Waterford Institute of Technology

南京信息工程大学
1960
NANJING UNIVERSITY OF INFORMATION SCIENCE & TECHNOLOGY

INTRODUCTION TO CLOUD SECURITY

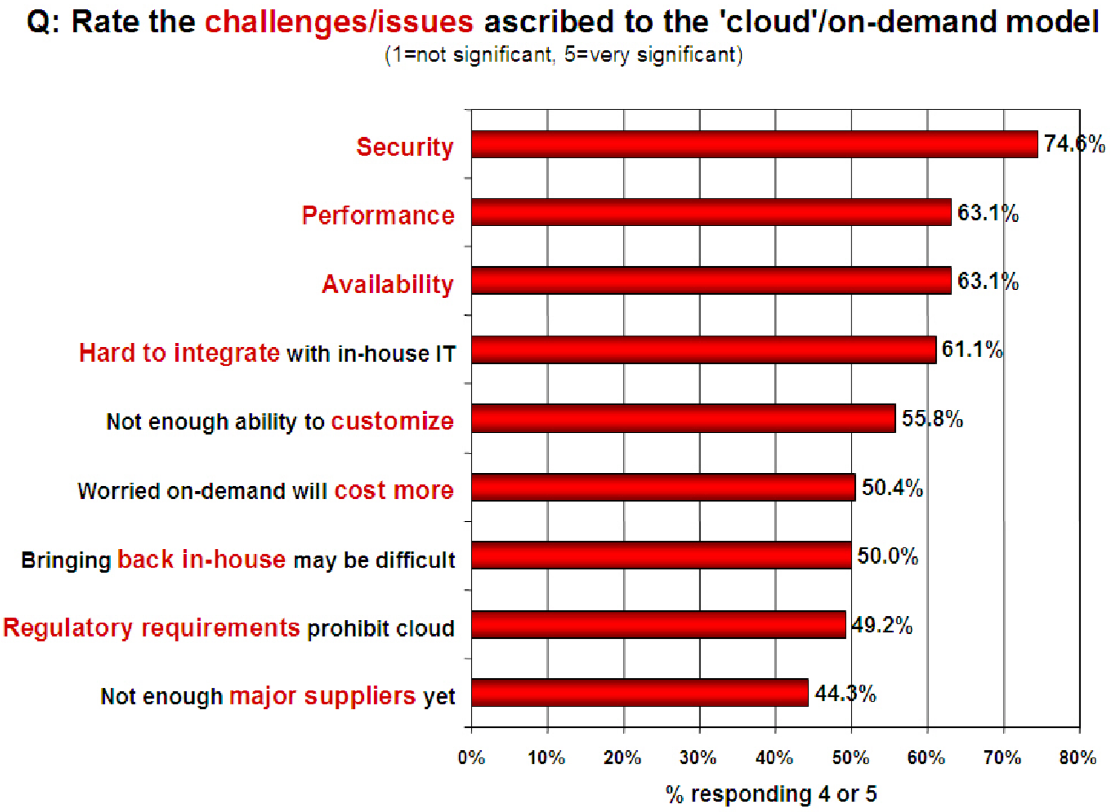
SAMITHA SOMATHILAKA

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



WHY IS CLOUD SECURITY IMPORTANT?

- For businesses making the transition to the cloud, robust cloud security is imperative.
- Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment.
- For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.

