
RED HAT
SUMMIT
LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.
June 11-14, 2013
Boston, MA
redhat.

CONTROLLING CLOUDS: BEYOND SAFETY

Gordon Haff
Cloud Evangelist, Red Hat
12 June 2013

Is it safe?

The First Word on Tech

INFOWORLD TECH WATCH

AUGUST 02, 2012

Dropbox fiasco serves as reminder of cloud-storage insecurity

End-user ignorance is demonstrably more dangerous when let loose on public clouds. IT admins must educate users to approach cloud storage cautiously

By Ted Samson | InfoWorld

Follow @tsamson_IW

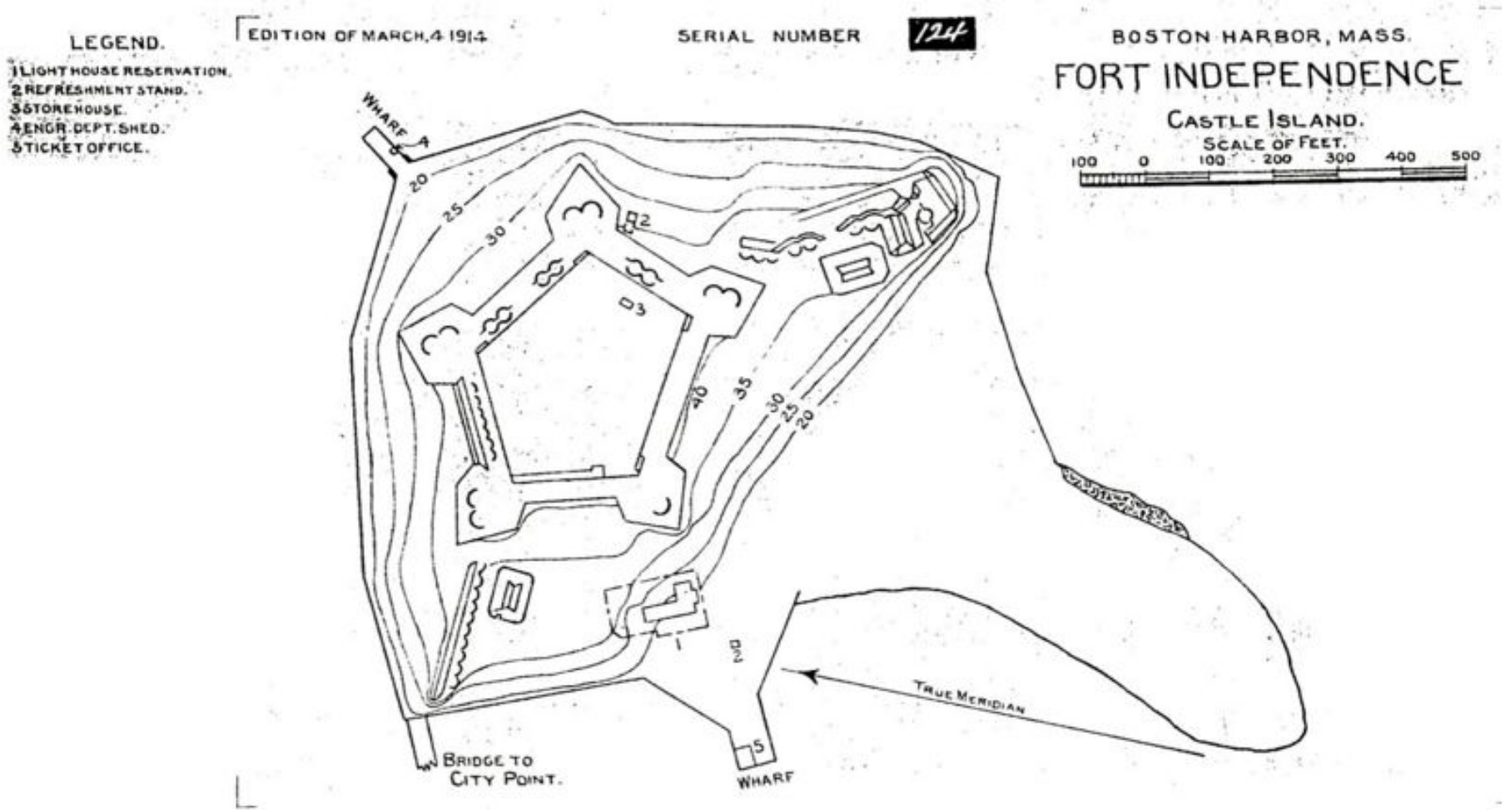
By ERIK SHERMAN / MONEYWATCH / August 8, 2012, 7:41 AM

