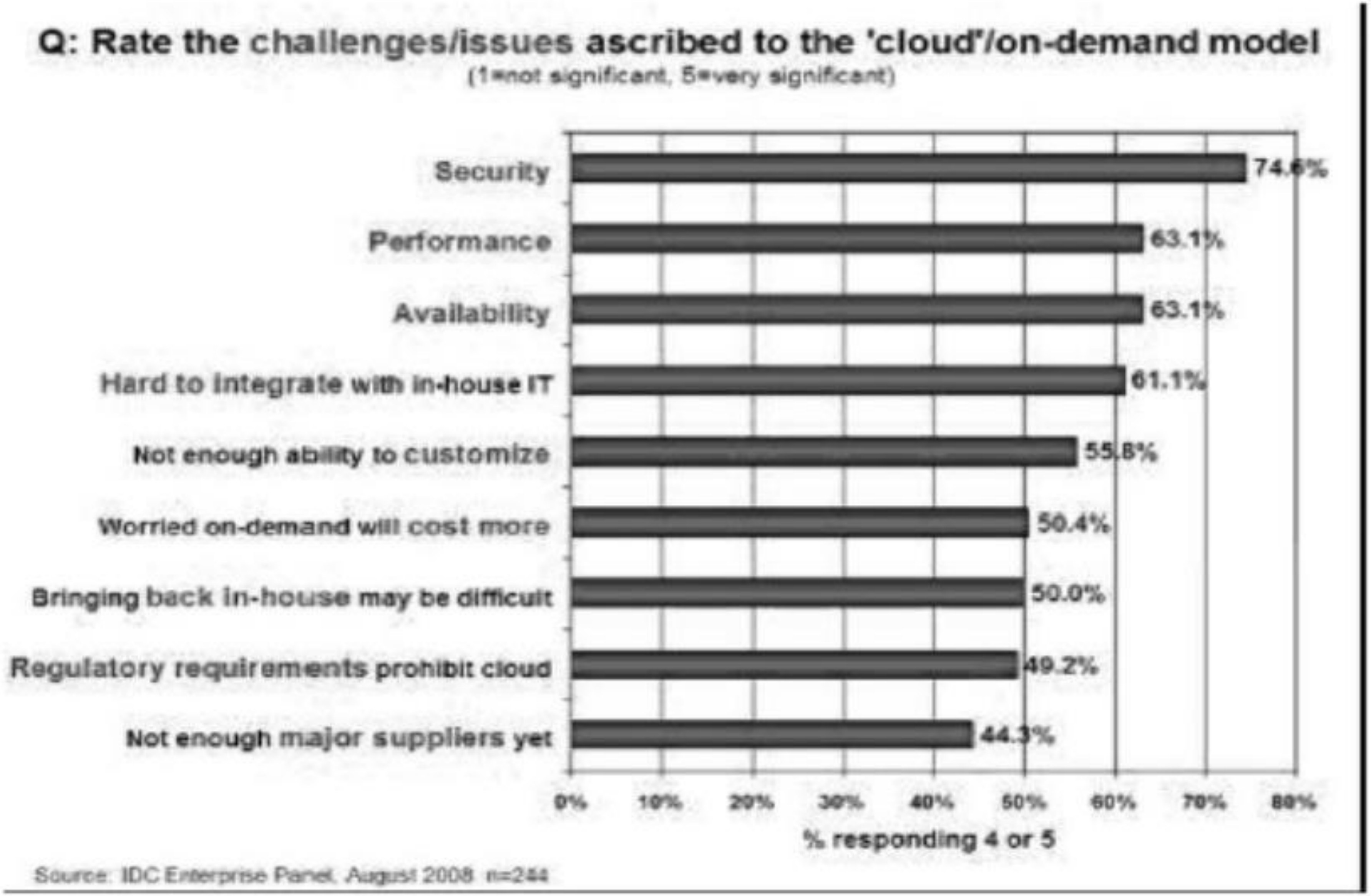
# Security in Cloud

Unit-iv



Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)

