Mythbusting the FUD Around Cloud Security

Keith Price  BBus, MSc, CISSP, CISM, CGEIT
Director & Principal Consultant
Agenda

• Psychology of Fear, Uncertainty, and Doubt
• Keith’s favourite cloud security FUDs
• State of cloud security 2010
• Cloud security and risk management
• Advice
Psychology of fear, uncertainty, and doubt

• FUD is a **tactic of rhetoric and fallacy** used in sales, marketing, public relations, politics, and elsewhere.

• The tactics person A uses to induce person B to do what person A wants person B to do.

• The term originated to describe **disinformation tactics** in the computer industry and has since been used more broadly.
  
  – First freely defined by Gene Amdahl (circa 1975) after he left IBM to found his own company, Amdahl Corp, with the statement: "FUD is the fear, uncertainty, and doubt that IBM sales people instil in the minds of potential customers who might be considering Amdahl products."

Psychology of fear, uncertainty, and doubt

• FUD is a manifestation of the appeal to fear.
• An appeal to fear is a fallacy in which a person attempts to create support for his/her idea by using deception and propaganda in attempts to increase fear and prejudice toward a competitor.
• The appeal to fear is common in marketing and politics.
FUD strategies

The four basic strategies are usually combined:

- Exaggerate your opponent's weaknesses
- Invent weaknesses for your opponent that do not exist
- Spin your opponent's strengths to present the appearance of weaknesses
- Associate your opponent with undesirable elements

Source: http://badtux.org/home/eric/editorial/fud101-1.0.0.html
Keith’s favourite cloud security FUD #1

The cloud is less secure than the enterprise.

• 48% of data breaches were caused by insiders.¹
• 93% increase in the volume of Web-based attacks in 2010 over 2009.²
• The Committee believes the expectation that end users should or can bear the sole responsibility for their own personal online security is no longer a tenable proposition.³

¹ - Verizon Data Breach Investigations Report 2010
² - Symantec Internet Security Threat Report Trends for 2010
Virtualised infrastructure is less secure than non-virtualised infrastructure.

• We continue to search for a link between data breaches and cloud-based or virtualized infrastructure but continue to find none.\(^1\)

• The traditional hardware security market (firewall, IPS, UTM, VPN, etc.) will continue to grow, but at a slower rate compared to virtual security appliances.\(^2\)

• Organizations should have the same security controls in place for virtualized operating systems as they have for the same operating systems running directly on hardware.\(^3\)

• The way to mitigate the potential risks of virtualization is to ensure granular, per-user application and data policies are enforced on virtualized systems.\(^4\)

---

1 - Verizon Data Breach Investigations Report 2010
2 - IDC, Virtual Security Appliances on the Rise, March 2010
3 - U.S. NIST Special Publication 800-125 Guide to Security for Full Virtualization Technologies
4 - Cisco Annual Report Mid-2010
Keith’s favourite cloud security FUD #3

It’s a new security model with radically new problems.

- It’s IT outsourcing – and we’ve been doing it since the 1950’s.
- Cloud computing is an expansion of outsourcing, server hosting, web-based computing, managed security services, and other past and present offerings.
- SaaS offerings in some ways resemble older application service providers (ASPs), but are browser based and use multi-tenant hosting models.
- Internal clouds are essentially data centre consolidation initiatives that heavily leverage virtualisation - architecturally akin to some IaaS deployments.
- The global cloud services market is estimated to reach USD 148.8 billion by 2014 from USD 68.3 billion in 2010. ¹

Cloud computing is optimised for scalability, resource utilisation, and performance, not security.

• Because their core business is based on securely storing customers’ data, major cloud providers have made progress in IT security.
• In fact, many of them offer more sophisticated end-to-end, base-level security and privacy protection than might be found in the data centres of any single enterprise.

Source: How Global Organizations Approach the Challenge of Protecting Personal Data, Accenture 2009
Secure cloud services – an example

Security on multiple levels including the physical, software, people, and processes.

