Auditing the Cloud: How 15 Minutes Can Save You From 15 Security Mistakes or More

Davi Ottenheimer

flyingpenguin

Introduction

Davi Ottenheimer

- ISACA Platinum Member (SV Board)
- 18th Year Security/Compliance
- QSA, PA-QSA, CISSP, CISM
- MSc Intl History, London School of Economics
- VMware vCloud Security/Compliance Architect

davi@flyingpenguin.com
@daviottenheimer | 415-225-7821

About Me

flyingpenguin
the poetry of information security

Davi Ottenheimer

- 18th year InfoSec
- ISACA Platinum Level (1997)
- Co-author

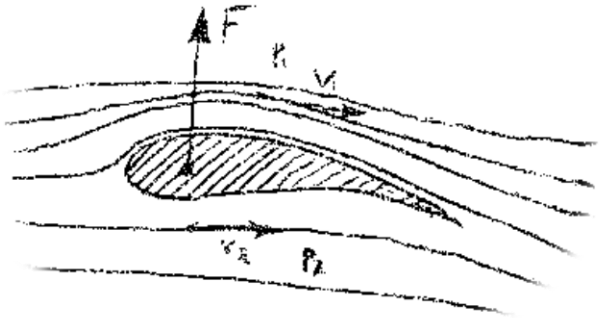
  Securing the Virtual Environment: How to Defend the Enterprise Against Attack (Wiley, 2012)

.

flyingpenguin

- flying \fly"ing\, a. [From fly, v. i.]

  moving with, or as with, wings; moving lightly or rapidly; intended for rapid movement



- penguin \pen"guin\, n.

  short-legged flightless birds of cold southern especially Antarctic regions having webbed feet and wings modified for water

Agenda

- Background
- Threats
- Lessons Learned
- Control Objectives

Compliance Versus Security

You have to do it

Security is X

X + Y

Agree

Will you do it?

