Cloud Security & Personal Identifiable Information

Ashish Dandekar,

Council Member,

Gerson Lehrman Group

Few aspects to share……

1. Are Clouds secure?
2. Cloud Security
3. Personal Identifiable Information
4. Guidelines for control of PII
5. The Standard

Are Clouds secure?

1. We often ask Service Providers as to “How secure your Cloud Services are?”
2. Most of the time we get a response… Our Cloud service is very secure?
3. What happens next……

Cloud Security

1. Cloud Security aspect or provisioning is usually based on requirements of customers.
2. No one cloud will be secure for all types of requirements.
3. Provisioned security is not just during first few weeks. It has to follow a continual assessment, validation and improvements.
4. So what is that MOST IMPORTANT SECURITY ASPECT which a customer fears during the contract?

Personal Identifiable Information (PII)

- Personally identifiable information (PII) is any data that could potentially identify a specific individual.
- Any information that can be used to distinguish one person from another and can be used for de-anonymising anonymous data can be considered as PII.
- Personally identifiable information (Aadhaar data, Gender, Card data, Birth dates with other associated credentials, Addresses, Names, Telephone Nos., etc.) is frequently targeted during Cyber-attacks.

Personal Identifiable Information (PII)

- There is no viable way to prevent data from being collected about us in the current age of computing.
- But if institutions insist on knowing our financial status, purchasing habits, health information, political preferences, and so on, they have a responsibility to keep this data safe from leaking to unauthorized recipients.
- General Data Protection Regulation (GDPR) is an initiative taken in the EU for PII, enforcing it from 25 May 2018, moving from the earlier Data Protection Directive 95/46/EC.

Are there guidelines for control of PII?

- ISO/IEC 27018:2014 is the first international standard comprising a set of privacy, security controls and guidelines for cloud vendors that process and store personal information on behalf of cloud customers in the public cloud.
- ISO 27018 compliant CSPs will not use customer data for their own independent purposes (advertising, marketing, etc.) without customer's express consent.
- ISO 27018 presents a way to differentiate CSPs by adopting a set of credible controls for the protection of their customers' personal information, which can be verified through independent audits.

ISO/ IEC 27018: 2014

- ISO/IEC 27018 are suggestive controls, summarised as follows:-
  - Support cloud customers' privacy obligations, such as enabling access, correction and erasure by individuals.
  - Process personal information only in accordance with the cloud customer's instructions.
  - Notify the cloud customer of law enforcement disclosure requests, where legally permissible.
  - Reject non-legally binding requests to disclose personal information and consult with the cloud customer first where possible before disclosing personal information.

ISO/ IEC 27018: 2014

- ISO 27018 Summary continued..
  - Seek consent from cloud customer & ensure proper controls are in place when engaging sub-contractors.
  - Refrain from using personal information for marketing without express consent of customer.
  - Promptly notify the cloud customer of unauthorised access to personal information, or an event that results in its loss, disclosure or alteration.
  - Develop a policy for the return, transfer, retention and disposal of personal information.

ISO/ IEC 27018: 2014

- ISO 27018 Summary continued..
  - Encrypt data when using portable devices and transmitting over public networks.
  - Specify and document the countries in which personal information may be stored, including by sub-contractors.
  - Refrain from unilaterally varying the contract to reduce technical and organisational measures for privacy and security protection.

Is there any relation with ISO 27001?

- ISO 27018 builds on ISO 27001, a comprehensive international security standard for implementing & maintaining an information security management system (ISMS).
- ISO 27001 defines a process and requirements to address an organisation's overall business risks by selecting adequate and proportionate security controls subject to 3rd party audits.
- ISO 27018 enhances security standards of ISO 27001 dedicatedly for cloud and includes a range of cloud-specific requirements.
- Specifically, ISO 27018 adds controls that reflect PII considerations specifically for cloud services.

Adoption of ISO 27018 & way forward

- Large CSP's are certified (AWS, MS, Google)
- TRAI had published a consulting paper on Cloud computing in Sept 2016.
- Govt. of India has published guidelines to all Government departments for adoption of Cloud services.
- Going forward, the standard is likely to be prescreptive.

Ashish Dandekar

Council Member,

Gerson Lehrman Group

dashish0402@gmail.com

+91-98203-45088