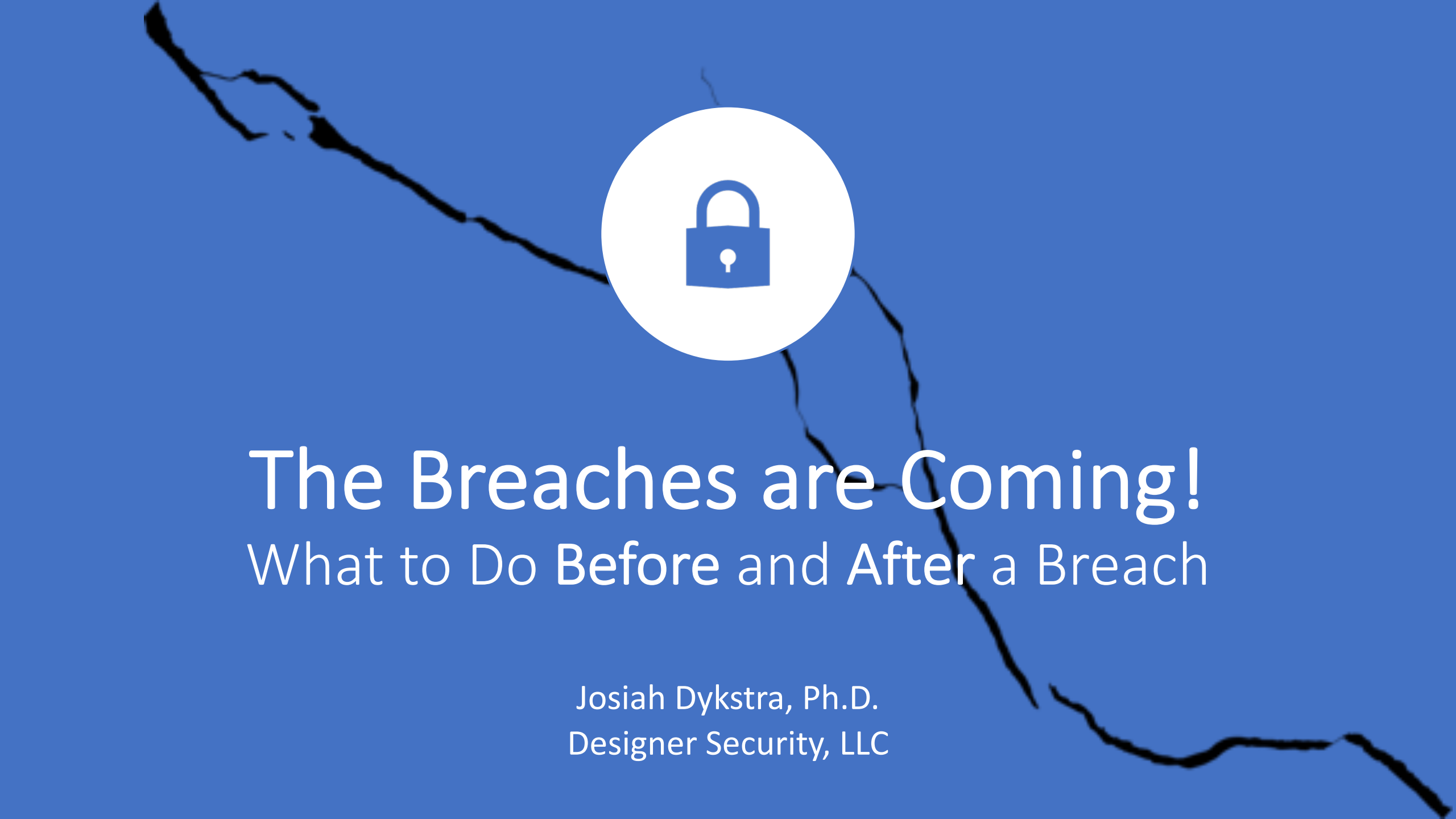


The Breaches are Coming!

What to Do **Before** and **After** a Breach

Josiah Dykstra, Ph.D.
Designer Security, LLC

About Josiah

Designer Security

Cybersecurity design, compliance, and training for Audiologists

- HIPAA Security Risk Assessments
- Security Awareness & Training
- Simulated Phishing Tests
- PCI DSS Credit Card Compliance
- Computer Security Implementation
- Security Policies

Disclosures

Financial Disclosures

Employee, U.S. Department of Defense
President, Designer Security, LLC
Author, O'Reilly Media, Inc.

