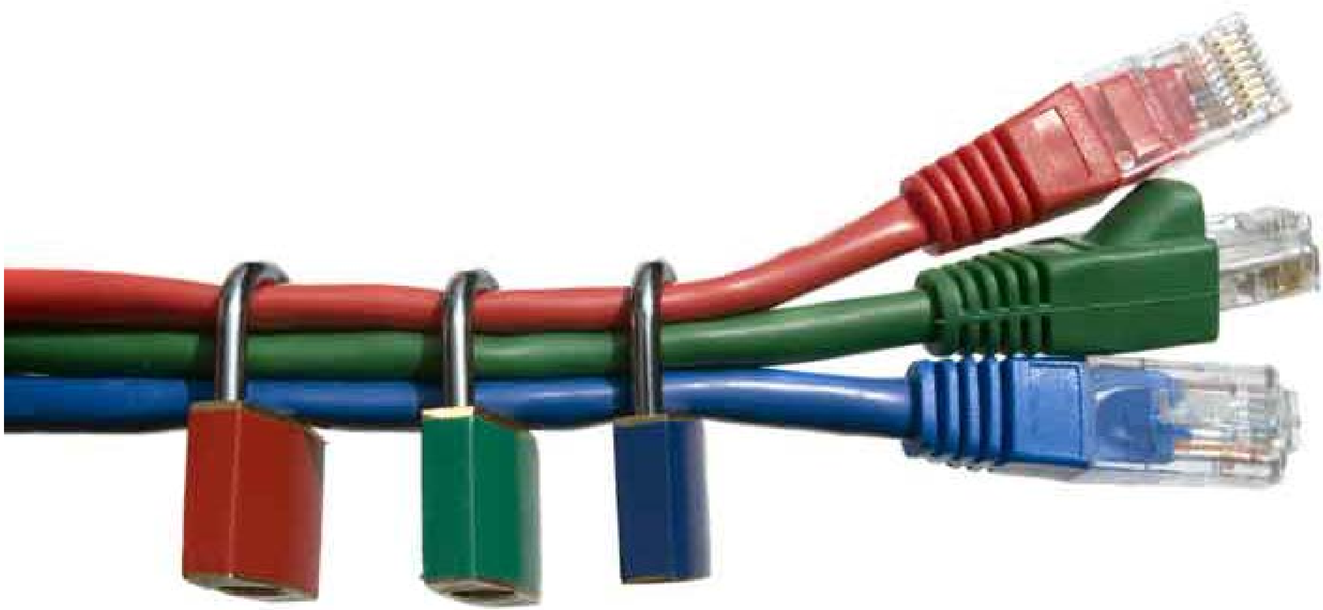
LeadingAge

ANNUAL MEETING AND EXPO

November 1–4, 2015 • Boston MA

Be the Voice 2015 ANNUAL MEETING AND EXPO

HIPAA Security Best Practices



LeadingAge™

Clint Davies

Principal

BerryDunn

cdavies@berrydunn.com

Dan Vogt

Senior Manager

BerryDunn

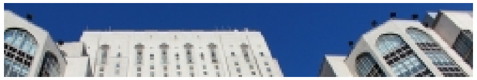
dvogt@berrydunn.com

Agenda

- Introductions
- HIPAA in the News
- Overview of the HIPAA Security Rule
- Risk Assessment Approach
- Top Issues Challenging IT Security
- Questions and Answers

HIPAA in the News[2]

Groups hit with record $4.8M HIPAA fine



Patient data popped up on Google

May 8, 2014

Email hack makes for HIPAA breach

'Patient information may be included in the provider's email account,'

