



Best Practices for Avoiding & Mitigating HIPAA Breaches in 2016

June 8, 2016

HiMSS[®]

CENTRAL & SOUTHERN OHIO *Chapter*

About Me

- 19 Years IT Consulting Experience
- PMP
- University Med Center Y2K to HIPAA to Managing Ethical Hackers
- Managing Partner of FOQUS Partners

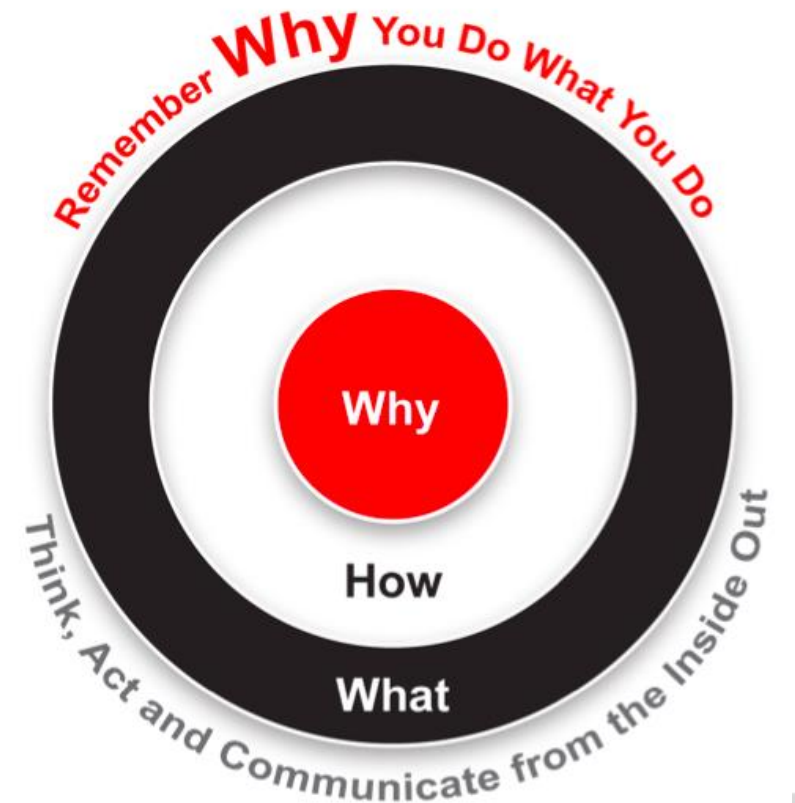


WHYs for Incident Response



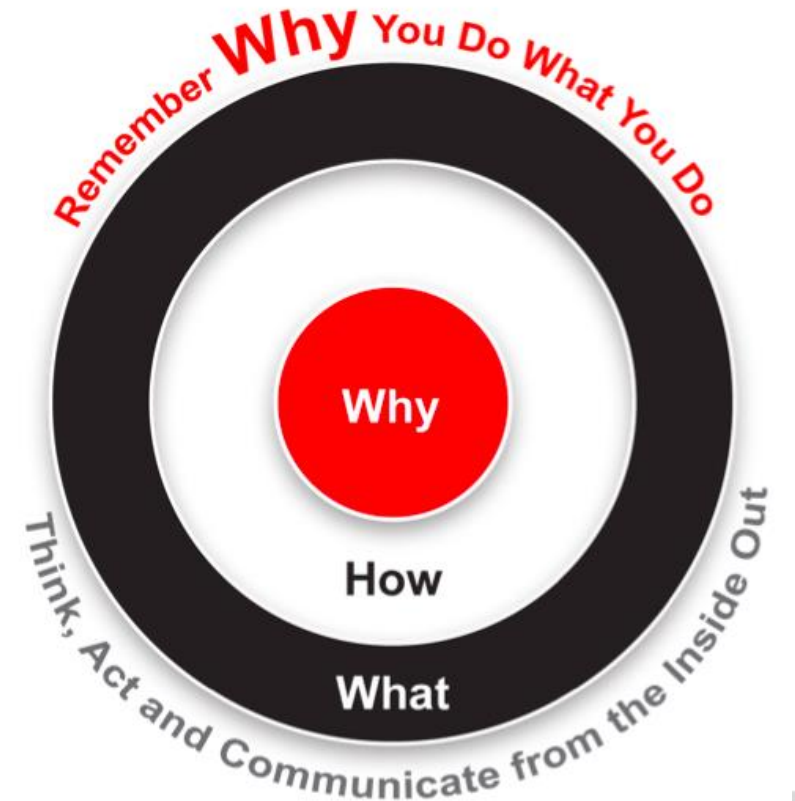
WHYs for Incident Response

- Ensure financially viable organization / reduce risks
- Build patient trust / protect privacy of patients
- Improve healthy outcomes
- Fight for good



