swiss security exchange

powered by Microsoft

Security in the Cloud

Sandy Porter
Strategy & Business Development Director
Avoco Secure

Agenda

swiss security exchange
powered by Microsoft

- Security in the Cloud

Positioning Security as an issue

swiss security exchange
powered by Microsoft

- A survey in August 2008 of business users and CIOs ascribed to the Cloud that the greatest challenge/ issue is security.

- SC congress in New York in December 2008: Two of the Jericho forum founding members strongly advocated that security must be addressed before you deploy any data in the Cloud.

Benefits from Cloud Computing

swiss security exchange
powered by Microsoft

- Quick, Cheap and Easy to Deploy
- Pay only for what you use
- Reduce internal IT cost
- Latest up to date software
- Sharing of systems
- Data sharing is simpler

Challenges for Cloud Computing

swiss security exchange
powered by Microsoft

- Security
- Privacy of Data
- Performance
- Availability
- Integration with internal systems
- Increased cost
- Regulatory requirement issues
- Data recovery

Drivers behind attacks

- Emerging cyber threats has identified that financial gain is the main driving force behind Web 2.0 attacks in the guise of, theft of private data, interception of web transaction and corporate espionage.

- Applications and data are moving off the PC and into the Cloud, more threats and attacks will follow.

Attack vectors

- Existing major attack vectors apply and some others are either created or escalated in importance.

- In the Cloud attacks issues include:

  – Larger attack surfaces, More exit and entry points, SaaS integration over the wire, Mash-ups - a web application that combines data from more than one source into a single integrated tool, Web Services interfaces e.g. - Browser vulnerabilities - Denial of Service, Data and Services could be anywhere, 3rd party data administrators access, Open Source software implementations, Shared documents, Virtualization of desktop and servers, “rogue” government data access, multiple customers running on one hosted web server/ database/ code version (multi-tenancy), etc…

- Which means:

  – They can be harder to manage in some cases and far more devastating in nearly all circumstances.

  – Conversely in some cases easier to manage or apply protection against.

  – The Cloud has the potential to avoid or recover from some attacks but make others more potent.

Malicious Attacks

swiss security exchange
powered by Microsoft

- Malicious attacks like Denial of Service has the potential to devastate.
- DOS could be instigated against infrastructure e.g. undersea cables, ISPs etc…which are outside your control.
- Answers?
  - A hybrid environment of cloud and desktop – accessing backed up data locally.
  - A dynamic secondary cloud infrastructure.
  - The requirement to make this seamlessly work is dynamic security layer applied to information which bridges these environments.

Cloud “Outsource” issue

- 3rd party data administrators access.
- Hosted anywhere in the world and in multiple tenancy environments.
- Failure to meet regulatory requirements for privacy or regulation.
- Failure of the provider.
- Unknown application stacks.
  - Conventional Outsourcing has strong SLAs and you should know where your data should be stored.

Data leakage

- Data is in a De-perimeterized environment in the Cloud.
- Insiders and outsiders unauthorised access to information is a high risk.
- Secure collaboration in the Cloud is a must and achieving will add real value.
- How can you address this and unlock value in the cloud?

An example of how the Cloud justified potential value before it truly existed

swiss security exchange
powered by Microsoft

- The 2004 Tsunami severed 5 out of 7 major undersea Telco cables.
- Some major financial institutions lost the ability to trade for 5 days.
- In one case compliance in one institution vetoed the use of another financial group's partially operating infrastructure to execute trades.
- The two options were send by courier on planes or use coded messages via Webmail.
  - A cloud application was still running when the critical infrastructure was down.
  - The major issue for the institution was who could see, access and utilise the data in the Webmail mails.
  - This raises the question: How do you generate *enough* **Trust** to place valuable in the Cloud?

Trusted sharing of confidential information in the Cloud

swiss security exchange
powered by Microsoft

- Within the Cloud, data must be considered in a new way.
  - Previously static data that did not get disseminated.
  - Data is now dynamic in an environment encompassing distributed computers and distributed citizens.
  - In a Cloud environment, the ability to link dynamic security **policies** to **identity, geographic location, audit** and **information** is a key enabling factor in creating solutions that will persistently secure and control that information.

Identifying Users in the Cloud

- New types of digital identity being developed
  - Follow Cloud model of geographic / location independence
- More liberating than existing desktop/device based methods (e.g. Smart card certificates)
  - But can utilise these systems to add security
- Examples include OpenID initiative and Information Cards such as Windows CardSpace
  - Windows CardSpace can act in both desktop and Cloud domains
  - Issue around security for OpenID

Controlling where data can be accessed in the Cloud

- New types of geographic controls linked to data are being developed.

- Data can access can already be limited to a:
  - room,
  - building,
  - zip/post code,
  - city,
  - country etc…

An example of applying security to data in the Cloud

swiss security exchange
powered by Microsoft

- The flexibility required by such a system becomes inherent by encapsulating the data as a protected, independent entity.

- This flexibility is multiplied many times by the linking of an identity to security policy, to control the access and use of the content.

- This linkage ensures that even if re-directed, accidentally or maliciously, or taken out of residence, access to the content will be prevented without the correct access token.

Summing up the components required to successfully protect encapsulated data:

- The data itself being viewed as a mini container and the protection being an inherent part of this, to create a secured data package.
- This secured data package being un-tethered (independent) and so retaining the natural fluid movement that is a defining aspect of unstructured data.
- Directly linking an identity or identities to the secured data package – setting a policy of belonging to (policy linkage).
- Driving the protection of the data package using policies
  - Applied automatically at any point in the data cycle
  - That can be changed on demand
- Applying an additional layer of controls to the use of the content after access to assure integrity.

