliest record type, at $180 per lost or stolen record.

https://www.ibm.com/security/data-breach.

HAWLEY TROXELL
ATTORNEYS AND COUNSELORS

6

# IBM REPORT AND HEALTHCARE




HAWLEY TROXELL ATTORNEYS AND COUNSELORS

7

# HOW HEALTHCARE IS IMPACTED

Ransomware statistics for 2020

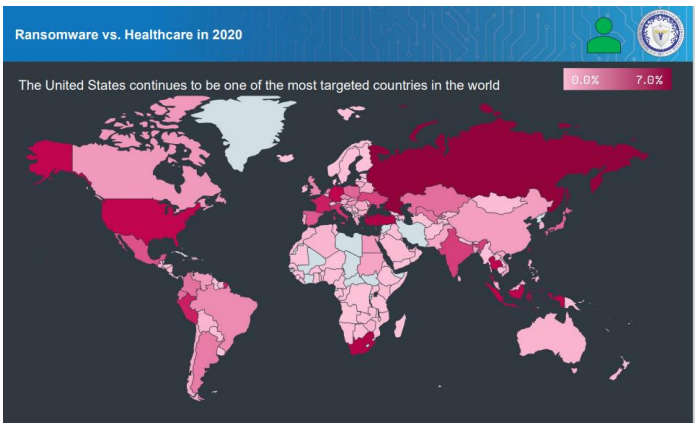
- 80 incidents (560 healthcare organizations impacted)
- Ambulances were rerouted
- Radiation treatments for cancer patients were delayed
- Medical records were rendered temporarily inaccessible and, in some cases, permanently lost
- Hundreds of staff were furloughed
- One healthcare organization in Vermont furloughed 300 staff, estimated the cost at $1.5M/day
- 250 US hospitals lost use of their systems for 3 weeks

https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

8

# U.S. IS A BIG TARGET




https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf

HAWLEY TROXELL
ATTORNEYS AND COUNSELORS

9

# BEST PRACTICES TO TAKE BEFORE A CYBEREVENT

- Think defensively
- Review Privacy Policies and NDAs
- Encrypt your data
- Review internal trainings and tools
- Review cyber insurance policy coverage caps
- Review contracts with cloud vendors
- Proactively engage response partners

HAWLEY TROXELL
ATTORNEYS AND COUNSELORS

10

## A REFRESHER: PRIVACY VERSUS CYBERSECURITY

- "Privacy" relates to a businesses' obligation to safeguard nonpublic personal information.
  - Contractual
  - Statutory
- "Cybersecurity" encompasses the confidentiality, integrity, and availability of data and systems.

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

11

## WHY ARE CYBEREVENTS EXPENSIVE?

- Hacks are different.
- Why?

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

12

## A HACK IS DIFFERENT. WHY?

1. You have to report a hack.
   a) Idaho Code §28-51-105
   b) Oregon Rev. Stat. §§ 646A.600 to .628
   c) Wash. Rev. Code §§ 19.255.010, 42.56.590
   d) Plus 47 others . . .
2. Once it is reported, bad things start to happen.

HAWLEY TROXELL
ATTORNEYS AND COUNSELORS

13

## IDAHO

Idaho Code Section 28-51-104(5): "Personal information" means an Idaho resident's first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:

(a) Social security number;

(b) Driver's license number or Idaho identification card number; or

(c) Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

HAWLEY TROXELL
ATTORNEYS AND COUNSELORS

14

## IDAHO (CONT'D)

Idaho Code Section 28-51-105: A city, county or state agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho **shall**, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident.

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

15

NCSL NATIONAL CONFERENCE OF STATE LEGISLATURES

# Security Breach Notification Laws

4/15/2021

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.

Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data or information brokers, government entities, etc.); definitions of "personal information" (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

16

# SAMPLE DATA BREACH DAMAGES: FLORIDA

The 2020 Florida Statutes

Title XXXIII
REGULATION OF TRADE, COMMERCE, INVESTMENTS, AND SOLICITATIONS

Chapter 501
CONSUMER PROTECTION

View Entire Chapter

501.171 Security of confidential personal information.—

(9) ENFORCEMENT.—

(a) A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the department under s. 501.207 against a covered entity or third-party agent.

