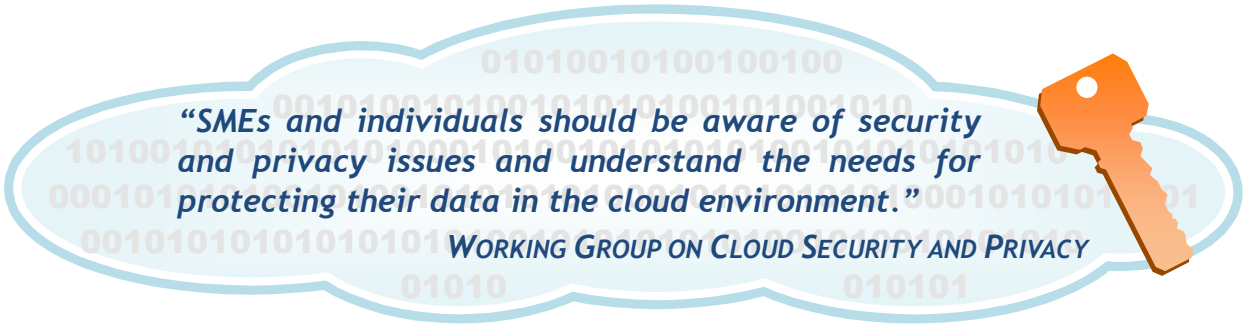
SECURITY CHECKLISTS FOR CLOUD SERVICE CONSUMERS



Purpose

Businesses and individuals are increasingly using cloud services for the benefits of convenience, ubiquity and cost effectiveness. This document provides three security checklists when considering the use of or when using cloud services.

Target Audience

The key target audience of this document is cloud service consumers, including small and medium sized enterprises (SMEs) as well as individuals.

Scope of Discussion

This document focuses on cloud-based consumer services which involve the storage and sharing by individuals of their own information and use of cloud applications installed on remote servers owned or operated by a third party service provider and accessed through the Internet or other network connection. Many of these services, especially those offering only basic provisions, could be free of charge, while some advanced services may require a subscription fee. Examples of such services include webmail, social networking sites, data storage, photo sharing sites, contact management, document management and others. Typically these services are known as "Software as a Service (SaaS)", a software delivery model in which software and associated data are centrally hosted within the cloud.

Security Concerns of Cloud Service Consumers

Many people are wary of using cloud services because of concerns about service outages, data loss, privacy issues, hacker compromising their access accounts, and compliance with legislation. For IT savvy enterprises, they are likely to have skills and resources to monitor the service level of their service provider, assess the service provider's security compliance, or implement their own additional security safeguards to protect their data.

On the other hand, for average cloud service consumers and SMEs, they may overlook their own rights and responsibilities, be confused about how to choose a cloud service provider that is trustworthy, and hesitant on whether their data has sufficient protection when using a cloud service.

What Cloud Service Consumers Should Be Aware Of?

Data processed or stored by cloud service consumers in a cloud service may contain valuable, sensitive and personal information. Knowing only the security measures applied by the cloud service provider is not sufficient to protect this data. For SMEs, they need to know what needs to be considered when selecting a cloud service provider, as well as what needs to be considered when using cloud services. All cloud service consumers, both responsible parties of businesses and individuals, are advised to have an in-depth understanding of the issues and concerns for protecting their data in the cloud environment.

Checklist for SMEs on selecting Cloud Service Provider

Terms of Service and Security & Privacy Policy

- Read the Terms of Service and Security & Privacy Policy. Note -
  - how your company can use the cloud service (i.e. acceptable usage policies, licensing rights or usage restrictions);
  - how your data is stored and protected;
  - whether the service provider has access to your data, and if so, how that access is restricted;
  - how to report an incident;
  - how to terminate the service and if data is retained after service termination;
  - whether the service provider will give advance notice of any change of terms;
  - whether the Privacy Policy follows the data protection principles of the Personal Data (Privacy) Ordinance[1]; and
  - the jurisdiction (Hong Kong SAR or other locations) that the Terms would apply.
- Negotiate the Terms of Service with the service provider if not all the terms are found acceptable. If you cannot find a service provider meeting your requirements, you should re-consider the use of cloud services.
- Understand whether there are "secondary uses" of your account information without your knowledge or consent. For example, information stored in the cloud may be used to tailor advertisements.

Data Ownership

- Check whether the service provider reserves rights to use, disclose, or make public your information.
- Check whether the intellectual property rights of data you own remain intact.
- Check whether the service provider retains rights to your information even if you remove your data from the cloud.
- Understand whether you can move or transfer your data and the service to another provider when you want to, and whether export utilities are available and are easy to use.
- Check whether data can be permanently erased from the cloud, including any backup storage, when you delete this data or when you end the service.

Additional Selection Considerations

- Understand the acceptable range of risks associated with the use of cloud services.
- Select a service provider with a service level agreement commensurable with the importance of your business function.
- Select a service provider that can explain clearly what security features are available, preferably supported by an independent information security management certification (e.g. ISO/IEC 27001).
- Select a service provider with no major security incident reported, or one that can provide transparency to previous security incidents with cause and remediation explained.
- Select a service provider that ensures data confidentiality by -
  - using encryption (e.g. Secure Sockets Layer (SSL)) to transmit data; and
  - using encryption to protect stored static data. (If not, you have to use your own encryption before storing data in the cloud. In that case remember to keep your encryption key safe.)
- Select a service provider that provides a simple and clear reporting mechanism for service problems, security and privacy incidents.
- Select a service provider that provides regular service management reports and incident problem reports.