October 14, 2014

HIPAA data breaches climb 138 percent

February 6, 2014

HIPAA breach is bad news for 729,000

Health system now to 'expedite' encryption

ALHAMBRA, CA | October 23, 2013

OCR: Be prepared for HIPAA audits

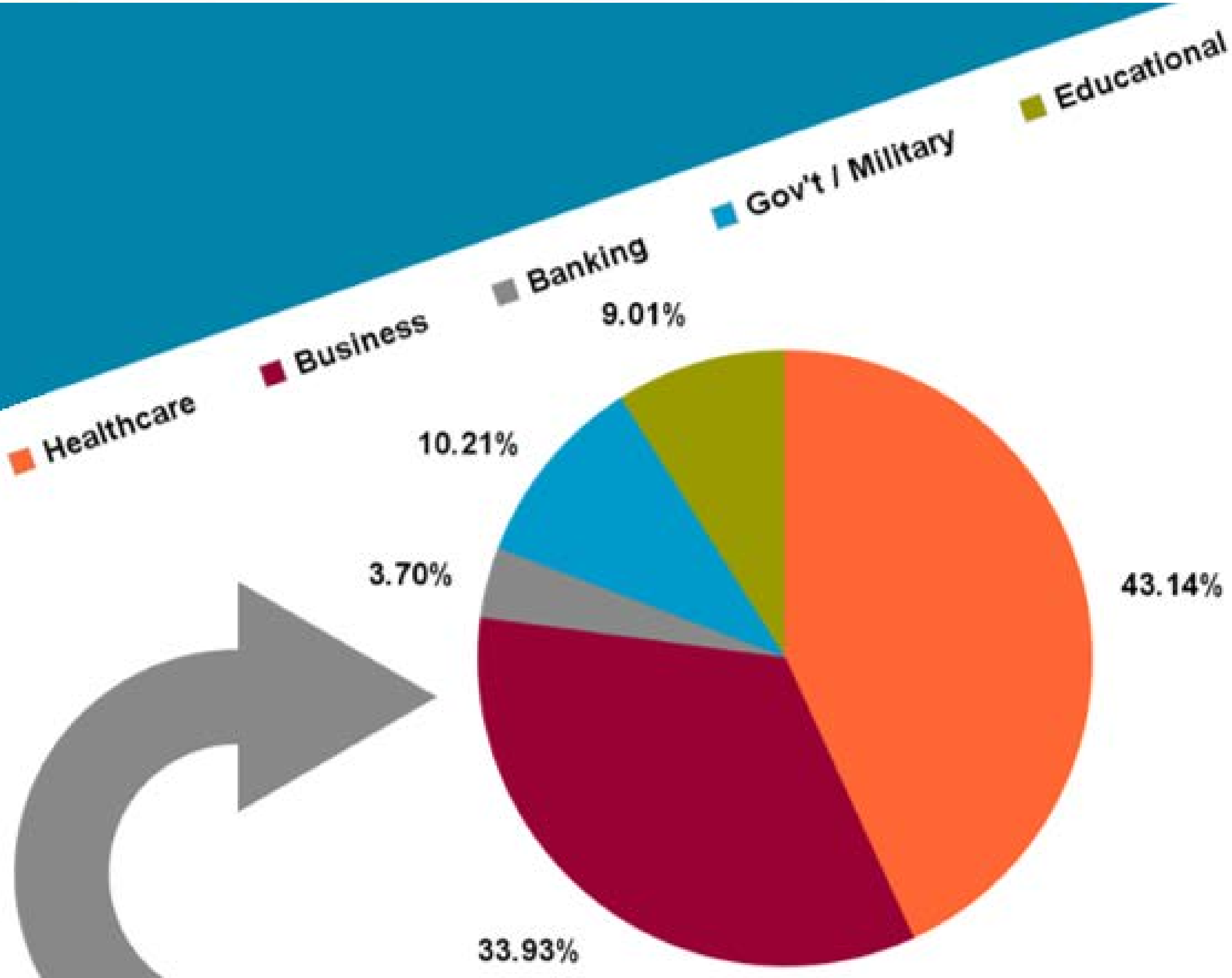
'The onus is on you to prove you had the proper systems in place.'

