Executive Order 13636: The Healthcare Sector and the Cybersecurity Framework

September 23, 2014

Executive Order: Improving Critical Infrastructure Cybersecurity

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

President Barack Obama

Executive Order 13636, *Feb. 12, 2013*

- The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure
- Version 1.0 of the framework was released on Feb. 12, 2014, along with a roadmap for future work

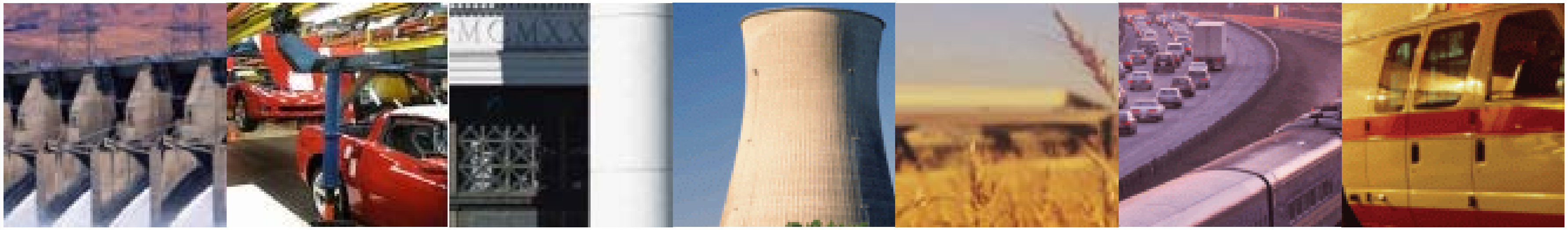
Based on the Executive Order, the Cybersecurity Framework Must...

- Include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks

- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk

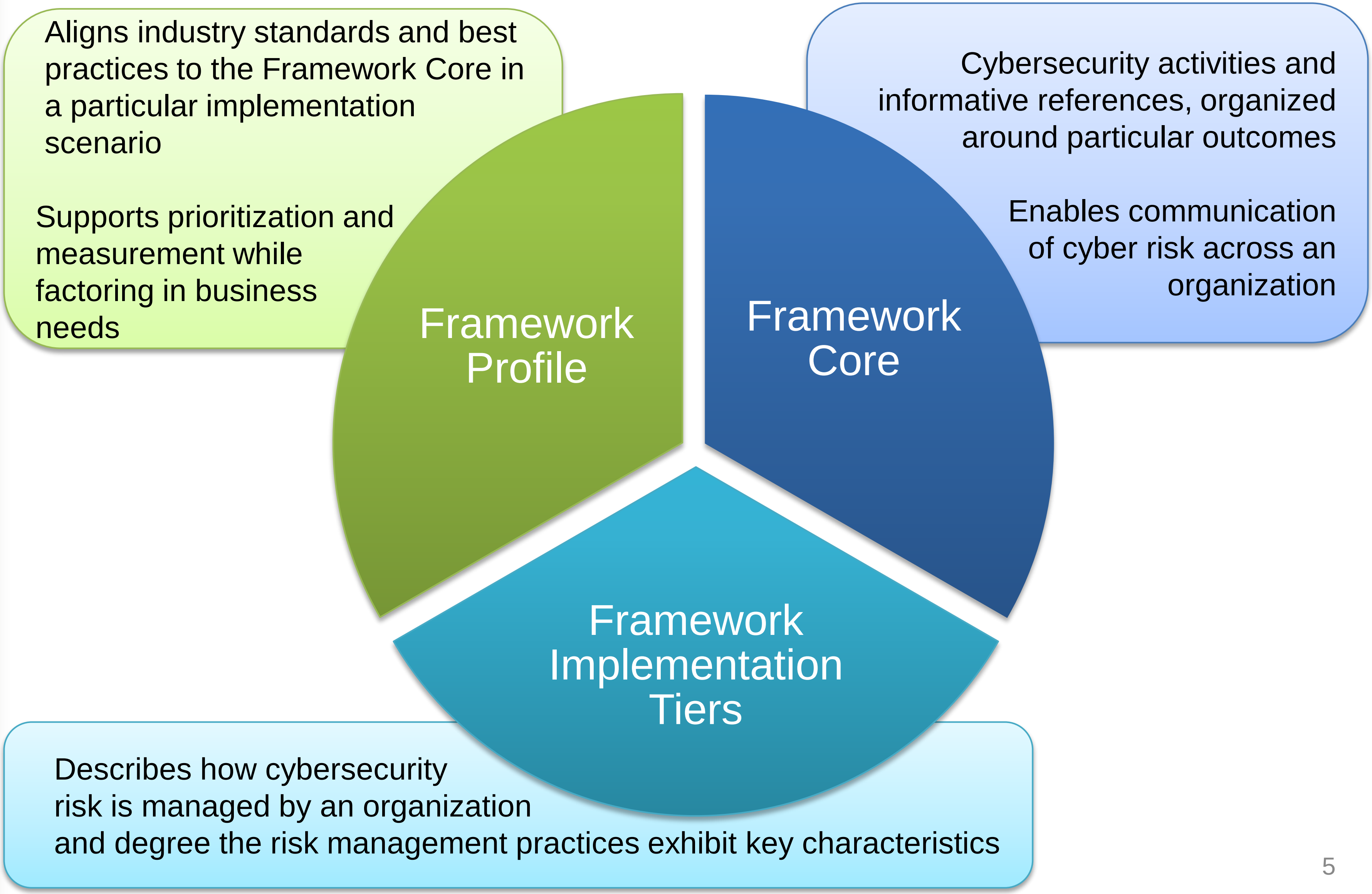
- Identify areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations

