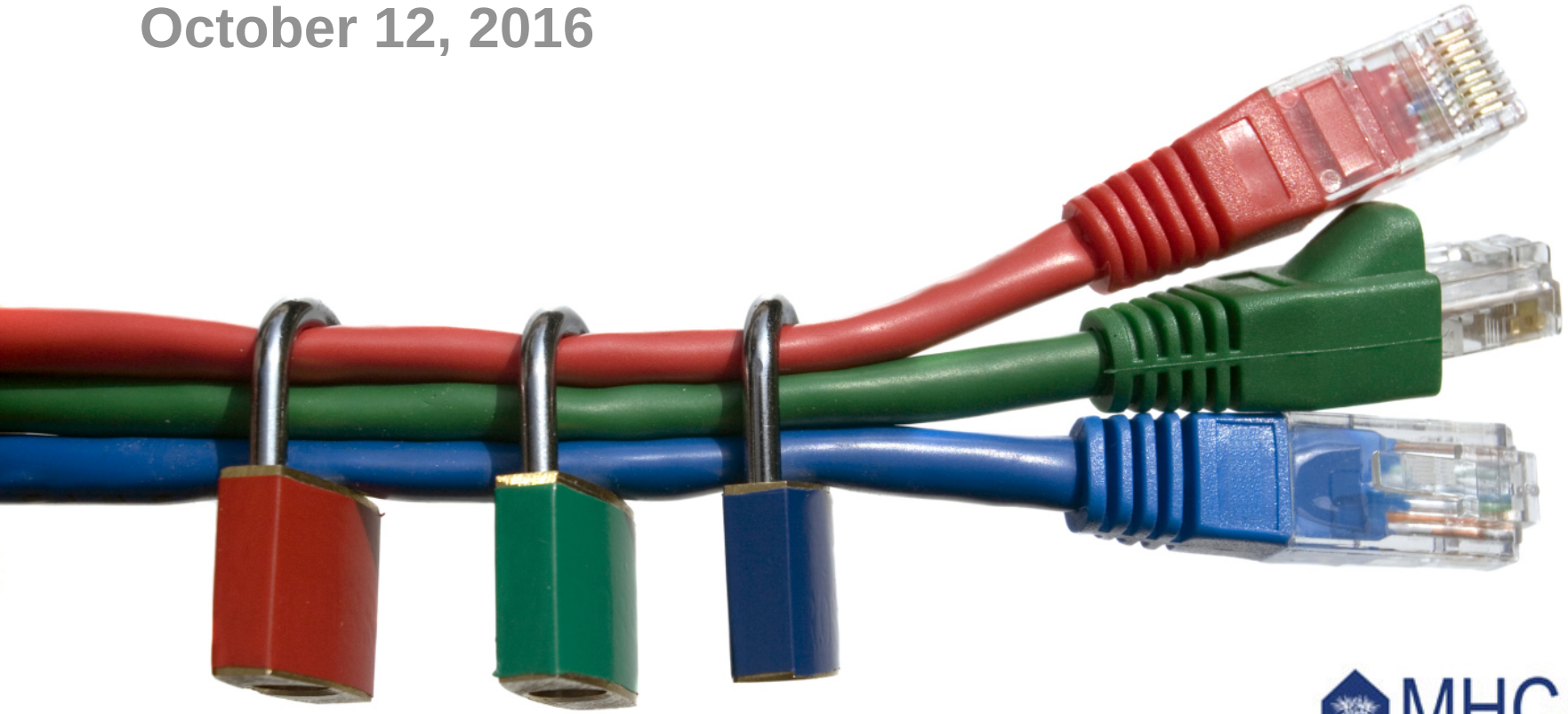
HIPAA Security: Keeping up with the risks

BerryDunn

October 12, 2016



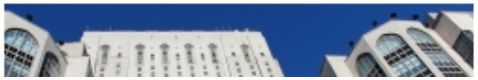
MHCA
Maine Health Care Association

AGENDA

- Overview of the HIPAA Security Rule
- Risk Assessment
- Top Issues Challenging IT Security

HIPAA in the News[2]

Groups hit with record $4.8M HIPAA fine



Patient data popped up on Google

May 8, 2014

HIPAA data breaches climb 138 percent

February 6, 2014

Email hack makes for HIPAA breach

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

October 14, 2014

Privacy & Security

Appalachian Regional back online three weeks after cyberattack

Hospital officials said operations are returning to normal while the cyberattack remains under FBI investigation.