Third big HIPAA breach

Doc loses unencrypted USB drive

ROCHESTER, NY | May 6, 2013

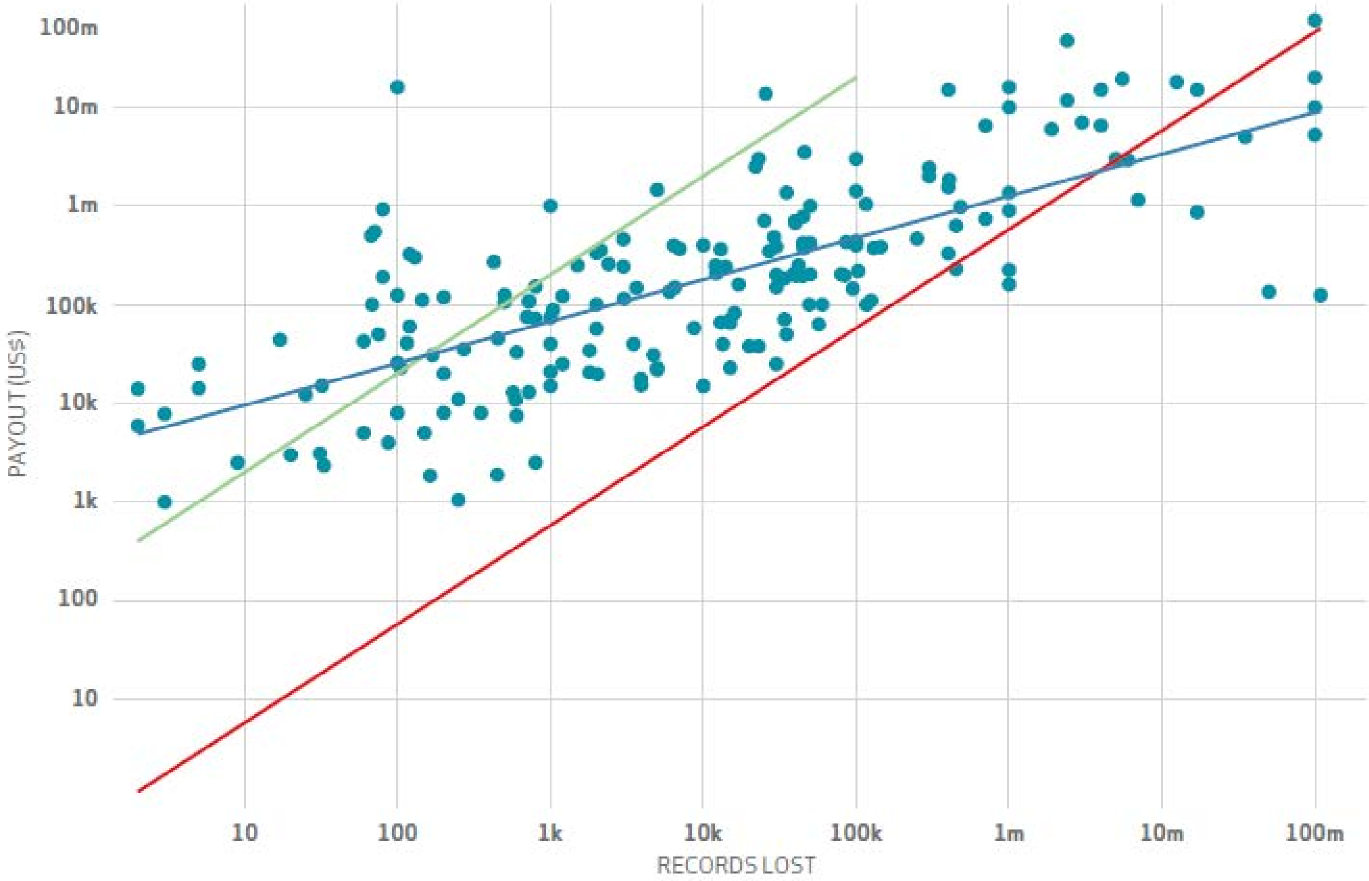
[2] http://www.healthcareitnews.com/



WHERE DID BREACHES OCCUR?