(b) In addition to the remedies provided for in paragraph (a), a covered entity that violates subsection (3) or subsection (4) shall be liable for a civil penalty not to exceed $500,000, as follows:

1. In the amount of $1,000 for each day up to the first 30 days following any violation of subsection (3) or subsection (4) and, thereafter, $50,000 for each subsequent 30-day period or portion thereof for up to 180 days.

2. If the violation continues for more than 180 days, in an amount not to exceed $500,000.

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

17

# TO REVIEW . . .

1. You have to comply with privacy laws, NDAs and contracts.
2. But if you have a data breach, you will also have to follow the relevant data breach reporting statutes even if you are otherwise, e.g., CCPA and GDPR compliant.

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

18

## TOP FIVE "CYBERSECURITY" THINGS COMPANIES ARE GETTING SUED FOR

1. Data Breach Reporting Violation
2. Negligence
3. Breach of contract
4. Shareholder suit
5. Regulatory/statutory violation
    a. HIPAA; GLB; COPPA
    b. GDPR, CCPA (California); Illinois (biometric data)

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

19

## "IT'S CLOUD ILLUSIONS I RECALL. I REALLY DON'T KNOW CLOUDS AT ALL."

BUT WAIT! DOESN'T MOVING TO THE CLOUD SOLVE MY DATA SECURITY AND HACKING CONCERNS?

Answer: No.

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

20

## "IT'S CLOUD ILLUSIONS I RECALL. I REALLY DON'T KNOW CLOUDS AT ALL."

1. Your cloud vendor contract disclaims any liability for hacks and breaches and data reporting.
2. The cloud and the move to mobile compound entry points.

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

21

## CYBERLIABILITY INSURANCE

- Hard to find?
- Typically expensive
- Should cover:
  - Data Breach Reporting Obligations
  - Online advertising injury
  - Intellectual property infringement allegations
  - Related privacy lawsuits against you
  - Theft of IP

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

22

## CYBERLIABILITY INSURANCE

Types of Cyber Insurance Coverage

- Date Privacy Coverage
- Liability Coverage for Loss or Breach of Data
- Coverage for Remediation Costs such as Customer Notification and Forensic Investigations
- Coverage for Regulatory Fines and/or Penalties Associated with Data Breaches

Other Types of Cyber Coverage

- Costs and Liability Arising out of Cybersecurity Incidents not involving Data Breaches
- Business and Contingent Business Interruption
- Cyber Extortion
- Media Liability

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

23

## CYBERLIABILITY INSURANCE

Three Reasons to Consider Cyber Insurance:

1. Insurance places a dollar value on an organization's cyber risk.
2. The underwriting process can help organizations identify cybersecurity gaps and opportunities for improvement.
3. Many cyber insurance policies bring supplemental value through the inclusion of risk mitigation tools as well as significant incident response assistance following a cyber incident

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

24

## CYBERLIABILITY INSURANCE

Typical First-Party Coverages:

- **Crisis Management & Identity Theft Response:** Expenses for communications to notify affected customers, provide credit monitoring services, conduct forensic investigations, and for expenses incurred in retaining a crisis management or public relations firm for the purpose of protecting/ restoring the organization's reputation.
- **Cyber Extortion:** Expenses to pay ransom or investigate a threat to release, divulge, disseminate, destroy, steal or use confidential information; introduce malicious code into a computer system; corrupt, damage or destroy a computer system; or restrict or hinder access to a computer system.

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

25

## CYBERLIABILITY INSURANCE

- **Data Asset Protection:** Recovery of your costs and expenses incurred to restore, recreate or regain access to any software or electronic data from back-ups or from originals or to gather, assemble and recreate such software or electronic data from other sources to the level or condition in which it existed immediately prior to its alteration, corruption, destruction, deletion or damage.
- **Network Business Interruption:** Reimbursement for loss of income and/or extra expenses

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

26

## CYBERLIABILITY INSURANCE

Typical Third Coverages:

- **Network Security Liability:** Covers claims from third parties arising from a breach in network security or transmission of malware/viruses to third-party computers and systems.
- **Privacy Liability:** Covers claims from third parties as a result of a failure to properly handle, manage, store or otherwise protect personally identifiable information, confidential corporate information and unintentional violation of privacy regulations.

