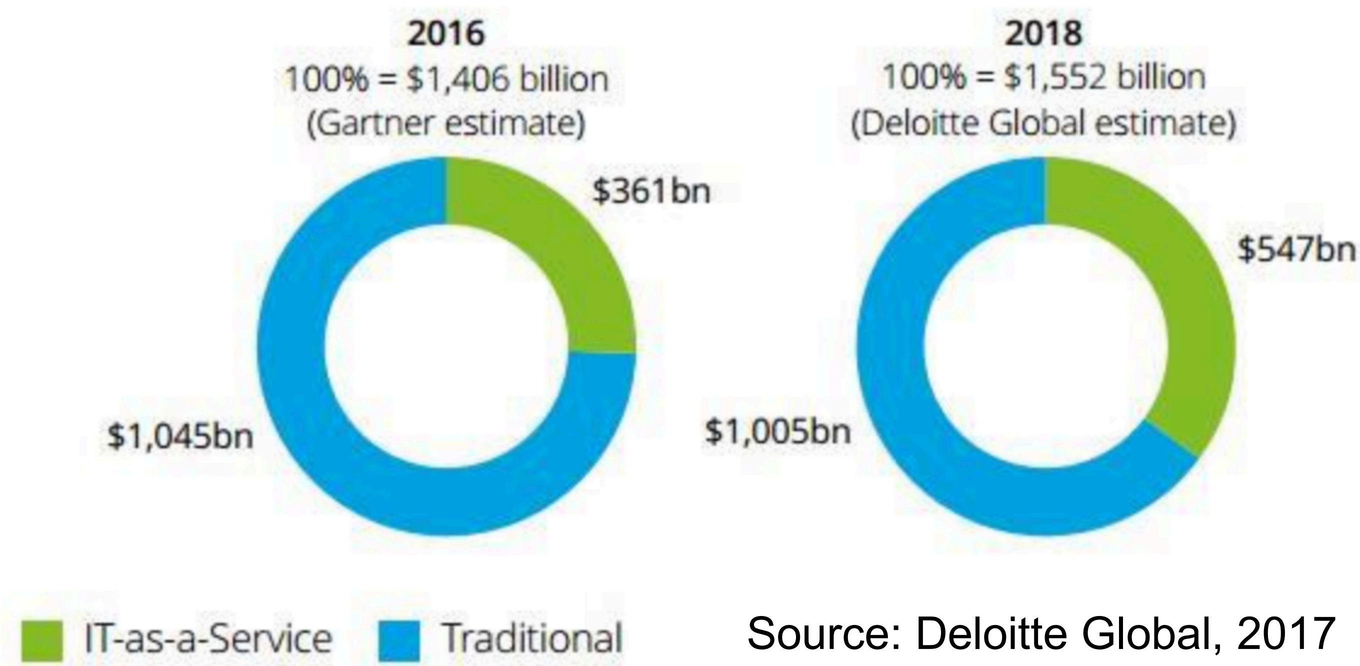
IFIP 10.4 Working Group 73rd Meeting
Goa, India, Jan 12-13, 2018

Hari Ramasamy
IBM Watson and Cloud

Intro to Workshop on *Emerging Challenges for Resilience of Cloud-based Operations: When Privacy meets Availability*

More and more Infrastructure, Apps, and Business Processes are being migrated to the cloud (cloud immigrant) or built directly on the cloud (cloud native)

- By 2021/21, IT-as-a-service (aka Cloud) will represent half of IT spend [Deloitte Global, 2017]



Source: Deloitte Global, 2017

- By 2020, a corporate “no-Cloud” policy will be as rare as a “no-internet” policy is today [Gartner, 2016]

