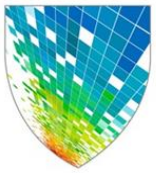
INSTITUTIONAL RISK MANAGEMENT SYMPOSIUM

Risk Management in Cloud Computing: Initiatives, Risks, and Best Practices

Jason Snyder and Walter Pizzano

Harvard University

June 22, 2015



HARVARD
INSTITUTIONAL
RISK MANAGEMENT
SYMPOSIUM
2015

Agenda

- Cloud & DevOps Benefits
- Harvard's Cloud & DevOps Vision
- BC/DR Business Requirements
- Program Organization & Approach
- Migrating Applications
- New Risks and Mitigating Existing Risks
- Significant CSP Risks and CSP Risk Responses
- University Support Mechanisms
- The Ideal Approach

Cloud & DevOps Benefits

Benefits of the Cloud

Migrating key Harvard Community information technology solutions to the cloud doesn't just improve efficiency and optimize cost — it also enables our systems to work more reliably in ever-shifting circumstances.

Reliability	Agility with Quality	Cost
• Managed System Updates	• Application Team Self-Service	• Economies of Scale
• Automated Failover	• Deployment Automation	• Utility: Pay as You Go
• Disaster Recovery	• Focus on IT Solutions	• Elastic Capacity: Pay for Use

Harvard's Cloud & DevOps Vision

The Vision for the Cloud & DevOps Program

To improve HUIT's delivery of information technology solutions to the Harvard Community, we will employ **new methodologies, tools, and processes** that will enable us to simplify and deliver **higher-quality solutions** with **improved robustness and resiliency** in a **more timely manner**.

Objectives

1. Develop training to transition staff from administrator roles to cloud and DevOps engineering roles
2. Lead staff transition process and create an empowered, service-focused culture
3. Implement application design and deployment patterns to maximize consistency, quality, and reliability
4. Migrate existing app workloads with a goal of 75% of existing compute from on-premise data centers to the public cloud
5. Establish operational toolsets and processes to ensure operational effectiveness, awareness, and partnership with service teams

Guiding Principles

1. We are committed to staff growth and development as we pursue program goals
2. We will ensure close collaboration between the program and other HUIT teams to maintain high levels of existing services
3. Improving deployment methods and processes are as important as the technologies we use
4. Consistent architectural and design patterns are critical to achieving enterprise-level results
5. Communicating with all employees, partners, and customers is crucial to program awareness and understanding

Key Performance Indicators

1. Percentage of HUIT employees who have successfully completed Cloud & DevOps training
2. Percentage of total apps migrated to cloud providers
3. Improved app availability from monitoring (uptime percentage)
4. Successful DR testing processes in place — average time to recovery for migrated applications
5. Percent deployment rollbacks
6. Cost of deployment solutions compared with onsite measurement

Migrating Applications: The Process

Phase A: Planning

Step 0: Prepare for Application Migration

Step 1: Hold Initial Engagement Meeting

Step 2: Perform Architectural Discovery

Step 3: Create Migration Schedule

Step 4: Perform Cost Comparison

Step 5: Conduct Kick-off Meeting

Phase B: Execution (Iterative Process)

Step 1: Replatform/ Remediate Application

Step 2: Integrate Application

Step 3: Migrate Environments

Step 4: Validate App & Complete Migration

Phase C: Operation & Optimization

Ongoing: Implement, Monitor, Optimize, Repeat

Ongoing: Decommission and Optimize Infrastructure

Cloud IaaS Magic Quadrant

Gartner's Magic Quadrant shows AWS as a clear leader overall in cloud IaaS.

HARVARD INSTITUTIONAL RISK MANAGEMENT SYMPOSIUM 2015

BC/DR Business Requirements

Goal: Solutions to withstand a range of incidents
Embed and build DR design into cloud architecture and migration

- Build new systems to incorporate DR needs

Current: BC/DR for mission-critical services using SunGard Availability Services with some failover to 1 Summer St.

Future: BC/DR embedded as required into cloud designs and SaaS offerings.

BC/DR Business Requirements

For critical apps that may not migrate immediately, we are exploring a POC for replacing Sungard.