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

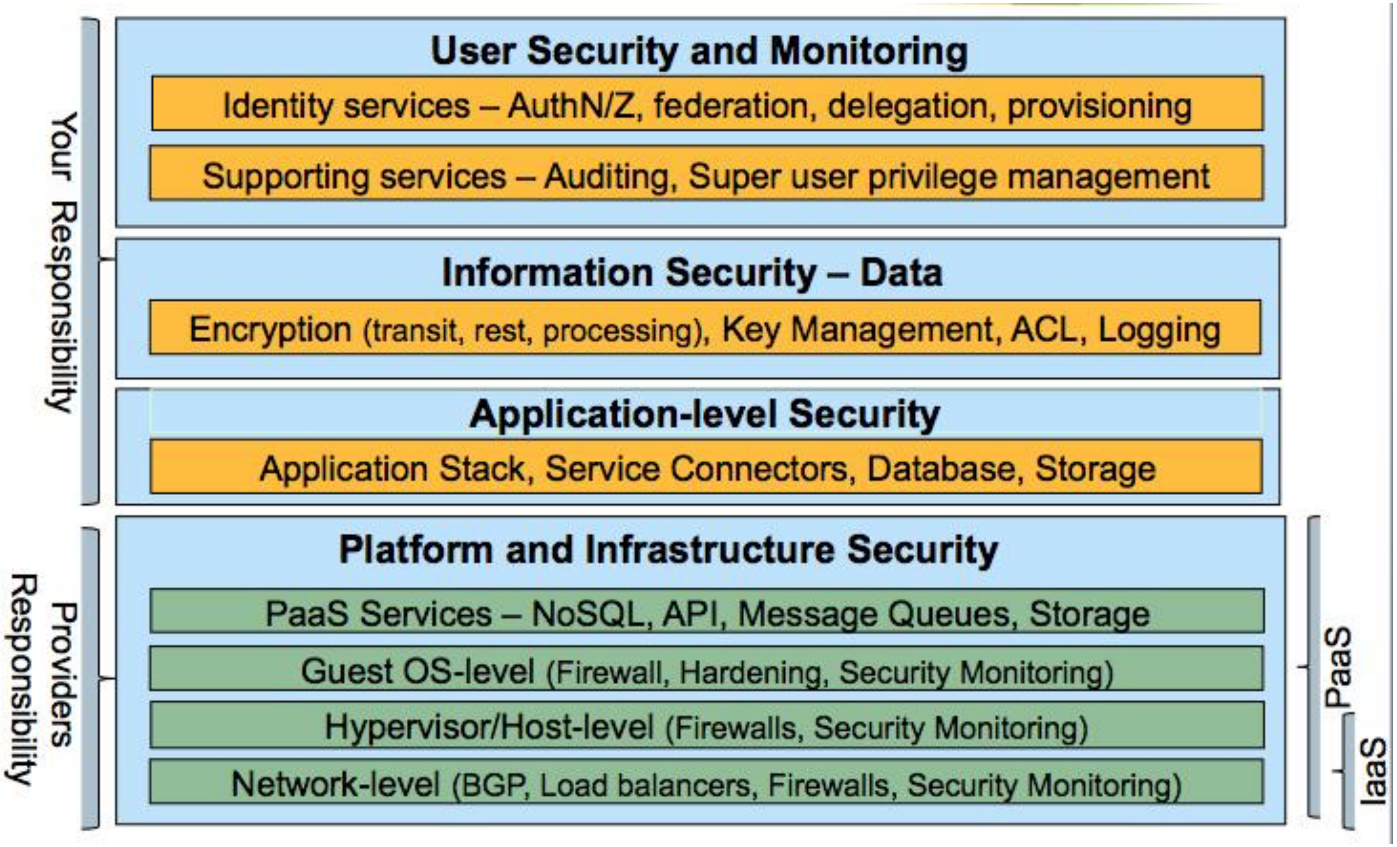
TAXONOMY OF FEAR (CONT.)

- 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?

SEGREGATION OF RESPONSIBILITY

- By definition, cloud security responsibilities in a public cloud are shared between the cloud customer (your enterprise) and the cloud service provider whereas in a private cloud, the customer is managing all aspects of the cloud platform.
- Cloud service providers are responsible for securing the shared infrastructure including routers, switches, load balancers, firewalls, hypervisors, storage networks, management consoles, DNS, directory services and cloud API.

SEGREGATION OF RESPONSIBILITY



Your Responsibility

User Security and Monitoring

Identity services – AuthN/Z, federation, delegation, provisioning

Supporting services – Auditing, Super user privilege management

Information Security – Data

Encryption (transit, rest, processing), Key Management, ACL, Logging

Application-level Security

Application Stack, Service Connectors, Database, Storage

Providers Responsibility

Platform and Infrastructure Security

PaaS Services – NoSQL, API, Message Queues, Storage

Guest OS-level (Firewall, Hardening, Security Monitoring)

Hypervisor/Host-level (Firewalls, Security Monitoring)

Network-level (BGP, Load balancers, Firewalls, Security Monitoring)

PaaS

IaaS

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 hackers 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.

DEVOPS, DEVSECOPS AND AUTOMATION

- Organizations that have embraced the highly automated DevOps CI/CD culture must ensure that appropriate security controls are identified and embedded in code and templates early in the development cycle.
- Security-related changes implemented *after* a workload has been deployed in production can undermine the organization's security posture as well as lengthen time to market.

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 hybrid and multicloud environments favoured by enterprises these days 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.

ADVANTAGES OF CLOUD SECURITY

THE CLOUD PERIMETER

- **Computing environments** — Cloud providers also offer private cloud environments, where you can rent computing power and space for private use. If you’re well versed in cloud computing, you can combine public and private clouds into a customized hybrid architecture. If you want to integrate a number of third-party cloud vendors into your overall cloud computing ecosystem, you can try the multi-cloud model
- **Infrastructure**—virtualized computing workloads such as virtual machines and servers
- **Platforms**—application development resources such as operating systems
- **Software**—cloud-based software such as Google Docs and Google Calendar
- **Databases**—database resources such as storage, recovery, and backup

CENTRALIZED SECURITY

- Just as cloud computing centralizes applications and data, cloud security centralizes protection.
- Cloud-based business networks consist of numerous devices and endpoints that can be difficult to manage when dealing with ideas such as **BYOD**.
- Managing these entities centrally enhances traffic analysis and **web filtering**, streamlines the monitoring of network events and results in fewer software and policy updates. Disaster recovery plans can also be implemented and actioned easily when they are managed in one place.

REDUCED COSTS

- One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware.
- Not only does this reduce capital expenditure, but it also reduces administrative overheads.
- Where once IT teams were firefighting security issues reactively, cloud security delivers proactive security features that offer protection 24/7 with little or no human intervention.

REDUCED ADMINISTRATION

- When you choose a reputable cloud services provider or cloud security platform, you can kiss goodbye to manual security configurations and almost constant security updates.
- These tasks can have a massive drain on resources, but when you move them to the cloud, all security administration happens in one place and is fully managed on your behalf.

RELIABILITY

- Cloud computing services offer the ultimate in dependability.
- With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.