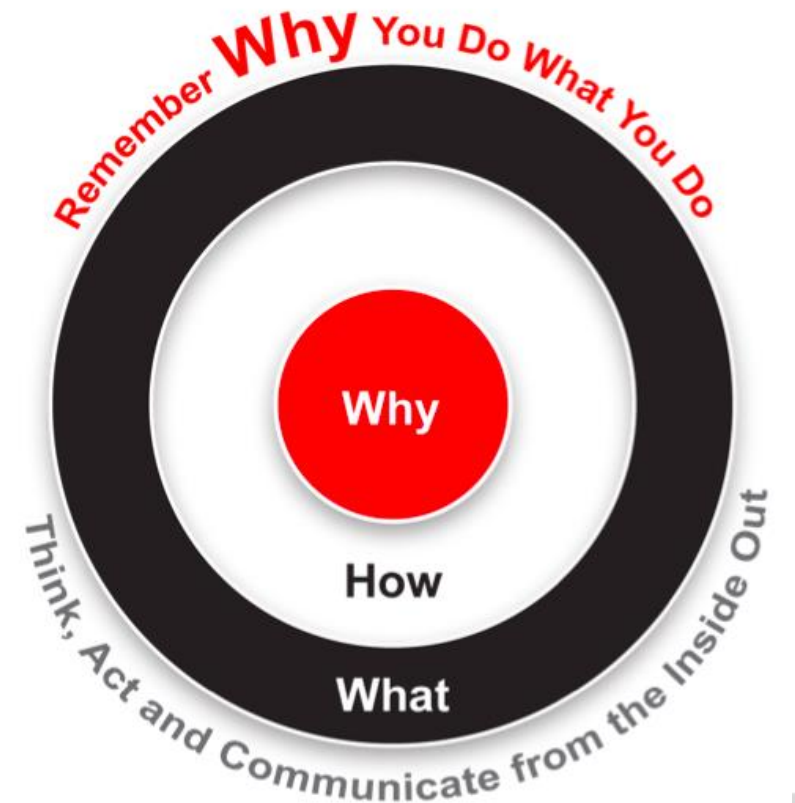
WHYs for Incident Response

- Ensure financially viable organization / reduce risks



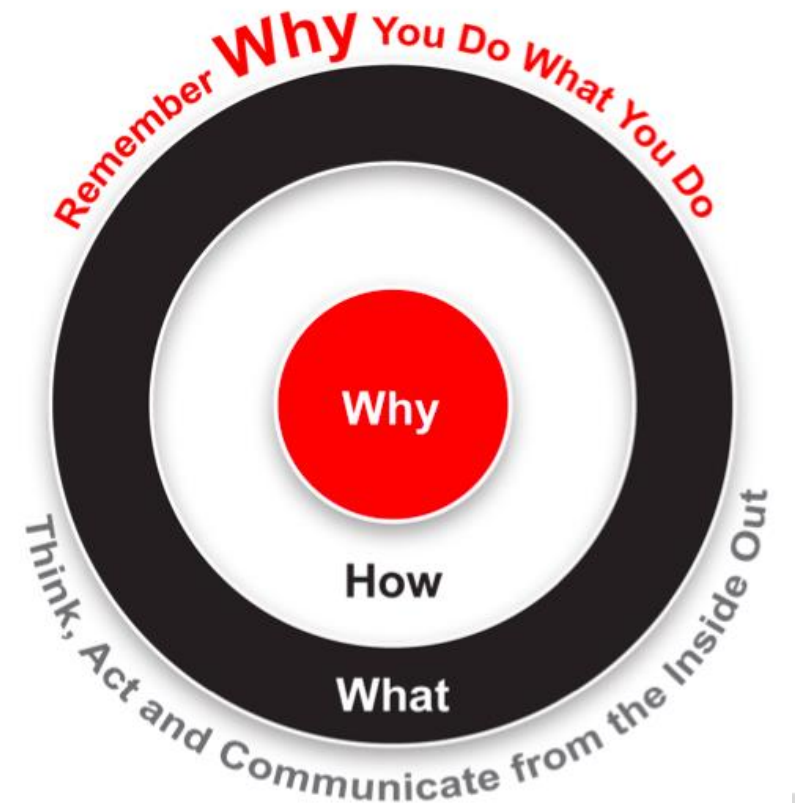
WHYs for Incident Response

- Ensure financially viable organization / reduce risks
- Build patient trust / protect privacy of patients
- Improve healthy outcomes



WHYs for Incident Response

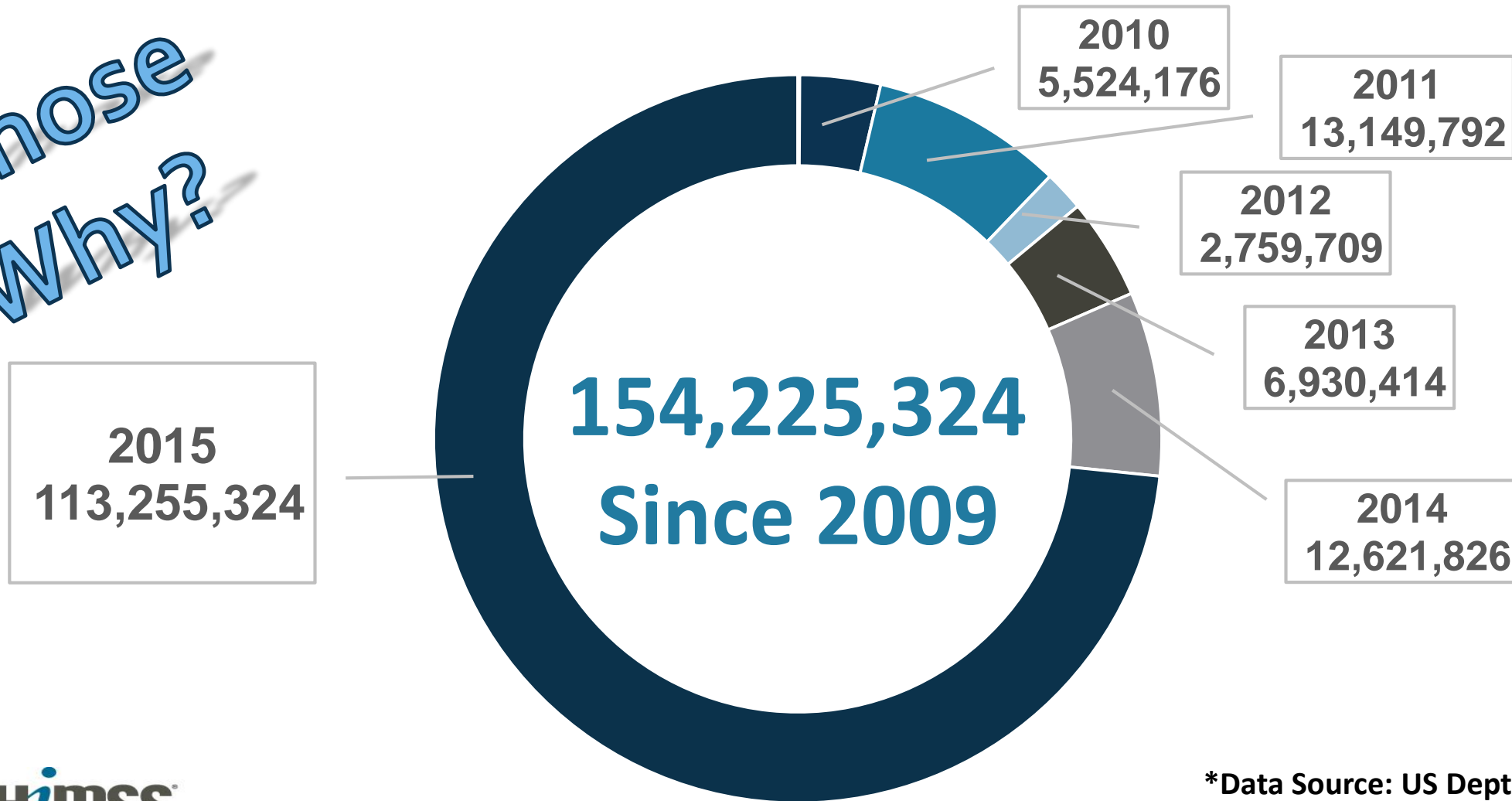
- Ensure financially viable organization / reduce risks
- Build patient trust / protect privacy of patients
- Improve healthy outcomes
- Fight for good