The Cybersecurity Framework Is for Organizations…



- Of any size, in any sector in the critical infrastructure
- That already have a mature cyber risk management and cybersecurity program
- That don’t yet have a cyber risk management or cybersecurity program
- With a mission of helping keep up-to-date on managing risk and facing business or societal threats

Framework Components



Framework Profile

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs

Framework Core

Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Framework Implementation Tiers

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Framework Core

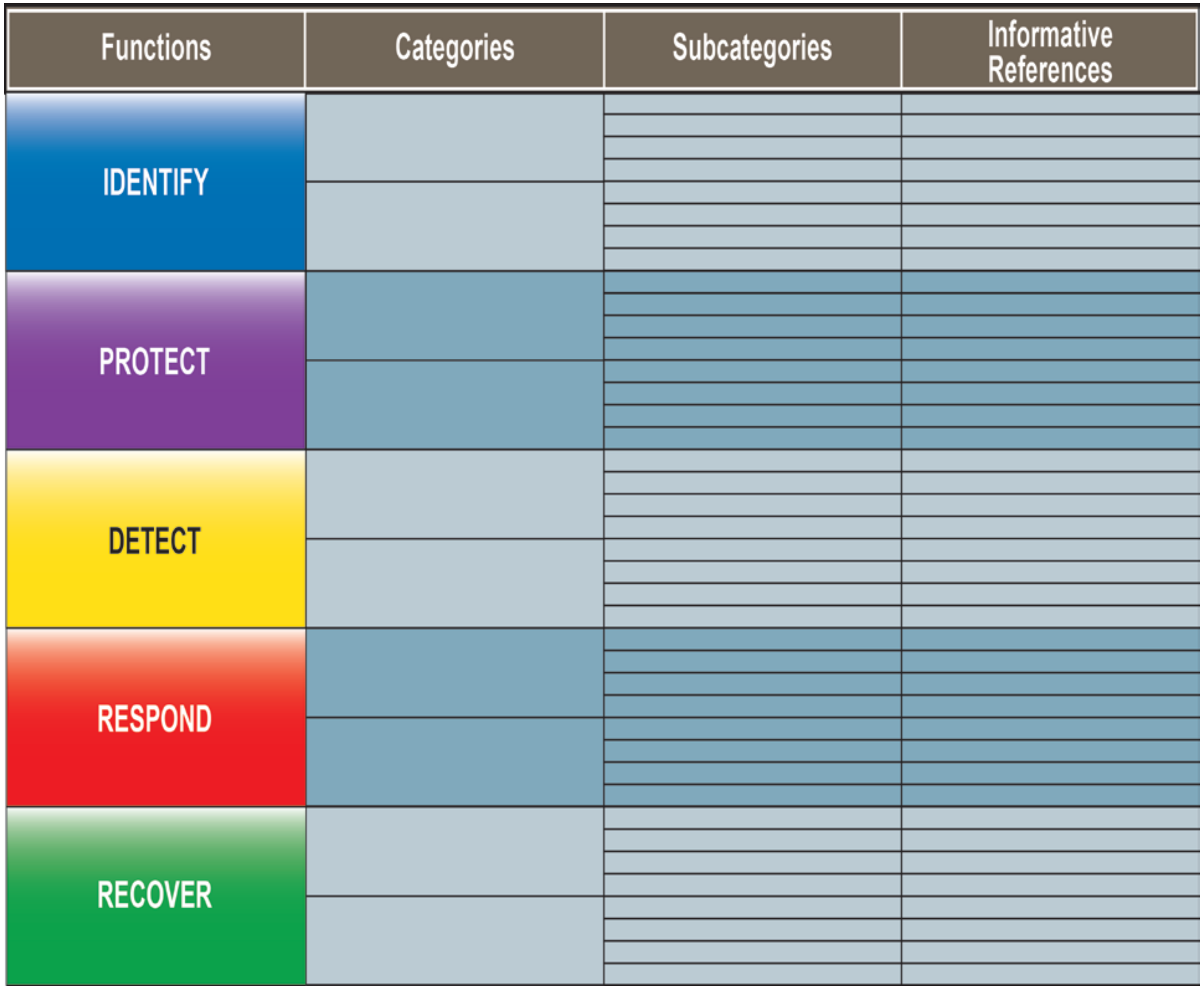
What assets need protection?