Goal	Sub-Goal
Replace Current BC/DR Solutions	Continuous data replication to geographically dispersed off-site data centers; Lower RTO and enhance RPO
	Support (and enhance) Harvard's cloud migration strategy
	Integrate with Harvard's network, security, server, and storage infrastructure
Provide Future BC/DR Solutions	Provide on-prem to multi-cloud BC/DR capabilities (AWS, Azure, Google, etc.)
	Provide inter-cloud to cloud BC/DR capabilities (AWS regions)
	Provide cloud-to-cloud BC/DR capabilities (AWS to Azure, etc.)
BC/DR 1.0	**In FY15, provide BC/DR capabilities for PeopleSoft and Aleph (LTS)**

IaaS Cloud at Harvard: New Risks

Risk	Description	Mitigation Approach
Cloud vendor lock-in	The leading vendor in IaaS by far is Amazon, who introduces proprietary architecture and coding dependencies for ongoing development	A cloud sourcing strategy is being developed, with Microsoft being reviewed as additional option; formalization of vendor SLA and contract terms required with AWS
Multitenancy	Multiple projects will work within similar data-center space in the cloud	Separation by org responsibilities, with security groups within the space additionally configured to segregate responsibility
Pay-per-use	A cost advantage — but this could introduce financial risk if creation is not managed	Embedded DevOps engineers will be centrally managed, sharing a common platform and using advanced monitoring toolsets
Data distributed outside Harvard	The cloud model requires Harvard to trust the infrastructure management of our vendor community	Cloud vendor contract language must be strong, allowing for Harvard to control ownership and access
Automated creation with limited organization controls	Infrastructure creation and account creation and management are distributed	Embedded DevOps engineers will be centrally managed; separation of duties is achieved by process, not people

IaaS Cloud: Mitigating Existing Risk

Existing Risk	Description	Cloud Improvements
Limited disaster recovery capabilities	The disaster recovery process is dependent upon SunGard and relies on restoring applications offsite from tape	Regional configuration and automatic recovery, if needed, with the appropriate application configuration
QA inconsistencies	No centrally coordinated QA approach for app deployment, resulting in inconsistent software quality	DevOps platform will allow automated QA testing, improving the consistency and speed associated with validating code
Limited architecture patterns	Today's infrastructure is deployed as independent one-offs, resulting in learning curves for ongoing management	Deployment platforms specific to arch patterns, with automation and deployment benefits encouraging consistency
Increasing data storage needs	Increasing capacity for information collection results in overwhelmed storage, higher costs, and lower service quality	Cloud storage options offer alternatives to local storage with advanced management and monitoring capabilities
Staffing	Infrastructure staff hiring is becoming harder, and internal support demands are increasing; according to Gartner numbers, Harvard staff levels are too low	Automation and consistent processes will make creatingsupporting infrastructure more efficient; cloud vendors provide some functions performed locally today

Significant CSP Risks

Chinese Hackers Force Penn State to Unplug Engineering Computers

Bloomberg Business May 25, 2015

CIOs Ignore the NIST Cybersecurity Framework at Their Own Peril

THE WALL STREET JOURNAL. | THE CIO REPORT

Data breach results in $4.8 million HIPAA settlements

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) initiated its investigation of New York and Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated September 27, 2010, regarding the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results. NYP has paid OCR a monetary settlement of $3,300,000 and CU $1,500,000, with both entities agreeing to a substantive corrective action plan, which includes undertaking a risk analysis, developing a risk management plan, revising policies and procedures, training staff, and providing progress reports.

HHR.gov May 7, 2014

UNIVERSITY OF MARYLAND'S RESPONSE TO DATABASE BREACH MAY COST MILLIONS

Capital News Service Feb 27, 2014

Significant CSP Risks

- Data security and integrity
- System availability
- Regulatory compliance
- Financial recourse for failures or breaches

CSP Risk Responses

- Data security and integrity
- System availability
- Regulatory compliance
- Financial recourse for failures or breaches