Non-Financial Disclosures

Cyber Advisory Board, Bowie State University
Distinguished Member, Association for Computing Machinery
Member, Human Factors and Ergonomics Society
Fellow, American Academy of Forensic Sciences
Member, American Association for the Advancement of Science

Learning Objectives

- Attendees will be able to describe the purpose and components of an incident response plan.
- Attendees will be able to explain how cyber insurance can offset risks of a data breach.
- Attendees will be able to list the first three things to do if a data breach occurs.

What is Your Risk Level?

Poll Question #1

How many auto insurance claims did you file for auto collisions in the past 5 years?

a) 0

b) 1

c) 2

d) 3

e) 4

f) 5+

Poll Question #2

What is the top reason that you have homeowners/renters insurance?

a) I cannot afford a loss
b) I want to protect my personal property
c) I am worried about the safety of my family
d) I am worried about the threat of fire, flood, burglary, etc.
e) I do not have homeowners/renters insurance

Data Breaches in Audiology

Q18. How many times was your practice hacked or the victim of a data breach within the past 12 months?

- 0 117
- 1-4 11
- 5-9 1
- 10+ 1

"Cybersecurity in Medical Private Practice: Results of a Survey in Audiology," Josiah Dykstra, Rohan Mathur, Alicia Spoor. *IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, December 2020.

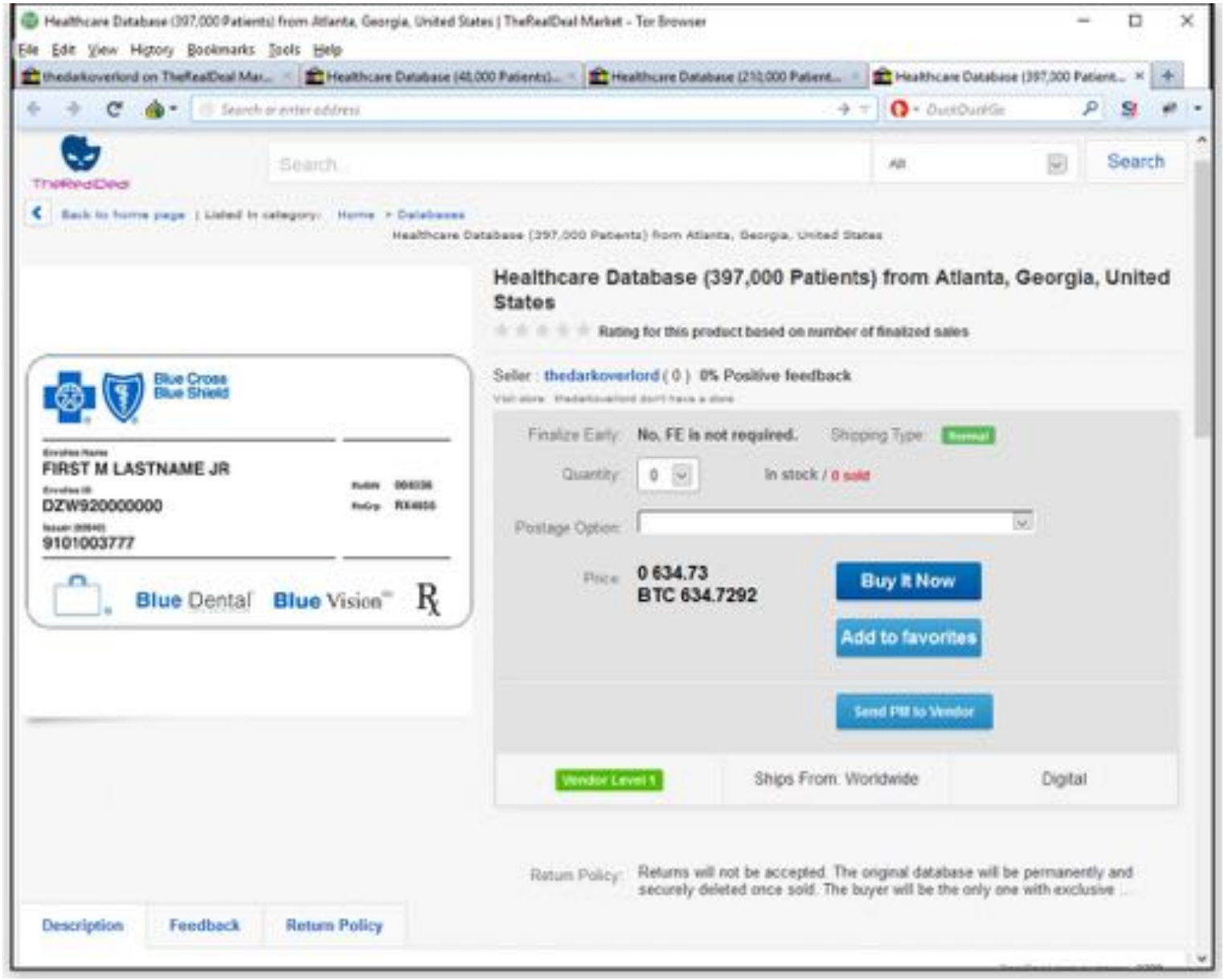
Watch a (fake) Data Breach!

