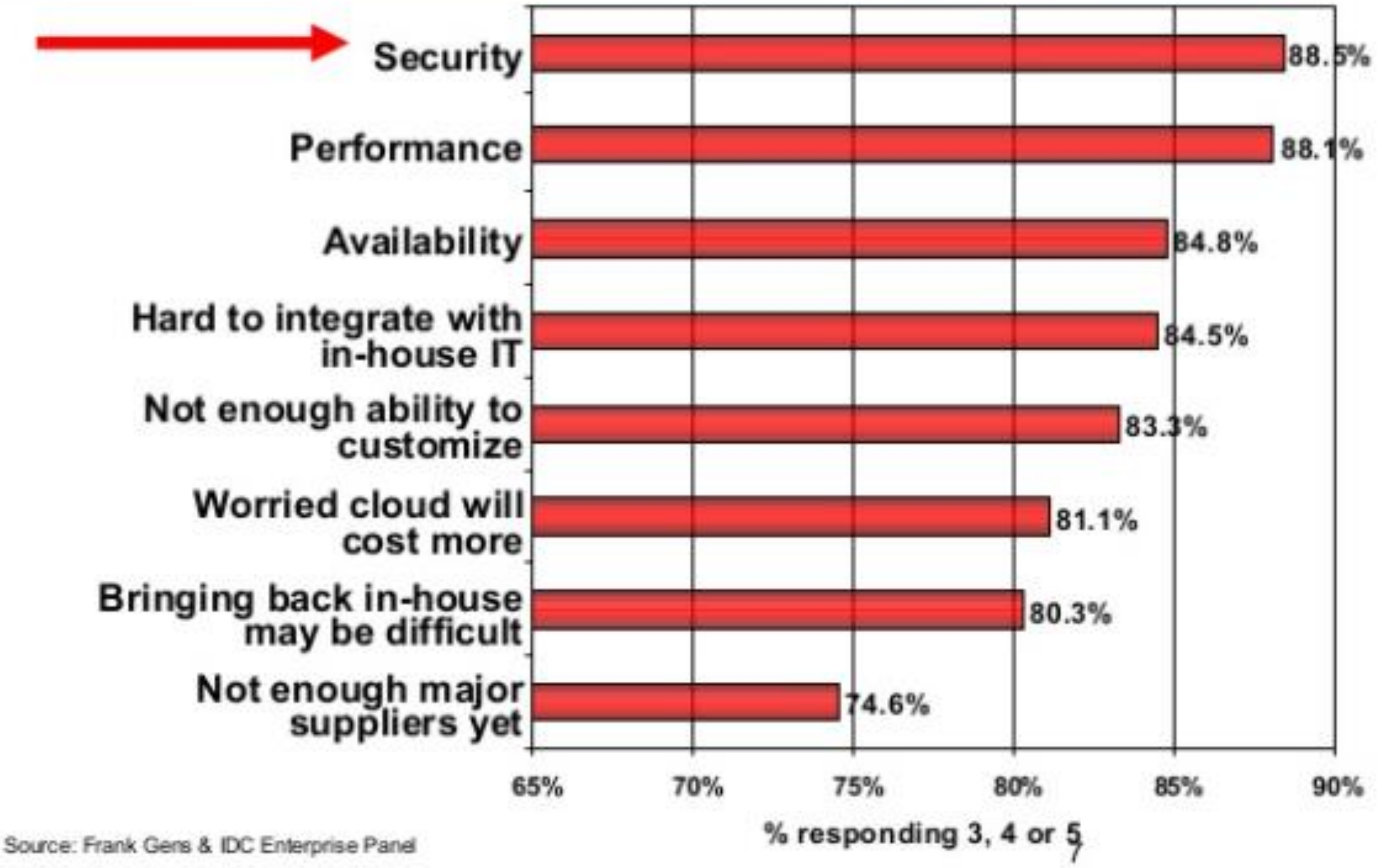
