KHIE
KENTUCKY HEALTH
INFORMATION EXCHANGE

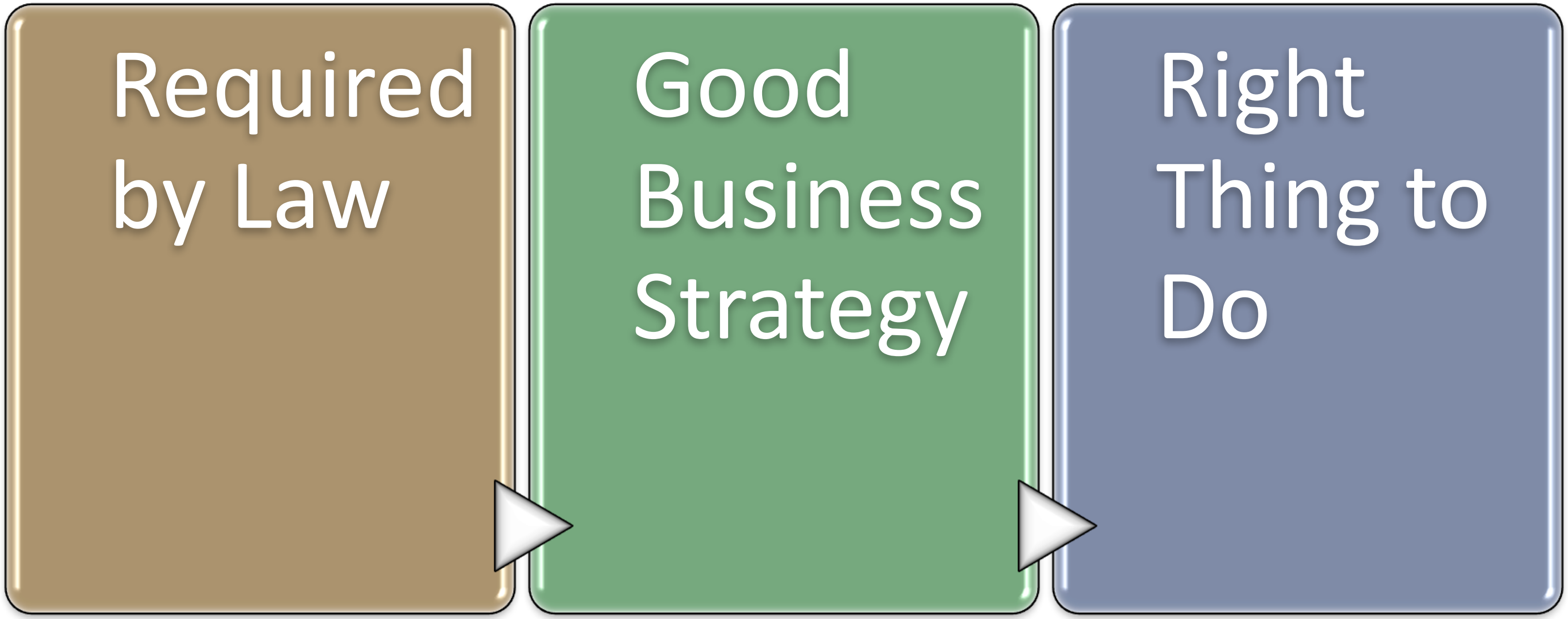
RHC Summit
6/9/2017

Cyber Security Issues

Dennis E. Leber CISO
CHFS

Kentucky
UNBRIDLED SPIRIT

Why is it Important?



