Five Steps to Secure Cloud-based Environments

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Cloud-based environments offer many advantages to organisations. However, they also introduce a number of technical security risks which organisations should be aware of such as:

- Data breaches
- Hijacking of accounts
- Unauthorised access to personal data

Organisations should determine and implement a **documented policy** and apply the **appropriate technical security and organisational measures** to secure their cloud-based environments. If organisations do not implement such controls, they may increase their risk of a personal data breach.[1]

Organisations should apply such technical security and organisational security measures in a layered manner consisting of but not limited to:

- Access controls
- Firewalls
- Antivirus
- Staff training
- Policy development

A **layered approach** to cloud-based security mitigates the risk of a single security measure failing which may result in a personal data breach.

Many cloud-based providers, such as Microsoft's Office 365 and Google's G-suite provide advanced settings and solutions which can assist organisations to appropriately secure their use of cloud-based services. These providers, in most cases, also offer best practice guidance to assist organisations in securing their cloud-based environments.

Additional information, advice, and best practice regarding security of cloud-based environments is also provided by agencies such as the European Union Agency for Network and Information Security (**"ENISA"**) https://www.enisa.europa.eu/, and the US-based National Institute of Standards and Technology (**"NIST"**) https://www.nist.gov/topics/information-technology.

The following guidance illustrates **five key ways** organisations can secure their cloud-based environments to **mitigate their risk** of a personal data breach.

[1] See the breach notification section of the DPC website for more information: https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification

1. Access Control and Authentication

Organisations should implement **strong password polices** to ensure that users accessing personal data within cloud-based environments do so in a secure manner.

Organisations should implement **two-factor authentication**. Two-factor authentication is an effective way to further enhance cloud-based security and is available from most cloud-based providers.

Organisations should be aware of and **document user access privileges** within their cloud-based environments. User access control is particularly important where group mailboxes or shared folders are utilised. Organisations should also document each user's specific access requirements and ensure that these are supported by an appropriate change control process.

Security measures applied by an organisation must be supported by **regular reviews** of user access to ensure that all authorised access to personal data is strictly necessary and justifiable for the performance of a specific function.

2. Review Default Security Settings

Organisations should **not rely on** cloud-based service providers' **default security settings**. Organisations should review the cloud-based security features available from the cloud-based service provider to ensure that they are applied appropriately and in a layered manner. Examples of security settings and controls provided by cloud-based service providers often include:

- Centralised administration tools
- Mobile device management
- Multifactor authentication
- Login alerts
- Encryption during message send and receive
- Encryption of message content
- Account activity monitoring and alerts
- Data loss prevention
- Malware protection
- Spam and spoofing protection
- Phishing protection

Organisations should also be aware that cloud-based services might be publically accessible and organisations should review and implement the appropriate security settings to **secure remote access**.

3. Seek Assurances from Your ICT Service Provider

Organisations may **utilise external ICT services** providers to implement their cloud-based environments. It is vital during such engagements that organisations **seek formal assurances** from their ICT service provider that the security controls which have been implemented meet an organisation's specific security requirements and protect the organisation's personal data.

Organisations should **proactively engage and conduct regular security reviews** with their ICT service providers to ensure the security controls in place are up-to-date and are effective to protect the organisation in an evolving threat landscape.

4. Clear Policies and Staff Training

Organisations should **ensure that staff receive appropriate training** on social engineering attacks, phishing attacks and security threat practices. Such training should be **supported by refresher training/awareness programmes** to mitigate the risk posed by an evolving threat landscape.

Organisations should **have clear policies in place** with respect to the usage and security of cloud-based services, especially where these services are being accessed outside of the organisation corporate network under Bring Your Own Device ('BYOD') policies.

Organisations should have clear **"employee leaver" and "succession" policies** in place and these should be applied to an organisations cloud-based environment.

Organisations should have a clear policy in place for **data retention** and conduct **regular reviews** to ensure that personal data is not retained longer than necessary or where the original purpose for the use of the personal data has ceased.

5. Know Your Data and Secure It

Organisations should **understand and monitor the types of data** that is stored in their cloud-based environments. Knowing the types of data stored in the Cloud enables an organisation to ensure the appropriate security and access controls are applied to protect the data.

Organisations should utilise **data classification methods** to identify the data which they store and process within Cloud-Based environments. The process of data classification enables an organisation to categorise their stored data in order to determine the appropriate security controls.

Organisations should **carefully evaluate cloud-based vendors** based on the **security** features they offer and how they specifically meet with their organisational requirements.

Who has access to your data, how is it secured, how often is the data backed up and if the cloud-based environment aligns to your organisational policies are all vital questions to ask of both your cloud-based service provider and / or the ICT service provider charged with implementing your environment.

Applying the appropriate security measures is **not a once off "*set and forget*" exercise**. Cloud-based security settings should be **reviewed on a regular basis** to ensure that they are still appropriate and up-to-date.