Checklist for SMEs on using Cloud Services

Identification and Authentication

- Use a strong authentication method, such as two-factor authentication, if available from the cloud service. Examples are combination of any two factors of: what you are (e.g. fingerprint), what you have (e.g. digital certificate) and what you know (e.g. password).
- Use strong passwords for each account.
- Use different passwords for different accounts.
- Use different accounts for different staff.
- Change passwords periodically.
- Delete access accounts or change passwords immediately when there are staff changes.

Cloud Administration

- Establish a simple access account policy for using the cloud service.
- Establish simple usage policies for your staff.
- Appoint suitable staff (who has a basic understanding of the characteristics of cloud services) as the cloud service administrator.
- Conduct regular reviews of access rights on staff having access to cloud data.
- Provide basic security awareness training for staff using the cloud service.

Data Protection

- Understand and keep a record of what type of data is stored in the cloud.
- Protect personal data according to the Personal Data (Privacy) Ordinance[1].
- Avoid sharing out data to unintended parties by -
  - ensuring only the intended recipients have the access permissions if you share sensitive data with others through the cloud;
  - ensuring any software running on the cloud service consumer's device that accesses a cloud service will only synchronize permitted data between the device and the cloud; and
  - defining proper default permissions of files or folders.
- Understand the location (and thus the jurisdiction) of your data including resilient copies, and assess whether there are impacts on security procedures in light of the differences in legal and regulatory compliance requirements.

Service Continuity

- Obtain service support contact information from the service provider; especially keep a list of telephone numbers for reporting computer security incidents.
- Evaluate the potential damage to the company when the service is unavailable, data is lost or when data is accessed in an unauthorized manner.
- Develop a business continuity plan and work out alternatives when the cloud service or data is not available.
- Prepare an exit strategy and ensure termination procedures permit the transfer of data back to the company.
- Perform a regular backup of your data stored in the cloud service.
- Maintain a local backup copy of your important data so that this data can still be available when the service provider is out of service temporarily (e.g. network outage) or permanently.

Checklist for Individuals on protecting their data in the Cloud Environment

Terms of Service and Security & Privacy Policy

- Read the Terms of Service and Security & Privacy Policy. Note -
  - how your data is stored and protected;
  - how to report an incident; and
  - how to terminate the service and if data is retained after service termination.
- Do not subscribe if you do not agree to the Terms and Policy. Be aware of the periodic changes of the Terms and Policy.

Data Protection

- Think twice when you want to store sensitive data in the cloud and assess the impact if this data is exposed.
- Avoid sharing out data to unintended parties by -
  - ensuring only the intended recipients have the access permissions if you share sensitive data with others through the cloud;
  - ensuring any software running on the cloud service consumer's device will only synchronize permitted data between the device and the cloud; and
  - checking if the default permission of files or folders you are using is appropriate. For example a pre-installed "Photo" folder may be public accessible by default and is not a favourable setting.
- Maintain a local backup copy of your important data so that this data can still be available when the service provider is out of service temporarily (e.g. network outage) or permanently.
- Ensure the service provider protects data confidentiality by -
  - using encryption (e.g. SSL) to transmit data; and
  - using encryption when storing static data. (If not, you have to use your own encryption before storing data in the cloud. In that case remember to keep your encryption key safe.)

Security of Access Accounts[2]

- Use strong passwords for access accounts.
- Use different passwords for different access accounts.
- Protect user names and passwords by -
  - keeping them in a safe place;
  - avoid sharing them with others;
  - turning off password saving in browsers and applications; and
  - avoid keeping passwords in plain text on the device.
- Ensure the above measures are also implemented onto any local program on a computer or mobile device that accesses the cloud services.
- Log off the cloud service if it is not required.

Security of Your own Access Device[3]

- Use only trustworthy devices to access cloud services. Avoid using public computers to process sensitive data in the cloud.
- Secure the access device physically. Protect the access device from unauthorized access.
- Use a screen saver to lock the computer or mobile device.
- Refrain from jailbreaking the access devices (i.e. remove usage and access limitation controls).
- Keep operating systems, browsers and applications of your access device, including computers and mobile devices, up-to-date with the latest software versions and security patches.
- Be cautious on browsing, especially not to click on any links from untrusted sources.

References

1. Refer http://www.pcpd.org.hk/english/ordinance/ordglance1.html#dataprotect on the data protection principles of the PDPO
2. Refer http://www.infosec.gov.hk/english/yourself/account.html on handling user accounts and passwords
3. Refer http://www.infosec.gov.hk/english/virus/geninfo_common.html on best practices of protecting your computer more effectively against virus and malicious code

InfoCloud website is established by the Expert Group on Cloud Computing Services and Standards. It serves as a one-stop portal for the general public and enterprises (especially SMEs) to effectively access information and resources on cloud computing technologies. The website provides sample use cases, guidelines and best practices for achieving the desired benefits in adopting the cloud computing model.

The Office of the Government Chief Information Officer of the HKSAR Government established the Expert Group with an aim to draw expertise from the industry, academia, professional bodies and the Government to drive cloud computing adoption and deployment in Hong Kong, as well as facilitate exchanges among cloud experts both within Hong Kong and with the Mainland. Working Group on Cloud Security and Privacy is one of the working groups set up under the Expert Group.

This document is one of its series of best practices and guidelines on cloud security and privacy published by the Working Group on Cloud Security and Privacy. With the collaborative efforts from members of the Working Group, deliverables are developed with a view to facilitating and promoting wider adoption of cloud computing and secure use of cloud services in local industry.