Required by Law

Good Business Strategy

Right Thing to Do

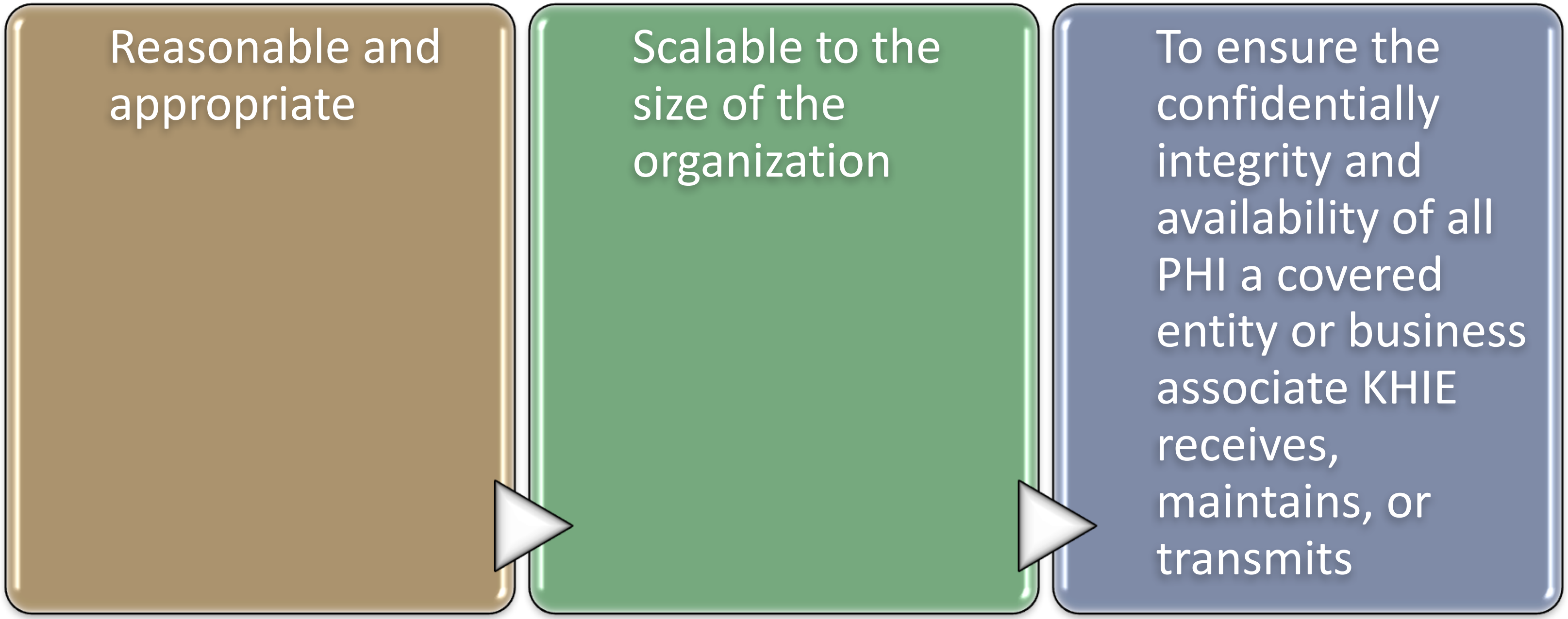
Why is it Important?

According to Bitglass' 2017 Healthcare Breach Report, 328 U.S. healthcare firms reported data breaches in 2016, up from 268 in 2015.

"Unauthorized disclosures continue to tick up and are now the leading cause of breaches as data moves to cloud and mobile and as external sharing becomes easier. Unauthorized disclosures includes all non-privileged access to PII or PHI," the report states. "Hacking and IT-related incidents doubled year-over-year, an indication that malicious actors are not letting up and are increasingly aware of PHI's high long-term value."

According to the 2016 Ponemon Cost of Data Breach Study, the average breach cost U.S. companies $221 per lost record last year, up from $217 per record in 2015 -- though the cost per leaked record for healthcare firms topped $402 in 2016.

