The Worst Mistakes in Cloud Security

Dr. Eugene Schultz, CISSP, CISM, GSLC
Chief Technology Officer
Emagined Security
Eugene.Schultz@emagined.com

ISSA-LA Security Summit
West Los Angeles, California
June 15, 2011

Outline

EMAGINED SECURITY

- Introduction
- Cloud service models
- The worst mistakes in cloud security
- Conclusion

About cloud computing (1)

EMAGINED SECURITY

- The Cloud Security Alliance defines cloud computing as "… an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them."
- Is not really a model—if anything, it is a *combination* of models
- Major step forward in technology arena--major potential impact
  - Mainframe -> PCs -> client server -> Internet -> Cloud computing
  - Is number one on Gartner's Strategic Technology List

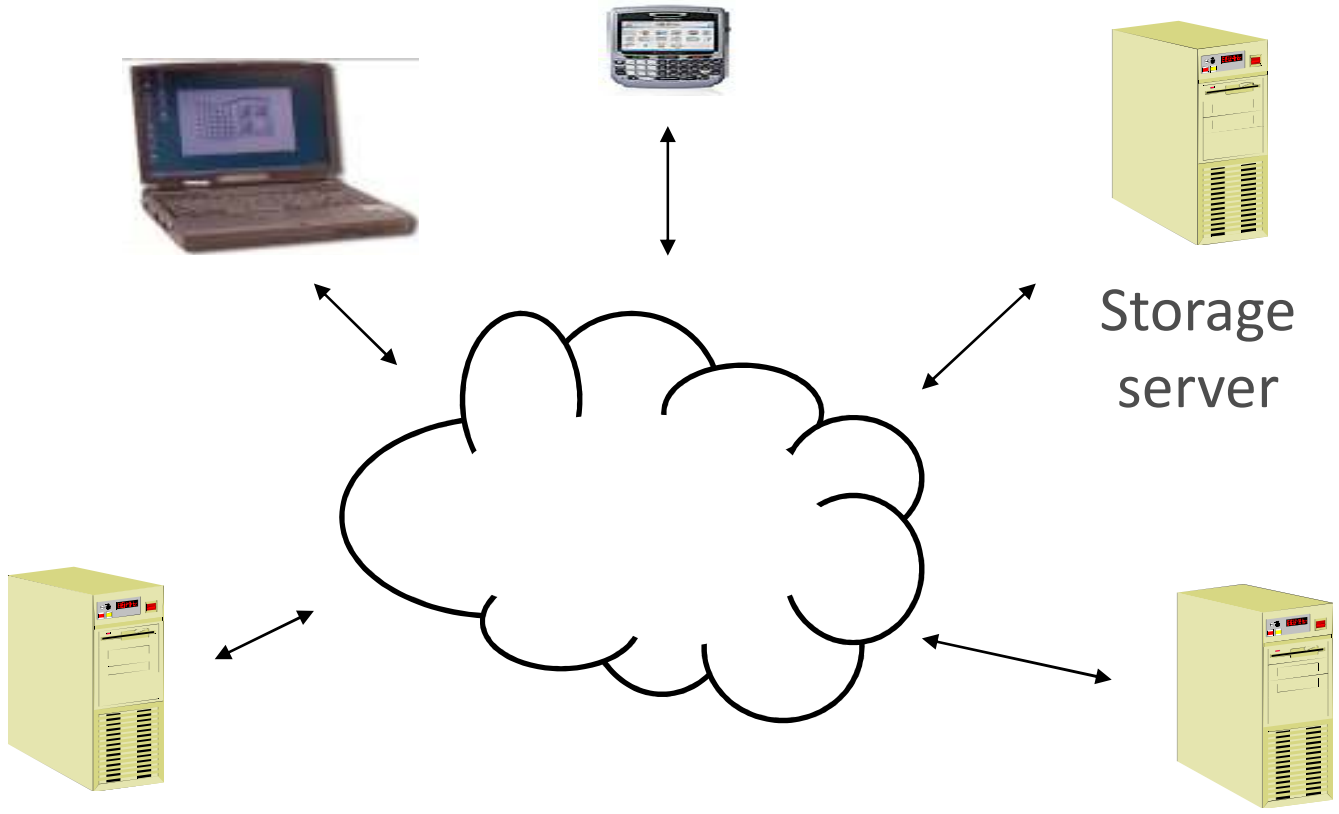
About cloud computing (2)