Recap of 2015 Health Data Breach Trends

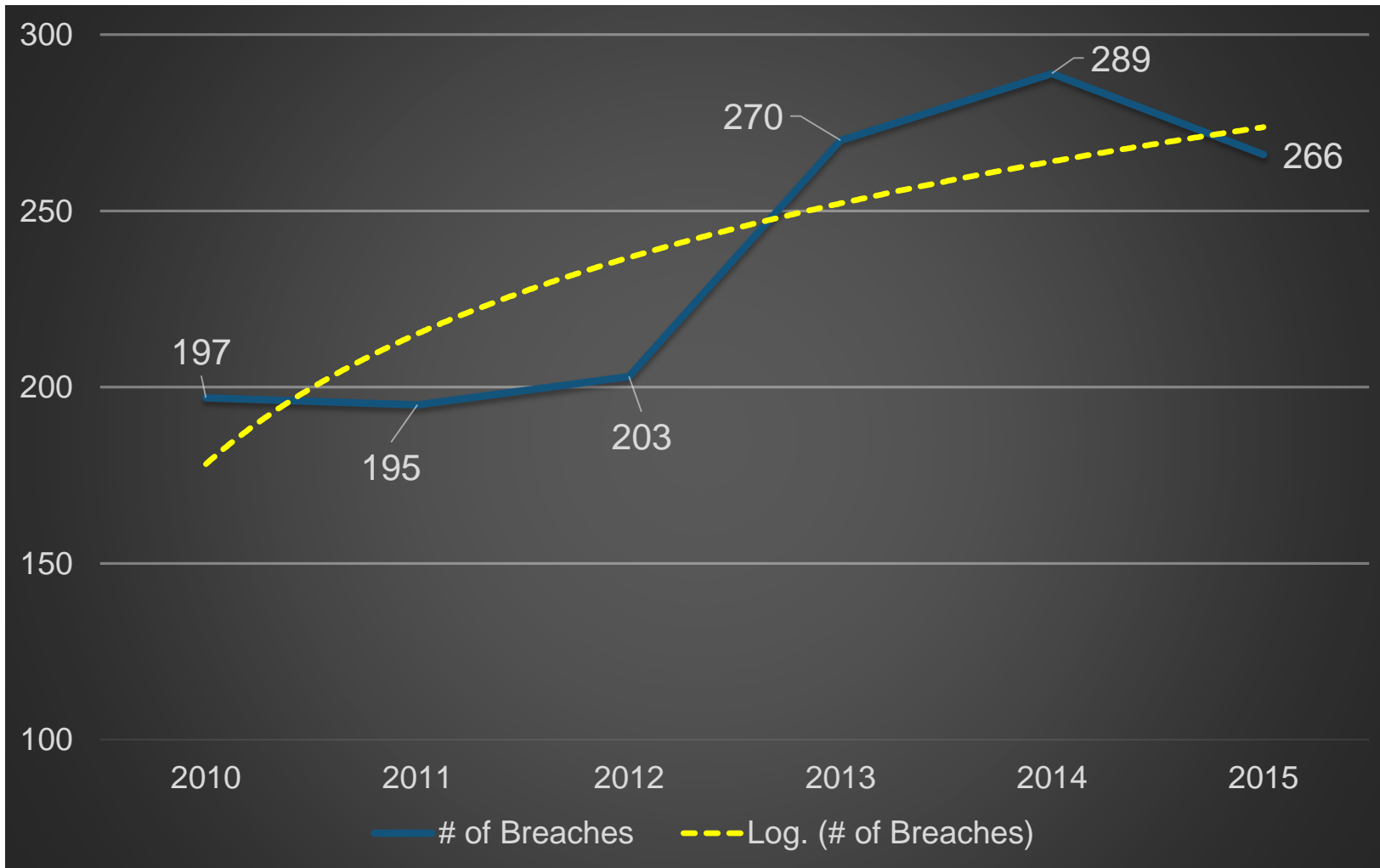
#1: Individuals Affected Skyrocketing

Whose
Why?



Recap of 2015 Health Data Breach Trends

#2: Rate of Increase for Reported Breaches Slowing



Recap of 2015 Health Data Breach Trends

What's the Data Telling Us?