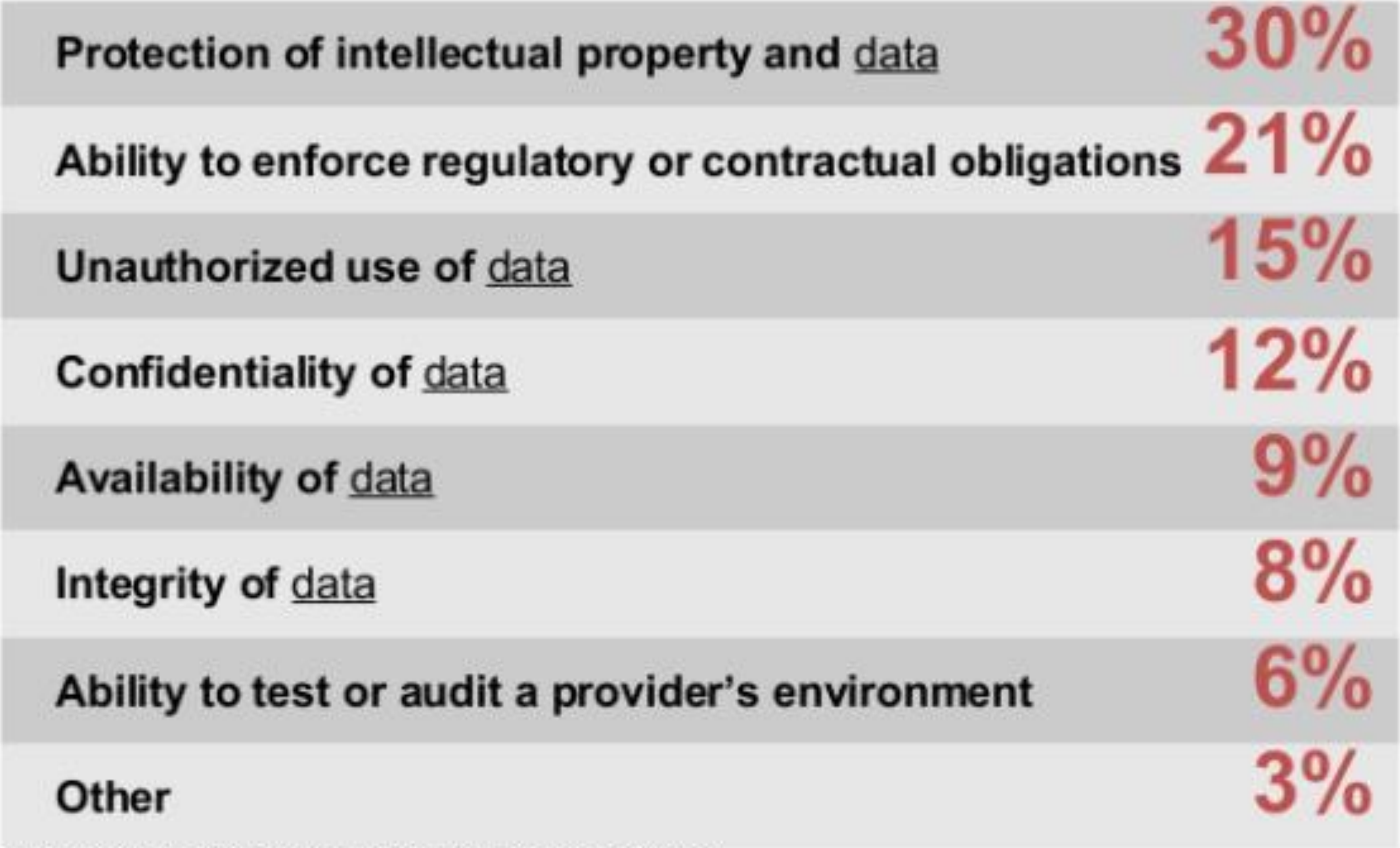
Cloud Security

