CLOUD COMPUTING AND VIRTUALISATION: TWO YEARS ON

Overview

In 2009, BCS hosted a Thought Leadership Debate on the subject of cloud computing and what the future might hold. Not unsurprisingly, all the issues identified were within the realm of our understanding and expectation at the time, although the full impact of the economic crisis was still not bedded in at the time. Since then, more realignments, reductions, maintenance freezing and a lack of investment are threatening many IT infrastructures. This level of restriction has increased the uptake of the cloud in a mainly misguided perception that it is the panacea for all possible IT management woes. This paper will revisit some of the issues and present an update.

Given all that we have learnt in the IT industry over the decades, it is disappointing to find the headlong progression into the cloud has been without, necessarily, a determined effort to build security in from the outset. We (the security profession) were still left on the outside of the original discussions and so we find ourselves playing catch up - in spite of there being many movements around the ethos of ‘build security in’, ‘privacy by design’ and ‘baking security in’.

Cloud anatomy

The cloud is a term used to describe the totality of the infrastructure, hardware, software, services, access, connectivity and all of the other elements required to host and deliver cloud computing services to subscribers.

Cloud computing is a model for enabling 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 (NIST).

Cloud computing solutions are deployed in one of four models:

1. Private cloud – where the cloud infrastructure is operated solely for an organisation. It may be managed by the organisation or a third party and may exist on-premises or off-premises.
2. Public cloud – where the cloud infrastructure is made available to the general public or a large industry group and is owned by an organisation selling cloud services.
3. Community cloud – where the cloud infrastructure is shared by several organisations and supports a specific community that has shared concerns such as mission, security requirements, policy, and compliance considerations. It may be managed by the organisations or a third party and may exist on-premises or off-premises.
4. Hybrid cloud – where the cloud infrastructure is composed of two or more clouds; such as a private cloud and a community or public cloud, that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability such as cloud bursting for load-balancing between clouds.

Almost 50 per cent of servers will be virtualised by 2012 (Gartner)
Virtualisation explained

Virtualisation is the creation of a virtual (rather than actual) version of something, such as a hardware platform, operating system, a storage device or network resources.

Multiple operating systems can run simultaneously on a single physical machine, sharing the resources of that machine.

It is a reduction strategy - reducing spend, energy usage and space utilisation.

Virtualisation options include:

- Migrate security and traffic management policies from physical to virtual infrastructures;
- Cost savings from reduction in physical network infrastructure and optimal use of servers;
- Securely connect physically separate data-centers and cloud networks;
- Simplify migration of applications to the cloud.

Types of Virtualisation

Currently, most of the activity in the virtualisation world focuses on server virtualisation - the data-centres or server farms. The three main types of server virtualisation are:

1. Operating system virtualisation (aka containers): Creates self-contained representations of underlying operating system in order to provide applications in isolated execution environments. Each self-contained environment (container) reflects the underlying operating system version and patch level.
2. Hardware emulation: Represents a computer hardware environment in software so that multiple operating systems can be installed on a single computer.
3. Paravirtualisation: A thin software layer that coordinates access from multiple operating systems to underlying hardware.

Major Players and Products in Virtualisation

This list represents some of the major players in virtualisation:

- VMware: Provides hardware emulation virtualisation products called VMware Server and ESX Server.
- XenSource: The commercial sponsor of Xen. Provides products that are commercial extensions of Xen focused on Windows virtualisation. XenSource was recently acquired by Citrix.
- OpenVZ: An open source product providing operating system virtualisation. Available for both Windows and Linux.
- SWsoft: The commercial sponsor of OpenVZ. Provides a commercial version of OpenVZ called Virtuozzo.
- OpenSolaris: The open source version of Sun's Solaris operating system provides operating system virtualisation and will also provide Xen support in an upcoming release.
Cloud and Virtualisation concerns

In spite of significant industry rhetoric and marketing hype, many organisations are reluctant to adopt cloud services and technology because of concerns over information security and a loss of control of their IT delivery. These fears were exacerbated in 2011 by news of outages by Amazon and the three-day loss of Blackberry services from RIM.

Cloud and virtualisation come together when the IT infrastructure is ultimately the same as the existing server environment only it has been virtualised and is being operated from a third party managed data centre running on Windows and Linux, with Windows and Linux vulnerabilities. Specific virtualisation concerns include needing to understand the method of virtual implementation. For example, in a credit card processing environment, or indeed any environment where important and sensitive information is being stored, processed or transmitted, logical segregation of virtual servers is required just as there would be physical separation with real servers. Where a consumer's environment is not logically or physically discrete from other consumers, all other consumers’ environments must be made compliant. Policy management needs to be well controlled across the virtualised environment in order to identify and distinguish each virtual machine and the information contained thereon. Assurance is needed that memory released by one guest using that storage is not disclosing content to the receiving guest servers using the same addresses.

