OCR Lessons Learned
– 5 Things Every Health Care Company Needs to Know Now

March 16, 2015 - HIPAA Summit 2015, Washington, DC

Booz | Allen | Hamilton

Presentation Agenda

I. Introduction

II. The Background—Audits, Protocols and Enforcements

III. Lessons Learned—Five Things You Need to Know Now

i. Know the Rules and Areas of Non-Compliance
ii. Know the Risks Specific to Your Organization
iii. Know the Data and the Flows – Internal and External
iv. Know Your Audit Process and Prepare
v. Know the Roadmap Ahead and Be Self-Aware

Introduction

Jim Koenig

Global Leader, Commercial Privacy Practice and
Co-Leader, Cybersecurity and Incident Response
Booz Allen Hamilton

- Previous expert to each of the OCR, FTC and CFPB
- Provided privacy and security services to provider, pharmaceutical, health insurance and companies in other industries
- Assists many organizations related to breaches, incidents, regulatory investigation, enforcement and Consent Decree/Corrective Action Plan compliance
- Co-Founder of IAPP
- Adjunct Faculty/Facilitator, Columbia University

Presentation Agenda

I. Introduction

II. The Background—Audits, Protocols and Enforcements

III. Lessons Learned—Five Things You Need to Know Now

i. Know the Rules and Areas of Non-Compliance
ii. Know the Risks Specific to Your Organization
iii. Know the Data and the Flows – Internal and External
iv. Know Your Audit Process and Prepare
v. Know the Roadmap Ahead and Be Self-Aware

Background

Statutory Basis. HITECH Section 13411 requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards.

Audit Program. To implement this mandate, OCR piloted a program and performed 115 audits of covered entities in 2012.

Goal and Objectives. To improve covered entity and business associate compliance with the HIPAA standards

- Examine mechanisms for compliance,
- Identify best practices
- Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
- Encourage attention to compliance with HIPAA

Audit Protocols—Eleven Modules

The audit protocol is organized around 11 different modules in 3 areas. Provides established criteria, audit testing procedures, work paper reference and applicability.

1. Breach Notification

Security

2. Administrative Safeguards
3. Physical Safeguards
4. Technical Safeguards

Privacy

5. Notice of Privacy Practices
6. Rights to Request Privacy Protection of PHI
7. Access of Individuals to PHI
8. Administrative Requirements
9. Uses and Disclosures of PHI
10. Amendment of PHI
11. Accounting of Disclosures

HIPAA Audits Are Coming – What you need to know

OCR's Enforcement Program Has Been Delayed

HIPAA Audit Program: OCR Program was scheduled to begin "desk audits" of 350 covered entities and 50 business associates beginning in the summer of 2014

Delayed Audits: These audits were delayed until 2015 due to:

- OCR's change in focus from "desk audits" to more onsite visits to CEs and BAs.
- OCR's planned updated web portal for reporting incidents, which may be used to do a scan of CEs and BAs that would be good candidates for audits

The Delay is an Opportunity to Get it Together

Know Where you Need to Focus: The 2015 audits will be:

1) Risk assessments and risk management (Security Rule)
2) Notices of privacy practices and access rights (Privacy Rule)
3) Content and timeliness of breach notifications (Breach Notification Rule)

Know Where to Start: To reduce the risk of enforcement against your organization, you should be doing the following now:

- Conduct a periodic risk assessment
- Update notices and access rights
- Review and/or revise your breach notification practices

Enforcement - Over $36 Million in Resolution Agreements & Fines for Variety of Issues

Covered Entity	Type of Breach	Amount	Date
Anchorage Community Mental Health	Unpatched and Unsupported Software	$150,000	Dec 2014
Parkview Health System	Paper records exposure	$800,000	June 2014
New York Presbyterian Hospital	Disclosure of ePHI on the internet	$3,300,000	May 2014
Columbia University	Disclosure of ePHI on the internet	$1,500,000	May 2014
Concentra Health Services	Unencrypted laptop	$1,725,220	April 2014
QCA Health Plan	Unencrypted laptop	$250,000	April 2014
Skagit County, Washington	ePHI posted on public server	$215,000	March 2014
Adult & Pediatric Dermatology of MA	Thumb drive loss	$150,000	December 2013
Affinity Health Plan	ePHI on copier hard drives	$1,215,780	August 2013
Wellpoint	ePHI posted on public server	$1,700,000	July 2013
Shasta Regional Medical Center	Disclosure to media outlets	$275,000	June 2013
Idaho State University	Disabled firewall	$400,000	May 2013
Hospice of North Idaho	Laptop theft	$50,000	December 2012
Massachusetts Eye & Ear Infirmary	Laptop theft	$1,500,000	September 2012
Alaska DHSS	Portable electronic device theft	$1,700,000	June 2012
Phoenix Cardiac Surgery	ePHI posted on public server	$100,000	April 2012
BCBS Tennessee	Hard drive theft	$1,500,000	March 2012
UCLA Health System	Unauthorized access of celebrity ePHI	$865,500	July 2011
Massachusetts General Hospital	Loss of paper records	$1,000,000	February 2011
Cignet Health	Refusal to allow patient record access	$4,300,000	February 2011
Management Services Org. of WA	3rd party disclosure without consent	$35,000	December 2010
Rite Aid Corporation	Improper PHI disposal	$1,000,000	July 2010
CVS Pharmacy, Inc.	Improper PHI disposal	$2,250,000	January 2009

Fortune Telling – What You Might See

Launch of Audits. Audits should move forward in 2015 combining desk review and onsite approaches. OCR conducting the audits itself; focusing on more high-risk areas; and potentially integrating the audits into OCR's formal enforcement program.

- **Risk-Based Approach.** Prior audits were done on a strict compliance approach. Guidance as to how more of a risk-based approach will be utilized – different than existing healthcare use of "risk base."

- **Revised Protocols.** Updated compliance protocols to be released. Likely updated for Omnibus Rule, revised risk areas, size and type of organization and risk-based approach.