Apple, Amazon prove the "cloud" isn't safe

13 Comments / 212 Shares / 90 Tweets / Stumble / @ Email More +

(MoneyWatch) Everyone in the high-tech industry, along with the usual ardent early-adopters, is betting heavily on the emerging Internet "cloud." What often gets overlooked are the drawbacks, as tech writer Mat Honan learned when hackers destroyed his digital life

The historical approach to security



More than keeping bad guys out

Audit

Regulations

Service Levels

Data security & portability

Ability to change providers

Consistency across environments

Interoperability through open APIs

Integration with existing applications

A few concepts

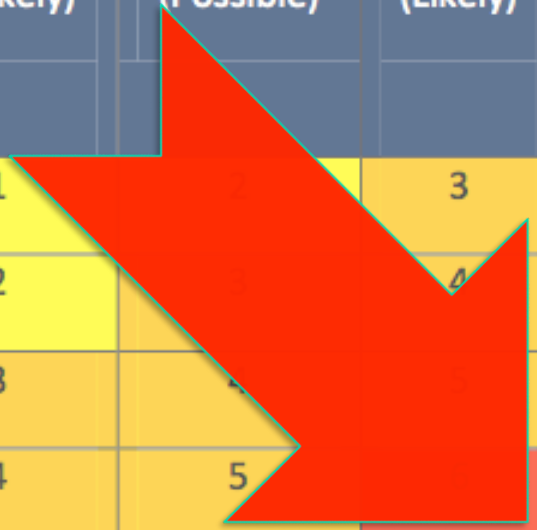
Balancing cost and benefit

Shared responsibility models

Certifications

Risk = Likelihood * Impact

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8



We have based the estimation of risk levels on ISO/IEC 27005:2008 (10).

