Australian Government

Department of Defence

Intelligence and Security

PROTECT

CYBER SECURITY OPERATIONS CENTRE

APRIL 2011, UPDATED SEPTEMBER 2012

Cloud Computing Security Considerations

Table of Contents

Cloud Computing Security Considerations

1. Cloud computing offers potential benefits including cost savings and improved business outcomes for Australian government agencies. However, there are a variety of information security risks that need to be carefully considered. Risks will vary depending on the sensitivity of the data to be stored or processed, and how the chosen cloud vendor (also referred to as a cloud service provider) has implemented their specific cloud services.

2. This discussion paper assists agencies to perform a risk assessment to determine the viability of using cloud computing services. This document provides an overview of cloud computing and associated benefits. Most importantly, this document provides a list of thought provoking questions to help agencies understand the risks that need to be considered when using cloud computing. Developing a risk assessment helps senior business representatives make an informed decision as to whether cloud computing is currently suitable to meet their business goals with an acceptable level of risk. The questions in this document address the following topics:

   a. availability of data and business functionality;

   b. protecting data from unauthorised access; and,

   c. handling security incidents.

3. The Australian Signals Directorate (ASD) strongly encourages both senior managers and technical staff to work through this list of questions together. The questions are intended to provoke discussion and help agencies identify and manage relevant information security risks associated with the evolving field of cloud computing. In particular, the risk assessment needs to seriously consider the potential risks involved in handing over control of your data to an external vendor. Risks may increase if the vendor operates offshore.

4. This document complements the advice on cloud computing in the *Australian Government Information Security Manual* (ISM). ASD recommends against outsourcing information technology services and functions outside of Australia, unless agencies are dealing with data that is all publicly available. ASD strongly encourages agencies to choose either a locally owned vendor or a foreign owned vendor that is located in Australia and stores, processes and manages sensitive data only within Australian borders. Note that foreign owned vendors operating in Australia may be subject to foreign laws such as a foreign government's lawful access to data held by the vendor.

Overview of Cloud Computing

5. Cloud computing as a delivery model for IT services is defined by the National Institute of Standards and Technology (NIST) as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1]

6. NIST specify five characteristics of cloud computing:

   a. **On-demand self-service** involves customers using a web site or similar control panel interface to provision computing resources such as additional computers, network bandwidth or user email accounts, without requiring human interaction between customers and the vendor.
   b. **Broad network access** enables customers to access computing resources over networks such as the Internet from a broad range of computing devices such as laptops and smartphones.
   c. **Resource pooling** involves vendors using shared computing resources to provide cloud services to multiple customers. Virtualisation and multi-tenancy mechanisms are typically used to both segregate and protect each customer and their data from other customers, and to make it appear to customers that they are the only user of a shared computer or software application.
   d. **Rapid elasticity** enables the fast and automatic increase and decrease to the amount of available computer processing, storage and network bandwidth as required by customer demand.
   e. **Pay-per-use measured service** involves customers only paying for the computing resources that they actually use, and being able to monitor their usage. This is analogous to household use of utilities such as electricity.

7. There are three cloud service models. A non-exhaustive list of example vendor services is provided to help the reader understand the cloud service models. Inclusion of an example vendor service does not imply ASD's support of the service.

   a. **Infrastructure as a Service** (IaaS) involves the vendor providing physical computer hardware including CPU processing, memory, data storage and network connectivity. The vendor may share their hardware among multiple customers referred to as "multiple tenants" using virtualisation software. IaaS enables customers to run operating systems and software applications of their choice. Typically the vendor controls and maintains the physical computer hardware. Typically the customer controls and maintains the operating systems and software applications.
   Example IaaS vendor services include Amazon Elastic Compute Cloud (EC2), GoGrid and Rackspace Cloud.

[1] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

b. **Platform as a Service** (PaaS) involves the vendor providing Infrastructure as a Service plus operating systems and server applications such as web servers. PaaS enables customers to use the vendor's cloud infrastructure to deploy web applications and other software developed by the customer using programming languages supported by the vendor. Typically the vendor controls and maintains the physical computer hardware, operating systems and server applications. Typically the customer only controls and maintains the software applications developed by the customer.
Example PaaS vendor services include Google App Engine, Force.com, Amazon Web Services Elastic Beanstalk, and the Microsoft Windows Azure platform.

c. **Software as a Service** (SaaS) involves the vendor using their cloud infrastructure and cloud platforms to provide customers with software applications. Example applications include email and an environment for users to collaboratively develop and share files such as documents and spreadsheets. These end user applications are typically accessed by users via a web browser, eliminating the need for the user to install or maintain additional software. Typically the vendor controls and maintains the physical computer hardware, operating systems and software applications. Typically the customer only controls and maintains limited application configuration settings specific to users such as creating email address distribution lists.
Example SaaS vendor services include Salesforce.com Customer Relationship Management (CRM), Google Docs and Google Gmail. Microsoft Office 365 (formerly called Business Productivity Online Suite) consists of Microsoft Office Web Apps, Microsoft Exchange Online, Microsoft SharePoint Online, Microsoft Dynamics CRM Online and Microsoft Lync.