Cloud providers can offer ‘virtual private servers’ (VPS). Each VPS:

- has its own processes, users, files and provides full root access;
- can have its own IP addresses, port numbers, tables, filtering and routing rules;
- can have its own system configuration files and can house an application;
- can have its own versions of system libraries or modify existing ones.

A VPS is not a virtual machine - it runs the same operating system (OS) as the root OS - Linux on Linux, etc. This is also known as operating system-level virtualisation.

Vulnerabilities with concurrent virtualisation still exist because security has not been built into the design process in all cases nor understood in a skills sense by those involved. Lower entry cost still does not necessarily mean lower life cost, or lower compliance management nor evidence costs.

Two years ago, we were clear that managing this landscape would require the following to be brought into scope of thinking:

- Restitution and redress;
- Jurisdiction;
- Responsiveness;
- Availability.

Various useful resources have been produced in the interim to help fill the gap of understanding. In particular, the ENISA Cloud Risk Assessment, which identified the following cloud related risks:

- Loss of Governance;
- Compliance Challenges;
- Changes of Jurisdiction;
- Isolation Failure;
- Cloud provider - malicious insider - privilege abuse;
- Management Interface compromise;
- Data Deletion Risks;
- Network Management.

And the Cloud Security Alliance, which identified some top threats that were in keeping, but more technically focused:

- Abuse and Nefarious Use of Cloud Computing;
- Insecure Application Programming Interfaces;
- Malicious Insiders;
- Shared Technology Vulnerabilities;
- Data Loss/Leakage;
- Account, Service and Traffic Hijacking.

Key risks to be managed in the virtualisation environment include:

- Rogue VMs;
- Mixture of VMs of different sensitivities on the same host;
- Falling out of compliance with software licence requirements;
- More entry points for attackers;
- Unauthorised software.

The single biggest vulnerability of virtual machines (VMs) is due to the ease in which users can create many VMs, which become very difficult to secure, monitor, and maintain. The effective change and configuration management processes so vital to physical infrastructure become even more critical with virtual infrastructure, as employees introduce potential risk by creating, using and de-provisioning virtual systems all within a short period of time.

Security requirements understanding for virtual environments is believed to not be mature - and yet at its core, security requirements don’t change drastically in a virtual environment. Security can be addressed by revisiting all the existing control areas in which it is known to impact:

- Patch management;
- Change management;
- Backup;
- Audit and monitoring;
- Firewalls;
- Incident response and forensics;
- Intrusion detection / prevention;
- Network access control;
- BCP;
- Antivirus.

They simply need to be adapted to work effectively for the environment, the requirements and the information assets that require protecting.

Securing virtualised environments requires:

- Understanding where and how virtualisation is used;
- Creation and enforcement of policy and standards;
- Selection of controls using defence in depth;
- Integrating virtualisation into change and vulnerability management;
- Auditing and enforcement.
Cloud Responsibilities

Cloud governance and compliance. Governance defines who’s responsible for what and the policies and procedures that your people or groups need to follow. Cloud governance requires governing your own infrastructure as well as infrastructure that you don’t totally control. Cloud governance has two key components: understanding compliance and risk and business performance goals.

There are risks that need to be managed and, at minimum, there is a significant amount of due diligence required by the customer of the service being sought or offered, to include:

- Fully specify Security Service Levels to address all of the following:
  - Data protection;
  - Compliance and e-discovery;
  - Integrity and confidentiality of data;
  - Availability and reliability of services;
  - Portability and interoperability of cloud services;
  - Infrastructure and network security;
  - Exit strategy: retrieval/destruction of data when service terminated.