EMAGINED SECURITY

- Cloud servers are often
  - Highly distributed—over a range of physical locations
  - Virtualized environments (covered later)—e.g., Amazon Elastic Computer Cloud (EC2) with massive data center virtualization
- Access devices—clients are getting thinner and thinner
  - Mobile devices being used increasingly to connect to cloud services
  - CSPs have developed mobile applications for access (e.g., iPhone AppsStore applications)

About cloud computing (3)

EMAGINED SECURITY



Major types of cloud service models (1)

- Software-as-a-Service (Saas)
  - Providing a complete software application to end users over the Web
  - Software is hosted on provider's platform(s) or downloaded to client's platform(s)
  - Typically involves a subscription fee or per-usage pricing model
- Infrastructure-as-a-Service (IaaS)
  - Providing fundamental IT resources (i.e., power, storage and memory) via a network (e.g., the Internet)
  - Based on virtualization and "virtualized infrastructure stacks"
  - Usually involves a subscription or per-usage (based on resources used) pricing scheme

Major types of cloud service models (2)

- Platform-as-a-Service (Paas)
  - Sometimes called “cloudware”
  - Includes
    - Web-based development tools such as Integrated Development Environment (IDE)
    - A run-time application platform that allows applications to run in the cloud (normally on top of IaaS and provided as SaaS)
  - Precludes the need to buy and manage necessary software and hardware throughout the Software Development Life Cycle (SDLC)

Major business benefits

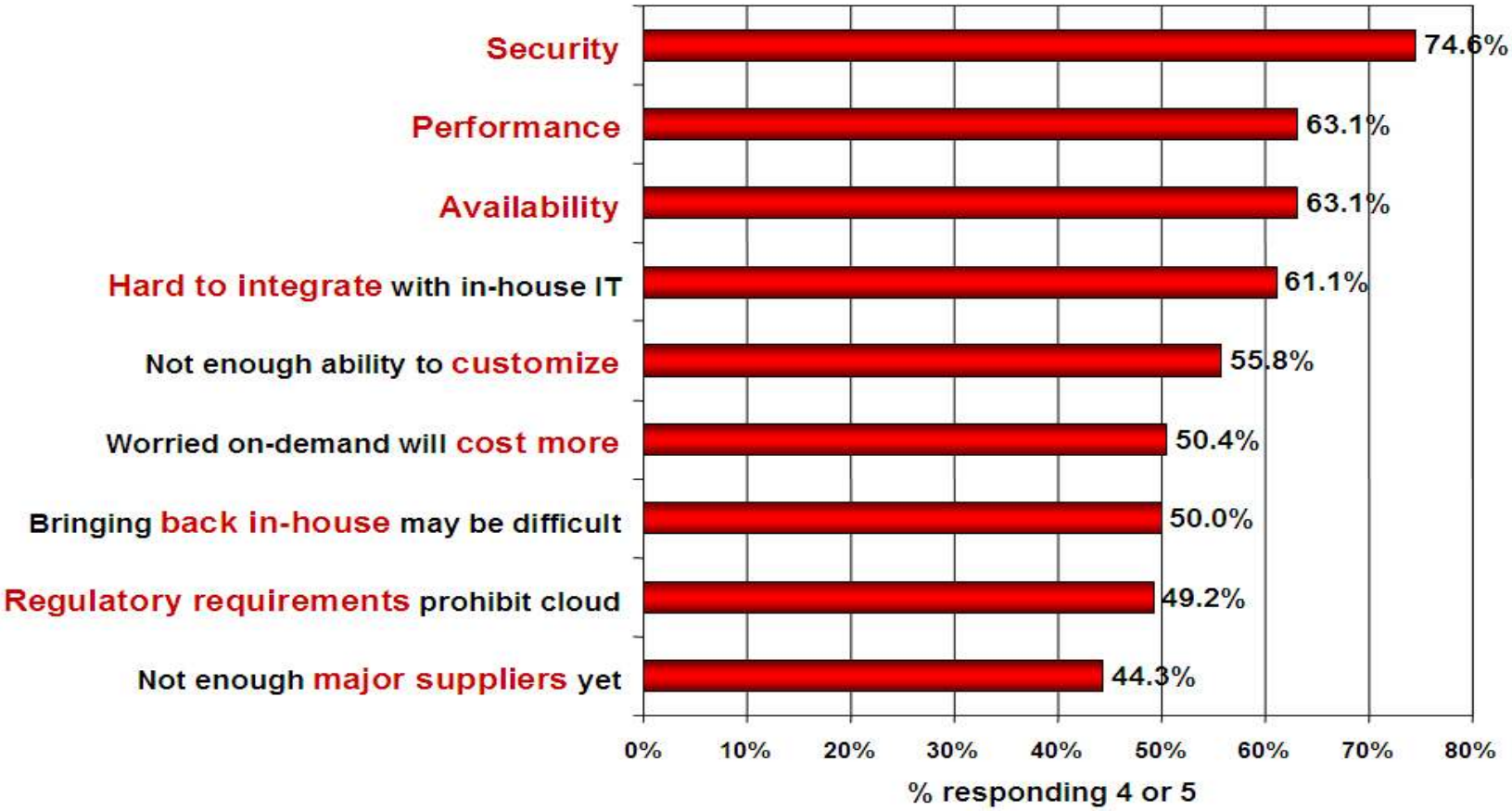
- Cost savings (particularly in terms of TCO)
- Greater business agility
- Potentially greater collaboration among employees
- Ability to get what you want when you want it (often)