8. A vendor adding the words "cloud" or "as a Service" to the names of their products and services does not automatically mean that the vendor is selling cloud computing as per the NIST definition.

9. There are four cloud deployment models:

a. **Public cloud** involves an organisation using a vendor's cloud infrastructure which is shared via the Internet with many other organisations and other members of the public. This model has maximum potential cost efficiencies due to economies of scale. However, this model has a variety of inherent security risks that need to be considered.

b. **Private cloud** involves an organisation's exclusive use of cloud infrastructure and services located at the organisation's premises or offsite, and managed by the organisation or a vendor. Compared to the public cloud model, the private cloud model has reduced potential cost efficiencies. If the private cloud is properly implemented and operated, it has reduced potential security concerns. A well architected private cloud properly managed by a vendor provides many of the benefits of a public cloud, but with increased control over security. A managed private cloud may enable enterprise customers to more easily negotiate suitable contracts with the vendor, instead of being forced to accept the generic contracts designed for the consumer mass market that are offered by some public cloud vendors.

c. **Community cloud** involves a private cloud that is shared by several organisations with similar security requirements and a need to store or process data of similar sensitivity. This model attempts to obtain most of the security benefits of a private cloud, and most of the

economic benefits of a public cloud. An example community cloud is the sharing of a private cloud by several agencies of the same government.

d. **Hybrid cloud** involves a combination of cloud models. An example is using commodity resources from a public cloud such as web servers to display non-sensitive data, which interacts with sensitive data stored or processed in a private cloud.

Overview of Business Drivers to Adopt Cloud Computing

10. Cloud computing has the potential to help agencies leverage modern technologies such as computer virtualisation and worldwide Internet connectivity. Some of the key business drivers are:

a. **Pursuing new business opportunities**, such as trialling new ideas to reach and interact with customers over the Internet;
b. **Reducing upfront costs** of capital expenditure of computer equipment and related expenses such as a physical data centre and support staff, while reducing the associated financial risk to the agency by replacing upfront costs with reasonably predictable operational expenditure, and only paying for the amount of computing processing and data storage that is actually used;
c. **Potentially reducing ongoing costs** due to the use of infrastructure and technical specialists that are typically shared among many customers to achieve economies of scale, however the cost of applying controls to help address security risks especially associated with shared infrastructure may reduce the potential cost savings of some types of cloud computing;
d. **Potentially improving business continuity** and the availability of computing infrastructure if users have guaranteed available network connectivity, where the infrastructure can rapidly and flexibly scale to meet peaks and troughs in usage demand, and with the computing infrastructure typically located in multiple physical locations for improved disaster recovery; and,
e. **Potentially reducing carbon footprint** due to the more efficient use of computer hardware requiring less electricity and less air conditioning.

11. There may be good business reasons to move publicly available data to the public cloud. If properly designed, a vendor's spare network bandwidth and spare computing capacity automatically helps to mitigate some types of distributed denial of service (DDoS) attacks. Technologies such as "anycast" and international Content Delivery Networks (CDN) can help to mitigate DDoS attacks by geographically distributing the network traffic and computer processing around the world. These technologies to improve the availability and business continuity of publicly available data are prohibitively expensive for every agency to build themselves, though are relatively inexpensive to rent from vendors. Although the availability of an agency's web site may not be affected by a DDoS attack, the agency may have to pay for the computer processing and network bandwidth consumed by the DDoS attack.

12. Agencies using cloud computing to store or process publicly available data such as a public web site may not be concerned about confidentiality. However, the agency's risk assessment should consider the availability and integrity of the public data, including reputational and other damage if the agency's system is offline, or is compromised and distributes misleading information or malicious content.

13. To enable an agency to focus on their core business, the acquisition and maintenance of specialist IT staff, computing software and hardware used to store and process data can be outsourced to a vendor. However, the agency is still ultimately responsible for the protection of their data.

Risk Management

14. A risk management process must be used to balance the benefits of cloud computing with the security risks associated with the agency handing over control to a vendor. A risk assessment should consider whether the agency is willing to trust their reputation, business continuity, and data to a vendor that may insecurely transmit, store and process the agency's data.

15. The contract between a vendor and their customer must address mitigations to governance and security risks, and cover who has access to the customer's data and the security measures used to protect the customer's data. Vendor's responses to important security considerations must be captured in the Service Level Agreement or other contract, otherwise the customer only has vendor promises and marketing claims that can be hard to verify and may be unenforceable.

