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).

Detailed Cloud Computing Security Considerations

18. This section provides a detailed list of security considerations that agencies can discuss both internally and with vendors that are transparent about their security measures. Some examples are provided to demonstrate that the security considerations are not theoretical. Questions are provided to provoke thought and discussion, rather than to be used simply as a checklist. Answers to these questions will assist agencies to develop a risk assessment and make an informed decision regarding whether the agency's proposed use of cloud computing has an acceptable level of risk. It is unlikely that any single vendor will provide suitable answers to all of the questions, so agencies should decide which questions are most relevant based on the agency's intended use of cloud computing.

Maintaining Availability and Business Functionality

19. Answers to the following questions can reveal mitigations to help manage the risk of business functionality being negatively impacted by the vendor's cloud services becoming unavailable:

a. **Business criticality of data or functionality.** Am I moving business critical data or functionality to the cloud?
b. **Vendor's business continuity and disaster recovery plan.** Can I thoroughly review a copy of the vendor's business continuity and disaster recovery plan that covers the availability and restoration of both my data and the vendor's services that I use? How much time does it take for my data and the services that I use to be recovered after a disaster, and do the vendor's other customers that are larger and pay more money than me get prioritisation?
c. **My data backup plan.** Will I spend additional money to maintain an up to date backup copy of my data located either at my agency's premises, or stored with a second vendor that has no common points of failure with the first vendor?
d. **My business continuity and disaster recovery plan.** Will I spend additional money to replicate my data or business functionality with a second vendor that uses a different data centre and ideally has no common points of failure with the first vendor? This replication should preferably be configured to automatically "failover", so that if one vendor's services become unavailable, control is automatically and smoothly transitioned to the other vendor.
e. **My network connectivity to the cloud.** Is the network connectivity between my agency's users and the vendor's network adequate in terms of availability, traffic throughput (bandwidth), delays (latency) and packet loss?
f. **Vendor's guarantee of availability.** Does the Service Level Agreement (SLA) guarantee that the vendor will provide adequate system availability and quality of service, using their robust system architecture and business processes? Availability may be affected by technical issues such as computer and network performance and latency, hardware failures and faulty vendor software.

   Availability may also be affected by deliberate attacks such as denial of service attacks against me or other customers of the vendor that still affects me. Finally, availability may also be affected by configuration mistakes made by the vendor including those resulting from poor software version control and poor change management processes.
g. **Impact of outages.** Can I tolerate the maximum possible downtime of the SLA? Are the scheduled outage windows acceptable both in duration and time of day, or will scheduled outages interfere with my critical business processes? Typical SLAs that guarantee 99.9%

availability can have up to nine hours of unscheduled outages every year without breaching the SLA.

h. **SLA inclusion of scheduled outages.** Does the SLA guaranteed availability percentage include scheduled outages? If not, the vendor may have numerous long scheduled outages, including emergency scheduled outages with little or no notice to customers, that do not result in a breach of the SLA. Vendors with distributed and redundant computing and network infrastructure enable scheduled maintenance to be applied in batches while customers are seamlessly transitioned to computing and network infrastructure that is still available and not part of the outage.

i. **SLA compensation.** Does the SLA adequately reflect the actual damage caused by a breach of the SLA such as unscheduled downtime or data loss? For example, most generic SLAs designed for the consumer mass market typically involve inadequate compensation such as a few hours of free service, or a credit, partial refund or other small discount on the monthly bill. The damage done to an agency's reputation is not repaired by receiving a token amount of free service or refunded money. For example, in February 2011 a major vendor accidentally deleted thousands of files belonging to a paying customer, admitted negligence, initially stated that the files were not retrievable, and offered free service worth approximately $100 as compensation. This example also highlighted deficiencies in staff training, business processes and backup implementation.

j. **Data integrity and availability.** How does the vendor implement mechanisms such as redundancy and offsite backups to prevent corruption or loss of my data, and guarantee both the integrity and the availability of my data? For example, in February 2011 a major vendor of email Software as a Service began deploying a software update that unexpectedly deleted all of the email belonging to tens of thousands of customers. This problem affected data in the vendor's multiple data centres, highlighting the importance of having offline backups in addition to redundant data centres.

k. **Data restoration.** If I accidentally delete a file, email or other data, how much time does it take for my data to be partially or fully restored from backup, and is the maximum acceptable time captured in the SLA?

l. **Scalability.** How much available spare computing resources does the vendor provide to enable my usage of the vendor's services to scale at short notice?

m. **Changing vendor.** If I want to move my data to my agency or to a different vendor, or if the vendor suddenly becomes bankrupt or otherwise quits the cloud business, how do I get access to my data in a vendor-neutral format to avoid vendor lock-in? How cooperative will the vendor be? How do I ensure that my data is permanently deleted from the vendor's storage media? For Platform as a Service, which standards does the vendor use that facilitate portability and interoperability to easily move my application to a different vendor or to my agency?