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

27

## BEST CYBERINSURANCE PRACTICES

- Obtain stakeholder buy in
- Consider premiums, deductibles and policy limits based on extent of costs to deal with, e.g.:
  - Litigation
  - Data breach reporting
- Cover data breach reporting obligations
- Cover remediation
- Cover “hacks”—most policies talk about networks, not incursions
- Will employee training and IT policies reduce premiums?
- No one size fits all

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

28

## BEST CYBERINSURANCE PRACTICES

- Both first- and third-party exposures should be contemplated.
- Remember that cloud vendors make no warranties
- Can you get indemnification anywhere?
- Read exclusions carefully
    a. Is a known vulnerability that you have not patched a pre-existing condition?
    b. Should an un-patched system be covered under a clause for errors and omissions?
    c. When an employee falls for a phishing attack and infects the network that way, is that covered?
- See next several slides for risks.

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

29

## TYPICAL CYBERRISKS/POSSIBLE EXCLUSIONS

- Loss of company confidential information
- Loss of or unauthorized access to and use of customer confidential information, which may include Personally Identifiable Information ("PII"). Such an event also typically triggers a state-by-state Data Breach Reporting Obligation ("DBRO") and breach of contract (NDA/privacy policy) litigation.
- Loss of company intellectual property ("IP"), such as trade secrets
- Loss or corruption of or company or customer data (as a form of property distinct from IP or PII)

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

30

## TYPICAL CYBERRISKS/POSSIBLE EXCLUSIONS

- Denial, impairment or interruption of service to a customer, e.g., a Dedicated Denial of Service ("DDOS") attack causing you to breach your TOS
- Loss of business opportunity by a customer
- Loss of business reputation and customer trust
- Libel, slander and defamation or other actionable oral or written disparagement
- Infringement of copyright, or misappropriation of ideas or plagiarism
- Infringement of trademark

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

31

## TYPICAL CYBERRISKS/POSSIBLE EXCLUSIONS

- Cybersquatting (trademark infringement that occurs through an internet domain name)
- Infringement of patent, namely in this context, a patent covering an online service or other internet-based functionality
- Cloud vendor and cloud issues e.g. data transfer, data loss, data corruption, since most cloud vendor (hosting) contracts DISCLAIM all liability for a hack of their servers!
- Actions of employees or other agents using mobile devices to transmit information

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

32

## TYPICAL CYBERRISKS/POSSIBLE EXCLUSIONS

- Cyberextortion and ransomware , e.g., “WannaCry”
- Website defacement
- Simple negligence by an employee or officer, e.g., leaving an unlocked, unencrypted mobile device in a public place causing loss of Data, IP or PII
- An undiscovered, inadvertent hole in the business’ internet security protocols creating a vulnerability
- The costs of remediating a cyberevent at the customer level, such as expenses incurred for identify theft correction, monitoring and protection.

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

33

## I SURVEYED RECENT DATA BREACH LAWSUITS: HERE ARE KEY TAKE-AWAYS FROM THE CASES

1. Standing allowed
2. Cases will increase, not decrease
3. Plaintiffs lawyers will be emboldened
4. Importance of attorneys’ fees awards
5. No real defenses, per se, to the “hack”
6. Even with defenses, cases still proceed to summary judgment stage ($$$)
7. Are you insured?

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

34

## BEST PRACTICES TO MITIGATE COSTS OF A CYBEREVENT: RECAP

- Think defensively
- Review Privacy Policies and NDAs
- Encrypt your data
- Review internal trainings and tools
- Review cyber insurance policy coverage caps
- Review contracts with cloud vendors
- Proactively engage response partners

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

35

Jonathan Wheatley
jwheatley@hawleytroxell.com

208.388.4914
www.hawleytroxell.com

HAWLEY TROXELL ATTORNEYS AND COUNSELORS

36