- Servers and infrastructure are located in the most secure types of data centres
- Multiple levels of access restrictions including biometrics
- On-premise security guards and security cameras, bullet proof glass
- Firewall and anti-virus protection on multiple levels
- 24x7 internal and external traffic monitoring with logging
- Very few staff have access to physical or logical levels of infrastructure
- Regular vulnerability testing
- All data is backed up on multiple servers in multiple locations on a daily basis
- Data encryption

Source: www.zoho.com
U.S. NIST cloud definition framework

Deployment Models
- Private Cloud
  - Software as a Service (SaaS)
- Community Cloud
  - Platform as a Service (PaaS)
- Public Cloud
  - Infrastructure as a Service (IaaS)

Service Models
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Essential Characteristics
- On Demand Self-Service
- Broad Network Access
- Rapid Elasticity
- Resource Pooling
- Measured Service

Common Characteristics
- Massive Scale
- Resilient Computing
- Homogeneity
- Geographic Distribution
- Virtualization
- Service Orientation
- Low Cost Software
- Advanced Security
State of cloud security 2010

Source: IBM Point of View, Security & Cloud Computing, Nov '09
State of cloud security 2010

- Groups of technology companies have banded together to develop a new, interoperable and highly secure computing infrastructure for the cloud.
- Uses secure cryptoprocessors derived from the Trusted Computing Group’s industry-standard, interoperable specifications.
- A “hardware root of trust” provides:
  - tamperproof measurements of every physical and virtual component in computing stack, including the hypervisor.
  - establishes a bottoms-up security posture based on hardware components embedded with inalterable security technology.
  - authenticates each and every part of the secure system
  - eliminates malware infiltrating the OS and penetrating the virtualisation layer
  - foreign software is instantly rejected for not meeting the system’s secure, recognised configurations

Source: Infrastructure Security: Getting to the Bottom of Compliance in the Cloud, RSA Security Brief, March 2010
Information security program maturity

Where you are on this curve translates to how ready you are for the cloud.
Risk management strategy

Managing the risk posed to information assets requires:
• A clear and communicated policy
• Classifying and labelling information
• Identification and valuation of ICT assets
• Procedures for use, distribution, storage, and disposal
• An awareness of the threats faced
• An awareness of your security state
• Security awareness training
• Detection & reporting of intrusions and misuse
• Correction of problems
• Periodic assessment

Source: Keith Price
Cloud security is a tractable problem

Primary consideration: Clouds are massively complex systems which are reduced to simple primitives and common functional units, replicated thousands of times.

- Increased redundancy and greater resiliency
- Fault tolerance and reliability
- Rapid re-constitution of services
- Low-cost disaster recovery and data storage solutions
- Simplification of compliance analysis
- Cloud homogeneity makes security auditing and testing simpler
- Data held by unbiased party
- Dedicated security team
- Greater investment in security infrastructure
- On-demand security controls
- Real-time detection of intrusion attempts
- Advanced honeynet capabilities
- Distributed denial of service protection

Source: U.S. NIST
Cloud maturity model

Source: IBM X-Force®
Rethink cloud security, don’t reinvent it

• It’s a paradigm shift as information and processes once under the organisation's control move to service providers.
• This changes security postures, granting less opportunity for preventive measures and creating a greater need for detection, deterrence, and response.
• Customers have less preventive control of the infrastructure with cloud and must seek instead to transfer risks (where possible) or improve detection and deterrence through monitoring, feedback, and audit.
• Organisations must accommodate themselves to security postures emphasising risk transfer, deterrence, monitoring, feedback, and audit more than preventive control.
• Information and IT security will evolve into a risk management and compliance function.
Advice

• Part of what you save should be spent on increased risk management activities
• Start developing your cloud based governance and information management frameworks now
• Form a review team from information security, technology risk, op risk, audit, legal, and compliance
• Create and enforce internal policies for appropriate and inappropriate cloud computing use cases
• Start with your dev/test environment, then your DMZ
Advice

- Consider data in motion and data at rest encryption
- Demand greater vendor transparency around security, with appropriate assessment criteria for third party audits
- Mandate by contract the permissible locations for your data (otherwise find an Australian-based provider with no foreign data centres)
- Negotiate the contract based on your specific needs. If you can’t agree, go to another provider.
Boo!
Questions?
keith@blackswangroup.com.au