LeadingAge™

Cost of a Data Breach



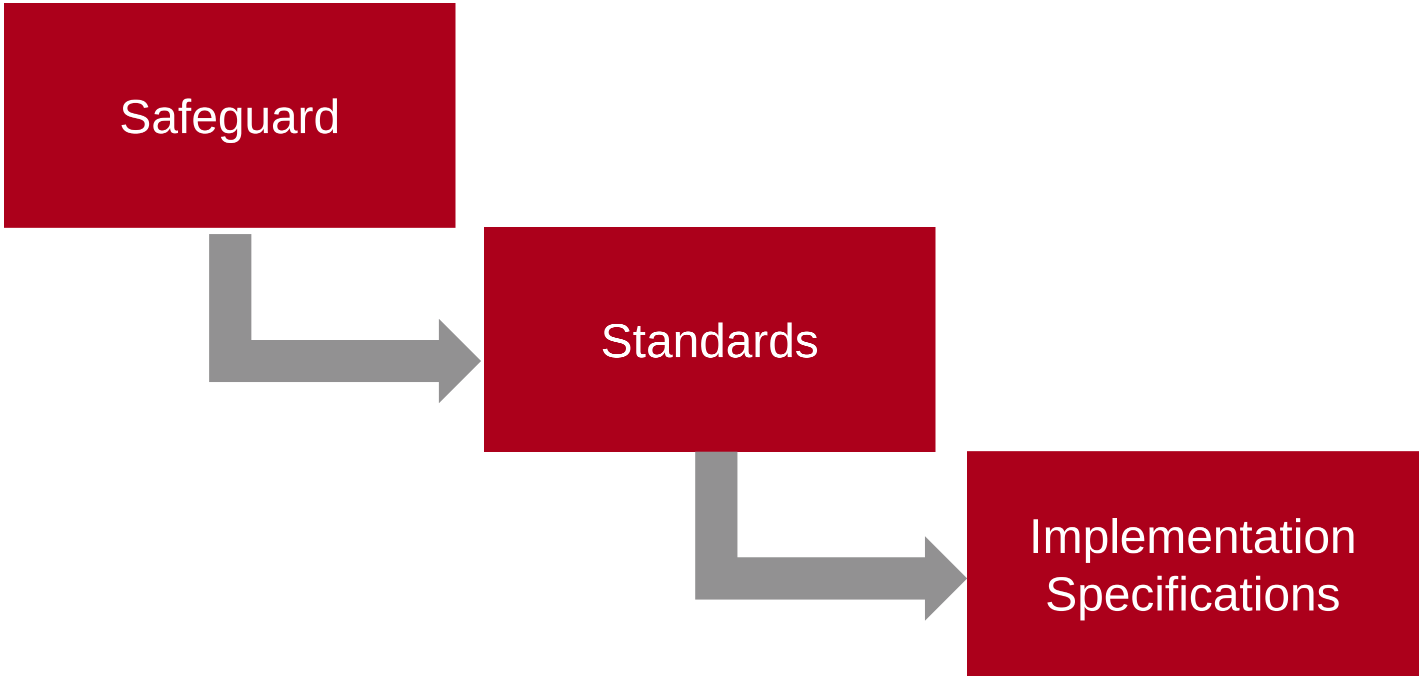
Source: Verizon 2015 Data Breach Investigations Report

Background

- Health Insurance Portability and Accountability Act (HIPAA)
- Established in 1996
- Privacy and Security Rules
- ARRA (2009)
- Omnibus Rule (2013)
- Today’s focus will be on Security Rule

Security Rule

The Security Rule is structured by:



Safeguard

Standards

Implementation Specifications

Security Rule

- Safeguards are organized into:
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards
- Implementation Specifications are either:
  - Required
  - Addressable

Security Rule

CMS recommends an approach[1]

- Assess current security, risks, and gaps
- Develop an implementation plan
- Implement solutions
- Document decisions
- Reassess periodically

[1] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf

Administrative Safeguards

Standard	Implementation Specification	R/A
Security Management Process	Risk Analysis	R
	Risk Management	R
	Sanction Policy	R
	Information System Activity Review	R
Assign Security Responsibility		R
Workforce Security	Authorization and/or Supervision	A
	Workforce Clearance Procedure	A
	Termination Procedures	A

Administrative Safeguards (cont.)

Standard	Implementation Specification	R/A
Information Access Management	Isolating Health Care Clearinghouse Functions	R
	Access Authorization	A
	Access Establishment and Modification	A
Security Awareness and Training	Security Reminders	A
	Protection from Malicious Software	A
	Log-in Monitoring	A
	Password Management	A
Security Incident Procedures	Response and Reporting	R

Administrative Safeguards (cont.)

Standard	Implementation Specification	R/A
Contingency Plan	Data Backup Plan	R
	Disaster Recovery Plan	R
	Emergency Mode Operation Plan	R
	Testing and Revision Procedures	A
	Application and Data Criticality Analysis	A
Evaluation		R
Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement	R

Physical Safeguards

Standard	Implementation Specification	R/A
Facility Access Controls	Contingency Operations	A
	Facility Security Plan	A
	Access Control and Validation Procedures	A
	Maintenance Records	A
Workstation Use		R
Workstation Security		R
Device and Media Controls	Disposal	R
	Media Re-Use	R
	Accountability	A
	Data Backup and Storage	A

Technical Safeguards

Standard	Implementation Specification	R/A
Access Control	Unique User Identification	R
	Emergency Access Procedure	R
	Automatic Logoff	A
	Encryption and Decryption	A
Audit Controls		R
Integrity	Mechanism to Authenticate Electronic PHI	A
Person or Entity Authentication		R
Transmission Security	Integrity Controls	A
	Encryption	A

All about assessing the risks!