Continued Enforcement Emphasizing Risk Assessment. To improve covered entity and business associate compliance with the HIPAA standards

	Last Year	This Year
Periodic Risk Assessment	☑	☑
Malware/Cyber	☑	☑
Third Parties	☑	☑
Interconnected		☑
Encryption – Ignored Risks		☑

Presentation Agenda

I. Introduction

II. The Background—Audits, Protocols and Enforcements

III. Lessons Learned—Five Things You Need to Know Now
   i. Know the Rules and Areas of Non-Compliance
   ii. Know the Risks Specific to Your Organization
   iii. Know the Data and the Flows – Internal and External
   iv. Know Your Audit Process and Prepare
   v. Know the Roadmap Ahead and Be Self-Aware

Preliminary Analysis Discussed by OCR

[redacted]

Common Privacy Areas:

- Notice of Privacy Practices
- Access of Individuals
- Minimum Necessary
- Authorizations

Common Security Areas:

- Risk Analysis
- Media movement and disposal
- Audit controls and monitoring

1. Policies and Procedures exist but are outdated or not implemented
2. HIPAA compliance programs are not a priority
3. Small providers are not in compliance
4. Larger entities demonstrate security challenges
5. Entities are not conducting Risk Assessments
6. Entities are not managing third party risks
7. Privacy challenges are dispersed in protocol - no trends by entity type or size

Presentation Agenda

I. Introduction

II. The Background—Audits, Protocols and Enforcements

III. Lessons Learned—Five Things You Need to Know Now

i. Know the Rules and Areas of Non-Compliance

ii. Know the Risks Specific to Your Organization

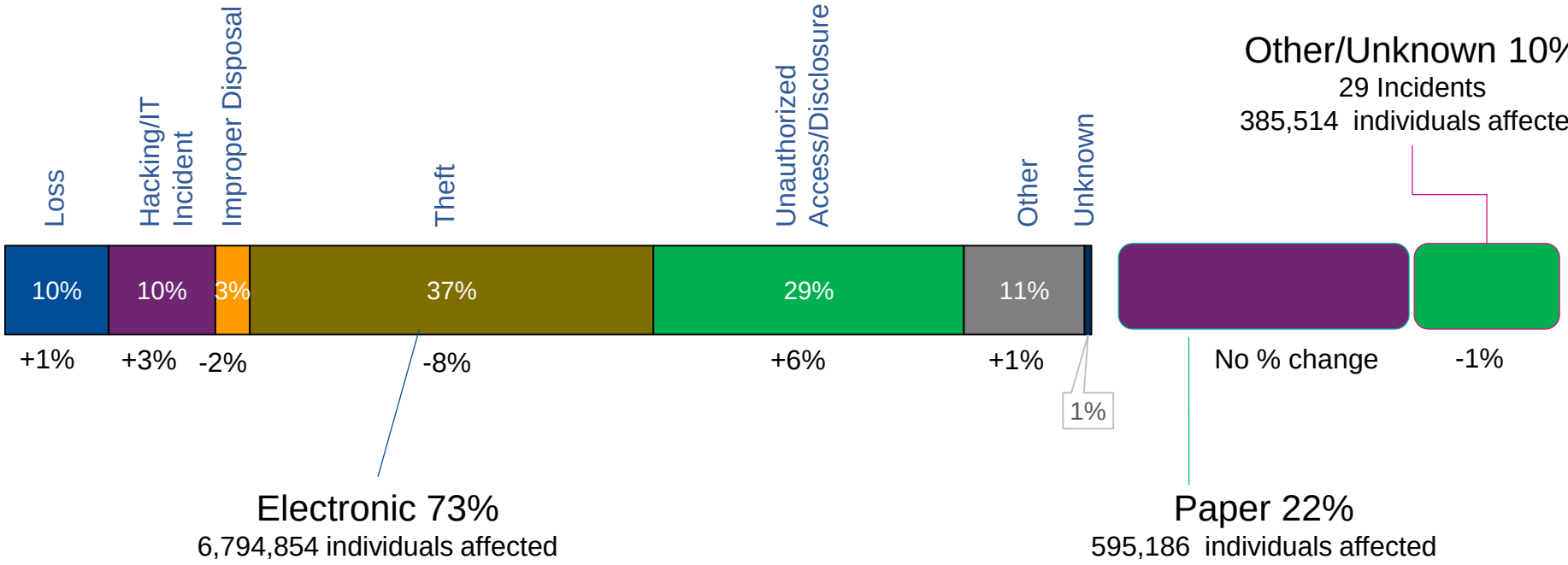
iii. Know the Data and the Flows – Internal and External

iv. Know Your Audit Process and Prepare

v. Know the Roadmap Ahead and Be Self-Aware

The Risk Landscape 2014

*Breach Data Composite for 2014



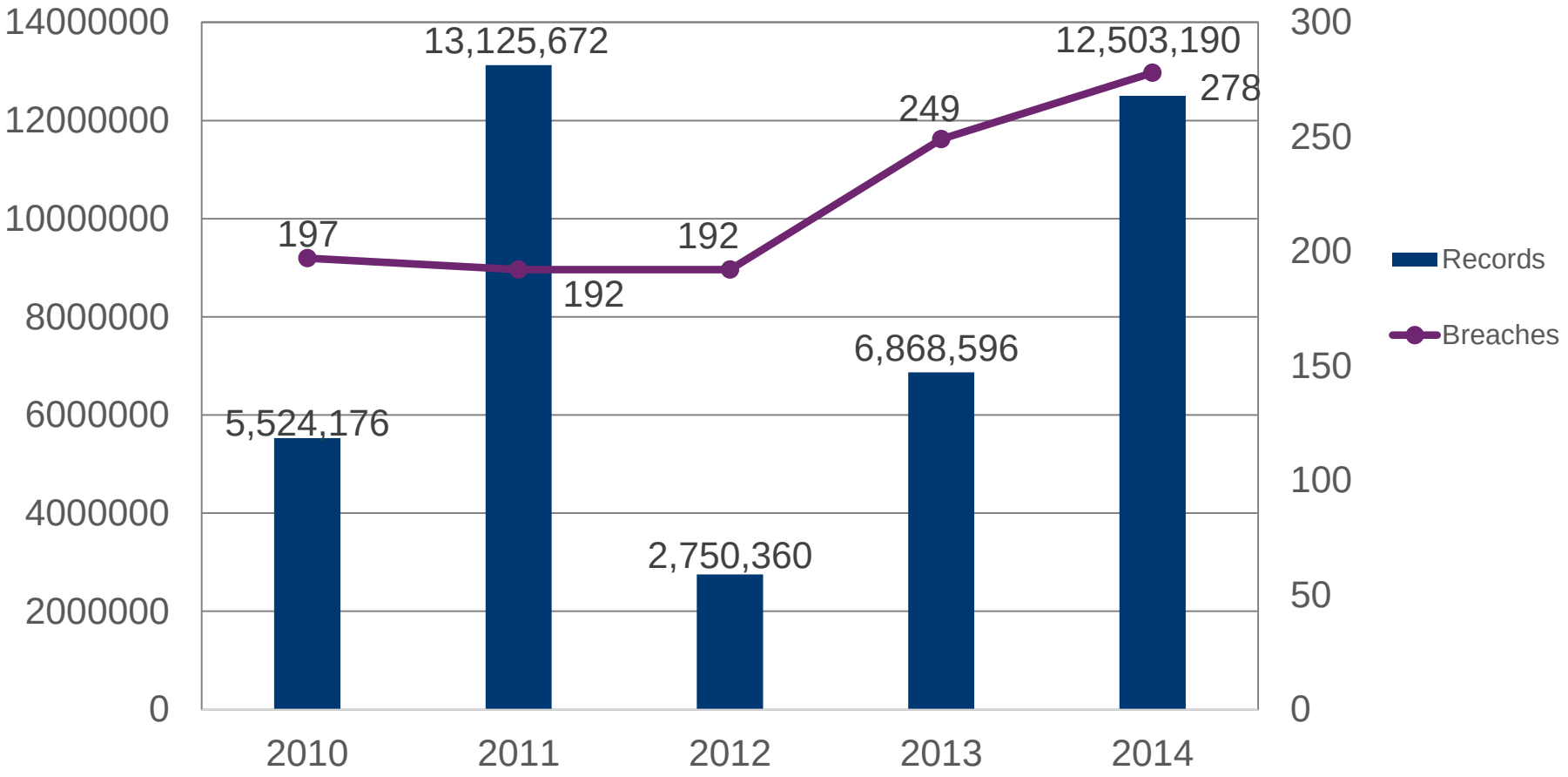
Source: US Department of Health and Human Services Office for Civil Rights