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



Source: Frank Gens & IDC Enterprise Panel

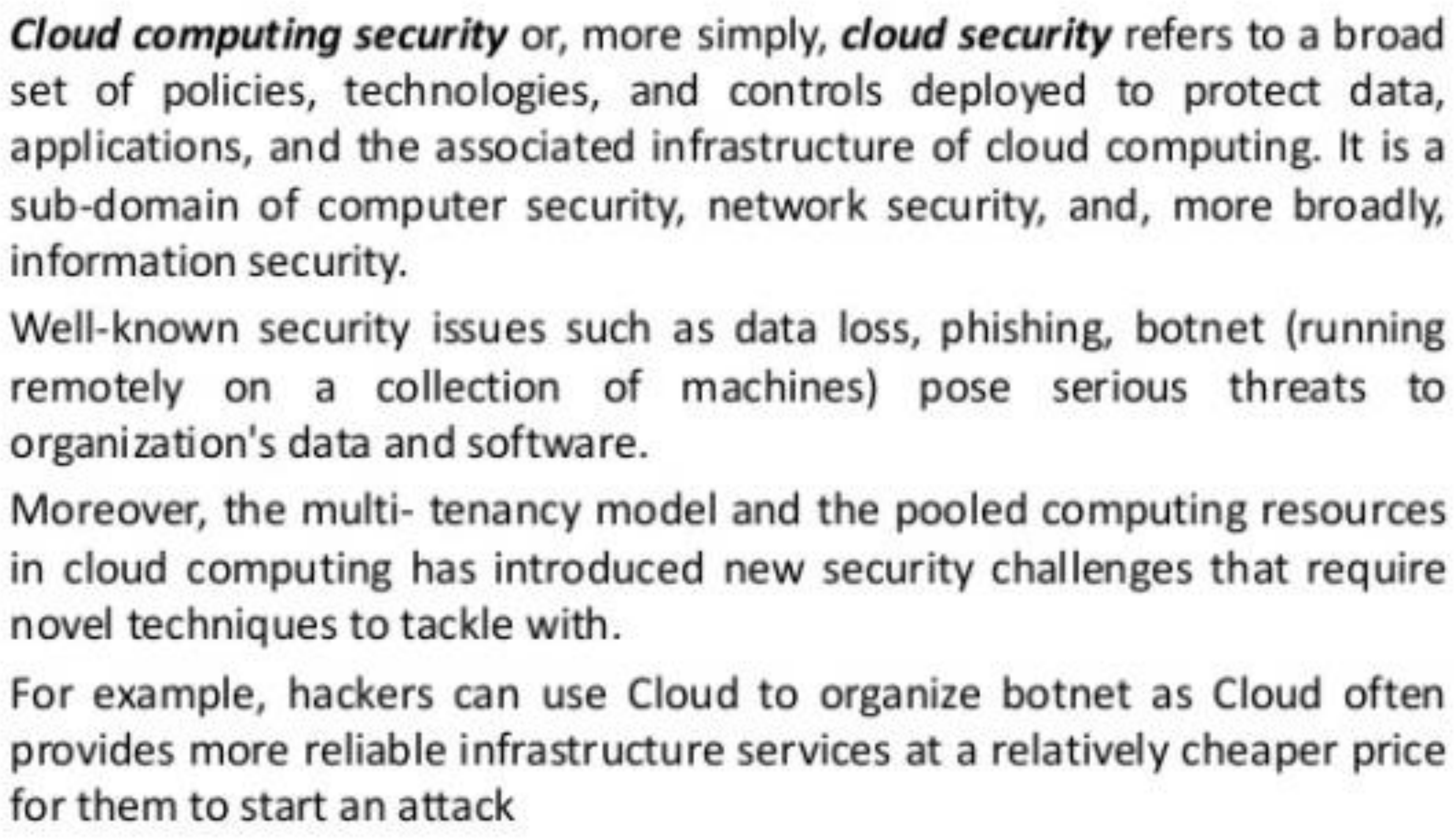
Specific Customer Concerns Related to Security



Protection of intellectual property and data	30%
Ability to enforce regulatory or contractual obligations	21%
Unauthorized use of data	15%
Confidentiality of data	12%
Availability of data	9%
Integrity of data	8%
Ability to test or audit a provider's environment	6%
Other	3%

Source: Deloitte Enterprise@Risk: Privacy and Data Protection Survey, 2007

Privacy and Security in Cloud



- ***Cloud computing security*** or, more simply, ***cloud security*** refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and, more broadly, information security.
- Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software.
- Moreover, the multi- tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with.
- For example, hackers can use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack

Threats, Vulnerability & Risk

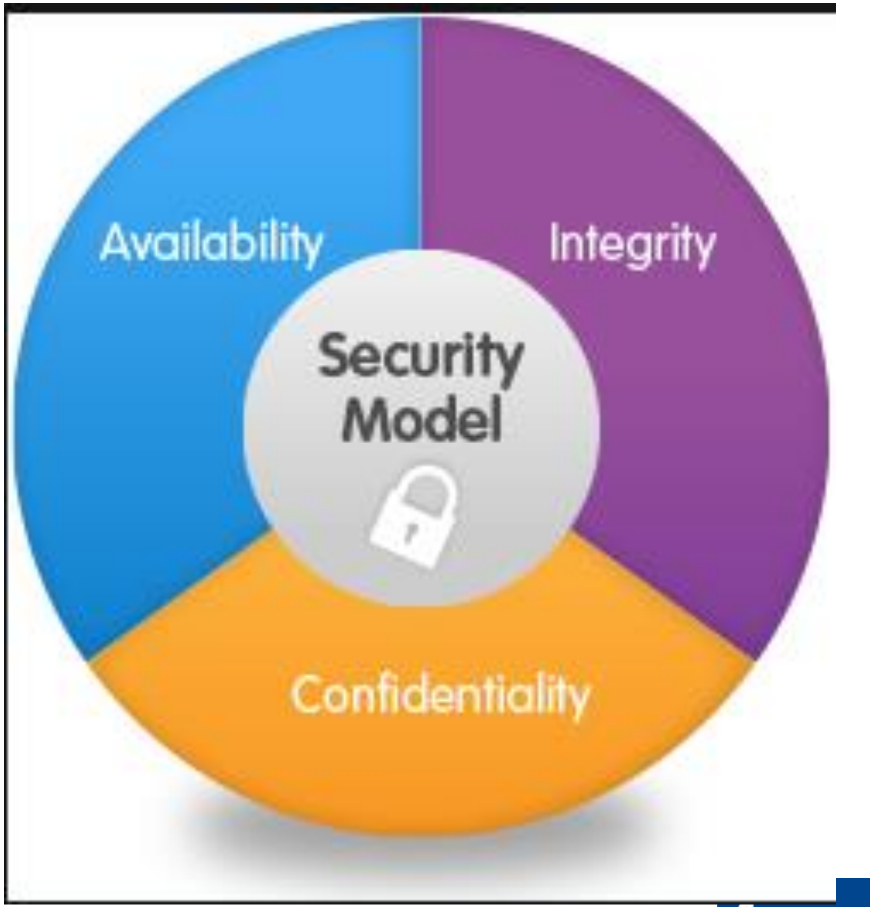
- Threat: event that cause harm to the system
  - Malicious
  - Accidental: unintentional deletion
- Vulnerability: weakness/ flows in a system
  - Increases the chance of attack
- Risk: ability of a threat to exploit Vulnerability and cause harm to the system
  - Threat and Vulnerability overlap