Source: IDC Enterprise Panel, August 2008 n=244

Figure 6.1 Results of IDC survey ranking security challenges

# Cloud security challenges

- In a shared pool outside the enterprise, you don’t have any knowledge or control of where the resources run.
- Storage services provided  by one cloud vendor may be incompatible with another vendor’s services if the customer decides to move on.
- While data in internet passes, who will control the encryption/decryption keys?  Most customers want their data encrypted both ways across the Internet using SSl(Secure Sockets Layer protocol).
- Data integrity- ensuring that data is identically maintained during any operation. It is assurance that the data is consistent and correct. It ensures that data really changes only in response to authorized transactions.
- cloud application undergo constant feature additions, and users must keep up to date with application improvements to be sure they are protected. The speed at which applications will change in the cloud will affect both the SDLC and security. The software companies has to keep with that even if they have a policy of changing only for 3 to 5 years. The user must constantly upgrade, because an older version may not function or protect the data.

- Many Compliance regulations require that data not be intermixed with other data, such as on shared servers or databases.
- Some countries have strict limits on what data about its citizen can be stored and for how long and some banking regulators require that customers financial data remain in their home country.
- It is the responsibility of data owner and not the provider to maintain their data upto the respective govt. rules.
- Security managers will need to pay particular attention to systems that contain critical data such as corporate financial information or source code during the transition to server virtualization in production environments.
- During outsourcing the security managers will need to work with their company’s legal staff to ensure that appropriate contract terms are in place to protect corporate data and provide for acceptable service-level agreements.