Concerns with cloud computing

EMAGINED SECURITY

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model

(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

The three worst cloud-related security risks

- Data security risks
- Denial of service
- Monitoring and auditing generally become much more difficult

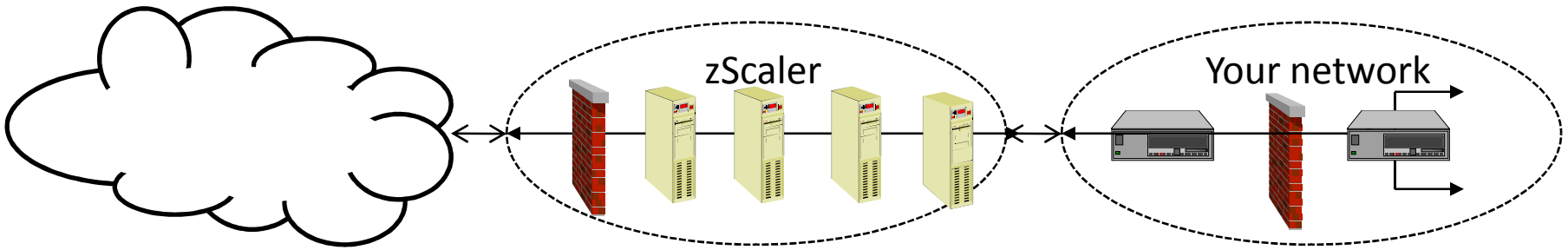
Mistake 1 – Assuming that the cloud is bad

- Cloud computing has until recently been justly criticized as very “green” and immature—BUT—this is starting to change
  - Leaders have emerged, and they are now delivering major quality cloud services
  - Some CSPs now deliver IT services that are better in terms of key performance metrics than we have in the past
  - The continued viability of lesser players is very much threatened

Mistake 2 – Assuming that going to the cloud will make security worse

EMAGINED SECURITY

- Like it or not, some CSPs now deliver information security risk management services better (and more cost effectively) than we have in the past!



Mistake 3 – Assuming that going to the cloud means you lose all control

- Some CSPs allow more customer control than do others
- You get as much control as the SLA says you do
- Even if you lose a lot of control, there are still many controls you can implement in your own network space

Mistake 4 – Failing to ensure that a suitable SLA is in place

EMAGINED SECURITY

- Because the cloud has generally limited our ability to control what we previously could control, the role/importance of extremely thorough and detailed SLAs and SOWs has increased dramatically
- Ensure that each SLA contains suitable security-related provisions

7.1. Quality of Service

The Supplier warrants that the Services will be performed in a professional and workmanlike manner consistent with industry standards reasonably applicable to such services. If the Client considers that a breach of this warranty has occurred and notifies the Supplier in writing stating the nature of the breach, then the Supplier will be required to urgently correct any affected services in order that they comply with the warranty.

7.2. Indemnification

If, as a result of the Supplier's negligence, the Client or Client's employees suffer injury or property damage, the Supplier will reimburse the Client for that portion of any damages for which the Supplier is found to be liable.