of Patients Affected Skyrocketing

+

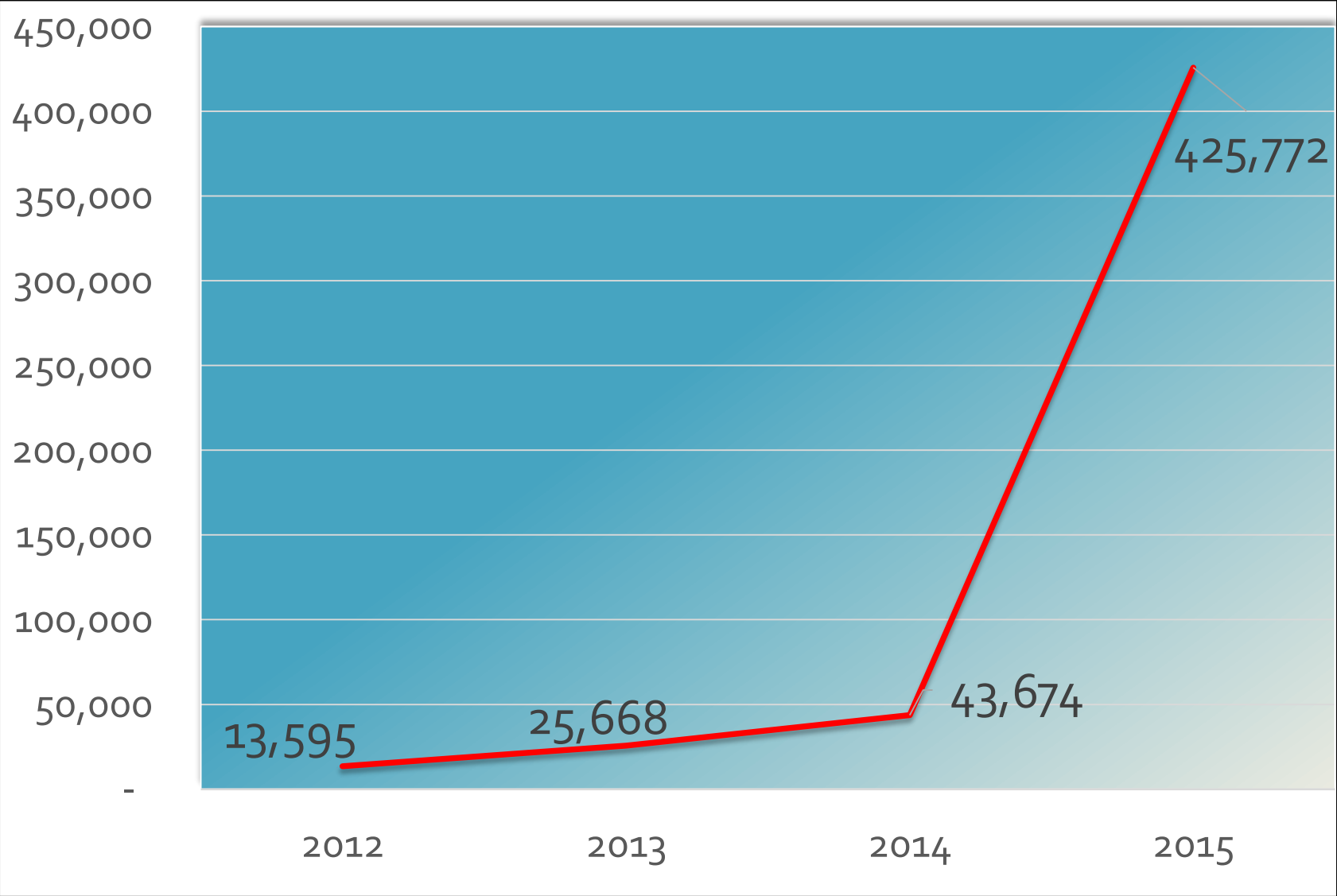
of Breaches Consistent

=

Average Impact of Breaches Increasing

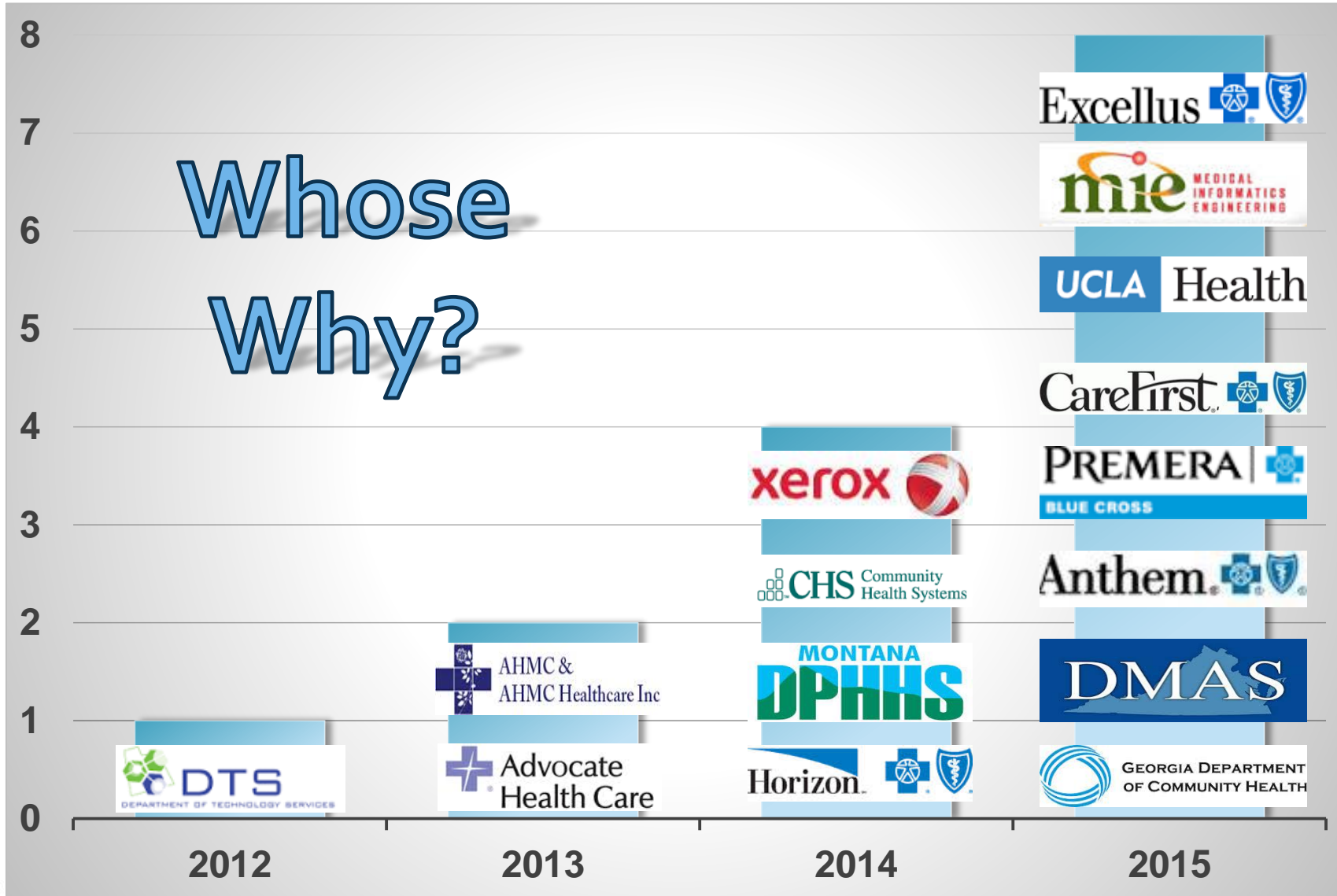


Average # of Patients Affected Per Breach



Health Breaches Affecting 500k+ Individuals

Whose
Why?



So What?

Ponemon Institute reports average cost of a healthcare data breach is \$363 per exposed personally identifiable record.

# of Exposed Personally Identifiable Records	Average Cost of Breach
1,000	\$363,000
5,000	\$1,815,000
10,000	\$3,630,000
50,000	\$18,150,000
100,000	\$36,300,000

Whose
Why?



\$359 in 2014

Recap of 2015 Healthcare Data Breaches

#3: Impact increasing, but organizations adopting best practices to reduce costs

Factors Driving
Costs Higher

- Increase in percentage of attacks criminal in nature
 - 2014 FBI bulletin black market valuations:

Health Record	Valid Credit Card
\$50	\$1

- Why is it so valuable?

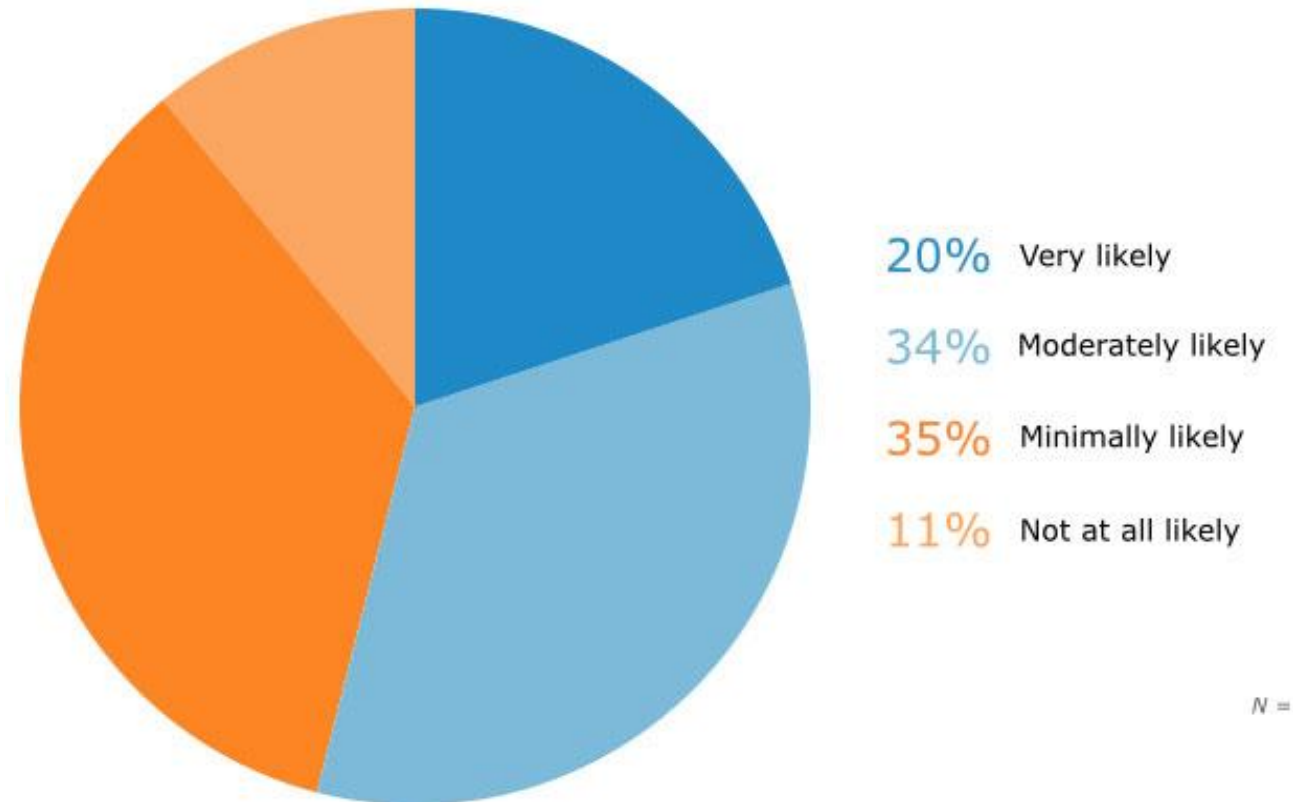
Recap of 2015 Healthcare Data Breaches

#3: Impact increasing, but organizations adopting best practices to reduce costs

Consequences of lost revenues increasing

Whose
Why?

Likelihood to Switch Providers After Security Breach



Recap of 2015 Healthcare Data Breaches

#3: Impact increasing, but organizations adopting best practices to reduce costs

Factors Driving
Costs Higher

- Increase in percentage of attacks criminal in nature
- Consequences of lost business increasing
- Detection & escalation costs increasing