- Clear division of liabilities and responsibilities (see table below for a ‘starter for ten’) - all of which depend upon the service model chosen (SaaS, PaaS or IaaS)

- Ask questions (see separate section below)

<table>
<thead>
<tr>
<th></th>
<th>Customer</th>
<th>Cloud Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawfulness of content</td>
<td>Full liability</td>
<td>Intermediary liability</td>
</tr>
<tr>
<td>European Data Protection Law status</td>
<td>Data controller</td>
<td>Data processor (external)</td>
</tr>
<tr>
<td>Identity &amp; Authentication</td>
<td>Own users and federation agreements with partners</td>
<td>Users required to manage the provided infrastructure</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Own infrastructure</td>
<td>Cloud service infrastructure (server, storage, bandwidth etc)</td>
</tr>
<tr>
<td>Security Management</td>
<td>Guest systems (IaaS)</td>
<td>Host systems and applications security policy, hardening, patching and monitoring</td>
</tr>
</tbody>
</table>

Skills and Competencies

The requirement for skills (and cries of apparent dearth) is constantly being referred to in the IT industry and beyond. With regard to cloud skills, there is even a specific website for this area - http://www.cloudskills.com/. In reality, it is important to see this for what it is - an amazingly resilient ability to turn an industry to meet an apparent customer demand - as opposed to what the customer really needs at the moment, in an austere environment - decent translation of the requirements and the ability to understand what is different compared to current working arrangements and therefore what the skills gap really is.

What is needed are security aware technical architects who can design the systems properly
from the outset and who will therefore be specialising in server virtualisation or cloud computing. Other skills that will be important to the cloud specialist will be project management, delivery capabilities and an understanding of project life cycles, which should be overlaid on the security development life cycle (SDLC). An understanding of how technology impacts the business is vital.

The following are job roles and skills the IT professional can invest in (according to Microsoft):

- **Business liaison**: Move skills up the stack in the decision process. Hone expertise to the business from within IT. Move into design and architecture roles. Determine whether to focus in-house or off-premises, define options whether the organisation decides to stay on-premises or moves to the cloud. Embrace change management and risk management.
- **Data-centre manager**: Reposition data-centre skills toward the hosted data-centre. Enhance automation skills. Work in standardised environments and with standardised applications as an option. Become good at management applications, scripting, and performance optimisation. Acquire best practices skills, such as information services technology management.
- **Security specialist**: Help businesses move core business processes and data securely to private, public, or hybrid cloud solutions. Security specialists need to stay abreast of new security models and technologies, such as data protection, privacy standards, securing message integrity (encryption, digital signing and malware protection), federated identity management, authentication methods, auditing and legislative / regulatory / standards compliance requirements.
- **Software architect**: Serve as a link between the organisation’s technical and business staff. Architects are asked to design and build complex distributed systems that exist both outside and inside an enterprise and the cloud. They need to acquire the new skills required to build infrastructure, platform, and software clouds. They need to understand how to design and construct multi-tenant and virtualised systems that can manage thousands of simultaneous users and isolate higher levels of the stack from physical component failures.

Other technical skills include:

- **Infrastructure skills** are also required in order to determine basic infrastructure requirements such as directory synchronisation, mail routing and namespace planning, Active Directory Federation Services, DNS, bandwidth, etc.
- **Migration and integration skills** - you will still manage your users and their mailboxes. Industry-specific data retention compliance, as well as implementing custom workflows, remains a responsibility.
- **Hybrid deployment skills** to determine coexistence and maintenance strategy between on-premises systems and the cloud.

From a business perspective, ask the following questions:

1. Which process, application and information can be moved to the cloud to gain efficiency and cost benefits while satisfying the organisation’s security and compliance requirements?
2. How can the organisation be harmed if systems, applications, services or information are accessed by unauthorised people and information is being made available to the public?
3. How are information and systems protected against unauthorised access (e.g. hacking, interception, user misuse) by the cloud service provider?
4. How can the organisation ensure the integrity, authenticity and reliability of information stored in the cloud?
5. What are the organisation’s responsibilities regarding the security of infrastructure and information in the cloud for the chosen cloud service and deployment models?
6. How can the organisation apply its records and information management programmes (e.g.
classification, retention) to the cloud environment?

7. What is the impact of outsourcing services and information to the cloud on the legislative and regulatory requirements of the organisation (e.g. DP, FOI, SOX, e-discovery, copyright, licensing etc.)?

8. How should the organisation audit and monitor cloud services and establish relevant service level agreements?

9. Will the organisation be able to negotiate contracts and agreements that fit their risk assessment and compliance environment?
   a) What are the total costs of setting up and managing the cloud services?
   b) In which format is information created, transferred and stored in the cloud?
   c) What implication does the format of information in the cloud have for access, retrieval and preservation?
   d) What metadata can be applied to information stored in the cloud and can it be managed and searched?
   e) Are there procedures to provision access and usage rights to information stored or processed in the cloud?
   f) How can retention schedules be applied to information stored in the cloud (e.g. manually, through the provider’s user interface, via metadata) and at what level?
   g) How will information be destroyed by the cloud provider (e.g. shredding of drives, deletion of nodes, crypto-shredding)?
   h) Is the destruction method in line with the compliance requirements of the organisation?