7.3. Third party claims

The Supplier warrants that any works of authorship written by the Supplier's personnel will not infringe any third party copyrights, patents or trade secrets. If a third party takes action against the Client for any infringes of this nature, then the Supplier will, at its own expense, settle the claim or arrange to defend the Client in such proceedings, and, in such circumstances, the Supplier will pay all settlement costs, damages, and legal fees and expenses finally so awarded.

7.4. Exclusions

The Supplier is not responsible for any infringements to third party copyrights, patents or trade secrets where the Client has made amendments to original documents and similar works prepared by the Supplier without the express approval of the Supplier, or where the Client fails to use the most recent versions of such works that have been delivered by the Supplier.

7.5. Remedies for breaches

In the event of any defective performance from the Supplier or failure to furnish the agreed level of service, the Supplier will make reasonable efforts to restore the service to a good operating condition on an urgent basis. If any penalties and refunds are payable in the event of defective service, the amounts claimable are as defined in Schedule K to this Agreement.

7.6. Force majeure

Except in respect of payment liabilities, neither party will be liable for any failure or delay in its performance under this Agreement due to reasons beyond its reasonable control, including acts of war, acts of God, earthquake, flood, riot, embargo, sabotage, governmental act or failure of the Internet, provided the delayed party gives the other party prompt notice of the reasons for such cause.

Mistake 5 – Overestimating your CSP's ability to provide data security

- Right now data security is just about the most difficult problem in information security
- Data security-related risks have been greatly magnified by cloud computing
- Guarantees and/or penalty clauses in the SLA are some of the best ways to ensure that your data are being suitably protected
- There are also many things you can do on your end

Mistake 6 – Underestimating legal issues associated with the cloud

- The contractual nature of relationships with CSPs makes cloud computing a lawyer's playground
- Moving to the cloud does *not* absolve an organization of legal and/or compliance-related responsibilities!

Mistake 7 – Assuming that the transition process will be easy

- Risks in connection with migration of in-house to cloud-based infrastructure are far greater than we ever initially imagined
  - Risks from having to bridge infrastructures
  - Failover considerations
  - Differences in authentication and authorization mechanisms
  - Change control—how do you do it?
  - There are many additional considerations…

Mistake 8 – Overlooking federated identity authentication methods

- A breakdown of traditional trust boundaries occurs in most cloud services
- CSPs that support SAML allow authentication through third-party authentication servers
  - Helps ensure that strength of authentication is at desired level
  - Greater operational efficiency
  - Helps alleviate the “all eggs in one basket” problem with CSPs

Mistake 9 – Assuming that your infosec practice will go on as usual

EMAGINED SECURITY

- The composition and function of information security practices will change drastically (and is, in fact, already doing so) because of organizations' moving to cloud services
- Governance level compatibility comprises a particular difficult issue

Mistake 10 – Ignoring cloud-related incident response issues

- Incident response in the cloud is generally more difficult because customers typically lose at least some control
  - Should CSP be given full control over incident response?
  - Shared control?
  - Is it possible for the customer to retain most of the control?
- Forensics investigations—how can they be conducted?

Mistake 11 – Failure to adequately monitor your CSP

EMAGINED SECURITY

- The ability to monitor what goes on in the cloud has become one of, if not the most critical part of information security in the cloud
- Your SLA will state what you can and cannot do
- Monitoring should include conducting audits, but in general auditing in the cloud is more difficult

Conclusion (1)

EMAGINED SECURITY

- Cloud computing is starting to grow up—this is a good thing
- The positives of cloud security are starting to become increasingly apparent
  - Up to now, it has in many respects been easier to see the negatives
- Whether or not you like it, you are (or soon will be) a player in the cloud arena
- Misconceptions and mistakes concerning security in the cloud arena can be very costly!
  - Come up to speed as soon as you can
  - Maintain a proactive focus--drastic changes in the cloud computing arena over the next few years are very likely to occur

Conclusion (2)

EMAGINED SECURITY

- Never forget that for better or worse, the link between your organization and cloud services is the Internet
- Good luck!

Questions?

EMAGINED SECURITY

Eugene Schultz
Emagined Security
2816 San Simeon Way
San Carlos, CA 94070
+1 (650) 593-9829
eugeneschultz@emagined.com
Web: www.emagined.com
Blog: baylinks.com/blogs
Dashboard:
dashboard.emagined.com

For a PDF copy of these slides send email to:
seminar@emagined.com