HIPAA



Reasonable and appropriate

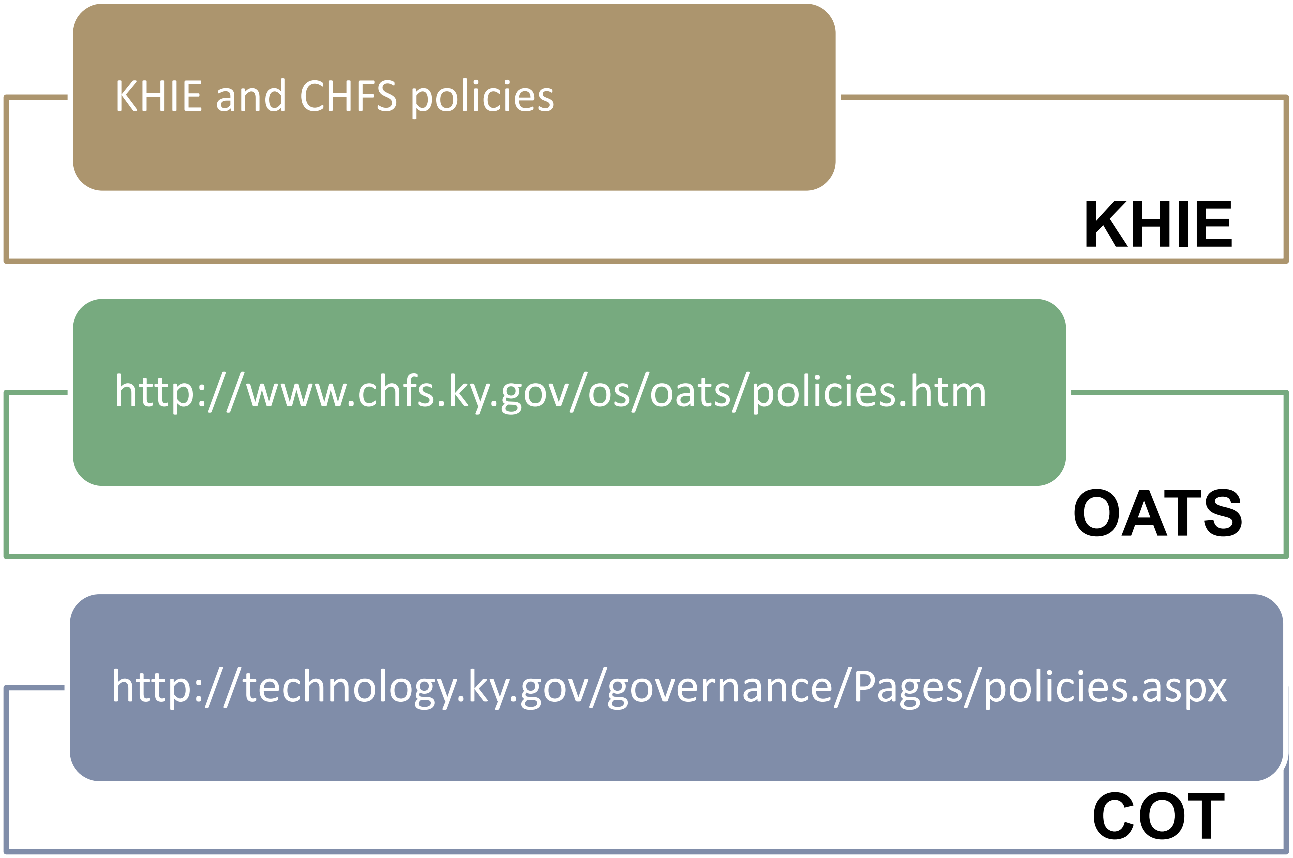
Scalable to the size of the organization

To ensure the confidentially integrity and availability of all PHI a covered entity or business associate KHIE receives, maintains, or transmits