*Represents percent of breaches where the breach type was mentioned (i.e., includes double counting in Electronic)

Individuals Impacted vs. Number of Breaches

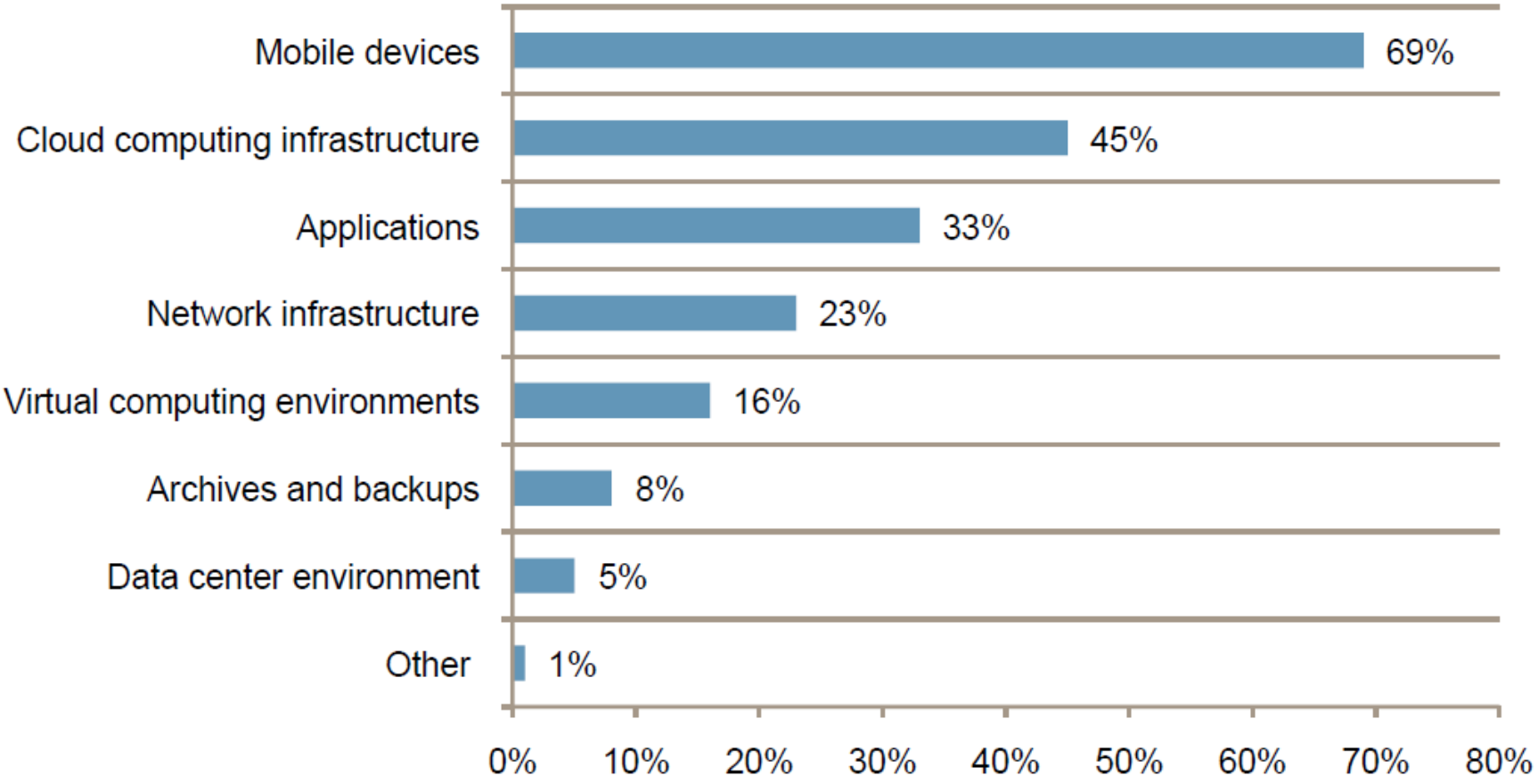
- Number of Breaches Up
- Number of People Impacted Up