Poll Question #2

When did a data breach occur?

a) When the phishing email was received
b) When the phishing email was opened
c) When the PDF attachment was opened
d) When the attacker accessed the victim's computer
e) No data beach occurred

PHI on the Dark Web



PHI on Twitter

Napkin Math

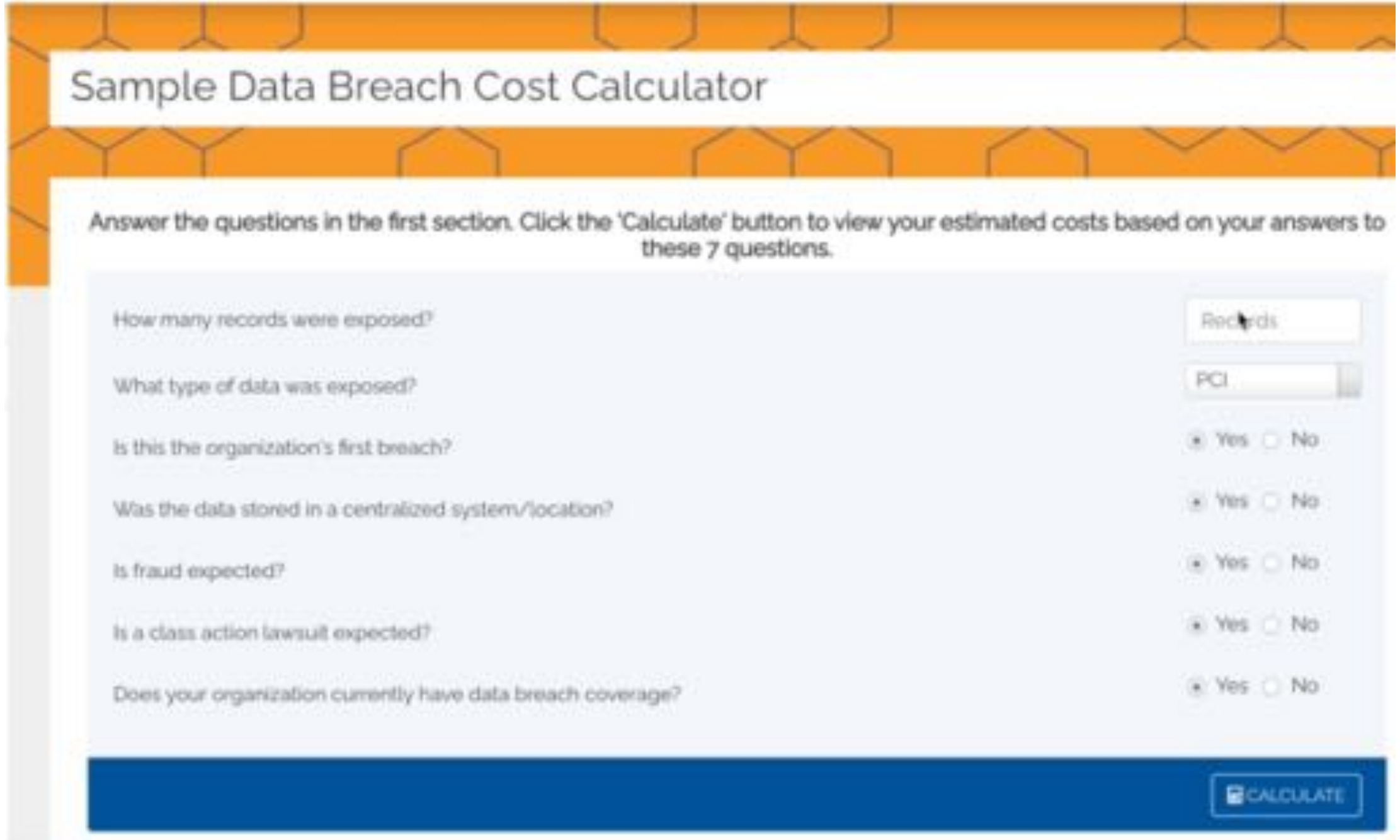
What might your fine be?