What safeguards are available?

What techniques can detect incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?



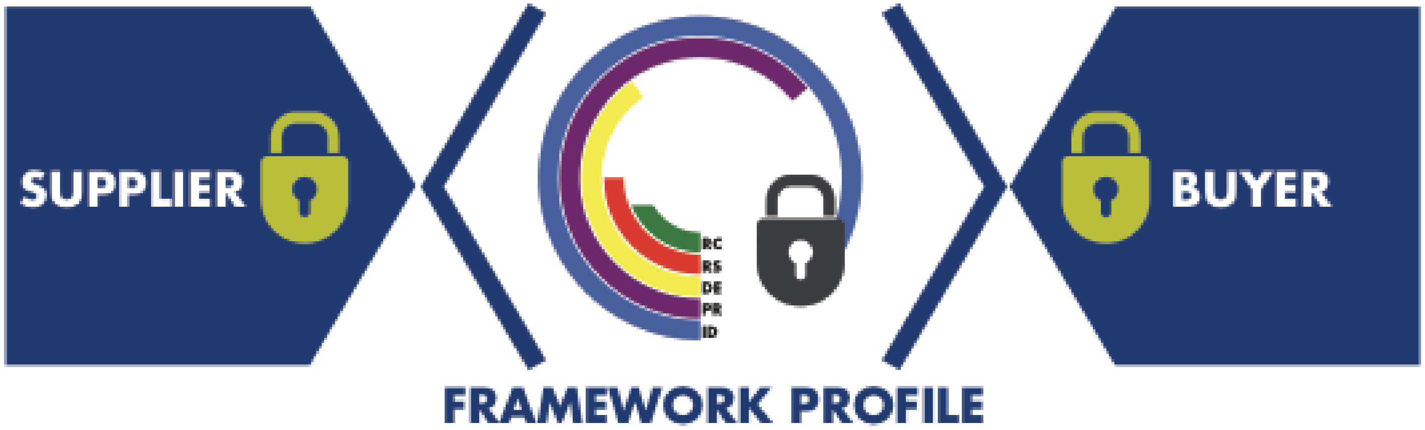
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Framework Profile

- Alignment of Functions, Categories, and Subcategories with business requirements, risk tolerance, and resources of the organization

- Enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities

- Can be used to describe current state or desired target state of cybersecurity activities