Summing up the components required to successfully protect encapsulated data contd:

swiss security exchange
powered by Microsoft

- These elements, built into the process of retaining data, will ensure privacy of the information due to a culture of 'belonging to…' built into the system:

- The security of the data is determined by the encryption and controlled access.

- The integrity is assured by the post access content control layer.

  Identities, geographic location, dynamic policies and claims being utilised to enforce "*where, when, why, who and how data can be accessed.*"

The Cloud opportunity

swiss security exchange
powered by Microsoft

- Cloud-based applications provide a unique opportunity to link identity to an individual resource, such as a cloud-based document.

- Instead of simply relying on access to the cloud to control access to the resources, access to each resource could be controlled regardless of whether it is still in the cloud or grounded, by binding together the resource and identity.

- And, by using the same identity to both access the cloud and access individual resources, the extra security and privacy issues are resolved without detriment to the user experience.

The Cloud opportunity

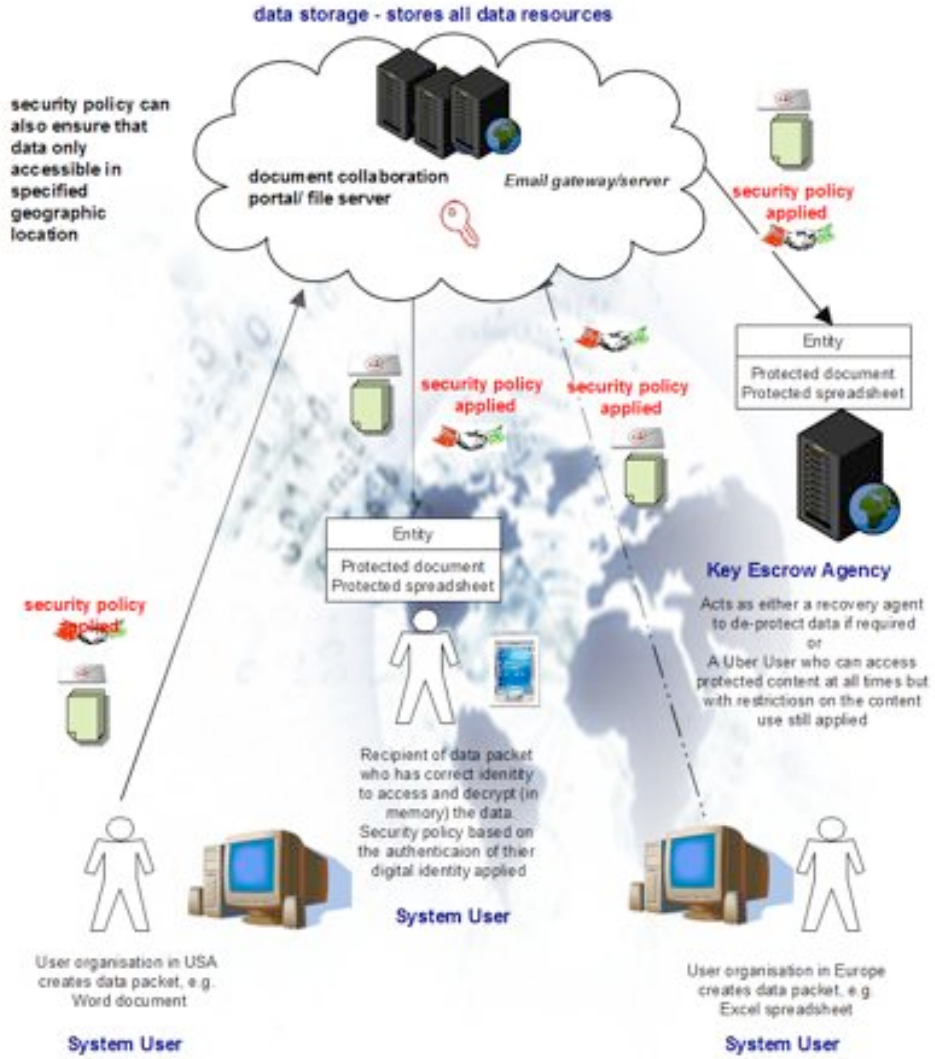
swiss security exchange
powered by Microsoft

- Because of the real-time nature of Cloud based applications, policies associated with content in the Cloud can be changed at any point, and automatically updated to reflect that change.

- This provides powerful workflow control.

- This will enable highly granular control.

An example diagram:



= security policy persistent once applied but can be dynamically updated to reflect changes in data status

Protected = Protection includes, encryption, access control and content usage restricitons (e.g. no copying, no printing, date use restrictions, *etc.* Accessand security policy linked to individual or group identity

data packets can include documents, emails, etc.

Sent using email as a service and content as a service

Important considerations for Cloud security to work.

swiss security exchange
powered by Microsoft

- Control in the Cloud needs to be elastic and extend beyond the Cloud boundaries by using the Cloud itself as a means of controlling information – preventing access of any information downloaded outside of the Cloud.
- Easy to use, interoperable Identities from multiple systems and their management.
- The ‘Chinese walls’ in the cloud are enforced and controlled exclusively by end users and organisations.
- Who should be the Key Escrow agency and where should it be based?
  - key escrow agencies for data are equivalent to banks are for money.
  - The best place for escrow - Switzerland?

Thank you

swiss security exchange
powered by Microsoft

Sandy Porter
sandy.porter@avocosecure.com
+44 (0)791 750 7636
www.avocosecure.com

Data in motion - which may be located anywhere - needs dynamic security - that is seamlessly applied to your information.