Total Breaches	278
Records Lost	12,503,190
Community Health	4.5 million records



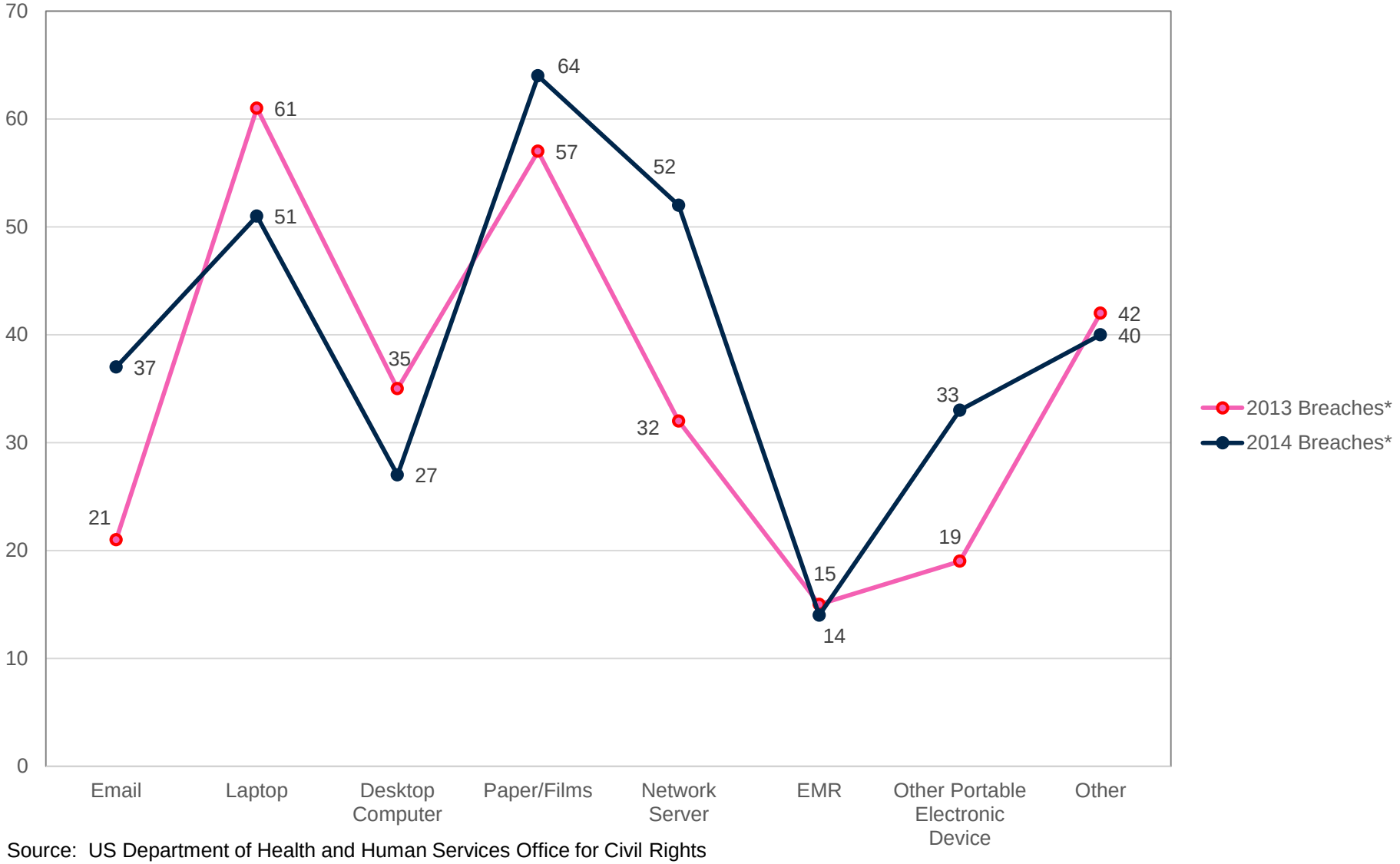
Source: US Department of Health and Human Services Office for Civil Rights

What Is The Greatest Risk to PHI & Other Regulated Data?



Source: Ponemon The Risk of Regulated Data ion Mobile Devices and in the Cloud (2014)

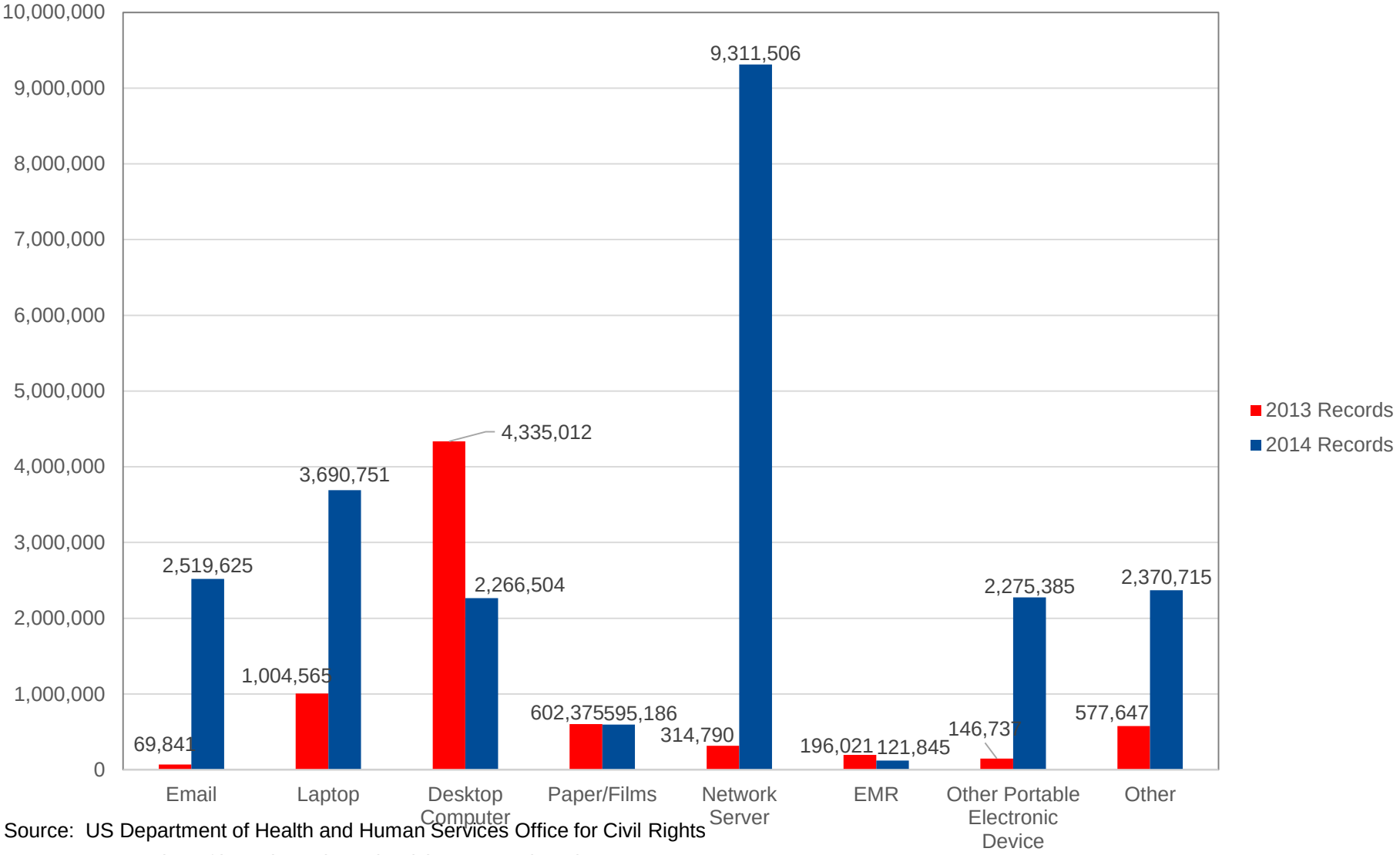
What Is Your Greatest Risk – How Do You Measure? 2013 vs 2014 – Number of Breaches



