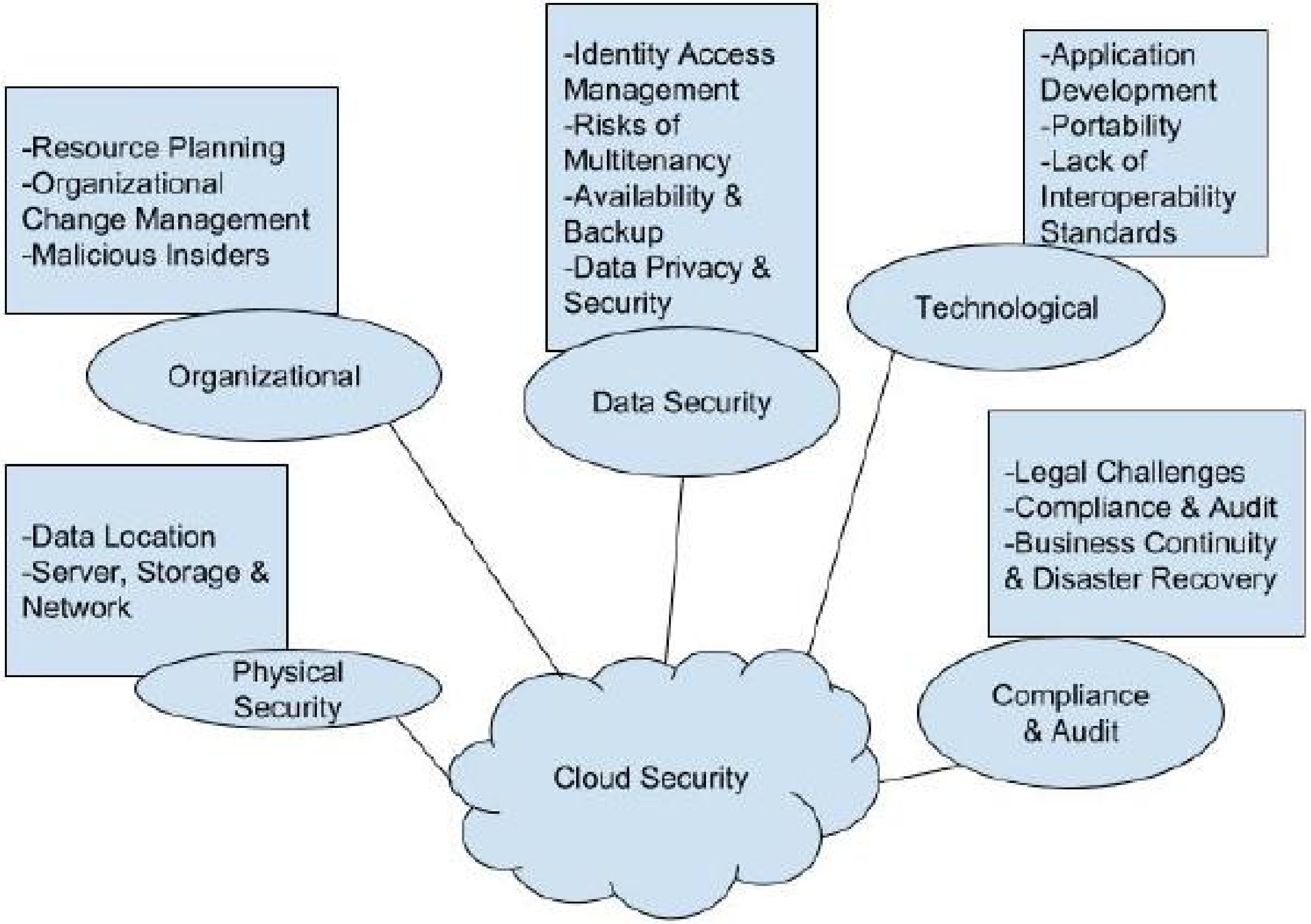
Security threats and vulnerabilities

greenwich.edu.vn

UNIVERSITY of GREENWICH

Alliance with FPT Education

Basic Security Risk Considerations(by CSP And CSC)



Organizational Security Risks

- If a CSP goes out of business or gets acquired by another entity
- There could be the threat of malicious insiders in the organization who could do harm using the data provided by their CSCs

Physical Security Risks

- The physical location of the cloud data center must be secured by the CSP in order to prevent unauthorized on-site access of CSC data
- Even firewalls and encryption cannot protect against the physical theft of data

Technological Security Risks

- These risks are the failures associated with the hardware, technologies and services provided by the CSP
- In the public cloud, with its multi tenancy features, these include resource sharing isolation problems, and risks related to changing CSPs, i.e. portability. Regular maintenance and audit of infrastructure by CSP is recommended.

Compliance and Audit Risks

- These are risks related to the law
- That is, risks related to lack of jurisdiction information, changes in jurisdiction, illegal clauses in the contract and ongoing legal disputes
- For example, depending on location, some CSPs may be mandated by law to turn over sensitive information if demanded by g

Data Security Risks

- The three main properties that we need to ensure are
  - Data integrity,
  - Confidentiality
  - Availability

Data Security Considerations

- When the processing and storage of such data is outsourced to infrastructure owned and maintained by a third party, this leads to a host of issues to consider when securing said data
- These issues are especially more pronounced in the public cloud, since multiple parties, some of which could be malicious, have to share this aforementioned infrastructure.

Data Security Properties

- Privacy
  - Privacy ensures that the personal information and identity of a CSC are not revealed to unauthorized users
- Confidentiality
  - This is related to data privacy since this is the property ensuring that the data that belongs to a CSC is not revealed to any unauthorized parties.
- Integrity
  - Refers to the confidence that the data stored in the cloud is not altered in any way by unauthorized parties when it's being retrieved
- Availability
  - Ensures that the CSC has access to their data, and are not denied access erroneously or due to malicious attacks by any entity

Data Stages

- Data-in-transit
  - This is when data is in the process of being transmitted either to the cloud infrastructure or to the computing device used by the CSC. Encryption is generally used here
- Data-at-rest
  - This is when data has been stored in the cloud infrastructure. The main issue with this stage for the CSC is their loss of control over the data
- Data-in-use
  - This is when data is being processed into information. Here, the issues might lie with the corruption of data while it is being processed

Methods to ensure Data security

- Authentication in the Cloud
  - Authentication for the CPC can be done either by the CSP or outsourced to third party specialists examples
- Encryption techniques in the cloud
  - Caesar Cipher
  - S-DES
  - RSA
  - Secure Socket Layer

Caesar Cipher

- It is a classical substitution cipher. A simple example of such a cipher replaces the letter of alphabet with a letter that is 3 paces ahead of it, for example "ZULU" will be converted into "CXOX".
- There are only 25 possible key options and as such this cipher can easily be brute forced

S-DES

- Simplified Data Encryption Standard has a process of key generation where instead of using a key as is for encryption and decryption, the key generation process of S-DES generates 2 sub keys after processing the initial 10 bit input
- It is not quite as widely used anymore since computing power has caught up with breaking it.

RSA

- A cryptographic algorithm whose encryption key is public and differs from the decryption key which is kept secret
- It is one of the more commonly used encryption algorithms nowadays

Secure Socket Layer (SSL)

- 128 bit encryption
- it is a commonly-used protocol for managing the security of a message transmission on the Internet and it uses public and private key encryption system

References

- http://www.cse.wustl.edu/~jain/cse570-15/index.html