Recap of 2015 Healthcare Data Breaches

#3: Impact increasing, but organizations adopting best practices to reduce costs

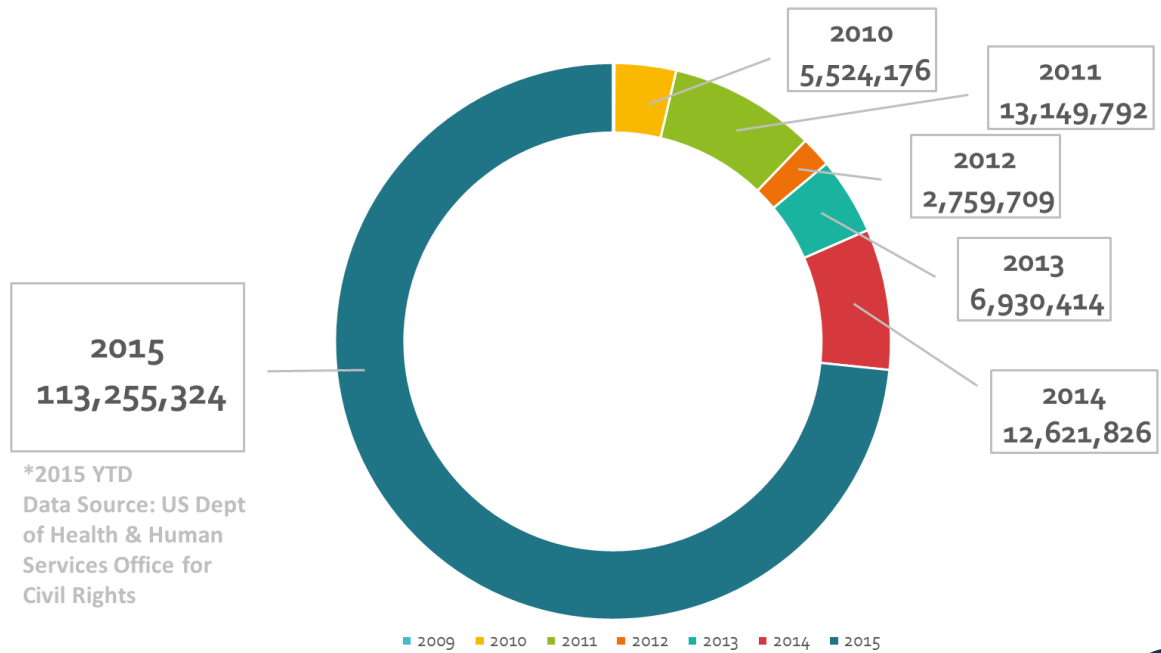
Factors Driving

Costs Higher

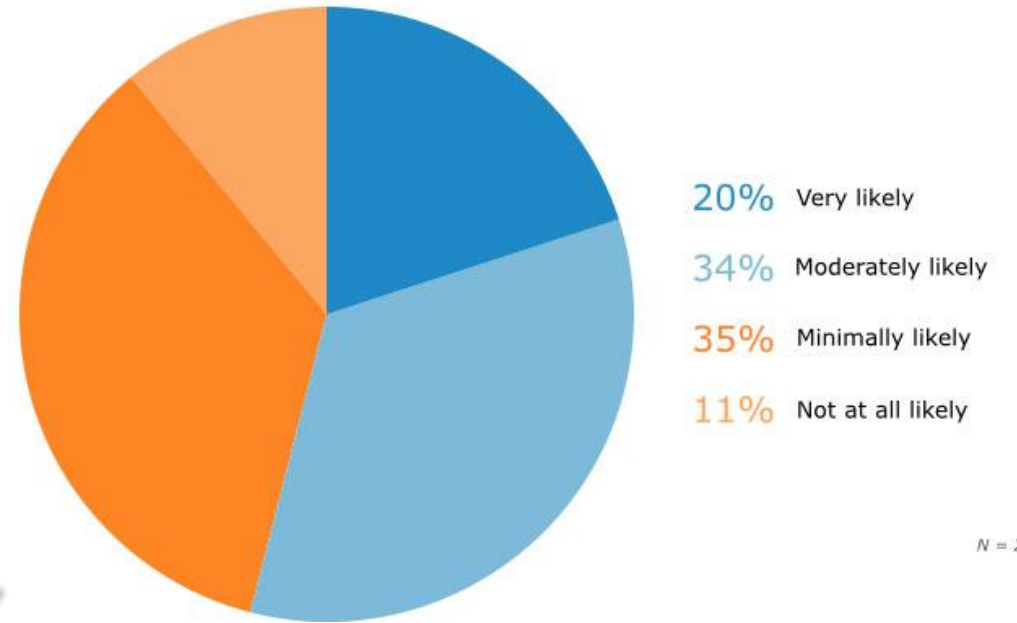
- Incident response team & plan (\$12.6)
- Extensive use of encryption (\$12.0)
- Employee training (\$8.0)
- Business continuity management involved (\$7.1)
- CISO appointed (\$5.6)
- Board of directors involvement (\$5.5)
- Insurance protection (\$4.4)

Whose
Why?

Recap



Likelihood to Switch Providers After Security Breach



Whose
Why?

Reasonable Measures for Incident Response

What Is “Reasonable”:

- 45 CFR 164.306(b): Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting ePHI; and as applicable to the covered entity or business associate –
 - A. Implement the implementation specification if reasonable and appropriate; or
 - B. If implementing the implementation specification is not reasonable & appropriate
 1. Document why it would not be reasonable and appropriate to implement the implementation specification; and
 2. Implement an equivalent alternative measure if reasonable and appropriate.



Average Time to Identify & Contain Breach

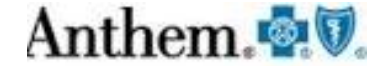
Malicious Attack	Human Error
256 Days*	158 Days*

*Data Source: Ponemon Institute

Trends in Reasonableness

Large Breaches Raising The Bar

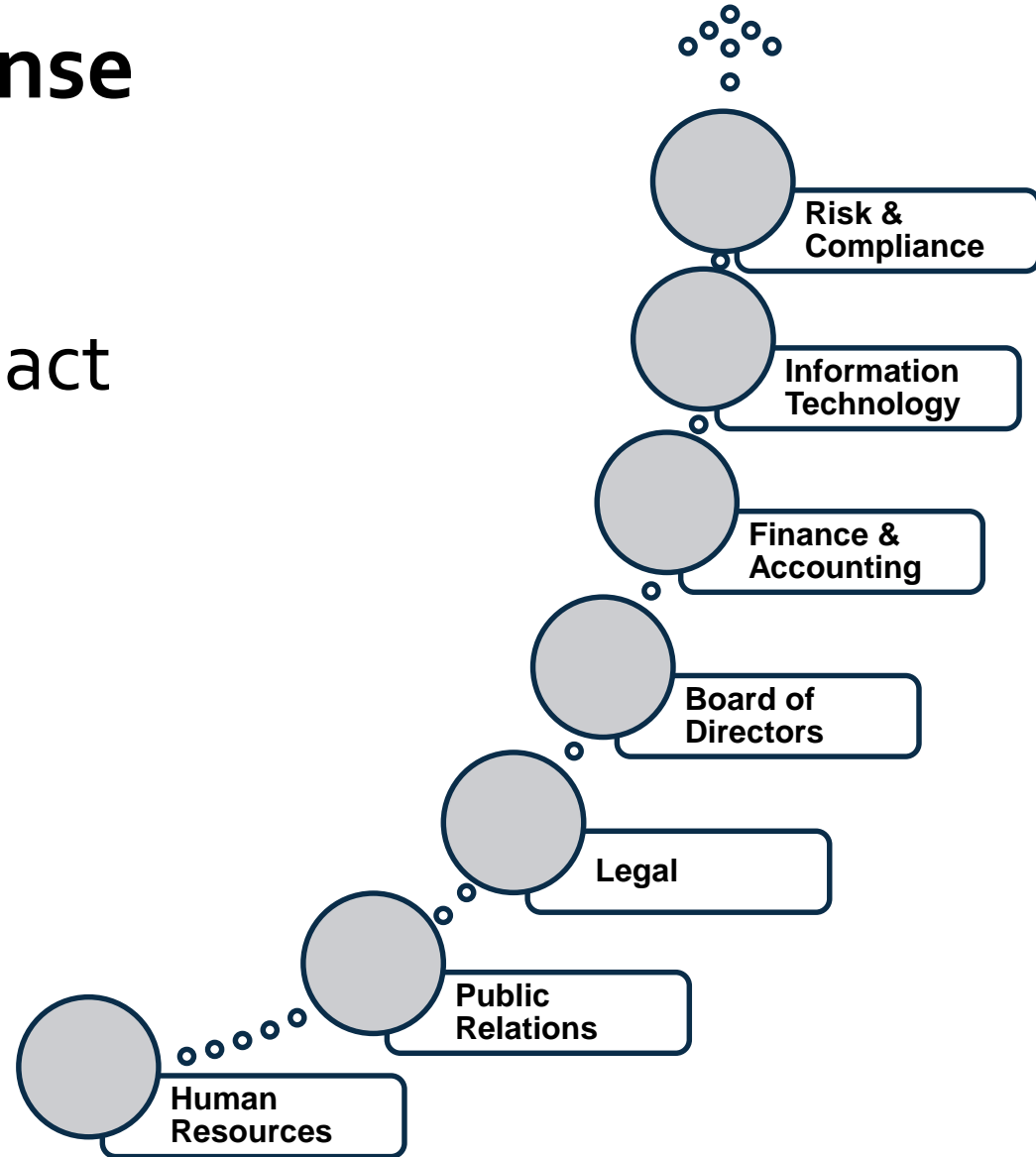
- Exposure
 - Notifications
 - Public hearings
 - Investigations
 - Media
- Lessons learned