From a technical perspective, ask the following questions:

1. How is identity and access managed in the cloud?
   • What extra security is provided to protect remote management capabilities?
   • What forms of authentication are used for management interfaces?
   • How is the management interface monitored?
   • Does the system allow for a federated IDM infrastructure which is interoperable both for high assurance and low assurance (e.g. username and password)?
   • Is the cloud provider interoperable with third party identity providers?
   • Is there the ability to incorporate single sign-on?
   • Does the client credential system allow for the separation of roles and responsibilities?
   • Is there mutual authentication?

2. Where will my data be geographically located?
   • In what country is the cloud provider located?
   • Where is the cloud provider’s infrastructure located?
   • Will the cloud provider use other companies whose infrastructure is located outside that of the cloud provider?
   • Where will the data be physically located?
   • Will any of the cloud provider’s services be subcontracted out or outsourced?
   • What happens to the data upon termination of the contract?
   • Do you rely on data dispersal algorithms?

3. How securely is my data handled?
   Can the provider:
   • Detail policies and procedures for backup? These should include procedures for the management of removal.
   • Detail the steps taken to ensure that data which has been deleted is completely wiped and cannot be accessed by other service users.
   • Ensure that devices containing sensitive information are physically destroyed or overwritten using techniques to make the original information non-retrievable.

4. How is access by privileged users controlled?
   • What checks are made on the identity of users with privileged access?
   • Are there different levels of identity checks based on the resources accessed?
What processes are in place for de-provisioning privileged credentials?
Are privileged credentials provisioned and de-provisioned simultaneously throughout the cloud system?

5. How is my data protected against privileged user abuse?
   - Do any accounts have system-wide privileges for the entire cloud system and, if so, for what operations?
   - How are the accounts with the highest level of privilege authenticated and managed?
   - How are privileged actions monitored and logged?
   - What recorded events result in action being taken?
   - What controls are employed to protect logs from unauthorised access or tampering?
   - What method is used to check and protect the integrity of audit logs?

6. What levels of isolation are supported?
   - What levels of isolation are used for virtual machines, physical machines, network, storage, management networks and management support systems?
   - Provide information on how multi-tenanted applications are isolated from each other.

7. How is my data protected in virtual environments?
   - PCI DSS specifies ‘one function per server’. This is taken by some auditors to limit virtualisation. Are virtual images hardened by default?
   - Is the hardened virtual image protected from unauthorised access?
   - Confirm that the virtualised image does not contain the authentication credentials.

8. How are the systems protected against internet threats?
   - Define the controls used to mitigate distributed denial–of-service (DDoS) attacks.
   - Do you have defences against internal as well as external threats?
   - Does architecture support continuous operation?
   - Is the network infrastructure secured to best practice specific standards (e.g. are MAC spoofing, ARP poisoning attacks etc prevented)?
   - Verify compartmentalisation of systems, networks, management, provisioning and personnel.
   - Verify providers patch management policies and procedures. These should be reflected in the contract.

9. How are activities monitored and logged?
   - What information is recorded in audit logs?
   - For what period is this data retained?
   - How is data segmented within audit logs so it can be made available to the end customer and/or law enforcement without compromising other customers?
   - How are audit logs reviewed?
   - What recorded events result in action being taken?
   - How is accurate event time stamping provided?

10. What kind of information security certification does the provider have?
    - Does the cloud provider comply with best practice?
    - Are they certified?

**Approaches**

Managing cloud services requires a clear picture of:

- the information management processes that need to be performed in the cloud;
- the compliance environment in which the organisation and the cloud provider operate;
- the specific contractual terms that relate to outsourcing to the cloud;
- the total cost involved in moving information and processes into the cloud;
- the strategies needed to ensure a seamless exit from cloud services.

As with any other IT strategic infrastructure plan, it is important to tackle some basic steps to identify and scope requirements rather than progressing headlong into a cloud or virtualisation
Planning for virtualisation:

- Evaluate your current server workloads - determine what your potential virtualisation use cases might be.
- Define your system architecture - what form of virtualisation will you use, and what kind of use case do you need to support?
- Select your virtualisation software and hosting hardware - evaluate the virtualisation software's capabilities to ensure that it supports your use cases. Be sure to look at the new virtualisation-enabled hardware systems.
- Migrate your existing servers to the new virtualisation environment - decide whether migration products can help you move your systems or if you need to move them manually - in either case, create a project plan to ensure everything is covered.
- Administer your virtualised environment - decide whether the virtualisation product management tools are sufficient for your needs or whether you should look to more general system management tools to monitor your environment.