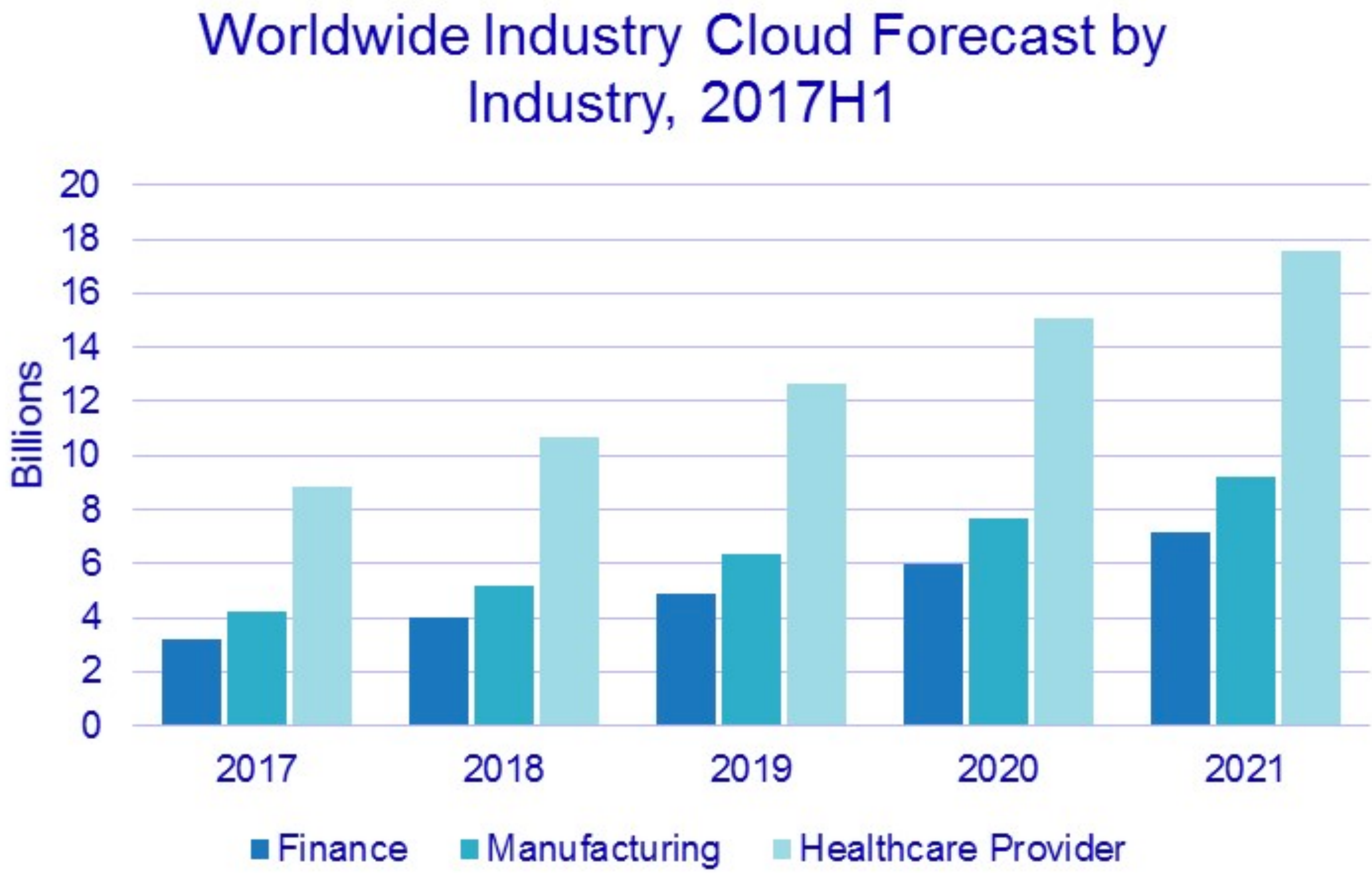
More and more Infrastructure, Apps, and Business Processes are being migrated to the cloud (cloud immigrant) or built directly on the cloud (cloud native)

Worldwide Public Cloud Services Forecast (Millions of Dollars)

	2016	2017	2018	2019	2020
Cloud Business Process Services (BPaaS)	40,812	43,772	47,556	51,652	56,176
Cloud Application Infrastructure Services (PaaS)	7,169	8,851	10,616	12,580	14,798
Cloud Application Services (SaaS)	38,567	46,331	55,143	64,870	75,734
Cloud Management and Security Services	7,150	8,768	10,427	12,159	14,004
Cloud System Infrastructure Services (IaaS)	25,290	34,603	45,559	57,897	71,552
Cloud Advertising	90,257	104,516	118,520	133,566	151,091
Total Market	**209,244**	**246,841**	**287,820**	**332,723**	**383,355**

Source: Gartner (February 2017)