How to Use the Cybersecurity Framework

The Framework is designed to complement existing business and cybersecurity operations, and can be used to:

- Understand security status
- Establish / Improve a cybersecurity program
- Communicate cybersecurity requirements with stakeholders, including partners and suppliers
- Identify opportunities for new or revised standards
- Identify tools and technologies to help organizations use the Framework
- Integrate privacy and civil liberties considerations into a cybersecurity program

Key Points about the Framework

- It’s a framework, not a prescription

- It’s the result of a public-private partnership

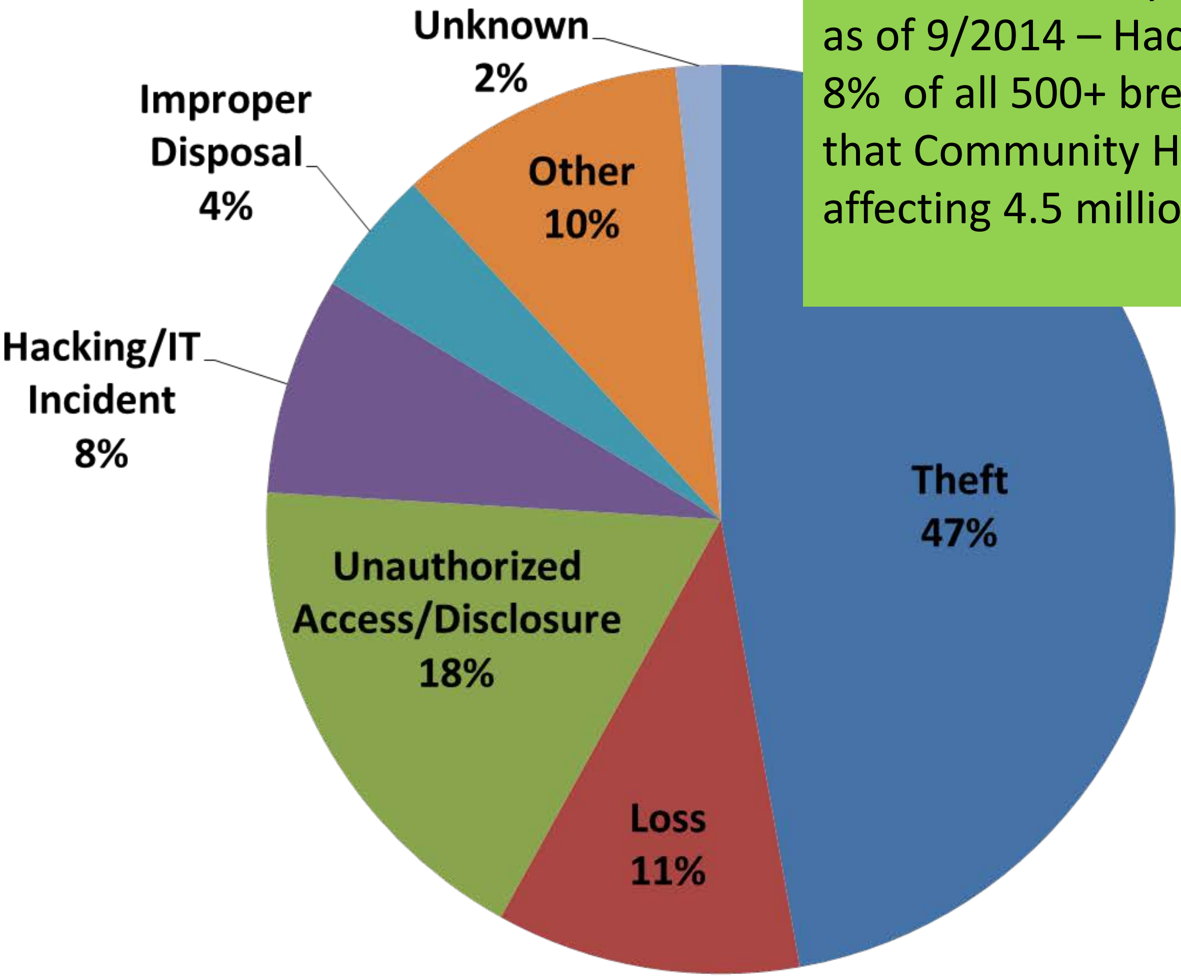
- The framework is a living document

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

The HIPAA Security Rule and the NIST Cybersecurity Framework

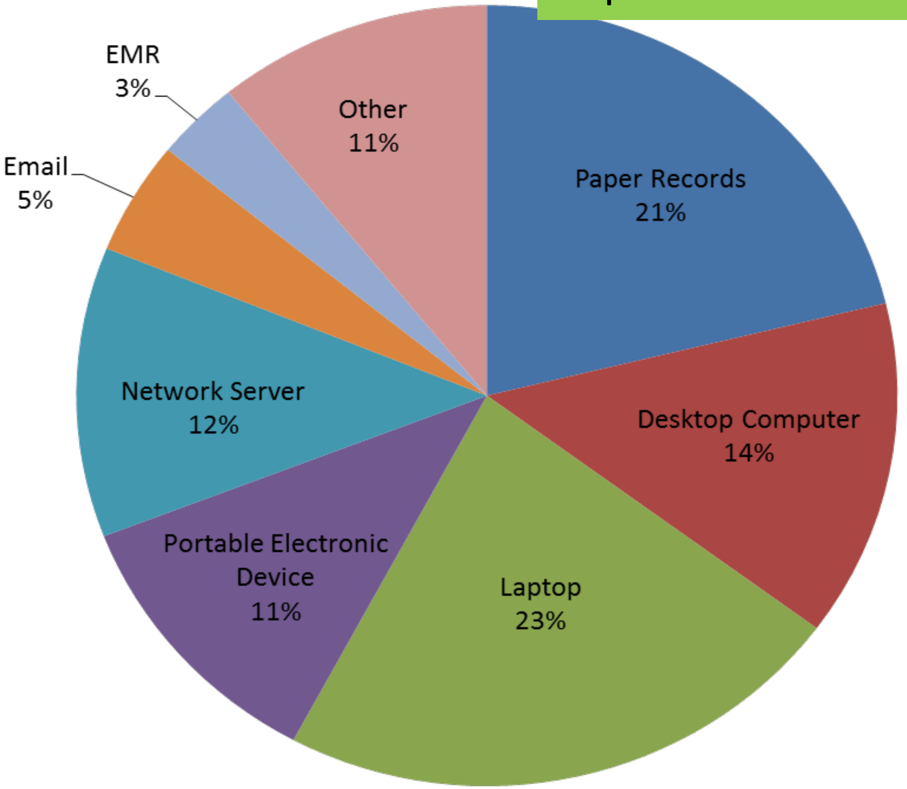
OCR/NIST Conference
September 23, 2014
Linda Sanches, Senior Advisor
HHS Office for Civil Rights (OCR)