By Beth Jones Sanborn | September 16, 2016 | 03:35 PM

SHARE 85

HIPAA breach is bad news for 729,000

Health system now to 'expedite' encryption

ALHAMBRA, CA | October 23, 2013

Third big HIPAA breach

Doc loses unencrypted USB drive

ROCHESTER, NY | May 6, 2013

Advocate Health Care to pay $5.6 million for potential HIPAA violations, the largest settlement yet for a single entity

OCR found the Illinois-based health system failed to conduct a thorough risk assessment and limit physical access to electronic health systems, among other infractions.

By Jessica Davis | August 04, 2016 | 03:22 PM

SHARE 104

Privacy & Security

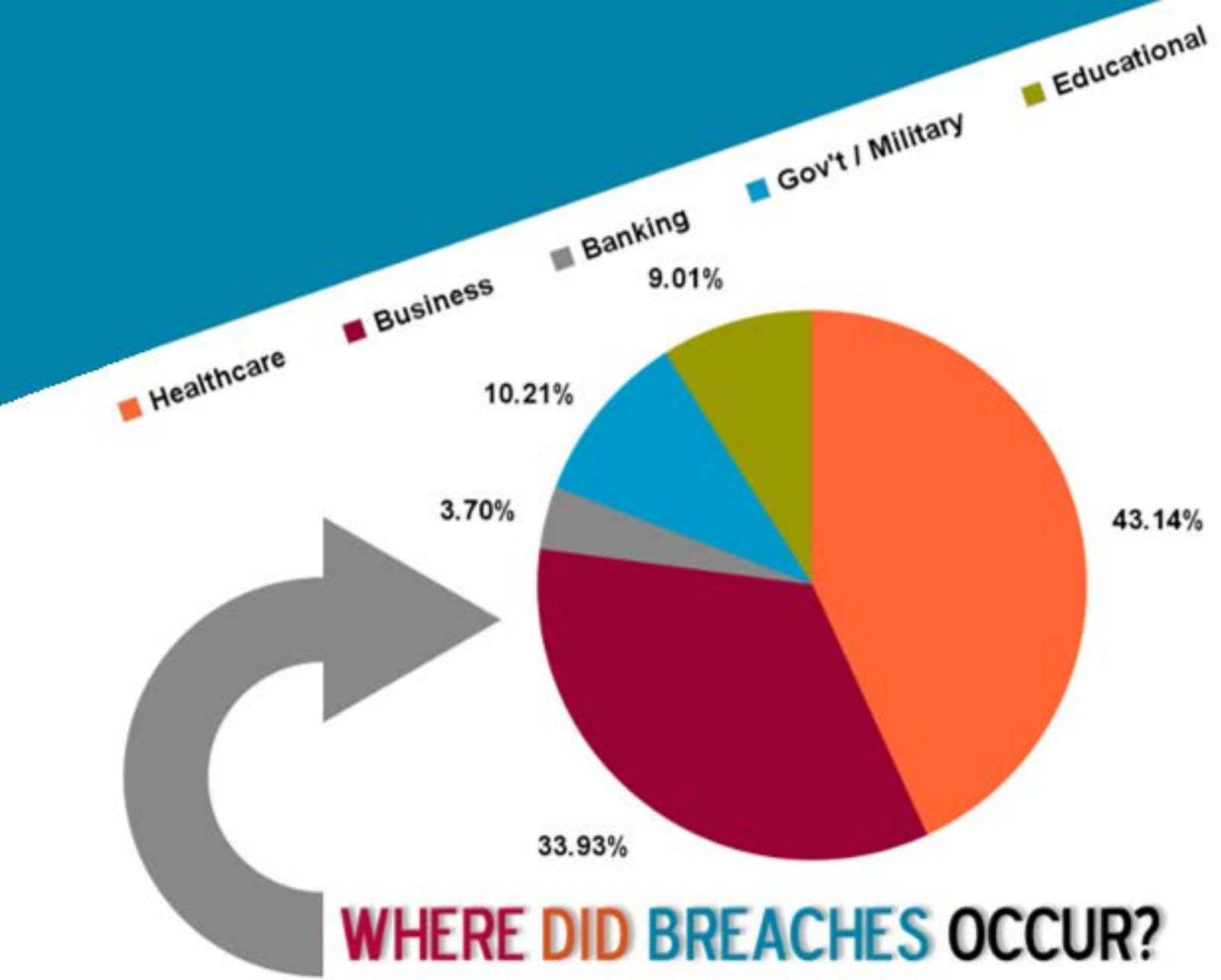
Care New England pays $400,000 HIPAA fine for lost PHI in business associate breach

The case, which also includes Women & Infants Hospital of Rhode Island, stems from lost backup tapes housing protected health information, the Office for Civil Rights said.