Likelihood and Impact

THE RISK ASSESSMENT PROCESS

1 PLANNING	2 EDUCATION + FACT FINDING	3 ANALYSIS	4 REPORT
Work with Project Team to develop workplan	Conduct educational work sessions	Analyze Questionnaire responses	Finalize reports with Project Team
Develop IT Security Risk Assessment Questionnaire	Facilitate meetings with units to walk through Questionnaire	Conduct follow-up as needed	Present outcomes and discuss next steps with stakeholders, including meetings with: • CIO • Information Assurance Committee • Group of stakeholders from participating units
Collaborate with Information Assurance Committee	Units complete and submit Questionnaires to BerryDunn	Develop overall Risk Assessment Report and unit specific reports	

1

PLANNING

Work with Project Team to develop workplan

Develop IT Security Risk Assessment Questionnaire

Collaborate with Information Assurance Committee

2

EDUCATION + FACT FINDING

Conduct educational work sessions

Facilitate meetings with units to walk through Questionnaire

Units complete and submit Questionnaires to BerryDunn

3

ANALYSIS

Analyze Questionnaire responses

Conduct follow-up as needed

Develop overall Risk Assessment Report and unit specific reports

4

REPORT

Finalize reports with Project Team

Present outcomes and discuss next steps with stakeholders, including meetings with:

- CIO
- Information Assurance Committee
- Group of stakeholders from participating units

Putting this to practical use – the Top 10 IT Security Control Risks and what you can do

#10

Segregation of Duties

#9

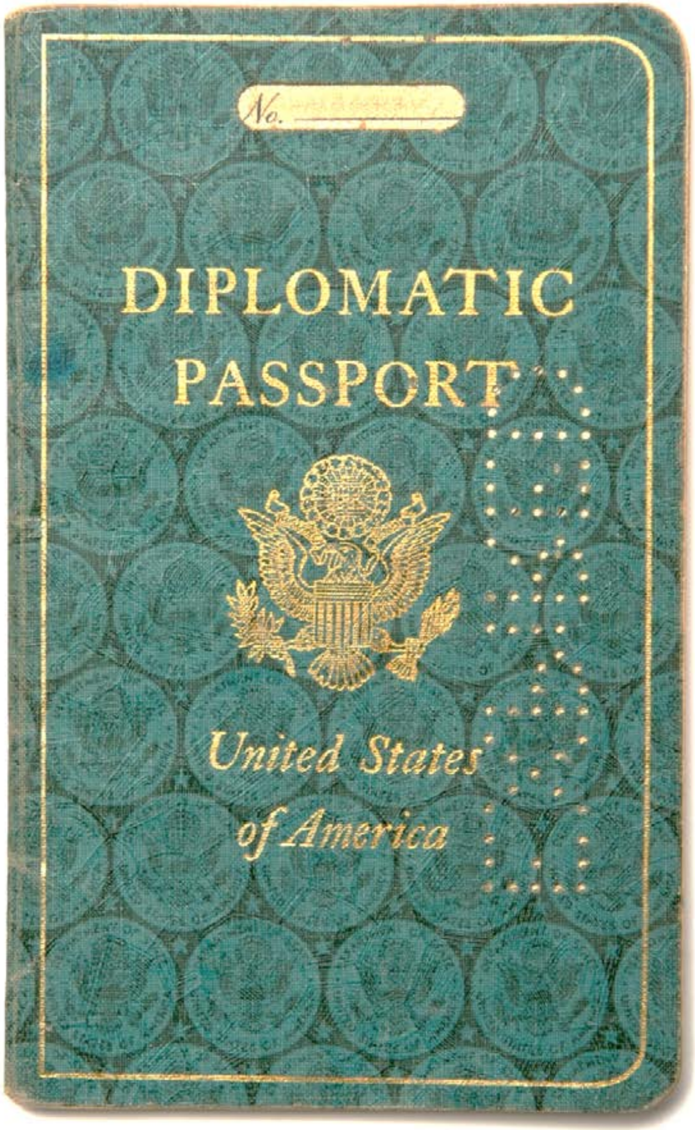
Finding and Maintaining Qualified Security Personnel