Cyber Security and Type of Breach



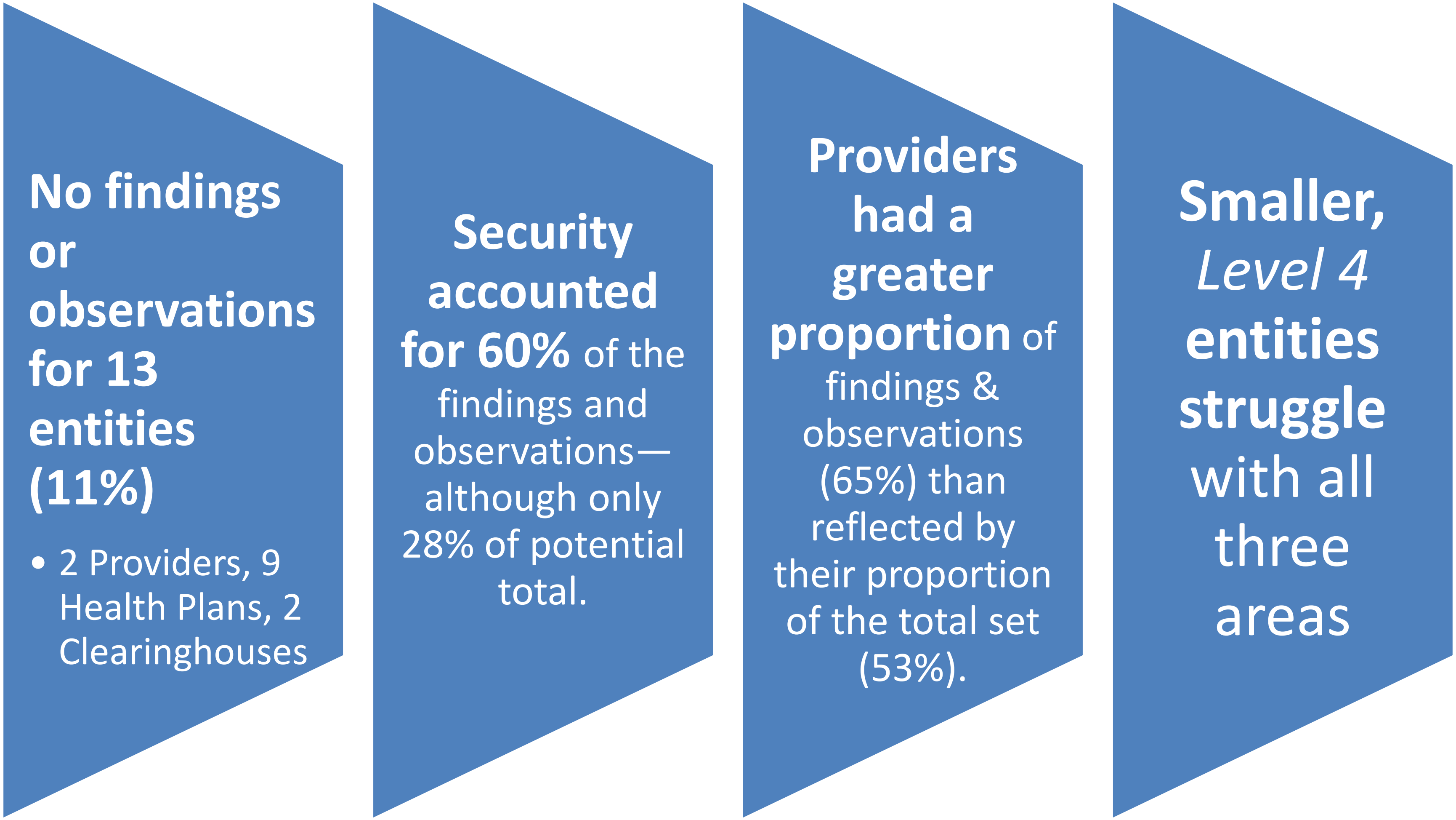
500+ Breaches by Type of Breach
as of 9/2014 – Hacking/IT incidents represent 8% of all 500+ breaches, but may rise now that Community Health has been reported affecting 4.5 million patients

500+ Breaches by Location of Breach



Paper accounts for 21% of incidents

Audit Findings and Observations



No findings or observations for 13 entities (11%)

- 2 Providers, 9 Health Plans, 2 Clearinghouses

Security accounted for 60% of the findings and observations—although only 28% of potential total.

Providers had a greater proportion of findings & observations (65%) than reflected by their proportion of the total set (53%).

Smaller, ***Level 4*** **entities struggle** with all three areas

Key Security Rule Findings

- 58 of 59 providers had at least one Security Rule finding or observation
- No complete and accurate risk assessment in two thirds of entities
  - 47 of 59 providers,
  - 20 out of 35 health plans and
  - 2 out of 7 clearinghouses

Key take away:

Most covered entities have not identified the risks and vulnerabilities of their environment, and therefore are failing to adequately safeguard PHI.

Appropriate Safeguards Prevent Breaches

- Evaluate the risk to e-PHI when at rest on removable media, mobile devices and computer hard drives
- Take reasonable and appropriate measures to safeguard e-PHI
- Store all e-PHI to a network
- Encrypt data stored on portable/movable devices & media
- Employ a remote device wipe to remove data when lost or stolen
- Train workforce members on how to effectively safeguard data and timely report security incidents

More Information

http://www.hhs.gov/ocr/privacy/