O'CONNOR DAVIES

Penn
UNIVERSITY of PENNSYLVANIA

Reining in Third Party Risk

October 14, 2015

Webinar Moderator

Nikki Pittman

Chief Audit Executive, University of Alaska

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

Speakers

Mark Bednarz
Risk Advisory Partner
O'Connor Davies, LLP

Kevin Secrest
IT Audit Manager
University of Pennsylvania

Learning Objectives

- Recognize the types of risks that should be addressed when transitioning functions to third party providers.
- Identify opportunities to improve third party risk management programs
- Understanding U Penn's approach to evaluating IT third party services
- Compare the intended uses of Service Organization Control reports and what to look for during the review.
- Internal Audit's role in third party risk management

Question 1

- Has Internal Audit conducted an engagement on the third party risk management program?
  A. Yes
  B. No
  C. Partially addressed in another internal audit engagement
  D. Not sure

Business Leaders Are Evaluating Outsourcing

Financial Services, Administrative & Human Relations

- Auditing and accounting
- Banking services and debit card
- Campus travel services
- Debt management
- Employee assistance programs
- Endowment fund and investment management
- Financial services
- Legal services
- Payroll
- Retirement programs
- Student loan collections
- Trademark and licensing
- Tuition plans
- Unemployment compensation
- Worker's compensation

Facilities & Grounds

- Architectural and engineering services
- Asbestos removal projects
- Campus master planning
- Construction projects
- Electrical
- Energy management
- Grounds management
- Hazardous waste management
- Hotel management
- Housing facility management
- Housekeeping / janitorial
- Facilities management
- Mechanical maintenance
- Real estate development/operations
- Refuse and waste management
- Residence management
- Research waste removal

Operations

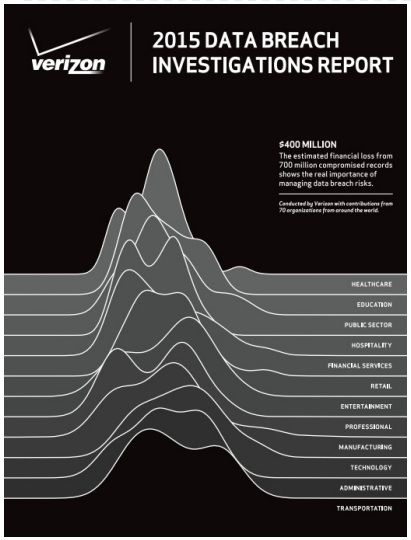
- Copy center / repro
- Data center operations
- IT/MIS
- Mailroom
- Printing and publications
- Security
- Sports marketing

Food Services, Retail, Sports & Entertainment

- Amusement center
- Athletic concessions
- Bookstore
- Computer store
- Day care centers
- Food service
- Golf courses
- Retail store/shopping areas
- Salon operations
- Sports venues
- Student laundry machines
- Vending services
- Video games machines

Source: NACUBO 2015 Annual Meeting - An Insider's Guide To Outsourcing (July 20, 2015)

Security Incidents Are On the Rise



Verizon 2015 Data Breach Investigation Report

Conducted by Verizon with contributions from 70 organizations from around the world

http://www.verizonenterprise.com/DBIR/2015/

	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services (52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85

Intertwining Risks

Question 2

- Has your institution been negatively impacted by a service provider?
  A. Yes
  B. No
  C. Not sure

Vendor Risk Management

Governance

- Define the goals and appoint champion
- Define organization structure & assign responsibilities
- Develop vendor management policy
- Taking a risk-based approach to EBR relationship
- Vendor selection and monitoring process
- Escalation process
- Provide training

Risk Management

- Determine risk factors
- Conduct risk assessment
- Establish risk levels
- Collection of data
- Address results with management
- Develop a remediation steps and communication back to the vendor