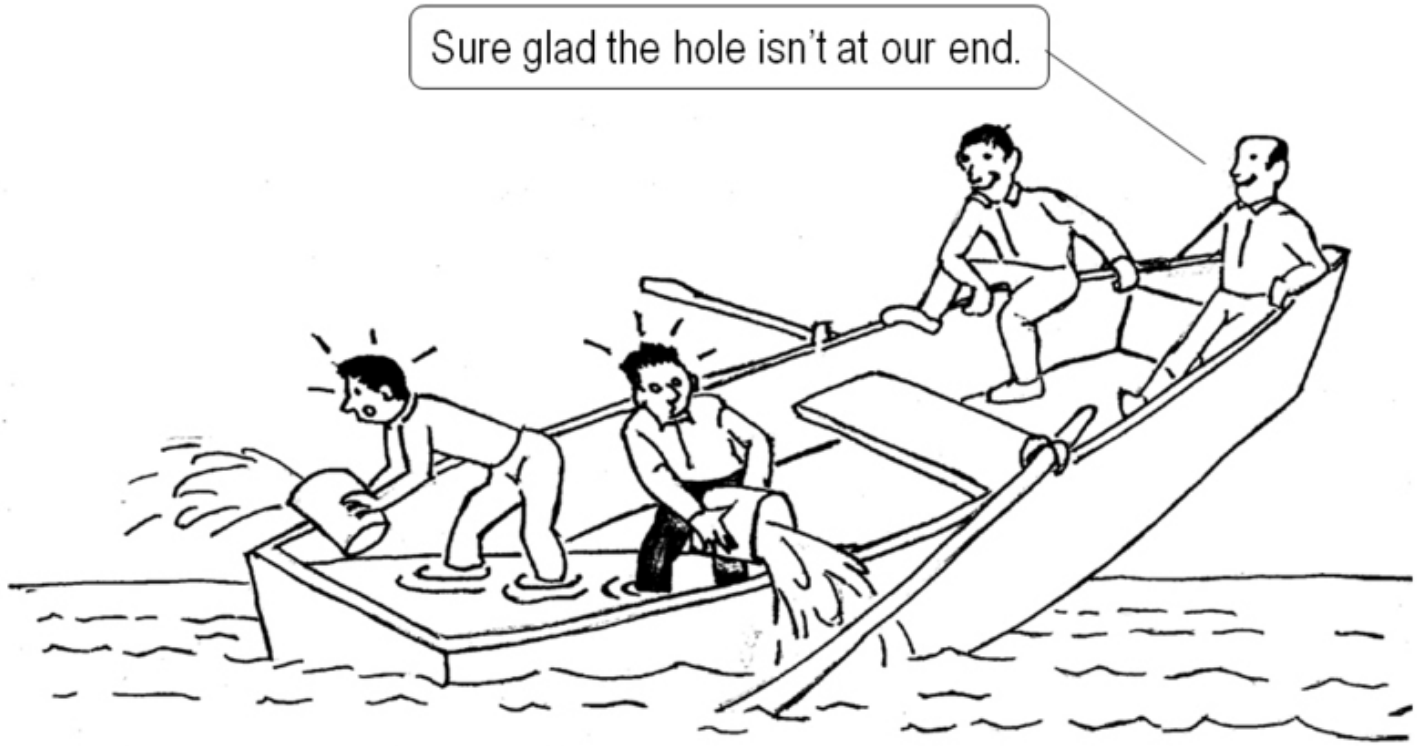
Source: ENISA

Example: Compliance challenges

R.3 COMPLIANCE CHALLENGES

Probability	VERY HIGH – depends on PCI, SOX	Comparative: Higher
Impact	HIGH	Comparative: Equal
Vulnerabilities	V25. Audit or certification not available to customers V13. Lack of standard technologies and solutions, V29. Storage of data in multiple jurisdictions and lack of transparency about THIS V26. Certification schemes not adapted to cloud infrastructures V30. Lack of information on jurisdictions V31. Lack of completeness and transparency in terms of use	
Affected assets	A20. Certification	
Risk	**HIGH**	

Shared responsibility



Applications

Operations

Infrastructure

Source: http://virtualization.sys-con.com/node/2459176

A cloud provider view of shared responsibility

SERVICE OWNER	SaaS	PaaS	IaaS
Data	Joint	Tenant	Tenant
Application	Joint	Joint	Tenant
Compute	Provider	Joint	Tenant
Storage	Provider	Provider	Joint
Network	Provider	Provider	Joint
Physical	Provider	Provider	Provider

Source: Cloud Security Alliance

The nice thing about certifications is that there are so many of them

- SAS 70
  - Specifically created for financial auditors of service organizations
- ISO/IEC 27001
  - Information security management system standard published in 2005
- PCI DSS
  - For organizations processing credit card transactions
- FedRAMP Security Controls
  - Framework for US Federal agencies
- HIPAA
  - US healthcare

SOC 2 and 3

- Report can be issued on one or more Trust Services Principles
  - Security
  - Availability
  - Processing integrity
  - Confidentiality
  - Privacy
- Type 1: Suitability of design
- Type 2: Suitability of design and effectiveness
- SOC 3 is a condensed public version of SOC 2
- Mostly in the US today