16. In some cases it may be impractical or impossible for a customer to personally verify whether the vendor is adhering to the contract, requiring the customer to rely on third party audits including certifications instead of simply putting blind faith in the vendor. Customers should consider which of the vendor's certifications are useful and relevant, how much the certification increases the customer's confidence in the vendor, what associated documents the customer can request from the vendor, and whether the contents of the documents are of high quality. For example, Statement on Auditing Standards (SAS) 70 Type II, superseded by a new standard in 2011, can involve the vendor deciding which aspects of their business are to be covered, and an independent accountant checking only these aspects. Therefore, customers should ask vendors exactly what aspects are covered. For vendors advertising ISO/IEC 27001 compliance, customers should ask to review a copy of the Statement of Applicability, a copy of the latest external auditor's report, and the results of recent internal audits.

Overview of Cloud Computing Security Considerations

17. This section provides a non-exhaustive list of cloud computing security considerations. Each security consideration listed has a reference to the associated paragraph in this document that contains more detailed information about the security consideration. Placing a cross instead of a tick beside any of the following security considerations does not necessarily mean that cloud computing cannot be used, it simply means that the security consideration requires additional contemplation to determine if the associated risk is acceptable. Cloud computing security considerations include:

☐ My data or functionality to be moved to the cloud is not business critical (19a).

☐ I have reviewed the vendor's business continuity and disaster recovery plan (19b).

☐ I will maintain an up to date backup copy of my data (19c).

☐ My data or business functionality will be replicated with a second vendor (19d).

☐ The network connection between me and the vendor's network is adequate (19e).

☐ The Service Level Agreement (SLA) guarantees adequate system availability (19f).

☐ Scheduled outages are acceptable both in duration and time of day (19g).

☐ Scheduled outages affect the guaranteed percentage of system availability (19h).

☐ I would receive adequate compensation for a breach of the SLA or contract (19i).

☐ Redundancy mechanisms and offsite backups prevent data corruption or loss (19j).

☐ If I accidentally delete a file or other data, the vendor can quickly restore it (19k).

☐ I can increase my use of the vendor's computing resources at short notice (19l).

☐ I can easily move my data to another vendor or inhouse (19m).

☐ I can easily move my standardised application to another vendor or inhouse (19m).

☐ My choice of cloud sharing model aligns with my risk tolerance (20a).

☐ My data is not too sensitive to store or process in the cloud (20b).

☐ I can meet the legislative obligations to protect and manage my data (20c).

☐ I know and accept the privacy laws of countries that have access to my data (20d).

☐ Strong encryption approved by ASD protects my sensitive data at all times (20e).

☐ The vendor suitably sanitises storage media storing my data at its end of life (20f).

☐ The vendor securely monitors the computers that store or process my data (20g).

☐ I can use my existing tools to monitor my use of the vendor's services (20h).

☐ I retain legal ownership of my data (20i).

☐ The vendor has a secure gateway environment (20j).

☐ The vendor's gateway is certified by an authoritative third party (20k).

☐ The vendor provides a suitable email content filtering capability (20l).

☐ The vendor's security posture is supported by policies and processes (20m).

☐ The vendor's security posture is supported by direct technical controls (20n).

☐ I can audit the vendor's security or access reputable third party audit reports (20o).

☐ The vendor supports the identity and access management system that I use (20p).

☐ Users access and store sensitive data only via trusted operating environments (20q).

☐ The vendor uses endorsed physical security products and devices (20r).

☐ The vendor's procurement process for software and hardware is trustworthy (20s).

☐ The vendor adequately separates me and my data from other customers (21a).

☐ Using the vendor's cloud does not weaken my network security posture (21b).

☐ I have the option of using computers that are dedicated to my exclusive use (21c).

☐ When I delete my data, the storage media is sanitised before being reused (21d).

☐ The vendor does not know the password or key used to decrypt my data (22a).

☐ The vendor performs appropriate personnel vetting and employment checks (22b).

☐ Actions performed by the vendor's employees are logged and reviewed (22c).

☐ Visitors to the vendor's data centres are positively identified and escorted (22d).

☐ Vendor data centres have cable management practices to identify tampering (22e).

☐ Vendor security considerations apply equally to the vendor's subcontractors (22f).

☐ The vendor is contactable and provides timely responses and support (23a).

☐ I have reviewed the vendor's security incident response plan (23b).

☐ The vendor's employees are trained to detect and handle security incidents (23c).

☐ The vendor will notify me of security incidents (23d).

☐ The vendor will assist me with security investigations and legal discovery (23e).

☐ I can access audit logs and other evidence to perform a forensic investigation (23f).

☐ I receive adequate compensation for a security breach caused by the vendor (23g).

☐ Storage media storing sensitive data can be adequately sanitised (23h).