By Bernie Monegain | September 26, 2016 | 10:41 AM

SHARE 53

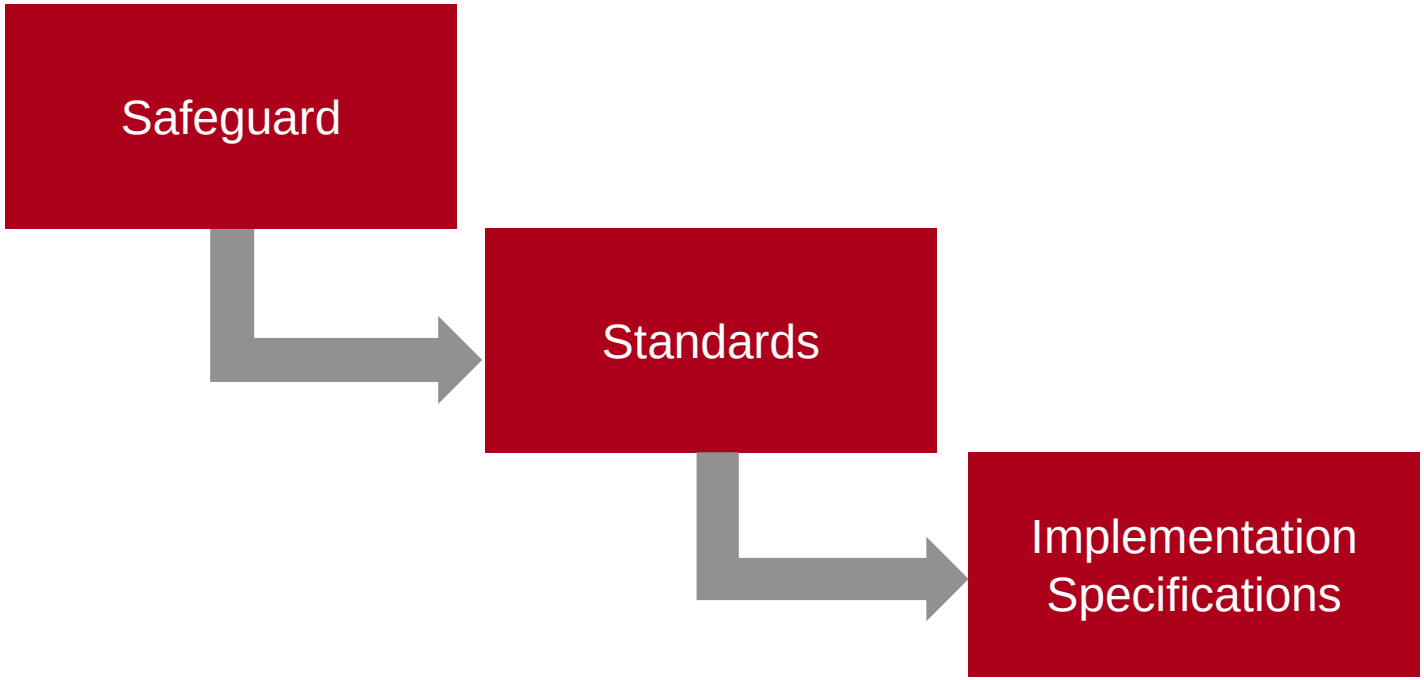
2 http://www.healthcareitnews.com/



Source: http://www.idtheftcenter.org/data-breaches-in-2013.html

Security Rule

The Security Rule is structured by:



Security Rule

- Safeguards are organized into:
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards

- Implementation Specifications are either:
  - Required
  - Addressable

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

Example Risk Assessment Process

Likelihood & Impact

Complicating the Situation

TOP 10 IT SECURITY CONTROL RISKS & WHAT YOU CAN DO

#10

LACK OF DATA CLASSIFICATION & HARDWARE INVENTORY

#9
LEGACY SYSTEMS AND KNOWLEDGE TRANSFER

#8

MEDICAL DEVICE HACKING

#7
LACK OF DEDICATED SECURITY ROLES

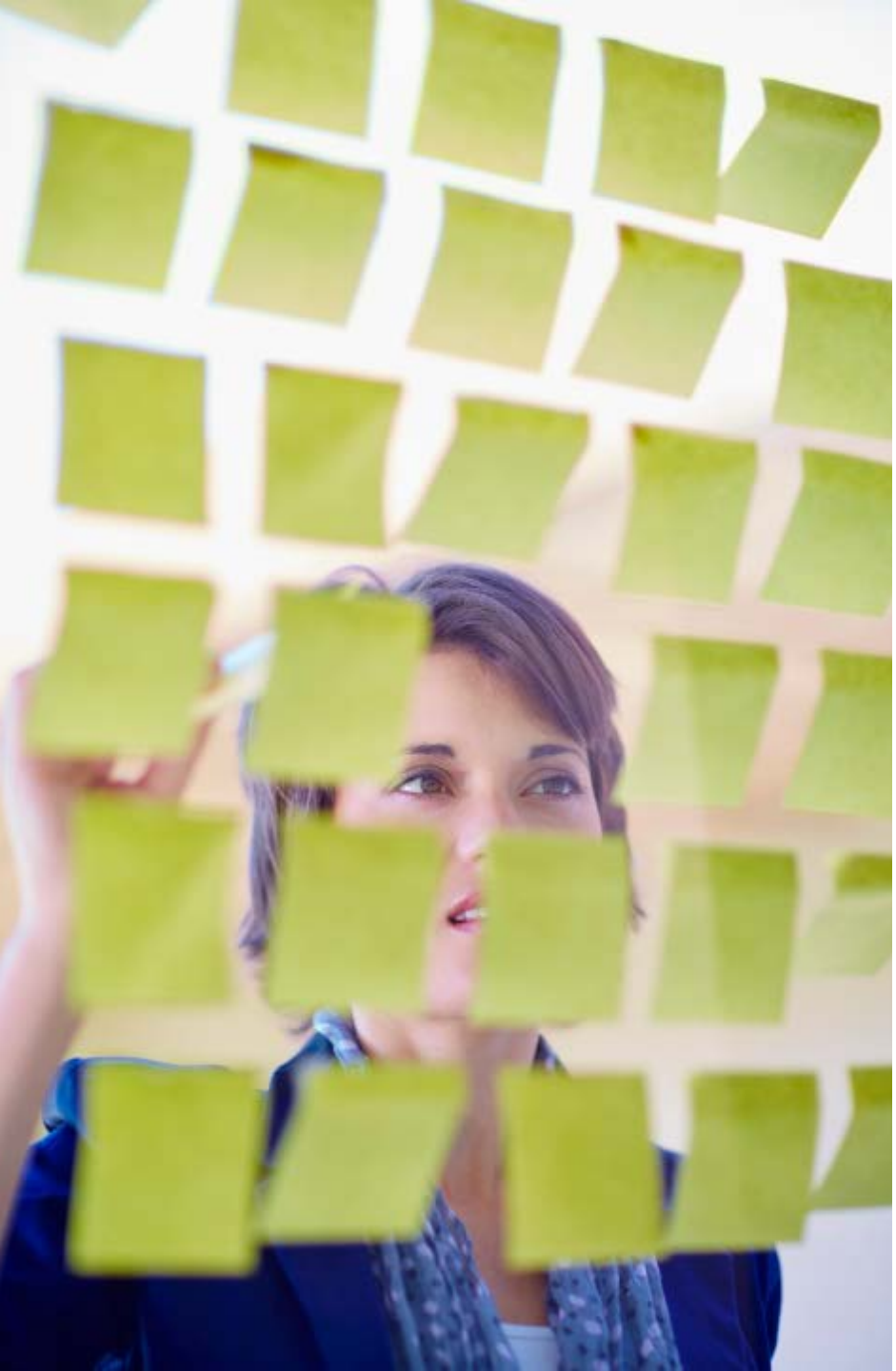
#6
MOBILE DEVICE SECURITY

#5

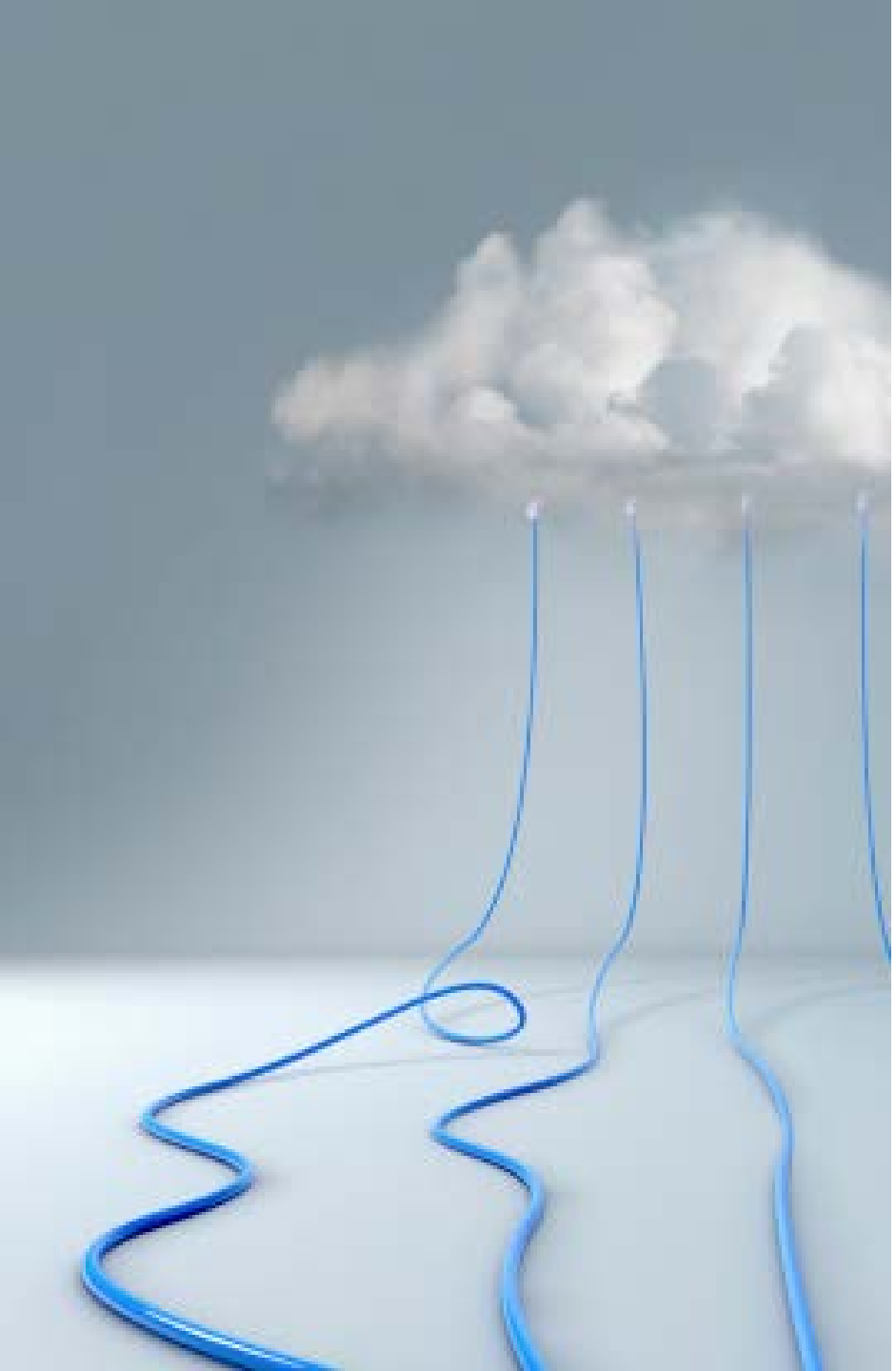
SPEAR PHISHING ATTACKS

#4

SECURITY TRAINING AND AWARENESS



#3
VENDOR MANAGEMENT



#2
PROPER VIRTUALIZATION CONFIGURATION

#1
EXTORTION ATTACKS

Questions?

Dan Vogt
Senior Manager
dvogt@berrydunn.com