Industry Clouds are the New Frontier in Cloud Adoption



Source: IDC 2017

Cloud has held and delivered on many promises for Business Resiliency

Self-service consumable	Self-service consumption by all stakeholders in an IT solution: architects, developers, deployers, customer users, administrators, cloud providers
Range of SLAs	Provides range of recovery performances for different criticalities of business functions
Efficient and cost-effective	• Efficient to implement and efficient use of resources • Pay for resiliency proportional to resiliency requirements • Pay for resiliency only upon activation of recovery and other resiliency functions • Automation at all phases of the life cycle
Scalable	• *Horizontal:* Scalable within a single cloud or across multiple clouds, where the cloud(s) may be public, private, or hybrid • *Vertical:* Provides resiliency across the logical stack, spanning infrastructure, platform, software, containers
Agile	• Automation and Orchestration • Quickly respond to changes in customer workload; quickly adjust resiliency solution
Flexible	Provides resiliency across application types, from cloud-native to traditional
New Resiliency Features	• Zero downtime deployments • Cloud Bursting • Auto-scaling across availability zones

Combination of Cloud-Native and DevOps has fundamentally transformed how Resiliency is Built and Managed for Enterprises

- DevOps core tenet: smaller changes rolled out faster
  – Easier to test changes completely
  – Easier to pinpoint issues
  – Easier to fix issues
  – Easier to roll back with less impact
- DevOps Version Control Tools
  – Enable easier rollback in case of issues

Lowers
Mean Time to Repair (MTTR)
[“2017 State of DevOps Report” by Puppet Labs + DORA]

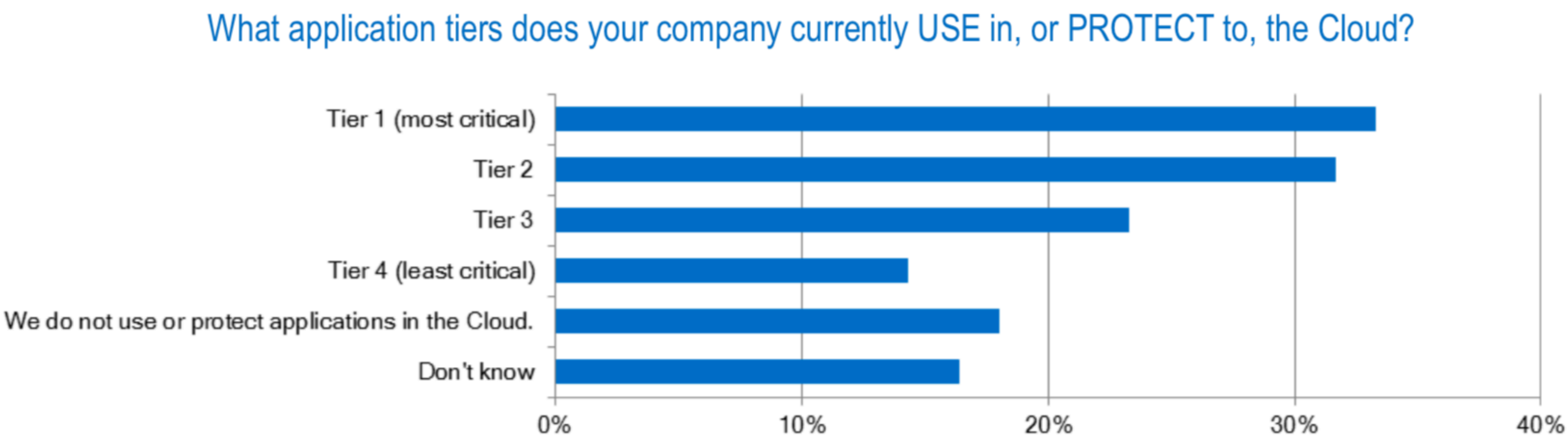
Reduces Expected Downtime

- Continuous Testing facilitates more testing, which means less surprises (issues) in production
- Standardized Configuration Management and portable development environments means more reproducibility, less variance, less entropy

Increases
Mean Time to Failure (MTTF)

DevOps practices enable BOTH agility and robustness.
Therefore, they are a positive influence on Resiliency.