Source: US Department of Health and Human Services Office for Civil Rights

*Represents number of breaches where the risk was mentioned

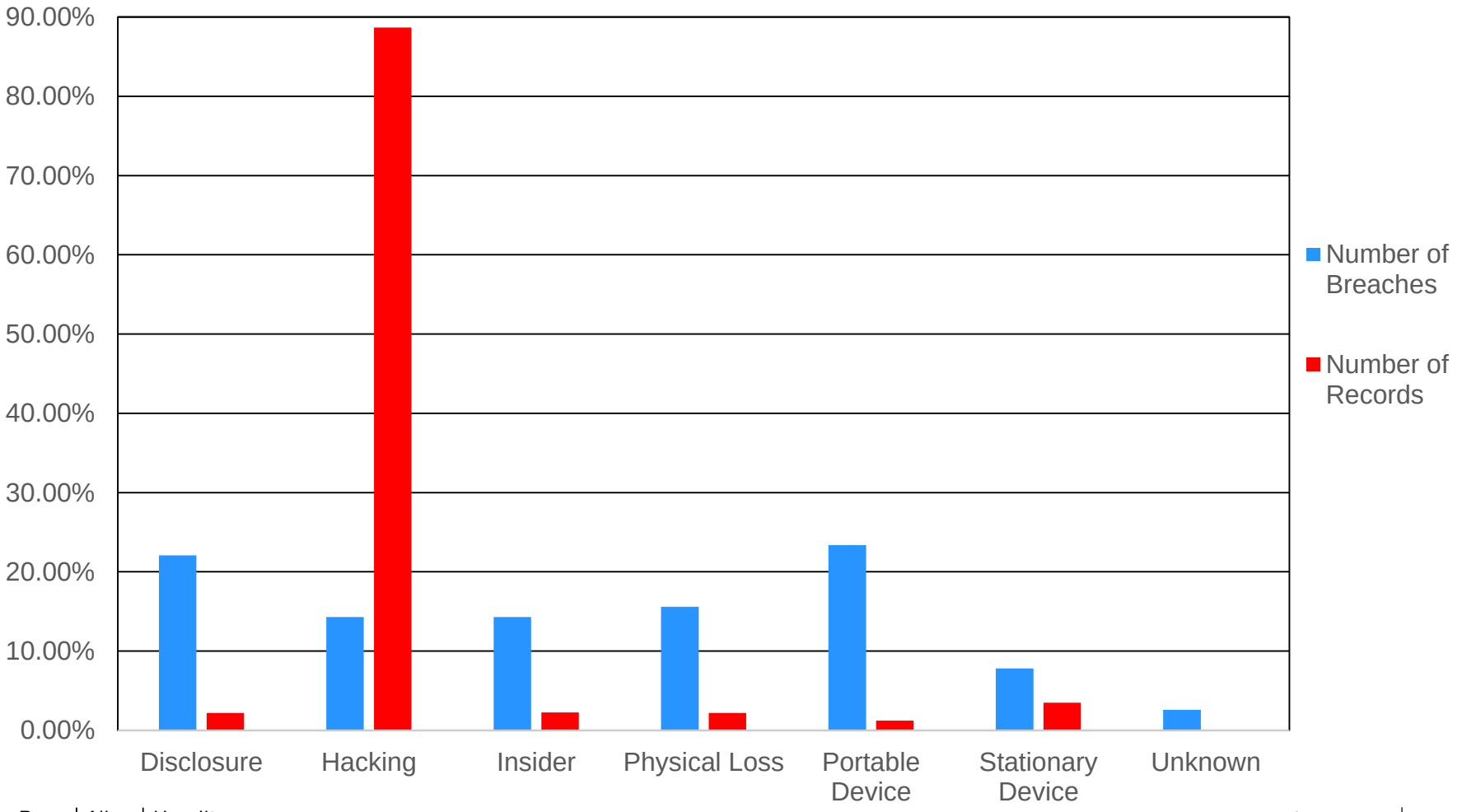
What Is Your Greatest Risk – How Do You Measure? 2013 vs 2014 – Number of Records



