Security Issues and Solutions Regarding the use of SaaS/Cloud Computing/Virtual Environments

Jason Cuddy
Vice President Product Development
Via680, LLC
(Formerly BizVeo)
www.via680.com
jcuddy@via680.com

What is intelliSling?

IntelliSling utilizes web-based communication tools to share information with, and collect valuable feedback from peers, employees, customers, and suppliers. It leverages a rich set of web based features and functionality that allow work across a continuum of a variety of types of communication.

Video Communication

Assessments

Analytics

IntelliSLING

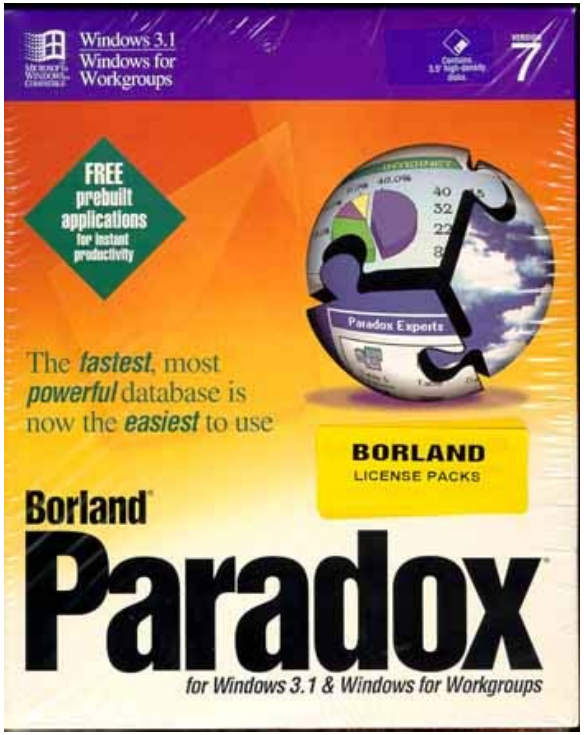
Why Cloud Computing?

- Cost Savings
- Ease of Implementation
- Availability
- Transparency
- Security

What are the advantages and disadvantages?

cupcdvum and the Internet meme

Back in the late 1990's and early 2000's, Borland made this a universal password for all password protected Paradox databases.



cupcdvum and the Internet meme

Lesson learned? No one would do something so short sighted in this age would they?

Facebook hides its privacy from Chuck Norris.

Cost and Resource Savings

Advantages 

- Large costs savings on server hardware and bandwidth.
- Cost savings on office space.
- Cost savings on personnel and IT.
- Off-site backup.
- Easily scalable.

Disadvantages 

- Employees and developers may not know system as well as an internal solution.
- Location of your data.
- Laws and regulations of these locations.
- Accountability if a breach occurs.
- What outside people have access to your data?

Forrester Research – Data Protection Heat Map

Gartner/NetworkWorld – 7 Cloud Computing Security Risks

Steps to take…

- Ensure the solution provider you are working with has experience with HIPAA/HITECH.
- If they do not, or you choose to host yourself, do a thorough security audit.
- Consult with security experts regarding hardware, software, operating systems, and procedures.
- Draft a HIPPA Breach Notification policy and ensure employees and partners are properly trained if a breach should occur. Practice and update it often.

Ease of Implementation

Advantages 

- Customers can be up and running in very little time.
- No need for internal server setups.
- Little to no need for firewall exceptions and other security steps.
- Providers' quickly monitor and patch servers.

Disadvantages 

- Customer expectations can be very high for updates and fixes.
- Dealing with customized solutions for specific customer can be cumbersome.

Steps to take…

- Develop a product road map and stick to it.
- Make your release schedule transparent to your customers.
- Determine the type of organization you are – customer driven, market driven, engineering driven.
- Allow your Product Managers to focus on strategy and your developers to focus on tactics.

Availability

Advantages 

- Availability anytime, anywhere 24/7/365.
- Employees are not limited to geographic locations.
- No need for on-site installs and sales/support staff.