Protecting Data from Unauthorised Access by a Third Party

20. Answers to the following questions can reveal mitigations to help manage the risk of unauthorised access to data by a third party:

a. **Choice of cloud deployment model.** Am I considering using a potentially less secure public cloud, a potentially more secure hybrid cloud or community cloud, or a potentially most secure private cloud?

b. **Sensitivity of my data.** Is my data to be stored or processed in the cloud classified, sensitive, private, or data that is publicly available such as information from my public web site? Does the aggregation of my data make it more sensitive than any individual piece of data? For example, the sensitivity may increase if storing a significant amount of data, or storing a variety of data that if compromised would facilitate identity theft. If there is a data compromise, could I demonstrate my due diligence to senior management, government officials and the public?

c. **Legislative obligations.** What obligations do I have to protect and manage my data under various legislation, for example the *Privacy Act 1988*, the *Archives Act 1983*, as well as other legislation specific to the type of data? Will the vendor contractually accept adhering to these obligations to help me ensure that the obligations are met to the satisfaction of the Australian Government?

d. **Countries with access to my data.** In which countries is my data stored, backed up and processed? Which foreign countries does my data transit? In which countries is the failover or redundant data centres? Will the vendor notify me if the answers to these questions change? Data stored in, processed in, or transiting foreign countries may be subject to their laws. Such laws range from Freedom of Information requests by members of the public, through to government lawful access mechanisms. For example, a foreign owned vendor may be subject to their country's laws even if the vendor is operating within Australia. If the vendor is subpoenaed by a foreign law enforcement agency for access to data belonging to the vendor's customers, the vendor may be legally prohibited from notifying their customers of the subpoena.

e. **Data encryption technologies.** Are hash algorithms, encryption algorithms and key lengths deemed appropriate by the ASD ISM used to protect my data when it is in transit over a network, and stored on both the vendor's computers and on backup media?

   The ability to encrypt data while it is being processed by the vendor's computers is still an emerging technology and is an area of current research by industry and academia. Is the encryption deemed strong enough to protect my data for the duration of time that my data is sensitive? For example, cloud computing processing power has already been used to significantly reduce the time and cost of using brute force techniques to crack and recover relatively weak passwords either stored as SHA1 hashes or used as Wi-Fi Protected Access (WPA) pre-shared keys.

f. **Media sanitisation.** What processes are used to sanitise the storage media storing my data at its end of life, and are the processes deemed appropriate by the ASD ISM?

g. **Vendor's remote monitoring and management.** Does the vendor monitor, administer or manage the computers that store or process my data? If yes, is this performed remotely from foreign countries or from Australia? Can the vendor provide patch compliance reports and other details about the security of workstations used to perform this work, and what controls prevent the vendor's employees from using untrustworthy personally owned laptops?

h. **My monitoring and management.** Can I use my existing tools for integrity checking, compliance checking, security monitoring and network management, to obtain visibility of all my systems regardless of whether these systems are located locally or in the cloud? Do I have to learn to use additional tools provided by the vendor? Does the vendor even provide such a mechanism for me to perform monitoring?

i. **Data ownership.** Do I retain legal ownership of my data, or does it belong to the vendor and may be considered an asset for sale by liquidators if the vendor declares bankruptcy?

j. **Gateway technologies.** What technologies does the vendor use to create a secure gateway environment? Examples include firewalls, traffic flow filters, content filters, antivirus software and data diodes where appropriate.

k. **Gateway certification.** Is the vendor's gateway environment certified against government security standards and regulations? For example, several major vendors in Australia use gateways certified by ASD for data classified up to IN-CONFIDENCE, PROTECTED and in some cases HIGHLY PROTECTED.

l. **Email content filtering.** For email Software as a Service, does the vendor provide customisable email content filtering that can enforce my agency's email content policy? For example, an agency may have a "blacklist" email policy of "No executable email attachments allowed" or better yet a "whitelist" policy of what is allowed (such as .doc .pdf .ppt .xls .jpg and .zip files containing the previously mentioned file types) and everything else is blocked by default. Spam filtering is not necessarily email content filtering, since unsolicited commercial spam email is not inherently malicious, and affects employee productivity instead of the security of the agency's computer network.

m. **Policies and processes supporting the vendor's IT security posture.** Can I have details of how the vendor's computer and network security posture is supported by policies and processes including threat and risk assessments, ongoing vulnerability management, a change management process that incorporates security, penetration testing, logging and regular log analysis, use of security products endorsed by the Australian Government, and compliance with Australian government security standards and regulations?