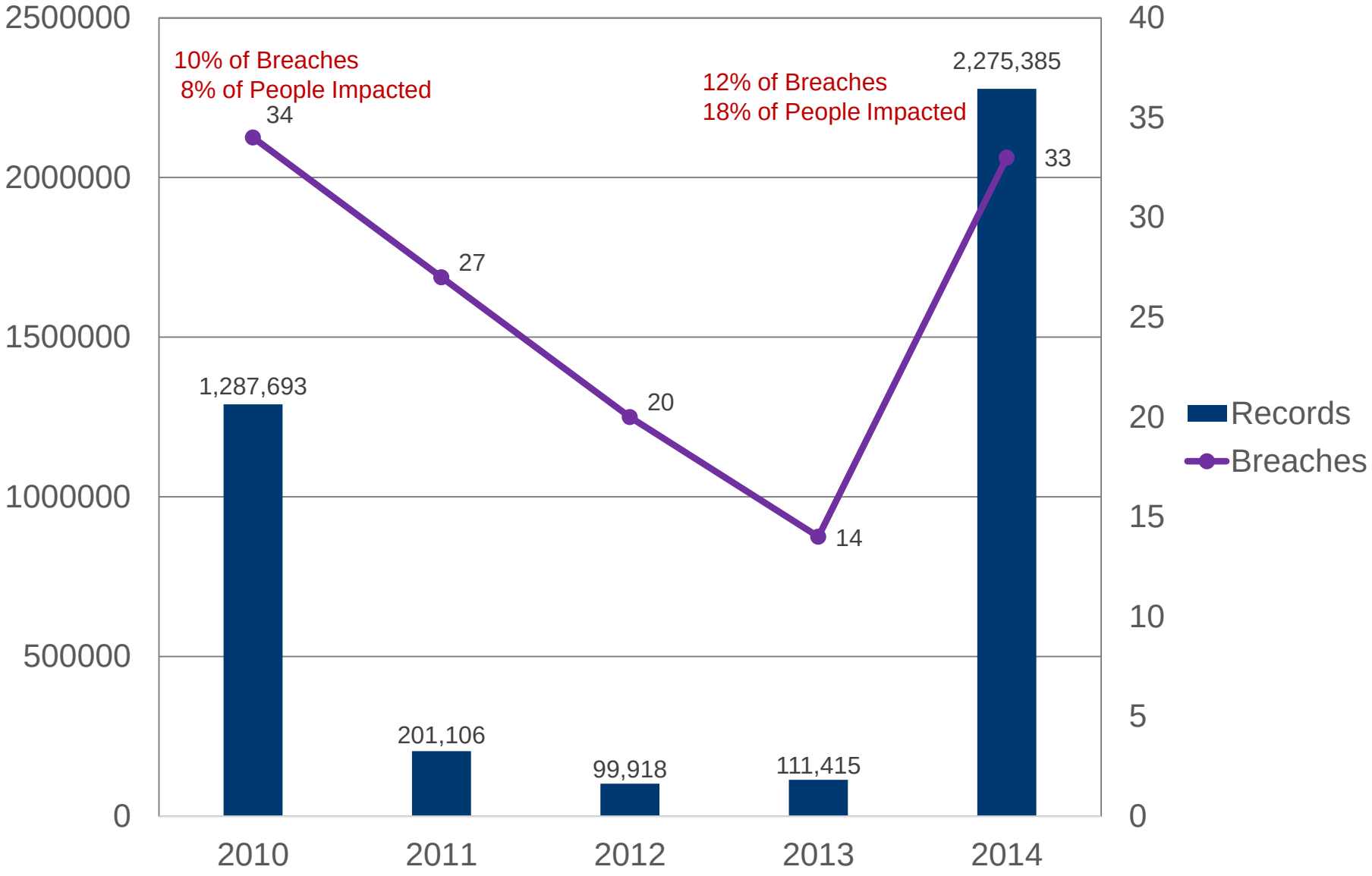
Source: US Department of Health and Human Services Office for Civil Rights

*Represents number of breaches where the risk was mentioned

What Is Your Greatest Risk – How Do You Measure?
2014 – Number of Breaches and Records

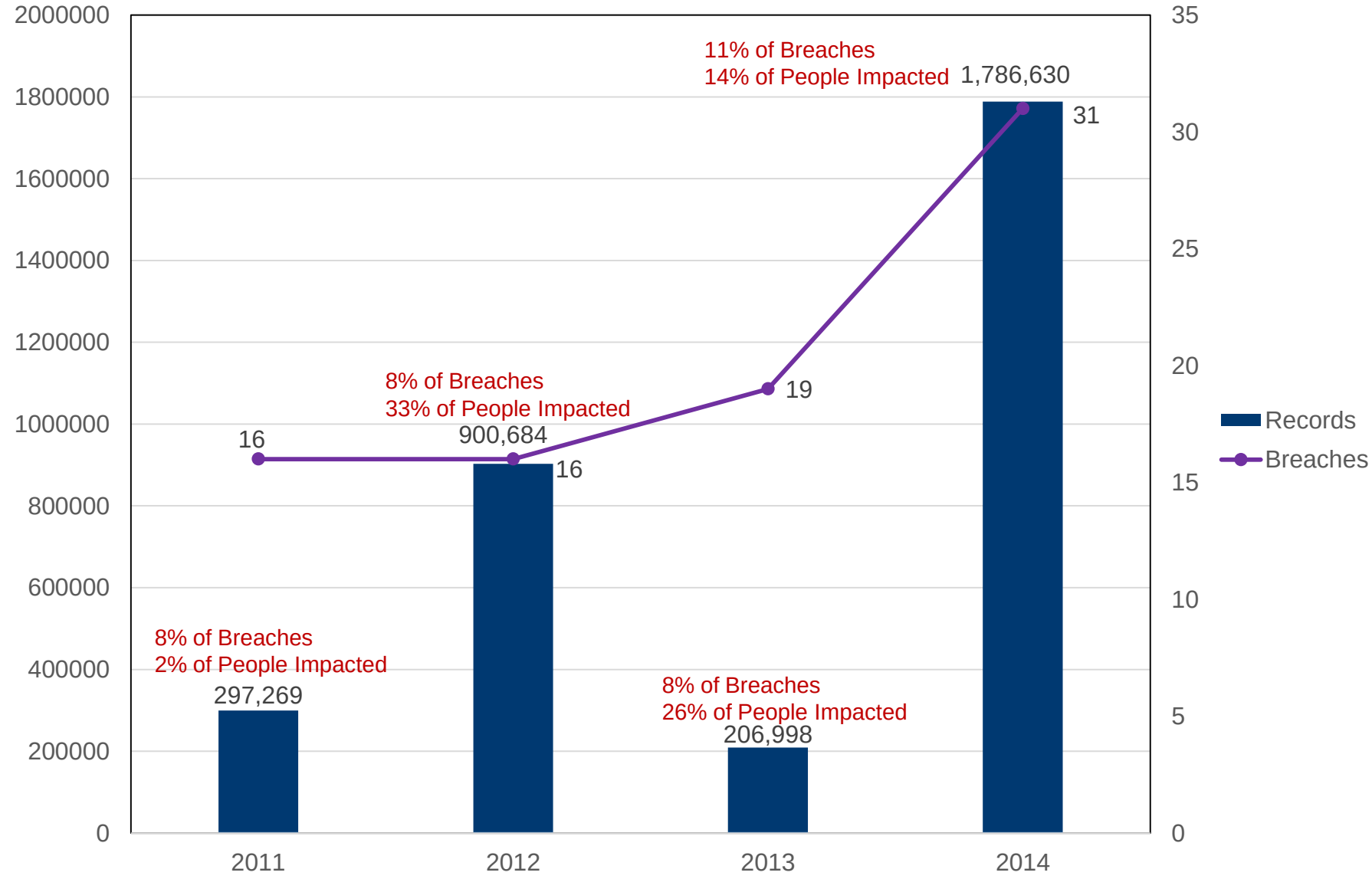


Portable Devices Over the Last 5 Years



Source: US Department of Health and Human Services Office for Civil Rights

Hacking Over the Last 5 Years



Source: US Department of Health and Human Services Office for Civil Rights

Business Associates Over the Last 5 Years

Business Associates Over the Last 5 Years

Presentation Agenda

I. Introduction

II. The Background—Audits, Protocols and Enforcements

III. Lessons Learned—Five Things You Need to Know Now

i. Know the Rules and Areas of Non-Compliance
ii. Know the Risks Specific to Your Organization
iii. Know the Data and the Flows – Internal and External
iv. Know Your Audit Process and Prepare
v. Know the Roadmap Ahead and Be Self-Aware