Patients x $100 = ? Didn’t know

Patients x $50,000 = ? Willful neglect

Does not include:

- Breach investigation
- Remediation
- Notification Letters
- …



https://eriskhub.com/mini-calc-usli

What is a Data Breach?

An *incident* that results in an *impermissible use or disclosure*

Your attorney should advise you when an *incident* is a data breach

State-level definitions

"Breach of security" of "personal information"

Example from Maryland

MD Comm L Code § 14-3504 (2015)

(a) "Breach of the security of a system" defined. -- In this section:

(1) "Breach of the security of a system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business; and

(2) "Breach of the security of a system" does not include the good faith acquisition of personal information by an employee or agent of a business for the purposes of the business, provided that the personal information is not used or subject to further unauthorized disclosure.

(b) Business owns or licenses personal data -- Investigation of breach. --

(1) A business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach.

HHS on Breach

A breach under the HIPAA Rules is defined as, "…the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.402.6

Unless the covered entity or business associate can demonstrate that there is a "…low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred. The entity must then comply with the applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements. See 45 C.F.R. 164.400-414.

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Email and HIPAA Violations

A single instance of an employee emailing PHI to a home computer could be classified as a data breach!

Cloud and HIPAA Violations

PHI may end up on personal devices

Crisis and Opportunity

"A *crisis* is a fluid and dynamic state of affairs containing equal parts danger and opportunity. It is a turning point, for better or worse."

Stephen Fink
Crisis Communications: The Definitive Guide to Managing the Message

Risk Factors

- **Retention**. The time that the data exists.
- **Proliferation**. The number of copies of the data.
- **Access**. The number of people with access and ways of accessing.

How Are Incidents Uncovered?

"Don't expect a mint on your pillow or a nightly offer of a "turndown service" from hackers to alert you to their presence. Breaches aren't discovered for months in 96% of cases."

Verizon 2018 Data Breach Investigations Report

How Are Incidents Uncovered?

SUSPICIOUS ACTIVITY

ALERT FROM THIRD PARTY

SECURITY EVALUATION

ROUTINE AUDIT LOG ANALYSIS

HIPAA Breach Notification Rule

45 CFR §§ 164.400-414

Individual Notice

No later than 60 days following discovery of a breach

Media Notice

500 residents in one state

No later than 60 days following discovery of a breach

Notice to the Secretary

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

What to Do Before a Breach

• Appoint a **Security Officer**	45 CFR 164.308(a)(2)
• Institute a **Security Awareness & Training Program**	45 CFR 164.308(a)(5)(i)
• Develop an **Incident Response Plan**	45 CFR 164.308(a)(6)(i)
• Develop a **Contingency Plan**	45 CFR 164.308(a)(7)(i)
• Implement a (offline!) data backup plan	45 CFR 164.308(a)(7)(ii)(A)
• Sign **BAAs**	45 CFR 164.308(b)(i)
• Conduct a **risk analysis**	45 CFR 164.308(a)(1)(ii)(A)
• **Encrypt** ePHI on all devices	45 CFR 164.312(a)(2)(iv)
• Evaluate your need for **cyber insurance**	

Incident Response Plan

- This plan covers more than just breaches
- Define what you mean by incidents or events
  - Example: “A security incident is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by us.”
- Roles and Responsibilities
  - Example: “All **employees** must report any suspected or confirmed security incident to the Security Officer immediately upon discovery.”
  - “When notified of a security incident, the **Security Officer** will perform a preliminary analysis of the facts and assess the situation to determine the nature and scope of the incident.”
  - “The Security Officer will contact the practice attorney.” List NAME and PHONE NUMBER.
  - “If advised by legal counsel, contact the cyber insurance carrier.” List NAME and PHONE NUMBER.
- Log all incidents and remedial action
  - Date of report, incident reporter, reported to, description, date closed, mitigation steps.
- Take detailed notes during the response process

Cyber Insurance

"…the purpose of insurance is to protect people from the full consequences of significant adverse events that occur with low probability and little predictability."