n. **Technologies supporting the vendor's IT security posture.** Can I have details of how the vendor's computer and network security posture is supported by direct technical controls including timely application of security patches, regularly updated antivirus software, defence in depth mechanisms to protect against unknown vulnerabilities, hardened operating systems and software applications configured with the strongest possible security settings, intrusion detection and prevention systems, and data loss prevention mechanisms?

o. **Auditing the vendor's IT security posture.** Can I audit the vendor's implementation of security measures, including performing scans and other penetration testing of the environment provided to me? If there is a justifiable reason why auditing is not possible, which reputable third party has performed audits and other vulnerability assessments? What sort of internal audits does the vendor perform, and which compliance standards and other recommended practices from organisations such as the Cloud Security Alliance are used for these assessments? Can I thoroughly review a copy of recent resulting reports? For example, a major vendor in Australia advertises that it uses "ISO 27001 accredited data centres which can be audited by you and your regulators".

p. **User authentication.** What identity and access management systems does the vendor support for users to log in to use Software as a Service? Examples include two factor authentication, synchronisation with the agency's Active Directory and other federated single sign-on.

q. **Centralised control of data.** What user training, policies and technical controls prevent my agency's users from using unapproved or insecure computing devices without a trusted operating environment to store or process sensitive data accessed using Software as a Service?

r. **Vendor's physical security posture.** Does the vendor use physical security products and devices that are endorsed by the Australian Government? How is the vendor's physical data centre designed to prevent the tampering or theft of servers, infrastructure and the data stored thereon? Is the vendor's physical data centre accredited by an authoritative third party? For example, several major vendors in Australia advertise using data centres accredited by the Australian Security Intelligence Organisation T4 Protective Security Section.

s. **Software and hardware procurement.** What procurement process is used to ensure that cloud infrastructure software and hardware has been supplied by a legitimate source and has not been maliciously modified in transit?

Protecting Data from Unauthorised Access by the Vendor's Customers

21. Answers to the following questions can reveal mitigations to help manage the risk of unauthorised access to data by the vendor's other customers:

a. **Customer segregation.** What assurance do I have that the virtualisation and "multi-tenancy" mechanisms guarantee adequate logical and network segregation between multiple tenants, so that a malicious customer using the same physical computer as me cannot access my data? For Infrastructure as a Service, the virtualisation software used to share hardware and provide each customer with their own operating system environment was typically not originally designed to provide segregation for security purposes. However, the developers of such virtualisation software are increasingly focusing their efforts on making their software more suitable for this purpose. What controls are in place to detect and prevent a tenant exploiting a publicly unknown or unpatched vulnerability in a hypervisor? For Software as a Service, the logical separation between customers is usually less well defined, and in some cases the separation mechanism may be retrofitted to an existing software application such as email server or database software. For example, in December 2010 a major vendor of Software as a Service admitted that a configuration mistake caused a security breach that resulted in the exposure of "offline" email address books belonging to customers, and confirmed there was unauthorised access by the vendor's other customers.

b. **Weakening my security posture.** How would using the vendor's cloud infrastructure weaken my agency's existing network security posture? Would the vendor advertise me as one of their customers without my explicit consent, thereby assisting an adversary that is specifically targeting me? For example, an adversary could use cloud infrastructure from the same vendor used by the target agency, to both serve malicious web content to the agency's users, and to exfiltrate the agency's sensitive data. This may enable an adversary to circumvent the agency's use of security technologies such as whitelisting which domains and IP address ranges can be accessed, and which web sites can run active content such as javascript in the web browser.

c. **Dedicated servers.** Do I have some control over which physical computer runs my virtual machines? Can I pay extra to ensure that no other customer can use the same physical computer as me e.g. dedicated servers or virtual private cloud?

d. **Media sanitisation.** When I delete portions of my data, what processes are used to sanitise the storage media before it is made available to another customer, and are the processes deemed appropriate by the ASD ISM? For example, a vendor advertises that when a customer deletes data, "the physical space on which the data was stored is zeroed over before the space is re-used by other data".