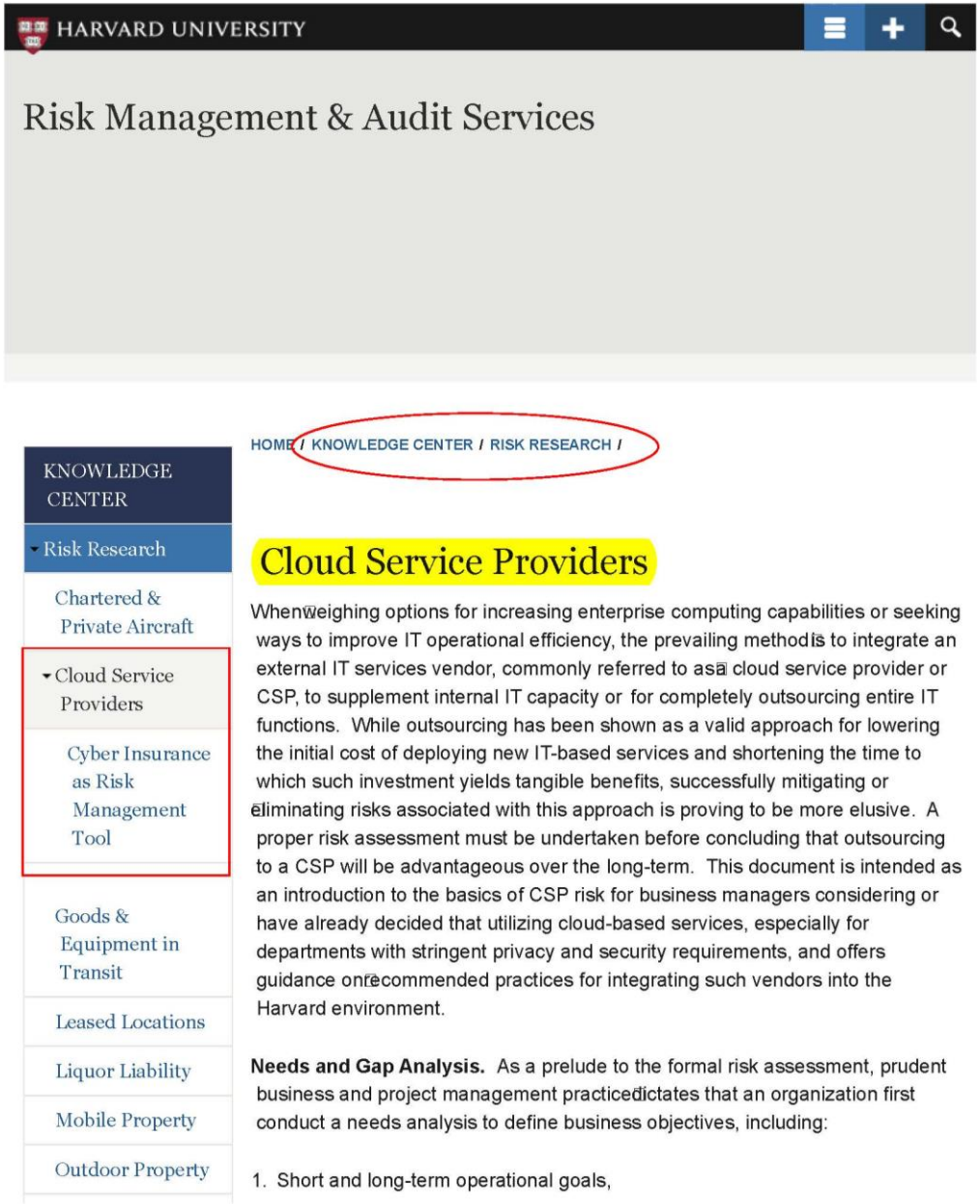
- Thorough vendor pre-selection vetting process
- Strong contract terms with recourse provisions
- Require vendor to have commercial insurance
- Audit and assess for compliance with terms
- Seek technical/expert assistance when in doubt

University Support Mechanisms

- **Expert resources:** HUIT, OGC, RMAS, Strategic Procurement, peer groups
- **Risk Research/Knowledge Center:** http://rmas.fad.harvard.edu/cloud-service-providers
- **Financial:** University's insurance is limited to damages caused to others; damages or expenses incurred by system owner should be considered entirely self-insured by School or Department
- **Internal funding:** Some limited loss recovery funds may be available through CADM

University Support Mechanisms

- Interest in a Vendor Risk Assessment Tool?
  - Survey-based
  - Scoring against in-place risk controls
  - First-pass vendor evaluation/grading tool