Douglas E. Hough
Irrationality in Health Care: What Behavioral Economics Reveals About What We Do and Why

Cyber Insurance in Audiology

24.4% of audiologists in our survey reported having cyber insurance

38.8% for those who spend > $500 per year reported insurance

Around 1/3 of US companies
Healthcare close to 65% in 2020

Cyber Insurance

- Triggers (event for policy to apply)
  - Data breaches
  - Cyber extortion including ransomware
  - Business email compromise
- Insurance often covers:
  - Business interruption
  - Ransomware payments
  - IT forensics
  - Data compromise protection (e.g., credit monitoring)
  - HIPAA fines/penalties
  - Legal fees and expenses
  - Notifying patients about breach
- Insurance may not cover:
  - New hardware
  - PCI fines
  - Reputation damage
  - Social engineering / “voluntary parting”

Insurance Application Questionnaire

Information Security

- Do you back-up mission critical data regularly, routinely store recent back-ups off-line and ensure your backups are well isolated from threats against your production systems?
- How often do you implement system security updates or patches?

Data Encryption & Physical Security

- Do you encrypt all electronic information that leaves your physical control (laptops, mobile devices, storage, etc.), using strong encryption and keys so that only you can decrypt it?

Security Protocols

- Do you use technical measures, devices or tools and techniques including: firewalls, anti-virus, passwords/authentication, to preclude unauthorized infiltration, modification or corruption of your network, including endpoints and sensitive assets within the network?

What to Do After a Suspected Breach

1. **Invoke your incident response plan**
   Ensure the right people do the right thing.
2. **Assess the probability of PHI compromise**
   A breach is presumed unless you can show a low probability of PHI compromise.
3. **Contact your attorney**
   They will advise whether you should also contact your insurance carrier and/or a forensic investigator.

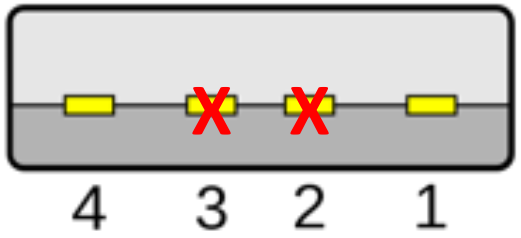
What NOT to Do Immediately

- Don’t panic. Hasty decisions cause more harm.
- Don’t cancel all your appointments.
- Don’t fire anyone.
- Don’t notify patients.
- Don’t wipe and re-install your systems.
- Don’t destroy any data. It may be needed for an investigation/claim.

What (More) to Do After a Suspected Breach

- **Define the incident**
  - What was observed (not what happened)?
  - Calculate 60 days from the discovery date
- **Stop the incident**
  - An attacker may still be present and/or active
- **Document** the incident
- **Notify** appropriate individuals/authorities/agencies
- **Prevent** the incident from happening again

What is that thing you gave us?!



Takeaways

Next week you should:

- Appoint a Security Officer
- Review data backups

In the next 3 months you should:

- Develop an Incident Response Plan
- Establish a culture of security

Within 6 months you should:

- Conduct a risk analysis
- Explore options for cyber insurance

Resources

Data Breaches: Crisis and Opportunity
Sherri Davidoff, Pearson, 2020.

HIPAA News Releases & Bulletins
https://www.hhs.gov/hipaa/newsroom/index.html

FBI Data Breach
https://tips.fbi.gov
https://www.fbi.gov/contact-us/field-offices

July 2021 Healthcare Data Breach Report
https://www.hipaajournal.com/july-2021-healthcare-data-breach-report/

Discussion & Questions

Josiah Dykstra, Ph.D.

Josiah@DesignerSecurity.com