Revolution in HIT and Healthcare Delivery Models

- **Health Information, IT and Sharing Revolutions.** Stimulus Bill provided funds driving HIT and analytics, but organizations go from 0 to 11 in IT maturity. Meaningful Use Stage 2.
- **Care without Walls.** Healthcare using new channels and new technologies to deliver treatments – i.e. telemedicine, social media, care without walls.
- **New, but Vulnerable, Healthcare Ecosystem.** All the new data sharing and movement of data creates new capabilities and new data vulnerabilities.
- **More Business Associates Needed to Enable and Support.** New business partners, business associates and independent contracts needed to deliver and host new healthcare delivery methods and new technologies.
- **New Cyber Threats Attacking Healthcare.** Many providers, payers, pharma, medical device and Bas have been the target of cyber attacks and incidents. HITRUST, HHS, FBI and DHS conducting an industry cyber exercise, offering cyber monitoring services and are forums for sharing best practices.

75% of Healthcare organizations indicate they have or plan to use data for secondary and new uses;
48% have implemented privacy and security safeguards

Compliance must manage a complex and dynamic information ecosystem

New Ways to Connect

Engaging a broad population of people on a personal basis, wherever they are, whenever they want to connect

- Bring Your Own Device - BYOD
- Telemedicine/Mobile Health
- Networked medical devices
- Social Media
- Remote Patient Monitoring

New Types of Information

Collecting, exchanging, and communicating an exponentially growing amount of information

- Electronic Health Records
- Personal Health Information
- Financial Data
- Multi-Media
- Internet-of-things

New Care Delivery Models

Putting patients at the center of care delivery, and treating all aspects of their health, through every stage of their lives

- Patient-Centered Care
- Process Reengineering
- Population Health
- Continuum of Care
- Preventative Care

New Insights to Uncover

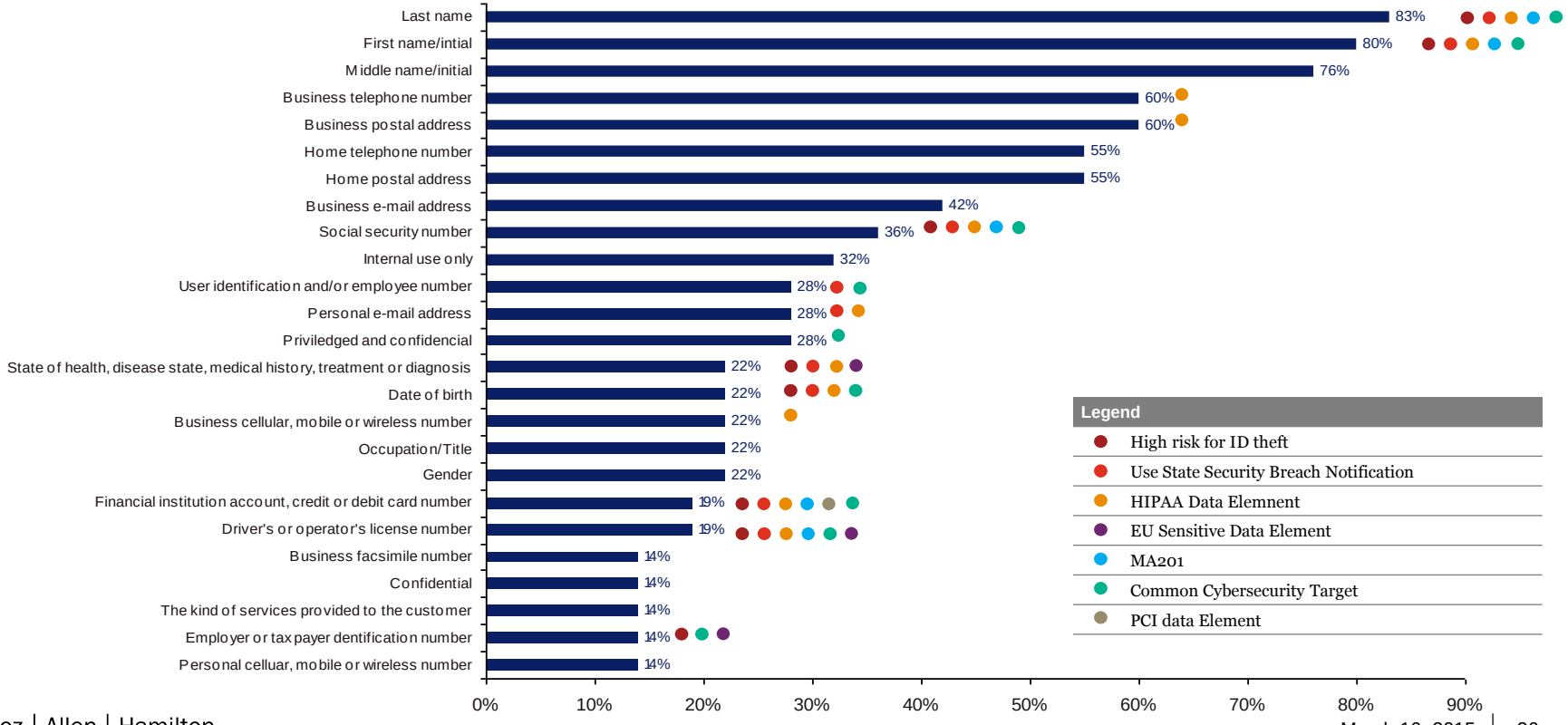
New analytic capabilities derived from the "Big Data" flowing through the ecosystem

- Data Aggregation
- Clinical Analytics
- Predictive Modeling
- Population Analytics
- Real-time Analytics

Data Element Inventories Being Developed for Incident Response and Risk Assessment

Data element inventory - Top 25 data elements. Used in new 4-point test to determine if there is little chance the PHI has been compromised.

Data Element Inventory Analysis. This report inventories and analyzes the extent and locations of high-risk and regulated personal information data elements. This chart graphically represents the concentrations of high-risk and regulated personal information and information at higher risk of identity theft or cybersecurity attack across the organization.