Security and Privacy Issues in Cloud Computing

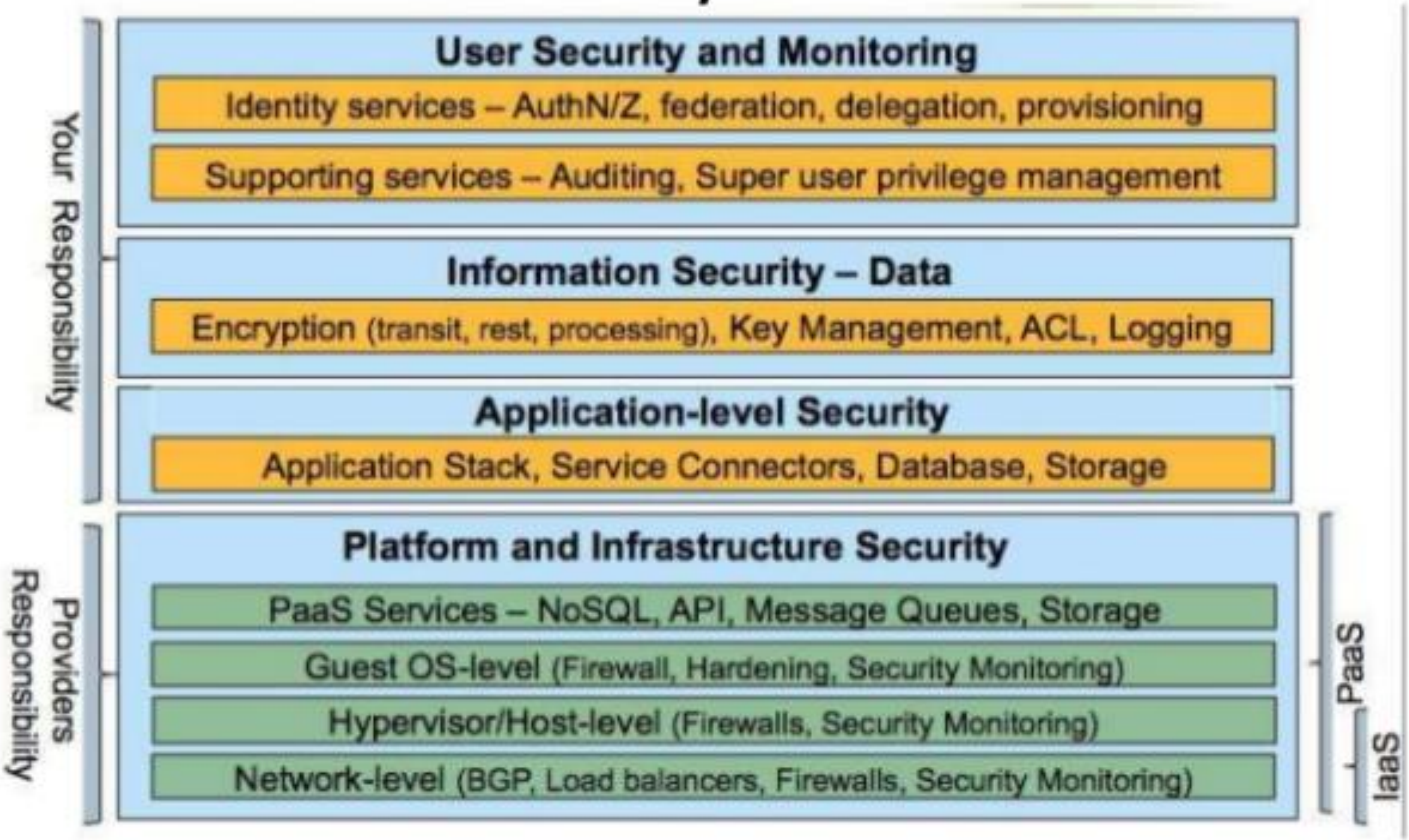
- Infrastructure Security
  - Network Level
  - Host Level
- Application Level
- Data and Storage Security
- Identity and Access Management (IAM)