Businesses are Entrusting Vital Assets to the Cloud



[Source: 2017 State of Resiliency Report, Vision Solutions Insights]

Substantial numbers of businesses place a high level of trust in Cloud systems

Of companies that use Cloud

- 33% are entrusting their most mission-critical (Tier 1) applications to Cloud
- 32% use or protect Tier 2 (essential) applications in the Cloud

Businesses are using the Cloud to make those vital assets resilient

- Cloud-based Disaster Recovery as-a-Service (DRaaS) revenue was $1.3B in 2015, and is expected to grow 20+% annually over the next three years [Gartner 2016]

Resiliency on the Cloud: Challenges [Wang et al. 2015]

- More Aggressive SLAs
- Scale & Diversity
- Inter-dependencies
- Coordination of recovery at infrastructure, platform, and app levels
- Resiliency of Cloud Management Capabilities
- Regulatory Requirements (e.g., locality restrictions, end to end security logging)
- Highly-impactful single points of failure
- Reconciling multi-tenancy with enterprise-class isolation requirements

Cloud Outages are a Reality

IBM

- Facebook was down for approximately 2.5 hours on September 23, 2010
- Amazon EC2 was down for more than 24 hours starting April 21, 2011
- Verizon Cloud was down for about 40 hours starting January 10, 2015.
- IBM Softlayer had a total downtime of around 17 hours in all of 2015.
- Rackspace had a total downtime of around 12.5 hours in all of 2015.
- Google Compute Engine Cloud was down for about 1 hour on February 18, 2015.
- Apple iCloud and iTunes store were down for about 12 hours on March 11, 2015.
- Microsoft Azure Cloud was down for more than 2 hours on March 16, 2015, and was down again on March 17, 2015.
- Apple iCloud was down for 7 hours on May 20, 2015.
- Amazon EC2 was down for almost 4 hours on August 10, 2015.
- Google Compute Engine Cloud was down multiple times during August 13, 2015 ~ August 17, 2015.
- Google Compute Engine Cloud was down for 70 minutes on November 23, 2015.
- Microsoft Azure Cloud was down for several hours on December 6, 2015.
- Some Salesforce customers in Europe experienced a CRM disruption for up to 10 hours due to a storage problem on March 3, 2016.
- IBM's Bluemix cloud was down for several hours on Jan 26, 2017.
- AWS storage outage caused much of the Internet and enterprise platforms (Slack, Quora) to be unavailable for 4 hours on Feb 28, 2017.
- Storage availability issues plagued Microsoft's Azure public cloud for more than eight hours on March 16, 2017.
- Several Microsoft business and consumer cloud services, including Office 365 storage, Xbox live, email services, became inaccessible due to problems authenticating users on March 21, 2017.
- Apple's iCloud Backup Service was unavailable millions of users for 36 hours on June 28, 2017.

[Sources: CRN.com, CloudHarmony]