Disadvantages 

- Accessibility means anyone has access.
- Fears that a breach can spread to multiple customer sites.

Steps to take…

- Take advantage of “Gray Hat” consultants. Pay them to break into your system and find your vulnerabilities.
- Although it can cause headaches with updates, consider running each customer’s site in their own virtualized environment.
- Do not share passwords across customers sites.
- Keep thorough logs, and audit your systems frequently. Err on the side of caution and investigate strange entries.

Transparency

Advantages 

- More SaaS solutions feel like desktop programs rather than Internet sites.
- Ability to work from multiple machines and multiple locations.

Disadvantages 

- Solutions can be less robust than desktop counterparts due to browser limitations.
- Externally hosted solutions can hit speed walls.
- Outages affect all customers and employees.

[Computer Weekly – Google Mail Collapses]

Steps to take…

- Look to emulate applications customers and employees are familiar with. Google is a good example.
- Outages can be expected from time to time. The key is to minimize the down time, and reduce the number of customers affected.
- Keep redundancies on various hardware solutions/datacenters, but always know where your data is.
- Develop an outage plan and practice the steps so employees are prepared if an outage occurs.

Security

Advantages 

- Cloud storage keeps everything centralized.
- Employees can travel with blank laptops to eliminate breaches if stolen, confiscated, or lost.
- Workstation failures do not cause data or time loss.

Disadvantages 

- If proper measures aren't taken, data can be exposed.
- Partnering with an inexperienced hosting provider can be difficult.
- Attempting to host yourself can be expensive and a tough learning experience for the uninitiated.

[TechWorld – Leading Vendors Team Up to Squash DNS Bug]

Steps to take…

- Determine the platform you will be using and hire experts that know it well.
- Do not hesitate to consult with security experts and HIPAA/HITECH consultants or seek the advice of others who have done this before.
- Partner with HIPAA/HITECH compliant organizations.
- Practice proper encryption methodologies, and test your applications often.
- Audits and logs!

Other Security Risks are Closer than you think.

- Employees
  - According to a 2008 survey, 66% of U.S. workers write down a password – mostly because there are too many to remember.
  - Accidental (or intentional) administrative privileges – sometimes an employee or a customer gets access they shouldn't have.
  - Open WiFi connections should be avoided as much as possible. Just because people CAN work from anywhere doesn't mean they should join the FREEWIFIHERE network while sitting at the auto mechanic's.
  - If you are partnering with a hosting provider, which employees have access to your data and/or your hardware?

Gawker - GCreep: Google Engineer Stalked Teens, Spied on Chats

Outdated Technologies

- Until Microsoft's aggressive campaign last year, IE 6 still had nearly a 12% market share – 8 years and 2 major revisions after its release. It has finally dropped to less than 5% in August 2010
- Windows XP still has an over 50% market share – 9 years and 2 major releases after its original release date.
- Browser plug-ins can also lead to large security holes.
- IT personnel can be hesitant to update software because many times updates break things, however patches are needed.

In summary…

- Work with a HIPAA/HITECH compliant cloud service or hosting solution.
- If that is not an option, do an independent security audit on your provider.
- If deciding to host internally, conduct a thorough security audit.
- Ensure your data is stored in locations where the law is on your side.
- Know which personnel at your provider has access to your data and how much.
- Set up proper audit trails.
- Segregate your customer's data – use separate virtualizations for each customer's site.
- Employ Gray Hat consultants to break into your system.
- Force security updates for older systems.
- Have a plan, periodically review it, update it, and stick to it!

Thank you!

"In theory there is no difference between theory and practice. In practice there is."

– Yogi Berra

"A smart person makes a mistake, learns from it, and never makes that mistake again. But a wise person finds a smart person and learns from them how to avoid the mistake altogether."

– Roy H. Williams

Additional Links…

- LastPass Technology Page
- Boston Globe – Please do not change your password.
- One Man's Blog – How I'd Hack your Weak Passwords
- Acid Web Browser Standards Tests
- Secunia PSI
- Amazon S3
- RSA – Secure Virtualization and Cloud