HARVARD UNIVERSITY

Risk Management & Audit Services

HOME / KNOWLEDGE CENTER / RISK RESEARCH /

KNOWLEDGE CENTER

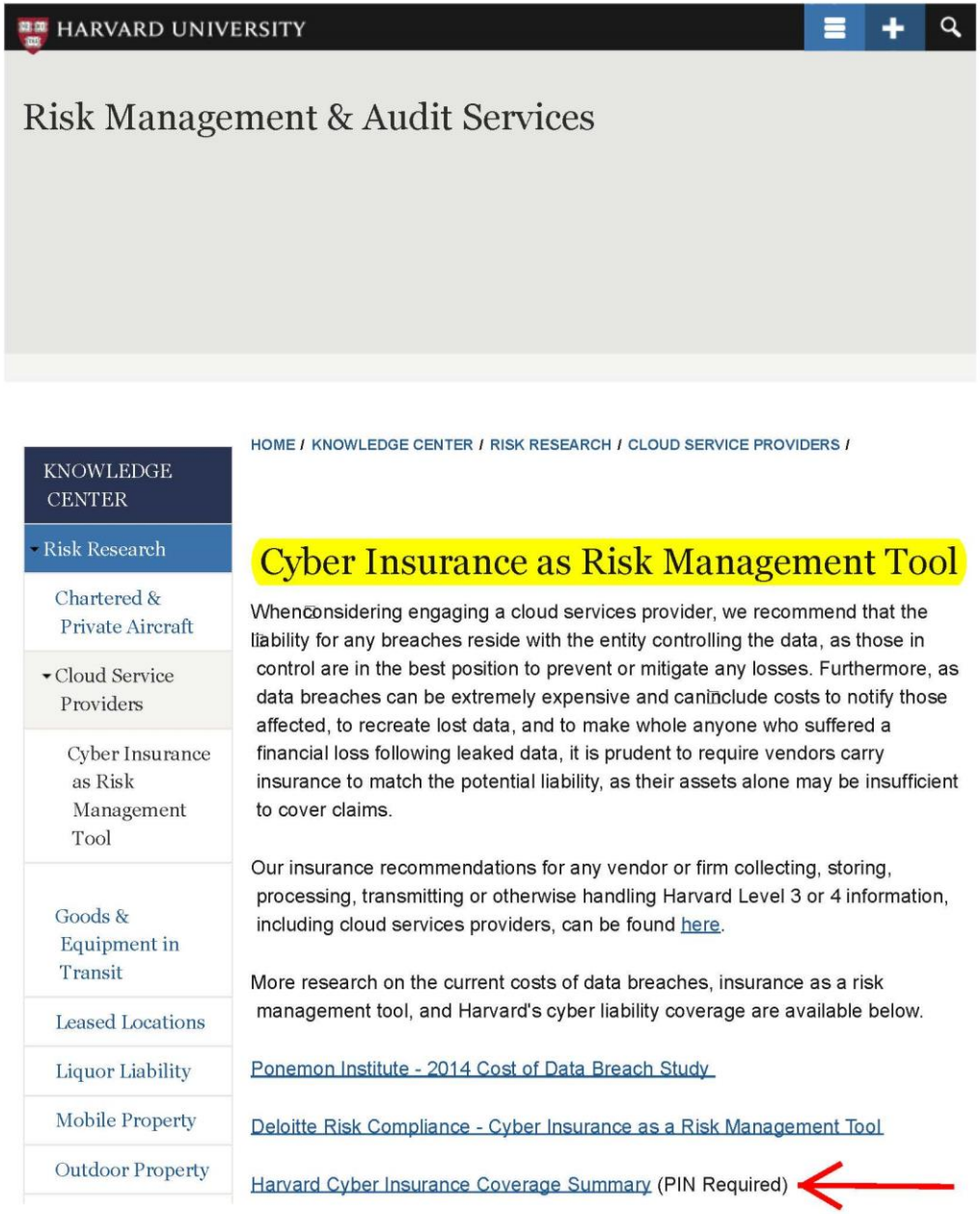
- Risk Research
  - Chartered & Private Aircraft
  - Cloud Service Providers
    - Cyber Insurance as Risk Management Tool
  - Goods & Equipment in Transit
  - Leased Locations
  - Liquor Liability
  - Mobile Property
  - Outdoor Property