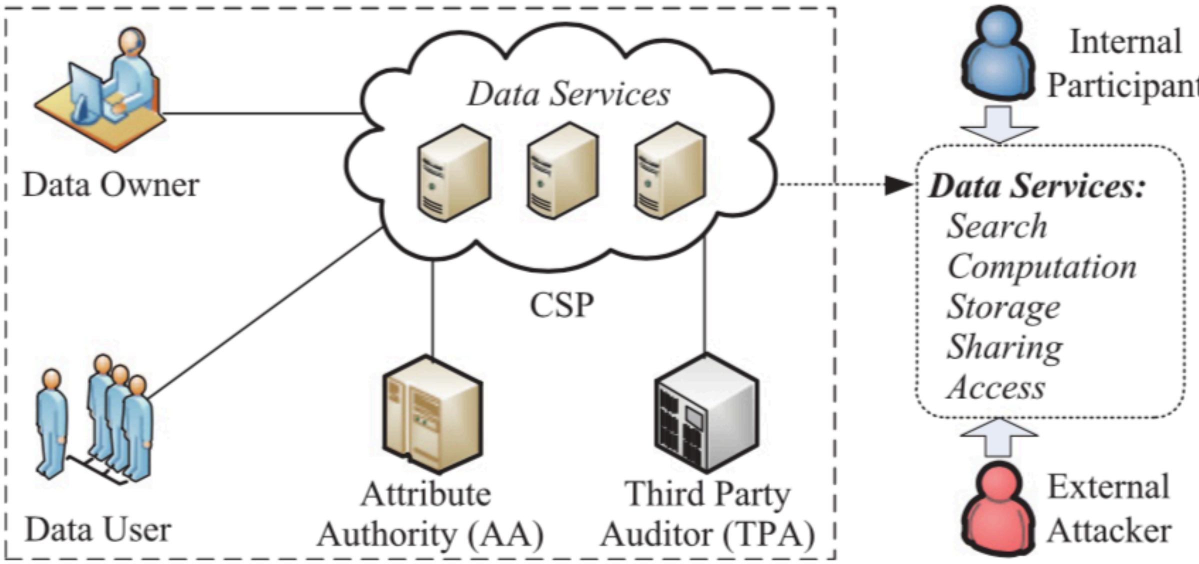
Recent Security and Privacy Breaches

- Cedars-Sinai Medical Center fires 6 for spying on patient medical records [July 2013].
- HIPAA breach - Oregon Health and Science University employees had been uploading PHI to a public cloud storage provider [Aug 2013].
- Laptop stolen, PII and PHI data of 700K California patients compromised [Oct 2013].
- Every single Yahoo customer account (> a billion) was impacted by 2013 Yahoo breach.
- Anthem / BCBS Insurance companies' 2015 data breach affected 80 million customers and resulted in a $115M settlement.
- Uber hacking incident compromised information of 57 million customers and drivers [Oct 2016]
  - Uber has agreed to 20 years of privacy audits due to failure-to-notify regulators about breach.
- Equifax, a top US credit agency, suffered a data breach affecting 143M customers [Sep 2017].
- Sensitive data on former U.S. military personnel exposed on Amazon S3 repository [Sep 2017].

Security and Privacy of Cloud Data Services

"You can have security without privacy, but you can't have privacy without security"
[Michael Chertoff, US Secretary of Homeland Security (2005-2009)]

System Model of Cloud Data Services
[Tung et al, 2016]



Security	Privacy
• Deals with how data is protected • More emphasis on technical controls • Protection of integrity and availability - plus confidentiality	• Deals with how data is collected, shared, and used • Focus on policies and procedures • Protection of confidentiality

Security and Privacy on the Cloud: Challenges

- Data Loss and User Privacy breaches magnified by scale
- Malicious Insiders (e.g., from the Cloud Service Provider or Third Party Auditor)
- Insecure cloud interfaces and APIs
- Account or Service Hijacking
- Attack propagation facilitated by multi-tenancy
- Security of Cloud Management Capabilities
- Regulatory Requirements (e.g., locality restrictions, end to end security logging)
- High-value targets for Denial of Service (Highly-impactful centralized control points)
- Reconciling multi-tenancy with enterprise-class isolation requirements

An Additional Challenge: Wrong Assumptions on Who Is Responsible for Protecting Data and Apps on the Cloud

- Of those who used Public Cloud:
  - 43% felt that the Public Cloud provider was responsible
  - 39% felt that the internal IT organization was responsible

    [Source: 2017 State of Resiliency Report, Vision Solutions Insights]
- Cloud service provider security concerns are valid, but needs to be balanced with cloud customer's security responsibilities
- By 2020, 95% of Cloud security failures will be the customer's fault [Gartner, 2016]
  - Cloud service providers will continue to improve security
    - Cloud security is an existential challenge for many cloud providers
    - Huge market incentives for cloud service providers to differentiate based on security
  - We need more focus on customer-side and end-user security

Security Threats, Requirements, and Solutions for Cloud Data Services [Tung et al, 2016]

Threats		Requirements		Solutions
Malicious attackers Curious CSP Vulnerable or greedy CSP Curious TPA	Data leakage or disclosure	Data confidentiality	Secure data search	Searchable Encryption (SE) [Wang et al. 2010]
			Secure data computation	Homomorphic Encryption (HE) [Gentry 2009b]
	Illegal access	Data access controllability	Secure data sharing	Selective Encryption [De Capitani di Vimercati et al. 2010]
				Attribute-Based Encryption (ABE) [Sahai and Waters 2005]
	Data corruption or loss	Data integrity	Secure data storage	Provable Data Possession (PDP) [Ateniese et al. 2007]
				Proof of Retrievability (POR) [Juels and Kaliski 2007]
	User privacy breach	Privacy preservability	Privacy preservation data access	Access Pattern Protection [Chor et al. 1998; Ding et al. 2011; Yang et al. 2011]
				Query Privacy Protection [Sun et al. 2013; Cao et al. 2014]
				Identity Privacy Protection [Wang et al. 2012a, 2012b; Nabeel et al. 2011]

Different schemes have been developed to address specific requirements.