Planning for the cloud

1. Preparing for the cloud
   a) Information classification - it may be that you have information that cannot be housed in any situation other than a safe and secure internally managed one - but you won’t know this until you identify, label and classify all your information assets.
   b) Risk assessment - is therefore a necessary step.

2. Operating in the cloud
   a) Security;
   b) Availability;
   c) Identity and access management;
   d) Monitoring, auditing and reporting.

Use the various toolkits now available:

- Virtual machine benchmarking guidelines from Center for Internet Security, benchmarks.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf
- Utilise the resources available from the Cloud Security Alliance (CSA) - https://cloudsecurityalliance.org/research/grc-stack/ including the Cloud Controls Matrix - https://cloudsecurityalliance.org/research/ccm/

Future Potential

As a result of a singular lack of understanding and cohesion between the sales forces, the technology implementers and the security professionals, we find ourselves at the apex of a dilemma. In all likelihood, there will be more data breaches as the reality of the dream that has been sold comes to fruition and the level of unmanaged and unmaintained infrastructure exacerbated by the economic crisis increases exponentially, at the expense of client data, trust
and the brand and reputation of a number of key infrastructure providers. Whatever is signed up
 to in contracts needs to be being matched by real, meaningful, professional delivery of a holistic
 service that can be evidenced across the governance, risk and compliance (GRC) frameworks
 that need to be in place.

**Conclusions**

Security depends on knowledge of virtualisation and technology for both installation and audit. It
depends on professionals determinedly pushing forward the need to adhere to best practice and
well honed principles. There's no real change there - but there is a real need to understand the
risks better.
<table>
<thead>
<tr>
<th>Annex 1</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td>Definitions in this area are helpful. The ones provided below are by no means universally accepted, but they are relevant to the issues described above.</td>
</tr>
<tr>
<td><strong>Bare Metal</strong></td>
<td>Virtualised servers in which the virtualisation software is installed directly on the machine rather than on an operating system. Because it installs on the machine, it is said to reside on ‘bare metal.’</td>
</tr>
<tr>
<td><strong>Client virtualisation</strong></td>
<td>Using virtualisation to enable a client device (like a laptop) to support isolated operating environments. Client virtualisation is often used to move workloads into isolated environments to reduce system administration requirements.</td>
</tr>
<tr>
<td><strong>Cloud computing</strong></td>
<td>A pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST)</td>
</tr>
<tr>
<td><strong>P2V</strong></td>
<td>Shorthand for ‘physical to virtual’ P2V stands for the process of migrating systems from the physical hardware they originally ran on to virtual operating environments running in a virtualised environment.</td>
</tr>
<tr>
<td><strong>Server virtualisation</strong></td>
<td>Running virtualisation software on server machines in order to host multiple operating system environments on a single piece of hardware.</td>
</tr>
<tr>
<td><strong>Storage virtualisation</strong></td>
<td>Using shared storage located on individual servers so that multiple servers can share a single storage device. Storage virtualisation is often implemented after initial server virtualisation efforts in order to centralize resources and reduce storage administration work.</td>
</tr>
</tbody>
</table>
References

Mike Small, ‘Is cloud computing worth the hassle?’


Cloud Security Alliance, ‘Top Threats to Cloud Computing V1.0’

vmware, ‘Harness the Full Potential of High-Performance IT Hardware’


vmware, ‘Security Design of the VMware Infrastructure 3 Architecture’

McAfee, ‘Virtualization, Security and compliance for virtualized environments’


Chan, Jason; ‘Virtualization: IT Audit and Security Perspectives’ ISACA-SV Spring 2010 Conference

Chaudhuri, Abhik; von Solms, SH (Basie); Chaudhuri, Dipanwita; ‘Auditing Security Risks in Virtual IT Systems’, ISACA Journal volume 1, 2011

Dai Zovi, Dino A, ‘Hardware Virtualization Rootkits’, Black Hat USA 2006

Kirch, Joel, ‘Virtual Machine Security Guidelines’


Williams, Brian; Cross, Tom; ‘Virtualisation System Security’, 2010, IBM (VirtualizationSecurity.pdf)