Cloud Service Providers

When weighing options for increasing enterprise computing capabilities or seeking ways to improve IT operational efficiency, the prevailing method is to integrate an external IT services vendor, commonly referred to as a cloud service provider or CSP, to supplement internal IT capacity or for completely outsourcing entire IT functions. While outsourcing has been shown as a valid approach for lowering the initial cost of deploying new IT-based services and shortening the time to which such investment yields tangible benefits, successfully mitigating or eliminating risks associated with this approach is proving to be more elusive. A proper risk assessment must be undertaken before concluding that outsourcing to a CSP will be advantageous over the long-term. This document is intended as an introduction to the basics of CSP risk for business managers considering or have already decided that utilizing cloud-based services, especially for departments with stringent privacy and security requirements, and offers guidance on recommended practices for integrating such vendors into the Harvard environment.

Needs and Gap Analysis. As a prelude to the formal risk assessment, prudent business and project management practice dictates that an organization first conduct a needs analysis to define business objectives, including:

1. Short and long-term operational goals,


HARVARD UNIVERSITY
Risk Management & Audit Services
KNOWLEDGE CENTER
Risk Research
Chartered & Private Aircraft
Cloud Service Providers
Cyber Insurance as Risk Management Tool
Goods & Equipment in Transit
Leased Locations
Liquor Liability
Mobile Property
Outdoor Property
HOME / KNOWLEDGE CENTER / RISK RESEARCH / CLOUD SERVICE PROVIDERS /
Cyber Insurance as Risk Management Tool
When considering engaging a cloud services provider, we recommend that the liability for any breaches reside with the entity controlling the data, as those in control are in the best position to prevent or mitigate any losses. Furthermore, as data breaches can be extremely expensive and can include costs to notify those affected, to recreate lost data, and to make whole anyone who suffered a financial loss following leaked data, it is prudent to require vendors carry insurance to match the potential liability, as their assets alone may be insufficient to cover claims.
Our insurance recommendations for any vendor or firm collecting, storing, processing, transmitting or otherwise handling Harvard Level 3 or 4 information, including cloud services providers, can be found here.
More research on the current costs of data breaches, insurance as a risk management tool, and Harvard's cyber liability coverage are available below.
Ponemon Institute - 2014 Cost of Data Breach Study
Deloitte Risk Compliance - Cyber Insurance as a Risk Management Tool
Harvard Cyber Insurance Coverage Summary (PIN Required)

The Ideal Approach

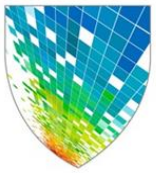
- Cloud service provider (CSP) risk management process starts BEFORE vendor selection step
- Driven by needs analysis, business objectives, and risk appetite
- Project sponsor/owner stays involved throughout vendor selection and vetting steps; don't just delegate and dump onto IT

Summary

- Business leader and/or project sponsor must recognize they own, and are accountable for, cloud service provider risk management
- RMAS, HUIT, and others are available to assist with exploring and optimizing options
- Harvard must incorporate the cost of risk into the evaluation of migrating to a cloud provider

Questions?

- Jason Snyder
  Managing Director, HUIT Architecture & Engineering
  jason_snyder@harvard.edu
- Walter Pizzano
  Director, Risk Strategy and Insurance
  walter_pizzano@harvard.edu



HARVARD
INSTITUTIONAL
RISK MANAGEMENT
SYMPOSIUM
2015

Don’t Miss It!

Ending Keynote Speaker: *Dr. Leonard Marcus*

Founding Director of the Program for Health Care Negotiation and Conflict Resolution at the Harvard T.H. Chan School of Public Health and Co-Director of the National Preparedness Leadership Initiative

Dr. Marcus will discuss how our individual risk tolerances affect our decision-making and how we can use the concept of “meta-leadership” to better act, collaborate, and direct others in high-stress, high-stakes situations.

He will also discuss “connectivity“, terrorism preparedness and emergency response as well as his research activities which include dilemmas facing emergency preparedness and response, from the 2005 Hurricanes Katrina and Rita to the frontlines of the Hezbollah-Israel war in 2006 to the 2013 Boston Marathon bombings.

HARVARD
INSTITUTIONAL
RISK MANAGEMENT
SYMPOSIUM
2015