#8

Lack of Management Support

#7

IT Diplomatic Immunity



#6

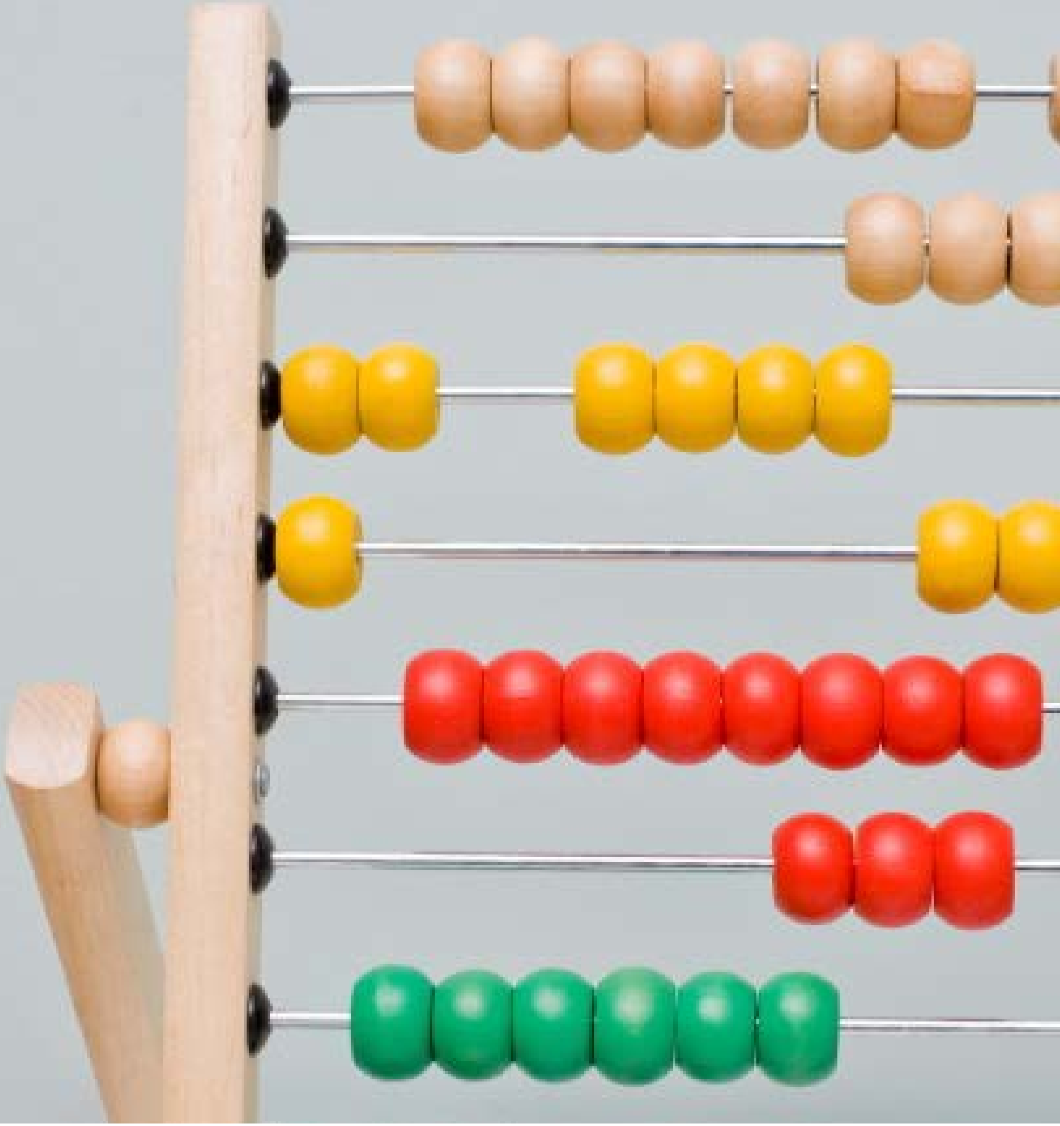
Data on User Owned Mobile Devices

#5

Lack of Encryption

#4

Outdated Operating Systems

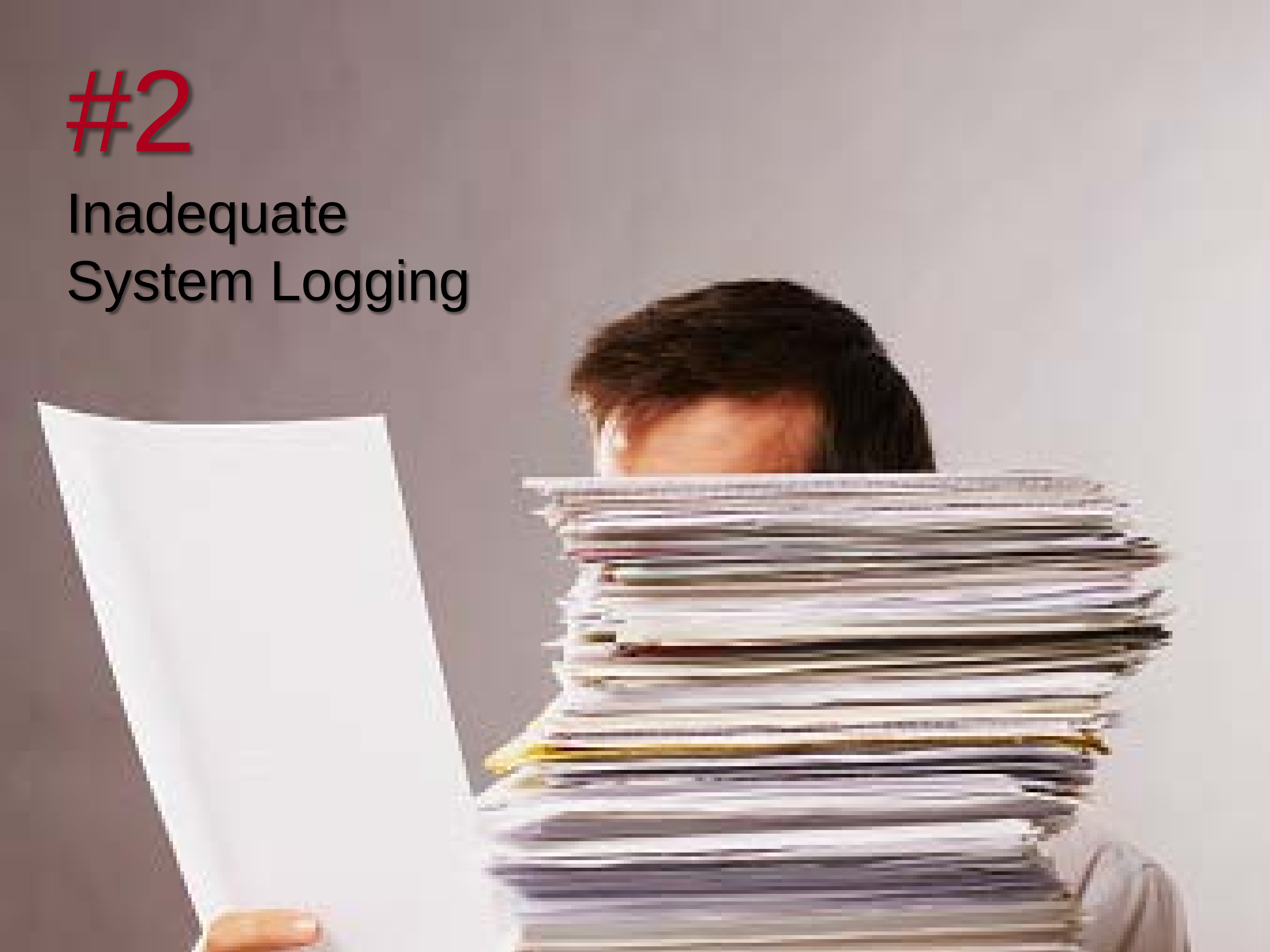


#3

Technology Innovations That Outpace Security

#2

Inadequate System Logging



#1

Overreliance on Security Monitoring Software

TAKEAWAYS

QUESTIONS?

Clint Davies
cdavies@berrydunn.com

Dan Vogt
dvogt@berrydunn.com