# Software-as-a-sevrice security

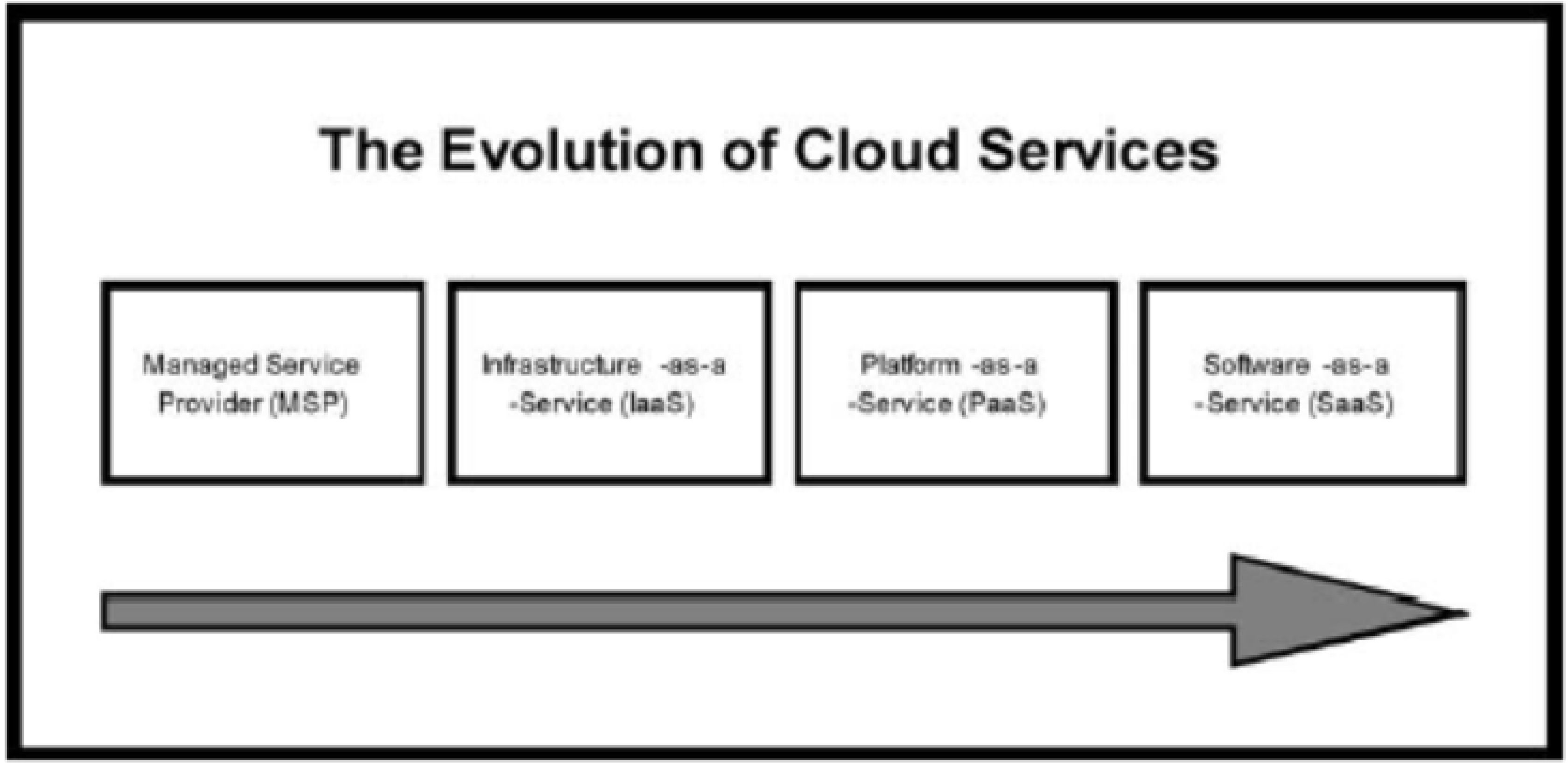

The Evolution of Cloud Services
Managed Service Provider (MSP)
Infrastructure -as-a -Service (IaaS)
Platform -as-a -Service (PaaS)
Software -as-a -Service (SaaS)

Figure 6.2 The evolution of cloud services.

- SaaS will remain the dominant model among others.
- Corporations or end users will need to research vendor’s policies on data security before using vendor services to avoid losing or not being able to access their data.
- Security issues

1. Privileged user access- inquire about who has specialized access to data, and about the hiring and management of such administrators.

2. Regulatory compliance- make sure that the vendor is willing to undergo external audits and/or security certifications.

3. Data location- does the provider allow for any control over the location of data.

4. Data segregation- Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

5. Recovery- find out what will happen to data in case of a disaster.

6. Investigative support- does the vendor have the ability to investigate any inappropriate or illegal activity?

7.Long-term viability- what will happen to data if the company goes out of business? How will data be returned, and in what format?

# Security Management (People)

- One of the most important actions for a security team is to develop a formal Charter –(a document, issued by a sovereign or state, outlining the conditions under which a corporation, colony, city, or other corporate body is organized, and defining its rights and privileges. )
- The roles and responsibilities must be clearly defined for the security team else it will result in confusion and does not help in meeting the goals.
- Morale among the team and pride in the team is lowered, and security suffers as a result.

# Security Governance

- A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies.
- A charter will be the first one to be delivered.
- Lack of security governance will lead to
  - Need of business not being met
  - Risk management
  - Security monitoring
  - Application security
  - Sales support
  - All the above places there will be server drawbacks

# Risk management

- Effective risk management entails:
  - Identification of technology assets
  - Identification of data and its links to business processes and data stores
  - Assignment of ownership and custodial responsibilities
- Maintain a repository of information assets.

# Risk assessment

- Security risk assessment is critical to helping the information security organization make informed decisions when balancing the dueling priorities of business utility and protection of assets.
- Lack of attention to completing formalized risk assessments can contribute to an increase in information security audit findings, can jeopardize certification goals and can lead to inefficient and ineffective selection of security controls that may not adequately mitigate information security risks to an acceptable level.
- A formal risk management must be carried over periodically or as-need basis
- Threat modeling to be done which makes the developer to work closely with internal security team and develop the programs in more secured level

# Security portfolio management

- Security portfolio management is the fundamental component.
- Lack of portfolio and project management can lead to projects never being completed or never realizing their expected return; unsustainable and unrealistic workloads and expectations because projects are not prioritized according to strategy, goals and resource capacity;
- Degradation of the system or processes due to lack of supporting maintenance and sustaining organization planning
- For every  new projects  and team, the team should have a project plan and manager with appropriate training and experience(both traditional and cloud environment practices)

# Security awareness

- People should be provided with knowledge and culture regarding the security or else they may be the point of threats entry.
- Social engineering attacks, lower reporting of and slower responses to potential security incidents and inadvertent customer data leaks are some of the place where security awareness is needed.
- Based on the user training program can be given.
- For eg for developers security awareness can be provided in the form of secure code and testing training , while customer service representatives can be provided data privacy and security certification awareness training.