Trends in Reasonableness

Organization-wide Response

- Not just an “IT Issue”
- Significant financial impact
 - Board of directors
 - Patient churn
- Employees
 - Awareness
 - Training



Trends in Reasonableness

Significant Financial Impact

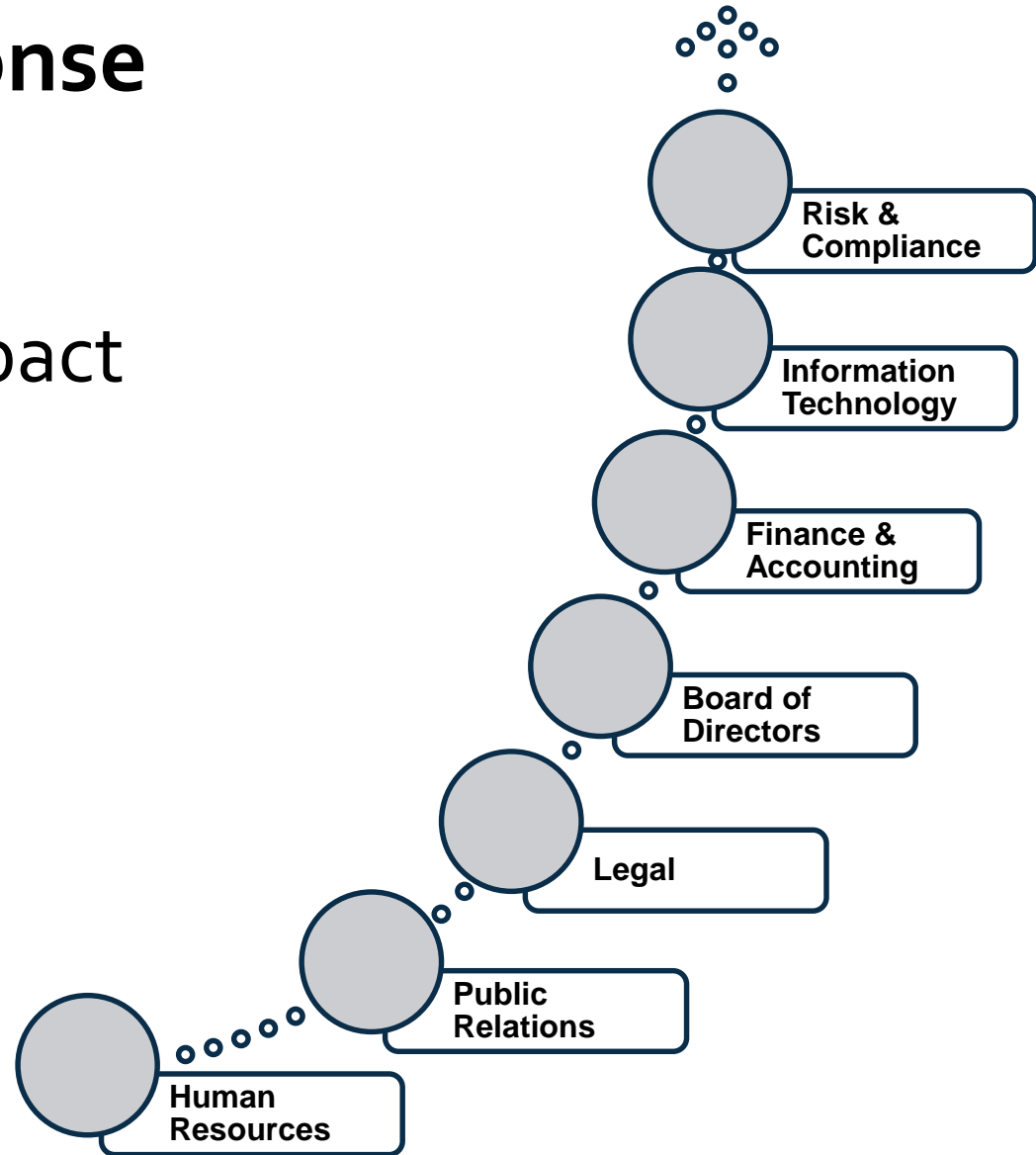
- Per exposed personally identifiable record*:
 - Avg cost of health data breach: **\$363**
 - Avg savings by involving Board of Directors: **\$5.50**
 - Avg savings by having CISO: **\$5.50**
- Breaches impacting patient decisions



Trends in Reasonableness

Organization-wide Response

- Not just an “IT Issue”
- Significant financial impact
 - Board of directors
 - Patient churn
- Employees
 - Awareness
 - Training



Trends in Reasonableness

Employees As Front-Line

- Most likely source of a breach
- Culture of security & privacy
 - Employees as front-line defense
 - Incidents as training input

Example:
Anthem. 



Trends in Reasonableness

Have An Incident Response Plan

- Regulatory reporting complexity increasing
- Eliminate ongoing threats
- Avg \$12.50 per record savings