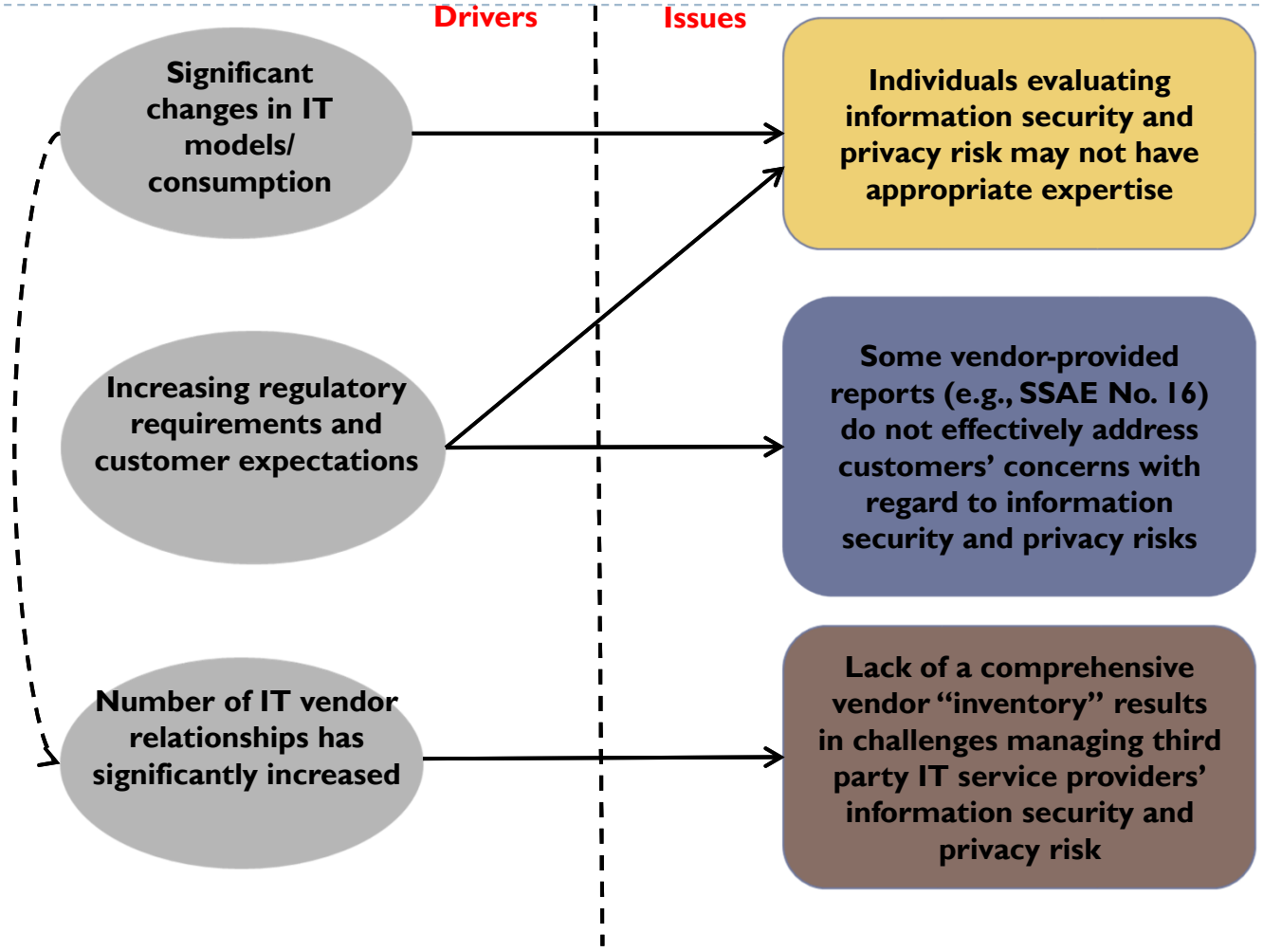
Contract Management

- Getting key stakeholders and Legal involved (drafting, reviewing)
- Keeping abreast of regulatory requirements or industry standards
- Maintaining position on key contract requirements and language
- Establishing KPI and SLA
- Process in place to modify and approve changes to contracts

Question 3

- Which of the following IT areas would be covered by a third party risk management program?
  A. Security
  B. Data classification
  C. Availability / Business continuity
  D. Only security
  E. A, B, and C

Evaluating IT Third Party Service Providers



Evaluating Third Party IT Service Providers (cont.): *Data Classification/Data Sensitivity*

- Effectively evaluating and performing due diligence on an IT third party requires first answering these questions:
  - What type of data is being exposed to the vendor?
  - Do you know what should be done to protect the data?
  - Is there a data classification policy/standards in your organization?

U Penn Data Sensitivity and Review Framework

Data Sensitivity and Review Framework for Evaluating Privacy and Security Safeguards in Cloud and Hosted Services

Data – HIGH sensitivity	Review procedure
Personally identifiable information types: • SSN • Credit card, debit card, or bank account number • Other data requiring notification in event of breach • Certain health information (treatment, diagnosis, certain care settings) • Certain student records (final grades, disciplinary, academic materials) • Certain HR records (salary, performance review, disciplinary) • Certain alumni data (giving, contact reports) • Other personal, highly sensitive data	**Legal** • **Require contract with strong privacy and security requirements.** • Consider need for FERPA, HIPAA, PCI, subcontractor, security assurances language. **Due diligence of security practices** Examples: • SOC Type II or ISO 27001 certification • Alternate third party certification based on recognized security controls • **SPIA for Vendors that is reviewed and accepted by information security and privacy personnel** • Other detailed security program documentation reviewed and accepted by information security and privacy personnel **Additional Risks and Mitigation** • Based on discussion/reviews, there may be additional steps necessary to address privacy and security concerns

U Penn Data Sensitivity and Review Framework (cont.)