KHIE
KENTUCKY HEALTH
INFORMATION EXCHANGE

Employee Policies

Manage the Privacy Rule by use of Policies and Procedures



KHIE and CHFS policies

KHIE

http://www.chfs.ky.gov/os/oats/policies.htm

OATS

http://technology.ky.gov/governance/Pages/policies.aspx

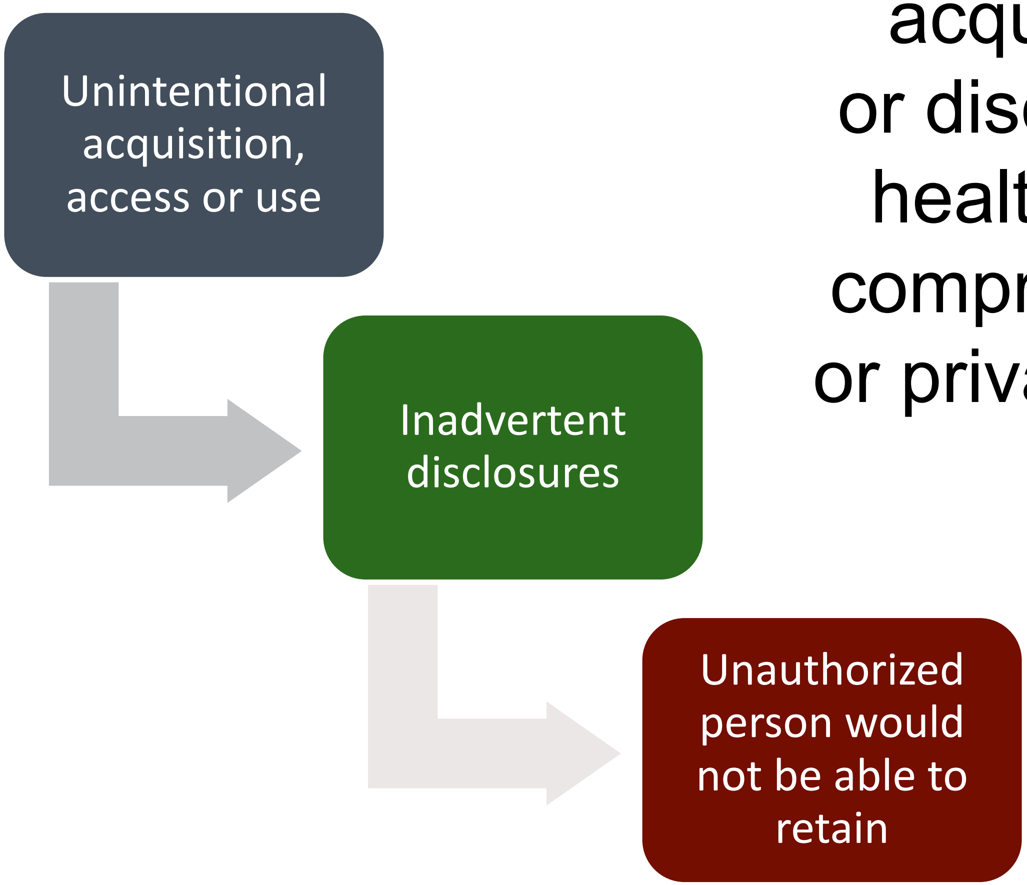
COT

Minimum Necessary

When using or disclosing PHI, KHIE must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Breach by a Different Name

Three Exclusions



Unintentional acquisition, access or use

Inadvertent disclosures

Unauthorized person would not be able to retain

Breach means the acquisition, access, use or disclosure of protected health information which compromises the security or privacy of the protected health information.