Table Courtesy: [Tung et al, 2016]

Security and Privacy Solutions for Cloud Data Services [Tung et al., 2016]

Current Solutions	Description
Searchable Encryption	Search words in an encrypted database.
Homomorphic Encryption	Allows one to performs computation without decrypting data.
Selective Encryption	Different keys are used to encrypt different pieces of data. User authorization to access a piece of data essentially requires knowledge of the key used to encrypt that piece.
Attribute-based Encryption	Allows derivation of key to decrypt data only by users who hold certain attributes. e.g., ID = X (OR) department = Y.
Provable Data Possession (PDP)	Probabilistic checks for the data owner to verify that the outsourced data on the cloud is intact without actually downloading the data.
Proof of Retrievability (POR)	Challenge-response audit protocol first that can prove for a user whether a target file is intact. Using POR, a user can retrieve all file blocks from the server with high probability.
Access Pattern Privacy	Private Information Retrieval (PIR) protocols allow user to query database while hiding the identity of the data-items she is after. Different types of user access (e.g., read or write, to location A or location B) should be indistinguishable.
Identity Privacy	Anonymous access techniques are adopted to protect user identity in order to avoid identity leakage when data access control is enforced.
Query Privacy	Allows user to search words in an encrypted database with privacy (e.g., in a way that query keywords cannot be deduced)

Different schemes have been developed to address specific requirements.

Trade-offs between resiliency, security, privacy and efficiency (practicability) on the cloud [Tung et al., 2016]

- Data De-duplication vs. Proof-of-retrievability (POR)
  - POR schemes usually require user-specific encoding for the same data
    - N-copies of the data for N customers
- Flexible data sharing (demanded by users) vs. Conventional Security (provided by CSPs)
- Data Retention requirements vs. Right-to-forget
- Privacy-preserving Data Access vs. User Accountability
- Privacy-preserving search vs. Query Accuracy
- Efficiency and Scalability of PDP schemes
- Efficiency of POR schemes with Dynamic data

Different schemes have been developed to address a subset of properties.
Integrating these schemes to achieve all properties simultaneously is a hard problem.
But is becoming a NECESSARY problem to address.

Integrating resiliency, security, privacy and efficiency on the cloud has become necessary

Typical Cost per Hour of Downtime by Industry

Brokerage Service	Energy	Telecom	Manufacturing
$6.48 million	$2.8 million	$2.0 million	$1.6 million

Retail	Healthcare	Media
$1.1 million	$636,000	$90,000

[Sources: Networking Computing, The Meta Group, and Contingency Planning Research, 2017 State of Resiliency Report, Vision Solutions Insights]

- Outages, Data Unavailability, and Data Breaches are prohibitively expensive (even fatal) for company's that utilize cloud hosted resources/services
- Resiliency, Security, and Compliance have become Key Differentiators for Cloud Service Providers
  - Huge market incentives for cloud service providers to differentiate based on integration of these properties
- Cloud Customers demand it
- Legal and Compliance Frameworks demand it

Abridged Workshop Program

- Friday Jan 12 Morning
  - Session 1 – Privacy-Preserving Cloud Applications *(Chair: Bojan Cukic)*
  - Session 2 – Dependable Cloud Computing *(Chair: Mohamed Kaaniche)*
- Friday Jan 12 Evening
  - Session 3 -- Cloud Operational Resiliency: Industry Best Practices *(Chair: Karama Kanoun)*
- Saturday Jan 13 Morning
  - Session 4 – Privacy-preserving Cloud Data Access *(Chair: Rui Oliveira)*
  - Session 5 – Cloud Security and Privacy *(Chair: Antonio Casimiro)*
- Saturday Jan 13 Evening
  - Session 6 - Workshop Wrap up

References

- [Gartner 2016] Gartner, Inc., Werner Zurcher, “Next Generation Disaster Recovery, A Cloudy Forecast,” August 2016.
- [Tung et al. 2016] Jun Tang, Yong Cui, Qi Li, Kui Ren, Jiangchuan Liu, and Rajkumar Buyya. “Ensuring security and privacy preservation for cloud data services,” ACM Computing Surveys. 49, 1, Article 13, June 2016.
- [Wang et al. 2015] L. Wang, H.V. Ramasamy, R.E. Harper, M. Viswanathan, and E. Plattier, “Experiences with Building Disaster Recovery for Enterprise-Class Clouds”, 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-2015)