Protecting Data from Unauthorised Access by Rogue Vendor Employees

22. Answers to the following questions can reveal mitigations to help manage the risk of unauthorised access to data by rogue vendor employees:

a. **Data encryption key management.** Does the vendor know the password or key used to decrypt my data, or do I encrypt and decrypt the data on my computer so the vendor only ever has encrypted data?

b. **Vetting of vendor's employees.** What personnel employment checks and vetting processes does the vendor perform to ensure that employees are trustworthy? Examples include thorough police background checks, as well as citizenship checks, security clearances and psychological assessments especially for employees with administrative privileges or other access to customer data. For example, in September 2010 a major vendor acknowledged sacking an employee for allegedly deliberately violating the privacy of users by inappropriately reading their electronic communications during a timeframe of several months.

c. **Auditing vendor's employees.** What robust identity and access management system do the vendor's employees use? What auditing process is used to log and review the actions performed by the vendor's employees?

d. **Visitors to data centre.** Are visitors to data centres escorted at all times, and is the name and other personal details of every visitor verified and recorded?

e. **Physical tampering by vendor's employees.** Is network cabling professionally installed to Australian standards or internationally acceptable standards, to help avoid the vendor's employees from accidentally connecting cables to the wrong computers, and to help readily highlight any deliberate attempts by the vendor's employees to tamper with the cabling?

f. **Vendor's subcontractors.** Do the answers to these questions apply equally to all of the vendor's subcontractors?

Handling Security Incidents

23. Answers to the following questions can reveal a vendor's ability to handle security incidents:

    a. **Timely vendor support.** Is the vendor readily contactable and responsive to requests for support, and is the maximum acceptable response time captured in the SLA or simply a marketing claim that the vendor will try their best? Is the support provided locally, or from a foreign country, or from several foreign countries using an approach that follows the sun? What mechanism does the vendor use to obtain a real-time understanding of the security posture of my use of the vendor's services so that the vendor can provide support?

    b. **Vendor's incident response plan.** Does the vendor have a security incident response plan that specifies how to detect and respond to security incidents, in a way that is similar to incident handling procedures detailed in the ASD ISM? Can I thoroughly review a copy?

    c. **Training of vendor's employees.** What qualifications, certifications and regular information security awareness training do the vendor's employees require, to know how to use the vendor's systems in a secure manner and to identify potential security incidents?

    d. **Notification of security incidents.** Will the vendor notify me via secure communications of security incidents that are more serious than an agreed threshold, especially in cases where the vendor might be liable? Will the vendor automatically notify law enforcement or other authorities, who may confiscate computing equipment used to store or process my data?

    e. **Extent of vendor support.** How much assistance will the vendor provide me with investigations if there is a security breach such as an unauthorised disclosure of my data, or if there is a need to perform legal electronic discovery of evidence?

    f. **My access to logs.** How do I obtain access to time synchronised audit logs and other logs to perform a forensic investigation, and how are the logs created and stored to be suitable evidence for a court of law?

    g. **Security incident compensation.** How will the vendor adequately compensate me if the vendor's actions, faulty software or hardware contributed to a security breach?

    h. **Data spills.** If data that I consider is too sensitive to be stored in the cloud is accidentally placed into the cloud, referred to as a data spill, how can the spilled data be deleted using forensic sanitisation techniques? Is the relevant portion of physical storage media zeroed whenever data is deleted? If not, how long does it take for deleted data to be overwritten by customers as part of normal operation, noting that clouds typically have significant spare unused storage capacity? Can the spilled data be forensically deleted from the vendor's backup media? Where else is the spilled data stored, and can it be forensically deleted?

Further Information

The Australian Commonwealth accepts no liability for the content on external third party web sites that contain additional information:

a. Australian Signals Directorate – *Australian Government Information Security Manual*
   http://www.asd.gov.au/infosec/ism
b. AGIMO - *Cloud Computing Strategic Direction Paper*
   http://www.finance.gov.au/cloud/
c. Attorney-General's Department - *Protective Security Policy Framework*
   http://www.protectivesecurity.gov.au/Pages/default.aspx
d. National Institute of Standards and Technology - *Cloud Computing*
   http://csrc.nist.gov/groups/SNS/cloud-computing
e. European Network and Information Security Agency
   Cloud Computing Security Risk Assessment
   http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
   Security and Resilience in Governmental Clouds
   http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds
f. Cloud Security Alliance
   Security Guidance
   http://www.cloudsecurityalliance.org/guidance
   Top Threats to Cloud Computing
   http://www.cloudsecurityalliance.org/topthreats.html
   Governance, Risk Management and Compliance Stack
   http://www.cloudsecurityalliance.org/grcstack.html
g. Delimiter - *The Australian Private Cloud: Who Sells It?*
   http://delimiter.com.au/2010/10/26/the-australian-private-cloud-who-sells-it
h. Torry Harris – *Cloud Computing Services: A Comparison*
   http://www.thbs.com/knowledge-zone/comparison-of-cloud-computing-services
i. CloudHarmony - *Cloud Speed Test*
   http://www.cloudharmony.com/speedtest
j. Web Hosting Talk
   http://www.webhostingtalk.com
   http://www.webhostingtalk.com.au

Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.