CIA Triad

CIA - Confidentiality, Integrity and Availability. The **CIA Triad** is actually a security model that has been developed to help people think about various parts of IT security



Cloud Security Architecture



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

Platform and Infrastructure Security

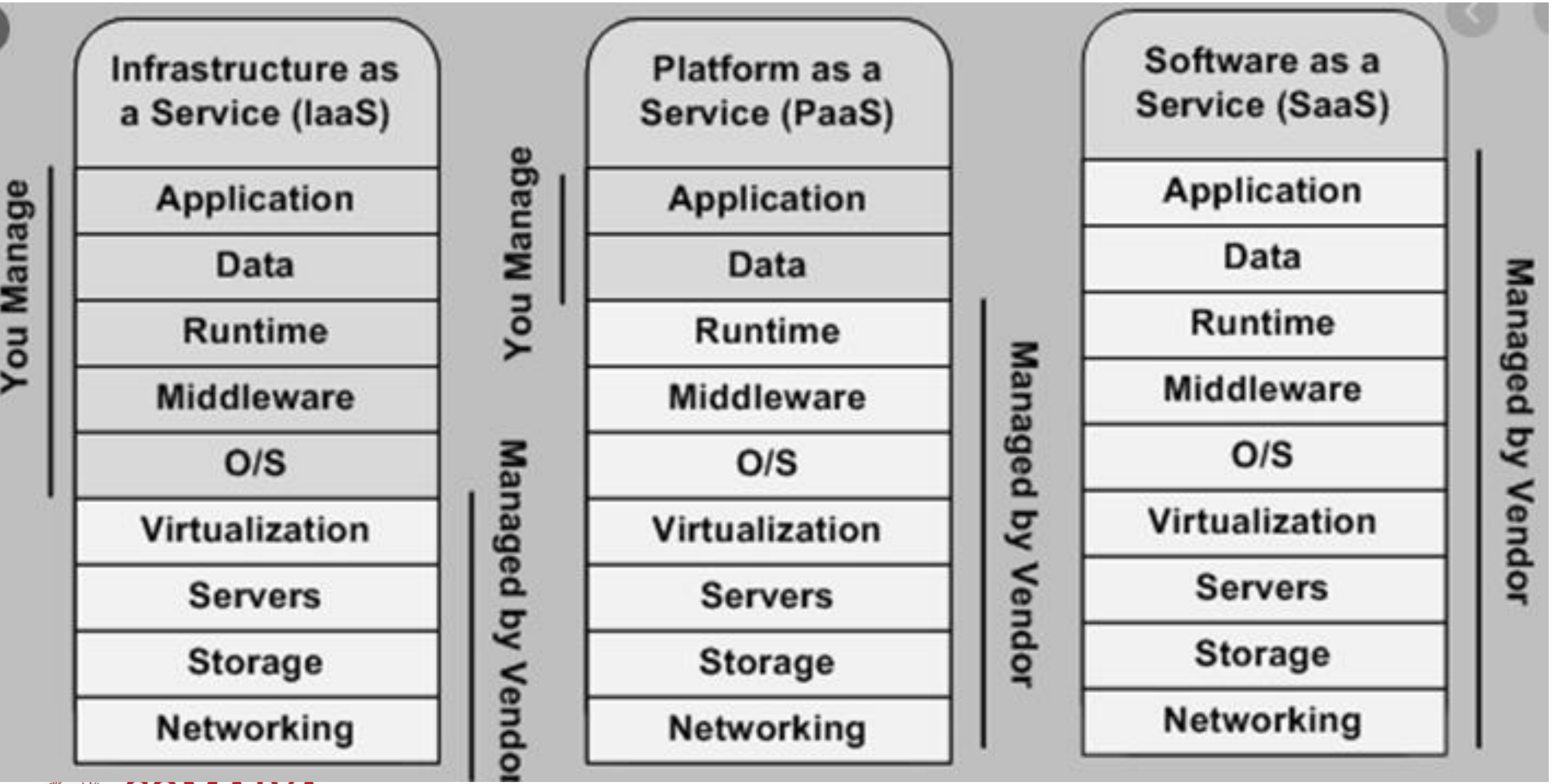
PaaS Services – NoSQL, API, Message Queues, Storage

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

Hypervisor/Host-level (Firewalls, Security Monitoring)

