INTRODUCTION TO CLOUD SECURITY

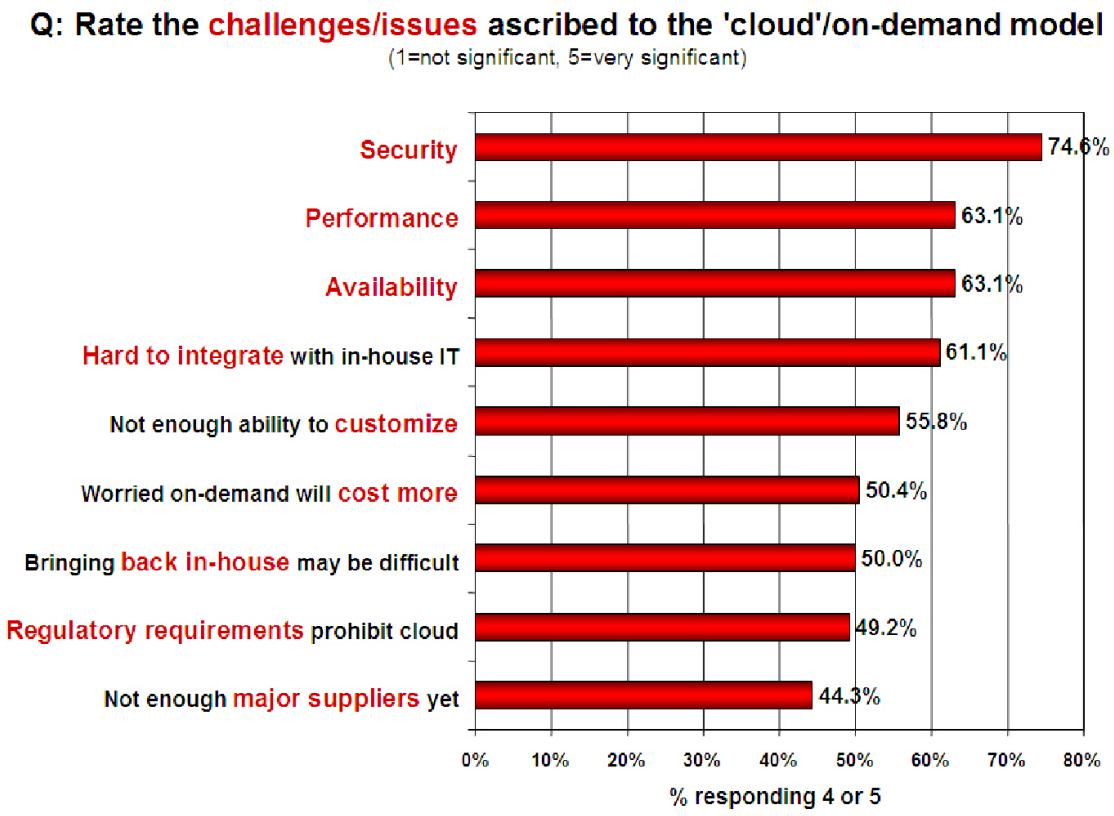
SAMITHA SOMATHILAKA

Department of Computing & Mathematics, WIT

IF CLOUD COMPUTING IS SO GREAT, WHY ISN'T EVERYONE DOING IT?

- The cloud acts as a big black box, nothing inside the cloud is visible to the clients
- Clients have no idea or control over what happens inside a cloud
- Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

COMPANIES ARE STILL AFRAID TO USE CLOUDS



TAXONOMY OF FEAR

- Confidentiality
  - Fear of loss of control over data
    - Will the sensitive data stored on a cloud remain confidential?
    - Will cloud compromises leak confidential client data
  - Will the cloud provider itself be honest and won’t peek into the data?
- Integrity
  - How do I know that the cloud provider is doing the computations correctly?
  - How do I ensure that the cloud provider really stored my data without tampering with it?

TAXONOMY OF FEAR (CONT.)

- Availability
  - Will critical systems go down at the client,
  - What if the provider is attacked in a Denial of Service attack?

TAXONOMY OF FEAR (CONT.)

- Privacy issues raised via massive data mining
  - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Increased attack surface
  - Entity outside the organization now stores and computes data, and so
  - Attackers can now target the communication link between cloud provider and client

TAXONOMY OF FEAR (CONT.)

- Auditability and forensics (out of control of data)
  - Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don’t maintain data locally
- Legal quagmire and transitive trust issues
  - Who is responsible for complying with regulations?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

CLOUD SECURITY CHALLENGES

- Increased Attack Surface
- Lack of Visibility and Tracking
- Ever-Changing Workloads
- DevOps, DevSecOps and Automation
- Granular Privilege and Key Management
- Complex Environments
- Cloud Compliance and Governance

INCREASED ATTACK SURFACE

- The public cloud environment has become a large and highly attractive attack surface for attackers who exploit poorly secured cloud ingress ports in order to access and disrupt workloads and data in the cloud.
- Malware, Zero-Day, Account Takeover and many other malicious threats have become a day-to-day reality.

LACK OF VISIBILITY AND TRACKING

- In the IaaS model, the cloud providers have full control over the infrastructure layer and do not expose it to their customers.
- The lack of visibility and control is further extended in the PaaS and SaaS cloud models. Cloud customers often cannot effectively identify and quantify their cloud assets or visualize their cloud environments.

EVER-CHANGING WORKLOADS

- Cloud assets are provisioned and decommissioned dynamically—at scale and at velocity.
- Traditional security tools are simply incapable of enforcing protection policies in such a flexible and dynamic environment with its ever-changing and ephemeral workloads.

GRANULAR PRIVILEGE AND KEY MANAGEMENT

- Often cloud user roles are configured very loosely, granting extensive privileges beyond what is intended or required.
- One common example is giving database delete or write permissions to untrained users or users who have no business need to delete or add database assets.
- At the application level, improperly configured keys and privileges expose sessions to security risks.

COMPLEX ENVIRONMENTS

- Managing security in a consistent way in the cloud environments requires methods and tools that work seamlessly across public cloud providers, private cloud providers, and on-premise deployments
  - Including branch office edge protection for geographically distributed organizations.

CLOUD COMPLIANCE AND GOVERNANCE

- All the leading cloud providers have aligned themselves with most of the well-known accreditation programs such as PCI 3.2, NIST 800-53, HIPAA and GDPR.
- However, customers are responsible for ensuring that their workload and data processes are compliant.
- Given the poor visibility as well as the dynamics of the cloud environment, the compliance audit process becomes close to mission impossible unless tools are used to achieve continuous compliance checks and issue real-time alerts about misconfigurations.