Example:
UCLA Health

**HAVE A PLAN.
EMERGENCIES ARE
EXPENSIVE.**



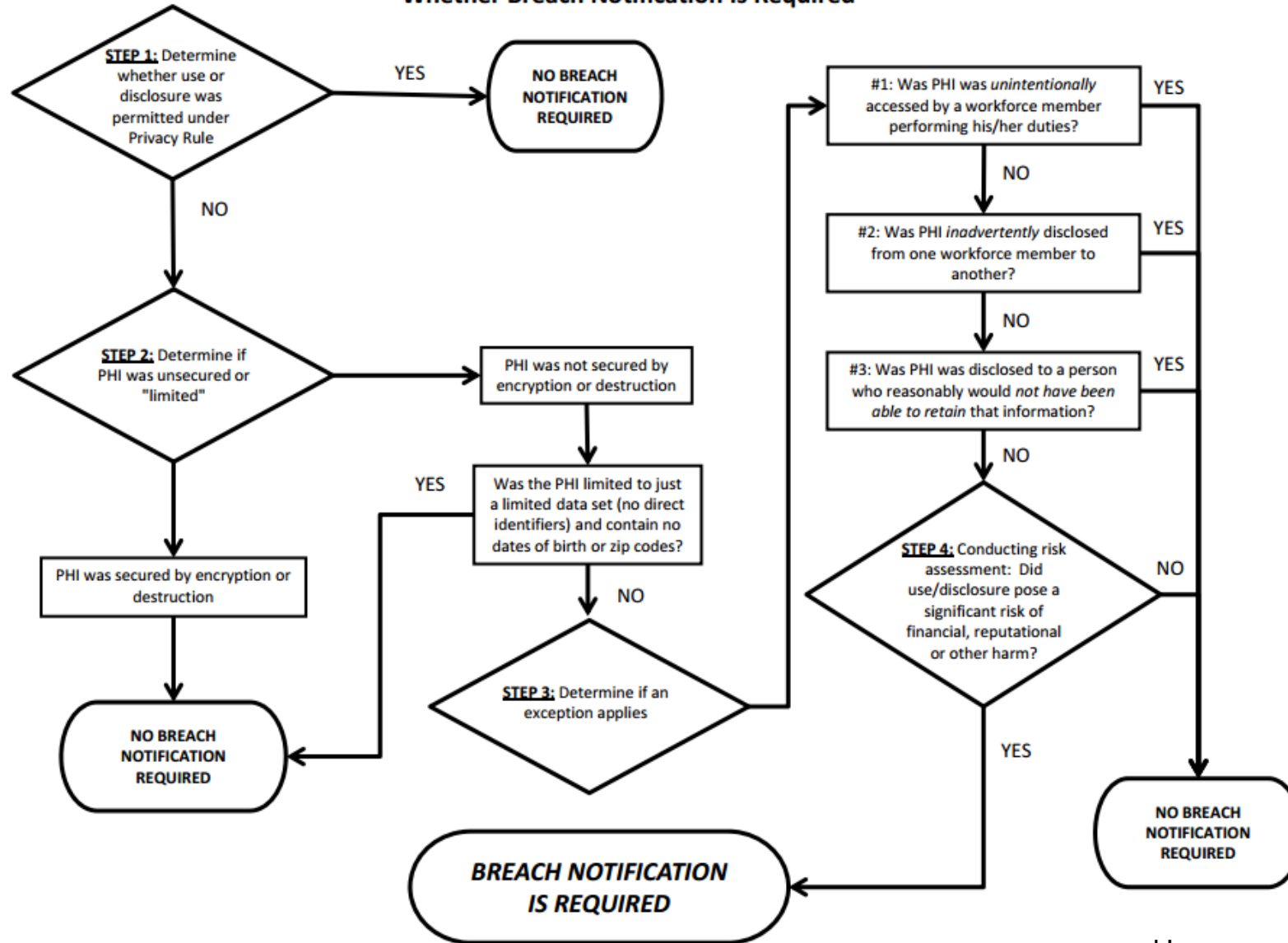
Incident Response Best Practices

Differentiate Incidents and Breaches

	Security Incident	Security Breach
What is it?	An event in violation of a security policy such as impersonation, denial of service, theft, intrusion, etc.	Incident resulting in release of protected personal or confidential data.
Regulatory Reporting Requirements	None today	Local, state & federal requirements
Formats	Paper, electronic device, electronic records, physical location	Paper or electronic records
Organizational Tasks	Investigation Remediation Risk Mitigation	Investigation Remediation Risk Mitigation +Notifications +Regulatory Reporting

Incident Response Best Practices

HIPAA/HITECH Decision Tree to Determine Whether Breach Notification is Required



Incident Response Best Practices

Differentiate Incidents and Breaches

- Decision Tree Tools

- Definition of Breach:

- <https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf>

- Guide to “Securing” PHI:

- <http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html>

Incident Response Best Practices

Differentiate Incident & Breach Types

Tip:
Prioritize

Incident Types	Breach Types
Social engineering / impersonation	Protected Health Information
Unauthorized physical or electronic access	Mental Health Information
System compromise	Personally Identifiable Information
Account compromise	PCI/Credit Card
Denial of service	Malicious/Theft
Network/ vulnerability scanning	Accidental/Loss
Physical loss/ destruction	Internal
Misconfiguration	External
Software vulnerability	Paper
Licensing violation	Electronic

Incident Response Best Practices

Document Breach Reporting Processes

- Regulations, Regulations, Everywhere!

**Tip:
Holistic**

Protected Data Types

Patient Health Data
Credit Card Data
Personally Identifiable Data
Education Data
SEC Data

Regulation Types

Federal
State
Local
Contractual

Incident Response Best Practices

Document Breach Reporting Processes

- Document reporting process by regulation
 - Define reporting teams (Legal, Risk, IT, etc.)
 - Identify internal reviews & approvals
 - Timeline requirements
 - Note: state and local reporting requirements vary

Tip:
Workflow

Incident Response Best Practices

Document Breach Reporting Processes

HIPAA Example:

- Report online at: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf
- > 500 individuals:
 - “Without unreasonable delay and in no case later than 60 calendar days from discovery of breach”
- < 500 individuals:
 - 60 days of the end of calendar year in which breach discovered
 - Can submit all on same day, but must be on individual submissions

Incident Response Best Practices

ORC Breach Portal Reporting



Form Approved: OM

Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

This site is available as we continuously work to make improvements to better serve the public. Should you need assistance with this site or have any questions, please email ocrprivacy@hhs.gov or call us toll-free: (800) 368-1019, TDD toll-free: (800) 537-7697.

To file a breach report, please enter information in the wizard pages below. A field with an asterisk (*) before it is a required field.

General | Contact | Breach | Notice of Breach and Actions Taken | Attestation | Summary

General: Please supply the required general information for the breach.

* Report Type: What type of breach report are you filing?

Initial Breach Report Addendum to Previous Report

→ Next

Incident Response Best Practices

* Please select one of the following:

- Are you a Covered Entity filing on behalf of your organization?
- Are you a Business Associate filing on behalf of a Covered Entity?
- Are you a Covered Entity filing on behalf of a Business Associate?

Covered Entity: Please provide the following information.

* Name of Covered Entity:
(No abbreviations, no acronyms):

* Type of Covered Entity:

* Street Address Line 1:

Street Address Line 2:

* City:

* State:

* ZIP:

Covered Entity Point of Contact Information

* First Name: * Last Name:

* Email:

* Phone Number: (Include area code):

Phone Number	Usage	Edit
<input type="text"/>	- Choose Usage -	Remove

[Add additional phone](#)

Incident Response Best Practices

* **Breach Affecting:** How many individuals are affected by the breach?

500 or More Individuals

Fewer Than 500 Individuals

Breach Dates: Please provide the start and end date (if applicable) for the dates the breach occurred in.

* Breach Start Date:

* Breach End Date:






Discovery Dates: Please provide the start and end date (if applicable) for the dates the breach was discovered.

* Discovery Start
Date:









* Discovery End
Date:

* Approximate
Number of
Individuals Affected
by the Breach:

* **Type of Breach:**




- Hacking/IT Incident 
- Improper Disposal 
- Loss 
- Theft 
- Unauthorized Access/Disclosure 

* **Location of Breach:**

- Desktop Computer 
- Electronic Medical Record 
- Email 
- Laptop 
- Network Server 
- Other Portable Electronic Device 
- Paper/Films 
- Other 

Incident Response Best Practices

* Type of Protected Health Information Involved in Breach:

- Clinical 
- Demographic 
- Financial 
- Other

* Brief Description of the Breach:

4000 / 4000

* Safeguards in Place Prior to Breach:

- None
- Privacy Rule Safeguards (Training, Policies and Procedures, etc.)
- Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.)
- Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.)
- Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

Incident Response Best Practices

General Contact Breach **Notice of Breach and Actions Taken** Attestation Summary

Notice of Breach and Actions Taken: Please supply the required information about notices and actions.

* Individual Notice Provided Start Date: Individual Notice Provided Projected/Expected End Date:

Was Substitute Notice Required? Yes No

Was Media Notice Required? Yes No

* Select State(s) and/or Territories in which media notice was provided:

- Alaska
- Alabama
- Arkansas
- American Samoa
- Arizona
- California
- Colorado
- Connecticut

* Actions Taken in Response to Breach:

- Adopted encryption technologies
- Changed password/strengthened password requirements
- Created a new/updated Security Rule Risk Management Plan
- Implemented new technical safeguards
- Implemented periodic technical and nontechnical evaluations
- Improved physical security
- Performed a new/updated Security Rule Risk Analysis
- Provided business associate with additional training on HIPAA requirements
- Provided individuals with free credit monitoring
- Revised business associate contracts
- Revised policies and procedures
- Sanctioned workforce members involved (including termination)
- Took steps to mitigate harm
- Trained or retrained workforce members
- Other

Incident Response Best Practices

General

Contact

Breach

Notice of Breach and Actions Taken

Attestation

Summary

Please complete the Attestation form.