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

Responsibilities



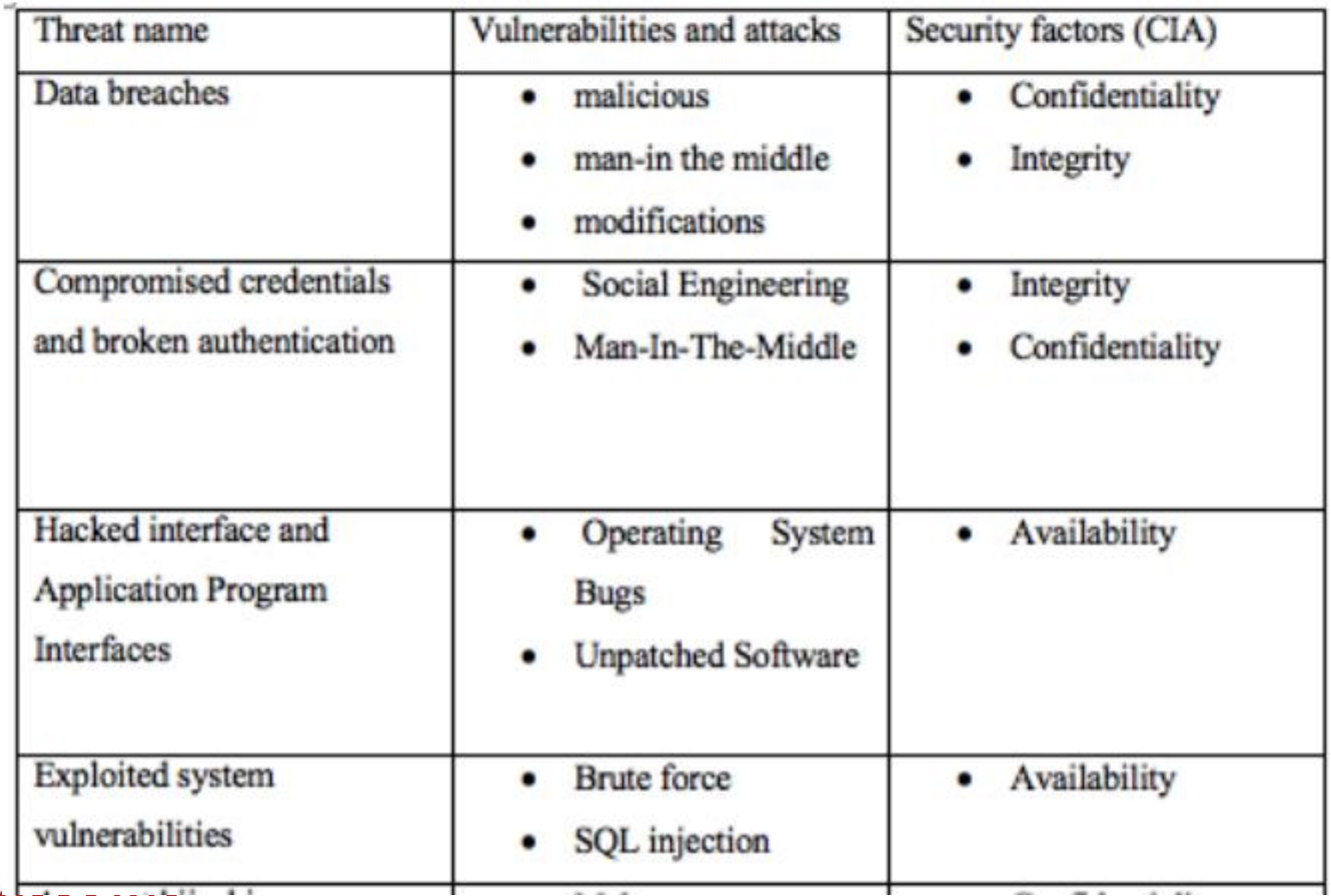
Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Application	Application	Application
Data	Data	Data
Runtime	Runtime	Runtime
Middleware	Middleware	Middleware
O/S	O/S	O/S
Virtualization	Virtualization	Virtualization
Servers	Servers	Servers
Storage	Storage	Storage
Networking	Networking	Networking

Infrastructure as a Service (IaaS): You Manage (Application to O/S); Managed by Vendor (Virtualization to Networking)

Platform as a Service (PaaS): You Manage (Application to Data); Managed by Vendor (Runtime to Networking)