See www.webtrust.org

Sources for a broader cloud governance view

Deloitte Cloud Computing Risk Intelligence Map

Cloud Computing Security Risk Assessment

CSIS 20 Critical Security Controls

Cloud Security Alliance STAR and Cloud Controls Matrix

Links:

http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/Deloitte%20Risk%20Map%20for%20Cloud%20Computing.pdf

http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

http://www.cloudsecurityalliance.org

http://www.sans.org/critical-security-controls/guidelines.php

Some things don’t change with cloud

Credit: Michael Rosenstein, cc/flickr
http://www.flickr.com/photos/michaelcr/1508784073/

If your security practices [4 letter word meaning not very good] in the physical realm, you’ll be delighted by the surprising lack of change when you move to cloud.

Chris Hoff,
Juniper Networks

CSA Cloud Controls Matrix: What is it?

- 98 “control areas” in 11 categories
  - Example: Security Architecture - Production / Non-Production Environments
- Each mapped to areas of relevance
  - Examples: IaaS, PaaS, SaaS, corporate governance, and supplier relationships
- Each mapped to relevant regulations and certifications

A detailed example: Security Architecture - Production / Non-Production Environments

- Definition: “Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets.”
- Applies across all areas of architecture and all cloud service models
- Applies to the service provider (internal *or* external) but not the customer/tenant
- Applies to controls including: NIST SP 800-53 R3 SC-2 and PCI DSS v. 2 6.4.1 and 6.4.2

11 Domains

Compliance (CO)

Data Governance (DG)

Facility Security (FS)

Human Resources (HR)

Information Security (IS)

Legal (LG)

Operations Management (OM)

Risk Management (RI)

Release Management (RM)

Resiliency (RS)

Security Architecture (SA)

Compliance

- Audit controls
  - Independent audits of organizational compliance and audits of third-party providers
  - Limitations of third-party auditability can be a concern for public cloud users
- Regulatory mapping
  - Can be especially important to understand where data resides

Data governance

- What is it and who owns it?
  - Classification is key to establishing data placement policies
- Retention and secure disposal policies
  - “Ensuring data is not recoverable by any computer forensic means”
- Do you have controls in place to prevent data leakage or intentional/accidental compromise between tenants in a multi-tenant environment?
  - Example is Red Hat’s use of SELinux to provide multi-tenant security in OpenShift