Data Sensitivity and Review Framework for Evaluating Privacy and Security Safeguards in Cloud and Hosted Services

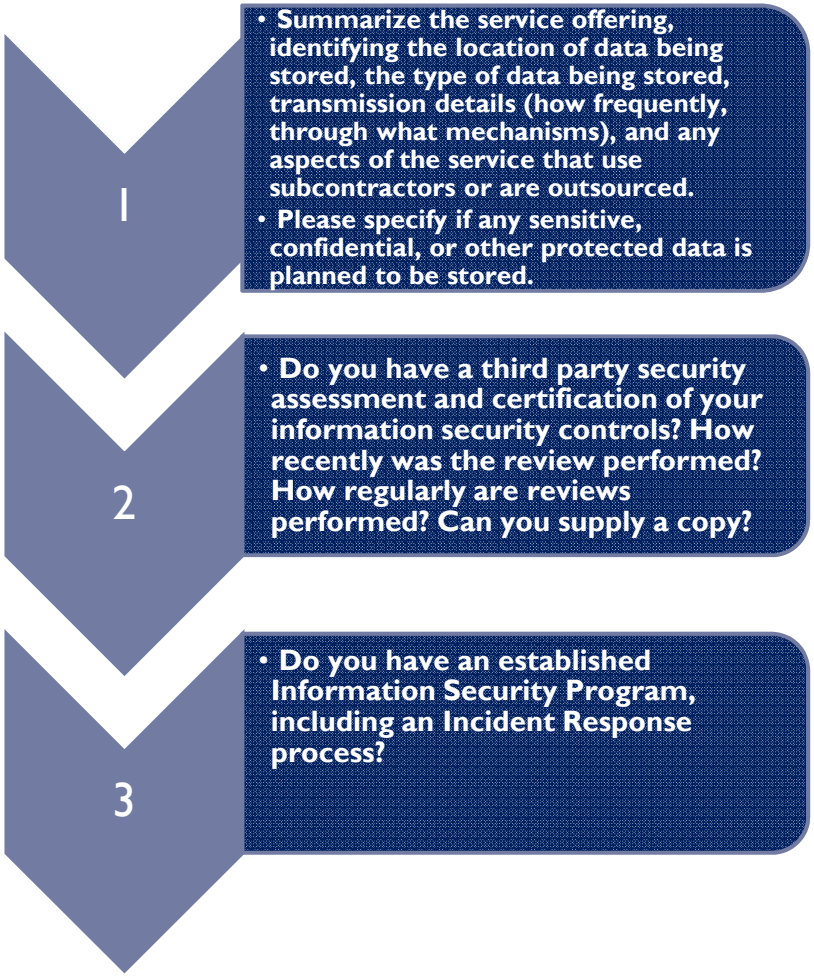
Data – MEDIUM sensitivity	Review procedure
Personally identifiable information types: • Contact information • All FERPA-protected information that is not included on the previous slide • Other personal, but not highly sensitive data	**Legal** • Require contract with strong privacy and security requirements.
	Due diligence of security practices Examples: • Any of the practices noted on previous slide • Review of Terms of Use and Privacy Policies by security or privacy personnel (note: determine whether Terms specify that they can be changed at any time)
	Additional Risks and Mitigation • Based on discussion/reviews, there may be additional steps necessary to address privacy and security concerns

U Penn Data Sensitivity and Review Framework (cont.)

Data Sensitivity and Review Framework for Evaluating Privacy and Security Safeguards in Cloud and Hosted Services

Data – LOW sensitivity	Review procedure
Data very unlikely to be identifiable or, if identifiable, is broadly public information	• Review of Terms of Use and Privacy Policies by security or privacy personnel (note: determine whether Terms specify that they can be changed at any time)

U Penn Security and Privacy Impact Assessment (SPIA)



SPIA for Vendors: Used to evaluate existing security and privacy posture and whether it meets Penn's current recommendations and guidelines

Access Penn's SPIA for Vendors template at:
http://www.upenn.edu/computing/security/cloud/spia_for_vendors.pdf

Monitoring

Manage vendor inventory

Process in place to notify incidents (security breach, insolvency)

Request information

- Vendor revised policies and procedures
- Independent assessments (i.e. SOC report)
- Internal information (i.e. complaints, incidents)

Risk evaluation:

- Tracking incidents and complaints
- Evaluate vendor value
- Assess third party relationships
- Discuss remediation steps with the outsourced provider

ISO/IEC 27001/27002 Standards

- ISO/IEC 27001 is a specification for an information security management system
- ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems
- The standards are open-ended → information security controls are "suggested"
- ISO/IEC do not actually perform certifications, but vendors can be certified through certification bodies
  - To maintain the certificate, the vendor will need to both review and monitor the information security management system on an on-going basis

Question 4

- Which type of Service Organization Control Report (SOC) evaluates the design and the operating effectiveness of the service organization's controls?
  - A. Type 1
  - B. Type 2
  - C. Readiness Assessment
  - D. A and B

Managing Third Party Risk: *Summary of SOC I, SOC II, SOC III*

Service Organization Control 1 (SOC 1)	Service Organization Control 2 (SOC 2)	Service Organization Control 3 (SOC 3)
SSAE No. 16 – service auditor guidance	**AT 101**	**AT 101**
Restricted Use Report (Type I or II report)	**Generally a Restricted Use Report** (Type I or II report)	**General Use Report** (with a public seal)
Purpose: Reports on controls for **financial statement audits**	Purpose: Reports on controls related to **compliance or operations**	Purpose: Reports on controls related to **compliance or operations**
	Trust Services Principles & Criteria: Security, Availability, Processing Integrity, Confidentiality, Privacy	

Excerpt from Trust Services "Security" Principle

3.0	**Procedures: The entity placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.**	
3.1	Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats.	A risk assessment is performed periodically. As part of this process, threats to security are identified and the risk from these threats is formally assessed. Security processes and procedures are revised by the security officer based on the assessed threats.
3.2	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:	
	a. Logical access security measures to restrict access to information resources not deemed to be public.	• Logical access to nonpublic information resources is protected through the use of native operating system security, native application and resource security, and add-on security software. • Resource specific or default access rules have been defined for all nonpublic resources. • Access to resources is granted to an authenticated user based on the user's identity.
	b. Identification and authentication of users.	• Users must establish their identity to the entity's network and application systems when accessing nonpublic resources through the use of a valid user ID that is authenticated by an associated password. • Unique user IDs are assigned to individual users.

Trust Services Principles, Criteria, and Illustrations:
http://www.webtrust.org/principles-and-criteria/item27818.pdf

Generally Accepted Privacy Principles:
http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_BUS_%200909.pdf

Putting on the Auditor's Hat

- Is this the right report?
- Is our location and service covered?
- Is it the correct period?
- What are the results of the Independent Auditor's Report opinion ?
- Did they cover all the control objectives?
- Did they use any subservice providers?
- Does the department have the appropriate internal controls to address the User Considerations section?
- Were the test steps sufficient?
- Evaluate the deviations.

Internal Audit's Role

- Biggest role is creating awareness throughout your institution
- Review and provide recommendations to the existing governance, system and processes related to vendor risk management program
- Review contracts to ensure that your organization has a means to assess the third party's control environment
- Also address third party risk with your IT security review
- Review, if applicable, independent auditor/security firm reports provided by third parties to determine their usefulness to the organization and whether there are issues that should be discussed
- Offer to your audit clients that you can assist in discussions with third party IT service providers about whether the vendor's existing reports/documentation effectively mitigates information security and privacy risk
- Offer to your audit clients the ability to assist with "right-to-audit" work
- Inspect policies and procedures to see if they have been updated to reflect new responsibilities

ACUA Resources

ACUA

- **Visit the ACUA webpage for Internal Audit Awareness Resources:** http://www.acua.org/ACUA_Resources/InternalAuditAwareness.asp

- **Promoting Internal Audit:** www.acua.org/movie

- **The ACUA Community (ACUA-C) forums have REPLACED the listserv!**
  - Using the link www.acua.org, navigate to "Networking" and select "Community"
  - Login and check it out!

- **ACUA-C Tip:** Login through the ACUA website and check the box for "Remember me." When you see a discussion in your email inbox which you would like to offer feedback or a response, just click on the link and it will take you directly to the desired discussion.

Upcoming Events

Webinar: Baker Tilly in December

Details to be announced

2016 Midyear Conference

April 10- 13, 2016

Portland Marriott Downtown Waterfront

Portland, OR

2016 Annual Conference

Sept 11- 15, 2016

Lowes Miami Beach Hotel

Miami Beach, FL

Questions?

Mark Bednarz
Risk Advisory Partner
O'Connor Davies, LLP
(646) 449-6376
mbednarz@odpkf.com

Kevin Secrest
IT Audit Manager
University of Pennsylvania
(215) 573-4495
ksecrest@upenn.edu