What others are doing

- Data mapping
- Data use and data element inventories
- Enhancing BAs with minimum security provisions, pre-contract assessments and post-contract audits
- Updating Incident response plans
- Enhancing access controls and access monitoring
- Building cyber capabilities

Presentation Agenda

I. Introduction

II. The Background—Audits, Protocols and Enforcements

III. Lessons Learned—Five Things You Need to Know Now

i. Know the Rules and Areas of Non-Compliance
ii. Know the Risks Specific to Your Organization
iii. Know the Data and the Flows – Internal and External
iv. Know Your Audit Process and Prepare
v. Know the Roadmap Ahead and Be Self-Aware

So You Got a Letter . . . A Few Tips for Audit Success

1. Process

Prepare. Many organizations conduct mock audits or other exercises to prepare and practice.

2. Documentation

Omnibus Rule Update. Ensure that the documentation for Programs is reviewed and updated, as necessary, to comply with the new Omnibus Rule requirements. Continue to monitor communications from OCR for revisions to the Protocol based on Omnibus.

Mapping of Documentation. Map policy documents to the specific areas of the document request list from OCR. The mapping document furnished along with Program documentation is helpful.

Include a Log of Revisions/Updates. The policies and procedures can include a revision history at the end of each document that provides a log of each revision/update that was made over time.

So You Got a Letter . . . A Few Tips for Audit Success (Cont)

3. Interviews

Prepare Responses for 10 Key Topics. We suggest focusing preparations and responses for, at a minimum, each topic below. Note, this is not an OCR list.

1. Business Associates
2. Training
3. Sanctions
4. Minimum Necessary Use
5. Accounting for Disclosures
6. Authorizations
7. Incident Response
8. Breach Tracking/Analysis/Notification
9. Notice of Privacy Practices
10. Physical Security

Pay Attention to Trends. Watch (i) OCR trends and compliance protocol changes, (ii) common areas of non-compliance and (iii) areas of enforcements and breaches.

Presentation Agenda

I. Introduction

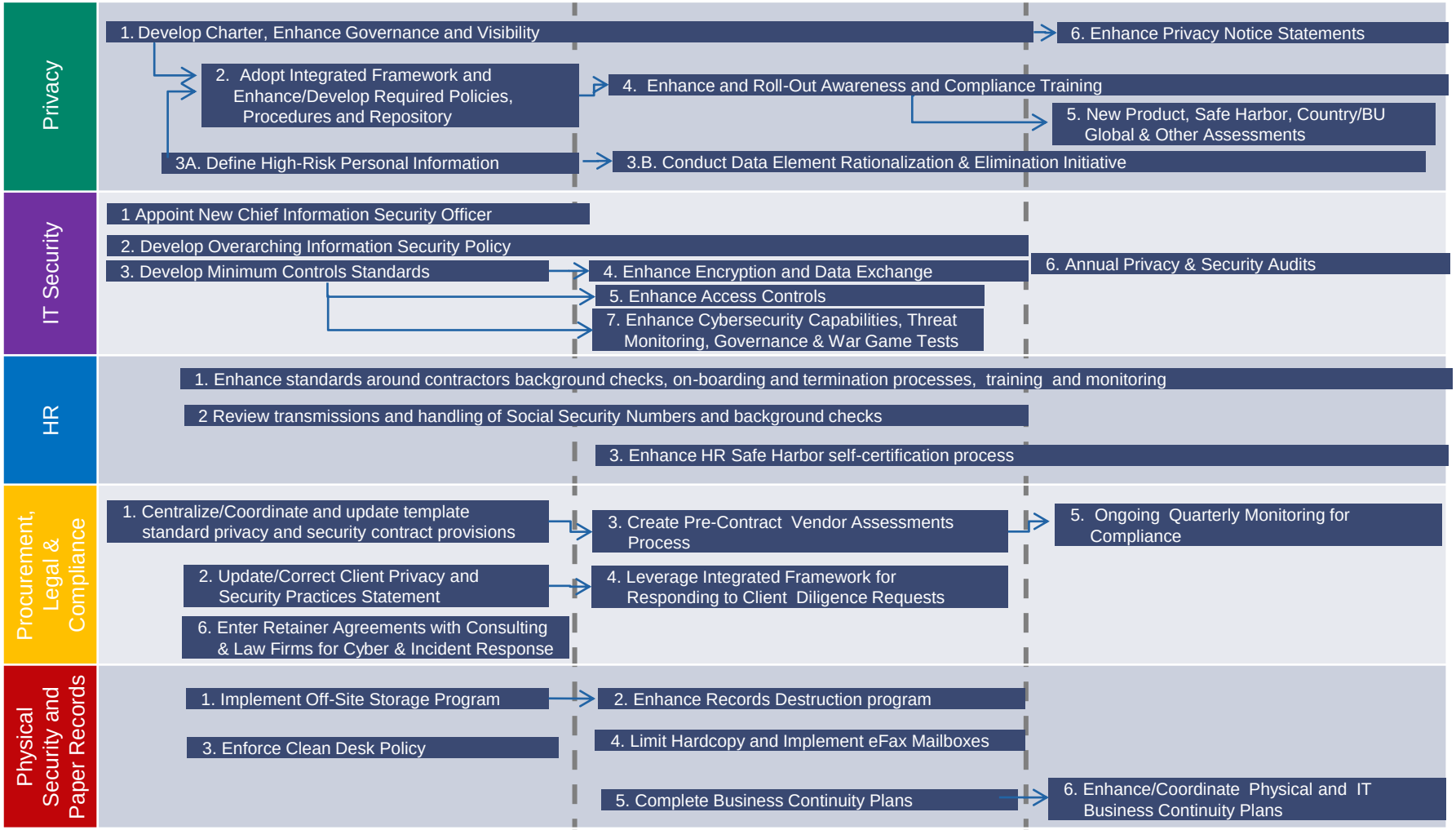
II. The Background—Audits, Protocols and Enforcements

III. Lessons Learned—Five Things You Need to Know Now

i. Know the Rules and Areas of Non-Compliance
ii. Know the Risks Specific to Your Organization
iii. Know the Data and the Flows – Internal and External
iv. Know Your Audit Process and Prepare
v. Know the Roadmap Ahead and Be Self-Aware

Integrated Privacy & Security Program Initiative Roadmap- The Secret Sauce – A Risk Management Plan You Follow

This page sets forth a typical, illustrative Gantt chart roadmap illustrating how such initiatives are typically coordinated/timed and the related key dependencies typically in 18 months, but can be accelerated to 12 months or spread over 24 months).



Thank you.

For more information on individual solutions and how we can support your success, please contact:

Jim Koenig
Principal, Global Privacy Leader;
Co-Leader, Cyber and Incident Response
Koenig_James@bah.com
Tel +610-246-4426

www.boozallen.com