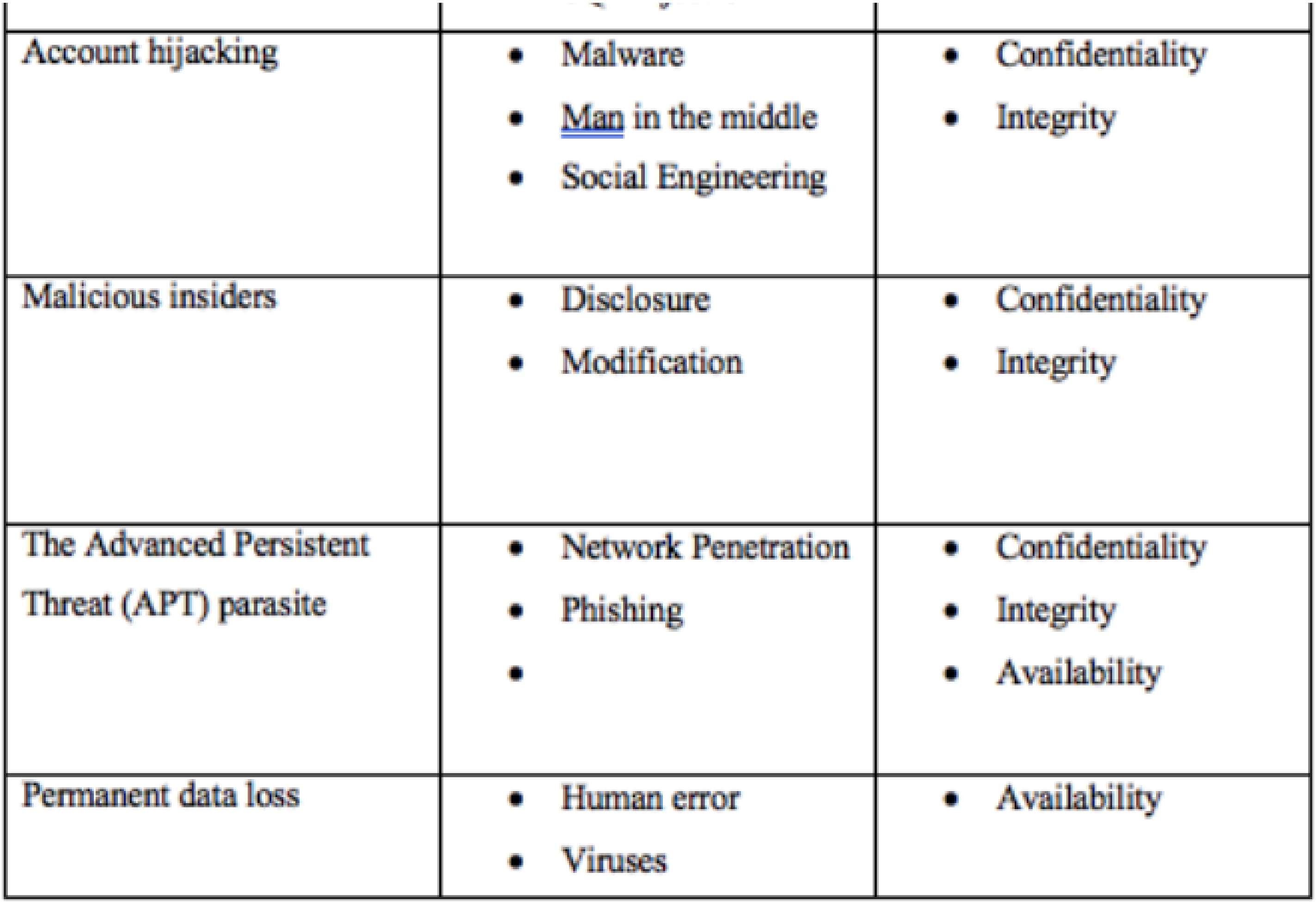
Software as a Service (SaaS): Managed by Vendor (Application to Networking)

Threats



Threat name	Vulnerabilities and attacks	Security factors (CIA)
Data breaches	• malicious • man-in the middle • modifications	• Confidentiality • Integrity
Compromised credentials and broken authentication	• Social Engineering • Man-In-The-Middle	• Integrity • Confidentiality
Hacked interface and Application Program Interfaces	• Operating System Bugs • Unpatched Software	• Availability
Exploited system vulnerabilities	• Brute force • SQL injection	• Availability

Threats



Account hijacking	• Malware • Man in the middle • Social Engineering	• Confidentiality • Integrity
Malicious insiders	• Disclosure • Modification	• Confidentiality • Integrity
The Advanced Persistent Threat (APT) parasite	• Network Penetration • Phishing •	• Confidentiality • Integrity • Availability
Permanent data loss	• Human error • Viruses	• Availability

Threats

Top 12 threads name by Cloud Security Alliance (CSA)

Threats indicate that hackers are exploiting vulnerabilities.

- Data breaches: A data breach its unauthorized access and attempt to get and recover data. Security breaches that you want to damage or disclose important and sensitive data or display it and offer it for sale or illegal sites. Both disclosure, modification, or collection of data, whether by intent or unintentionally, directly or indirectly by user or attacker, that considered as data breach crimes.
- Compromised credentials and broken authentication: Authentication management is always difficult for organizations to confront and find solutions to fill loopholes and attackers inability to access permissions.