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

* Name:

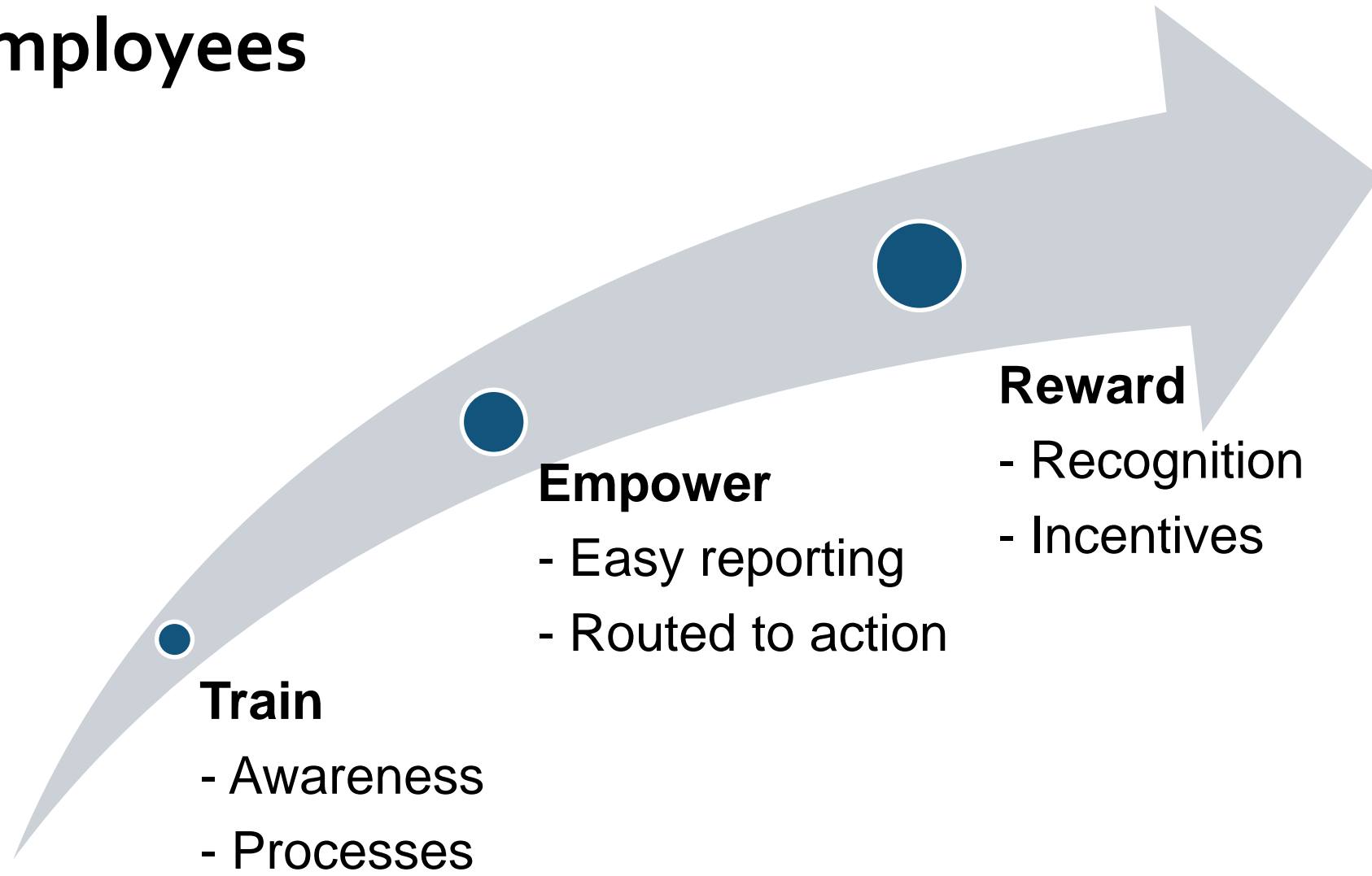
Date: 01/25/2016

← Back

→ Next

Incident Response Best Practices

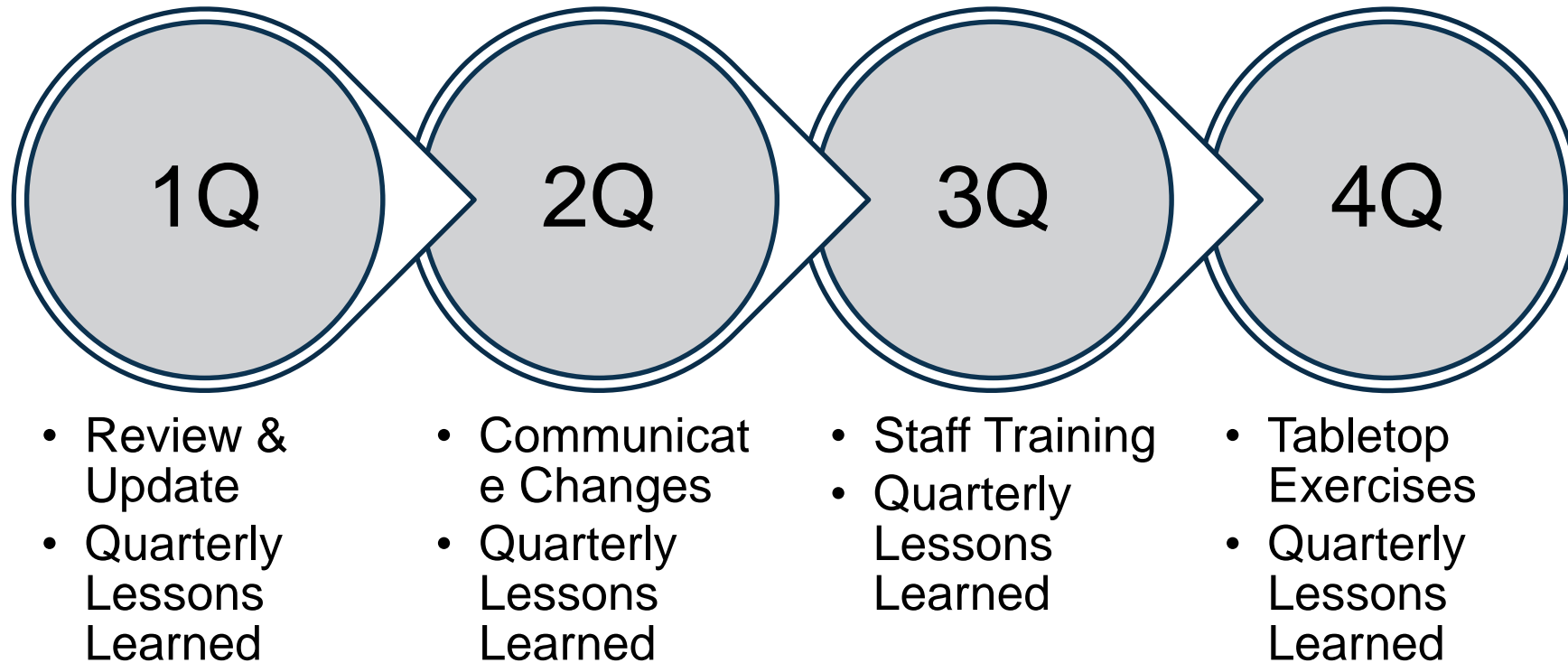
Engage Employees



Incident Response Best Practices

A Living Plan

Schedule proactive tasks



Q&A



Thank you

Patrick Quirk

: PQUIRK

: @PQVIEWS

Patrick@FOQUSPartners.com

859-312-7267