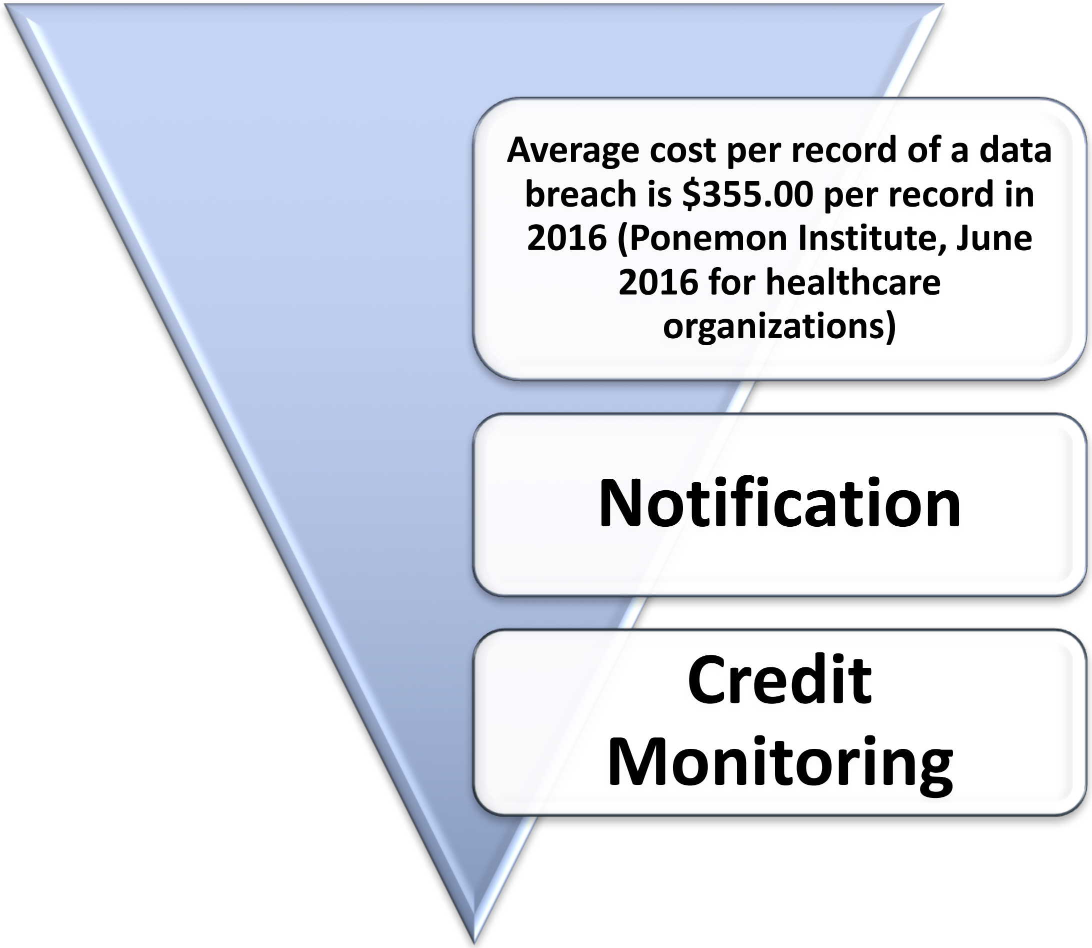
“Risk Assessment” must include:

- ○ The nature and extent of the PHI involved;
- ○ The unauthorized person who received/used the PHI;
- ○ Whether the PHI was actually acquired or viewed; and
- ○ The extent to which the risk to the PHI has been mitigated.

“Security Breach” means:

Unauthorized acquisition, distribution, disclosure, destruction, manipulation or release of unencrypted or unredacted records or data that compromises or the agency reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one or more individuals

Data Breach Mop Up



Average cost per record of a data breach is $355.00 per record in 2016 (Ponemon Institute, June 2016 for healthcare organizations)

Notification

Credit Monitoring

OCR

Office of Civil Rights

HHS.gov

OCR

About OCR

How To File a Complaint

Frequently Asked Questions

Job and Intern Opportunities

News Room

Part of the U.S. Department of Health and Human Services

Enforces civil rights from health care providers receiving federal financial assistance from HHS, one of the most active federal regulators

- Where does your data reside?
- Who has access to PHI?
- How do you restrict access to PHI?
- How does your agency train your employees annually?

Office for
Civil Rights

Human Element

Humans are still the weakest Link

- Phishing, Hacking, malware account for 43% of incidents
- Up 12% from 2016
- 25% of those were human error
- 23% was ransomware
- 18% due to lost or stolen devices
- 3% internal theft

Human Element

Humans are still the weakest Link

- Innocent employees who inadvertently download malicious content or reveal sensitive data.
- Careless, negligent, or employees who lack technical knowledge.
- Disgruntled employees who intentionally leak data.

Managing Insider Threats

What is it?

Insider Threat is a current or former employee, contractor or business partner who:

✓Has or had authorized access to an organization’s network, system, or data

✓Has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability (CIA) of the organization’s information or information systems

Most common insider crimes

- Unauthorized access
- Unintentional exposure of private or sensitive data
- Viruses, worms or other malicious code
- Theft of intellectual property

Workforce actions to prevent insider threats

- Avoid printing PHI, PII, other confidential information
- Guard confidentiality of passwords and credentials

CERT Program, Carnegie Mellon

For additional information contact: dennis.leber@ky.gov