Threats

- Hacked interface and Application Program Interfaces: The cloud service providers use application program interfaces (APIs) to provide different services to consumers, as a result of which there are no complications and a strong policy to limit access or exploit vulnerabilities increases the chances of risks and exploitation of attackers and the ability to access. The attacker manipulates, responds, eavesdropping and a lot of attacks that may harm the victim.
- Exploited system vulnerabilities: Attackers exploit software weaknesses or break the firewall barrier and enable it to gain access to systems. This is one of the biggest faults and security holes in the cloud

Threats

- Account hijacking: It is the process that make attacker stole accounts, which is the ability of the attacker to access data and steal the account and may perform actions and activities such as eavesdropping and stealing the e-mail of an individual, organization, or any account linked to the computer, and then steal login data. The attacker can manipulate the data, modify and launch various attacks such as phishing, fraud, exploitation of software vulnerabilities.
- Malicious insiders: People who have the ability and authority to access the systems and exploit the trust granted to them to intrusion and try to access confidential and sensitive files to damage the institution that’s by firewall or Intrusion Detection System (IDS).

Threats

- The Advanced Persistent Threat (APT) parasite: The attacker's infiltration and access to the systems and the establishment of an infrastructure that enables the attacker to steal information. These types of attacks are difficult to detect because they develop and reach in advanced stages through several techniques such as direct piracy, phishing, penetration across the network and the use of insecure programming interfaces.
- Permanent data loss Data loss is the result of natural causes, such as natural disasters such as floods, or a human reason such as unintentionally or intentionally deleting data, viruses or power outages.

Threats

- Inadequate diligence: The companies use the services provided by service providers without prior knowledge and sufficient experience in the cloud, in addition to that without knowledge of the consequences and risks of the cloud.
- Cloud service abuses: Service providers provide consumers with unlimited computing, storage capacity, and trial periods, where anyone can start using cloud services where malicious code authors and criminals may be able to misuse the cloud and initiate unethical and harmful attacks and activities. Cloud services provided by Twitter, Amazon and Facebook.

Threats

- Denial-of-Service (DoS) attacks: The attacker's attempt to make the services unavailable or block the services, by sending several requests without a response to make the service be an excess of unanswered requests and try to begin slow down and eventually stop, by launching UDP flooding, SYN flooding, ICMP flooding attacks, buffer overflow attacks.
- Shared technology, shared dangers: In a multi-sectoral framework, problems occur in technology. Service delivery is on demand by shared infrastructure, which is the access of different users to the same virtual machine.

Security for Services

- IaaS Application:
  - User: Applications on VM, Servers, N/W
  - Provider: any attack to VM can never penetrate to the physical resources
- PaaS Application:
  - User: Applications deployed on PaaS
  - Provider: PaaS platforms
- SaaS Applications:
  - User: Operational level, authentication & access
  - Provider: consumer with ill intention can’t cause harm

Security for Availability

- Physical/ Technical problem may cause server down
- Loss of availability
- For uninterrupted availability:
  - Power supply
  - Measures against fire
  - Cooling
  - Restriction to the physical access to servers, N/W devices etc.

Security and Privacy Issues in Cloud Computing

- Infrastructure Security
  - Host Level
  - Network Level: Encryption and digital signature
- Application Level
- Data and Storage Security
- Identity and Access Management (IAM)

Host Security

Host level Security

- Physical machine
- Threats:
  - Weak access control to hypervisor
  - VM escape problem are prone to threats
  - VM have many nodes, so any threats is easy to amplify, called velocity of attack
- Action by provider
  - Host based IPS and IDS to monitor OS and log files
  - Enable event logging for all security & user activities

Host level Security

- PaaS and SaaS:
  - Providers:
    - Takes entire responsibility to make host secure
    - Not sharing the details of host, OS or security
  - Consumer:
    - SaaS consumer don’t have access to the OS abstraction layer of OS of host
    - PaaS have indirect access to the OS abstraction layer

Host level Security

- IaaS:
  - Providers:
    - Security of physical resources using abstraction.
  - Consumer:
  - VMs and N/W devices from malicious applications
  - Strategies to limit the access
  - Open only required ports (SSH, port 22, HTTP port 80)

Data and Storage/ Information Security

Data level Security

- Data Security during transfer
  - Encryption
  - Traffic Analysis
  - Covert channel
- Data Security at rest
  - Encryption
  - Access control: firewall, IDS
- Availability by backup and redundant systems
  - Reputed service providers ensures 99.9% uptime
  - Amazon promises 99.95% uptime.

IAM Security

References

- *Cloud Computing*, Sandeep Bhowmik
- Cloud computing Black Book, Kailash Jayaswal
- https://www.slideshare.net/rajsarode29/chap-6-cloud-security
- A Comprehensive Survey on Security Threats and Countermeasures of Cloud Computing Environment file:///C:/Users/Admin/Downloads/3662-Article%20Text-6861-1-10-20210423.pdf
- Botnet: https://www.paloaltonetworks.com/cyberpedia/what-is-botnet