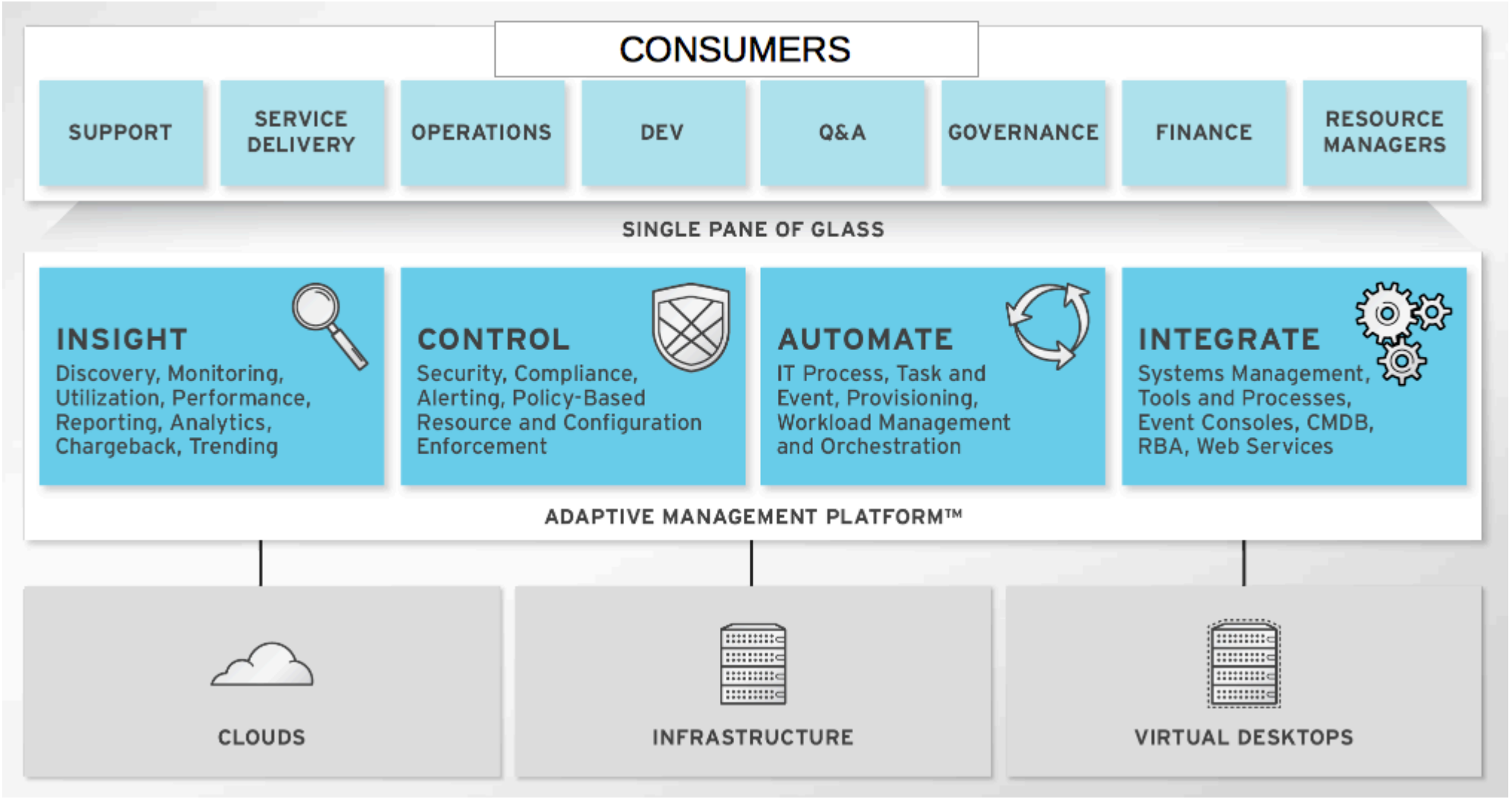
Information security

- Broader than just data
  - Management oversight of security policies, access policies for contractors, enforcement of logouts, etc.
- IS-01 includes a requirement for a management program that includes
  - Administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction
- Establishment and implementation of encryption policies
  - Red Hat has been actively involved in Keystone, OpenStack's identity and authentication service

Information security (continued)

- Preparing for and responding to incidents (including legal response as needed)
- Timely deprovisioning of user access based on change of status
- Acceptable use policies and remediation for violations
- Asset returns
- Access to audit tools

Automating policy-based compliance with Red Hat CloudForms



Security architecture

- Minimum standards for implementing and enforcing (through automation) user credential and password controls
- Multi-factor authentication for all remote access
- Segmentation and restricted connections in network environments especially between trusted and untrusted networks
  - “Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations”
  - An interesting developing area

A few related sessions

- SELinux for Mere Mortals (Th 10:40a, Room 302)
- Under the Hood of OpenShift, Turbocharged by Red Hat Enterprise Linux (Th 3:40p, Room 304)
- Setting Up Red Hat Identity Management (Th 2:30p Room 206)
- OpenShift Deep Dive: Running a Large, Public PaaS (Th 4:50p, Room 310)
- Stitching Infrastructure Layers with Identity Management Thread (F 9:45a Room 312)

QUESTIONS?

Thank you.

Gordon Haff

ghaff@redhat.com

Twitter: @ghaff

Google+: Gordon Haff

Blog: bitmason.blogspot.com