# Education and training

- Programs should be developed that provide a baseline for providing fundamental security and risk management skills and knowledge to the security team and their internal partners.
- This entails a formal process to assess and align skill sets to the needs of the security team and to provide adequate training and mentorship—providing a broad base of fundamental security, inclusive of data privacy, and risk management knowledge.
- As the cloud computing business model and its associated services change, the security challenges facing an organization will also change

# Policies, standards and guidelines

- Policies should be developed, documented and implemented along with documentation for supporting standards and guidelines.
- They should be reviewed then and there at regular intervals

**Secure Software Development Life Cycle(SDLC)** – consists of six phases

**Phase 1 : Investigation** -Define project processes and goals, and document them in the program security policy

**Phase 2: Analysis-** Analyze existing security policies and programs, analyze current threats and controls, examine legal issues, and per

form risk analysis

**Phase 3.Logical design:** Develop a security blueprint, plan incident response actions, plan business responses to disaster, and determine the feasibility of continuing and/or outsourcing the project.

**Phase 4.Physical design:** Select technologies to support the security blueprint, develop a definition of a successful solution, design physical security measures to support technological solutions, and review and approve plans.

**Phase 5.Implementation:** Buy or develop security solutions. At the end of this phase, present a tested package to management for approval.

**Phase 6.Maintenance:** Constantly monitor, test, modify, update, and repair to respond to changing threats.

-

# Security Architecture Design

- A security architecture framework should be established with consideration of processes (enterprise authentication and authorization, access contr ol, confidentiality, integrity, nonrepudiation, security management, etc.), operational procedures, technology specifications, people and organizational management, and security program compliance and reporting.
- Documentation is required for privacy controls, management controls and metrics specific to asset classification and control, physical security, system access controls, network and computer management ,application development and maintenance, business continuity and compliance.
- Technology should be concentrated more on the following layers

1. Authentication
2. Authorization
3. Availability
4. Confidentiality
5. Integrity
6. Accountability
7. Privacy

# Data security

- The ultimate challenge in cloud computing is data-level security, and sensitive data is the domain of the enterprise, not the cloud computing provider.
- Security will need to move to the data level so that enterprises can be sure their data is protected wherever it goes.
- For example, with data-level security, the enterprise can specify that this data is not allowed to go out- side of the United States. It can also force encryption of certain types of data, and permit only specified users to access the data. It can provide compliance with the Payment Card Industry Data Security Standard (PCI DSS).
- True unified end-to-end security in the cloud will likely requires an ecosystem of partners.

# Application security

- It is one of the critical success factors for SaaS applications
- The security team should provide the security requirement for the product development engineers to implement along with their applications.
- External penetration tests should be done periodically and assurance should be given to the customers regarding this.
- Since most connections between Saas companies and their providers are through web, providers should secure web applications by following Open Web Application Security Project (OWASP)15 guidelines for secure application development (mirroring Requirement 6.5 of the PCI DSS, which mandates compliance with OWASP coding practices)
- Locking down ports and unnecessary commands in Linux, Apache, MySQL, PHP should be done.

# Virtual Machine Security

- The providers must advise their customers on how to prepare their virtual machine for migration when needed.
- Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection can all be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premises to public cloud environments.
- By doing so critical applications and data can be moved to the cloud securely.
- To facilitate the centralized management of a server firewall policy, the security software loaded onto a virtual machine should include a bi-directional stateful firewall that enables virtual machine isolation and location awareness.
- Integrity monitoring and log inspection software must be installed.
- This connection of VMs to their mother ship, makes it more secure because of centralized monitoring.

# Identity Access Management(IAM)

- Least privilege state should be granted to customers.
- The principle of least privilege states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary.
- Trust assumptions, privacy implications, operational aspects of authentication and authorizations will be challenged.
- The providers must provide end-to-end trust and identity throughout the cloud and the enterprise.
- Find the right balance between usability and security, if not both business and IT groups may be affected by barriers to completing their support and maintenance activities efficiently.