Change

- Many things the same

  Confidentiality, Integrity, Availability

- Many things different

  Elasticity, Mobility, Automation, Sharing

PRIVACY
TRUST BARRIER
PERIMETER
SEGMENTATION…

VIRTUALIZATION
BROKERING
PROXYING
FEDERATION

Cloud Security and Compliance

88% would use cloud more if

same or better security

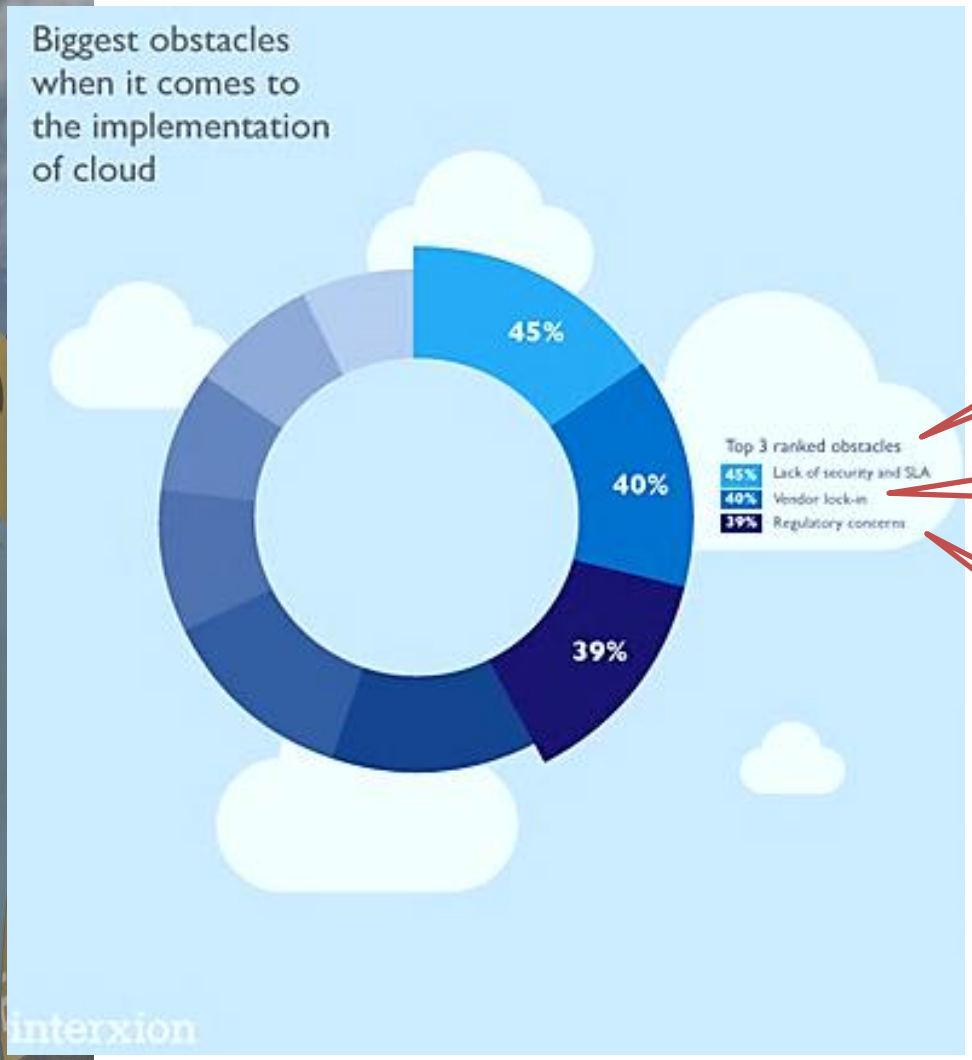
as their internal datacenter

Global Study of CIOs and
Top IT Decision Makers

CIO IDG INTERNATIONAL DATA GROUP

Base: 636 Total respondents; 234 US respondents; 202EMEA respondents; 200 APAC respondents
Source: CIO Global Cloud Computing Adoption Survey January 2011

Cloud Security and Compliance



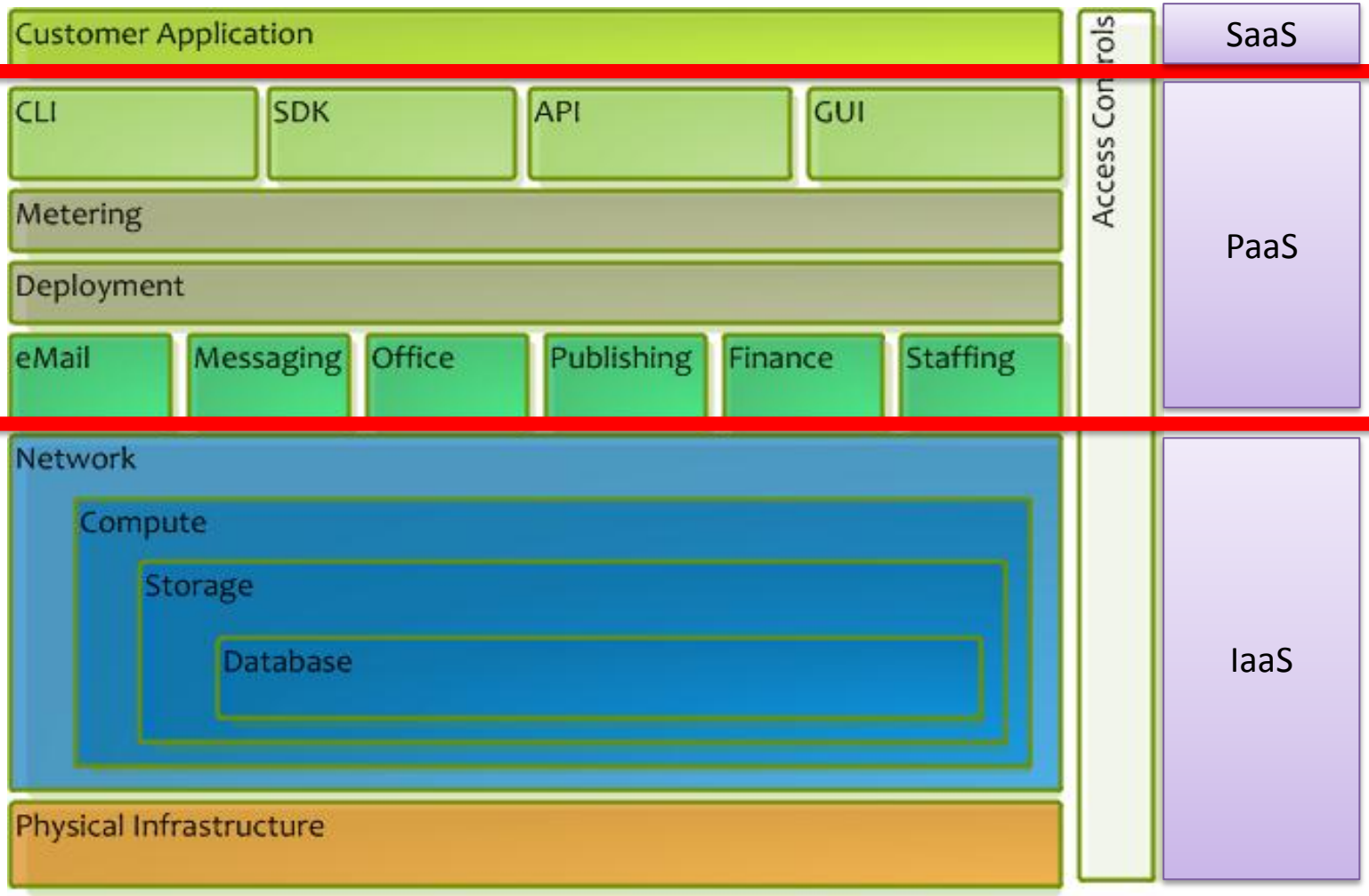
Lack of Security and SLA — 45%

Vendor lock-in — 40%

Regulatory concern — 39%

http://www.interxion.com/cloud-insight/

Cloud Security and Compliance



Example Control Objectives

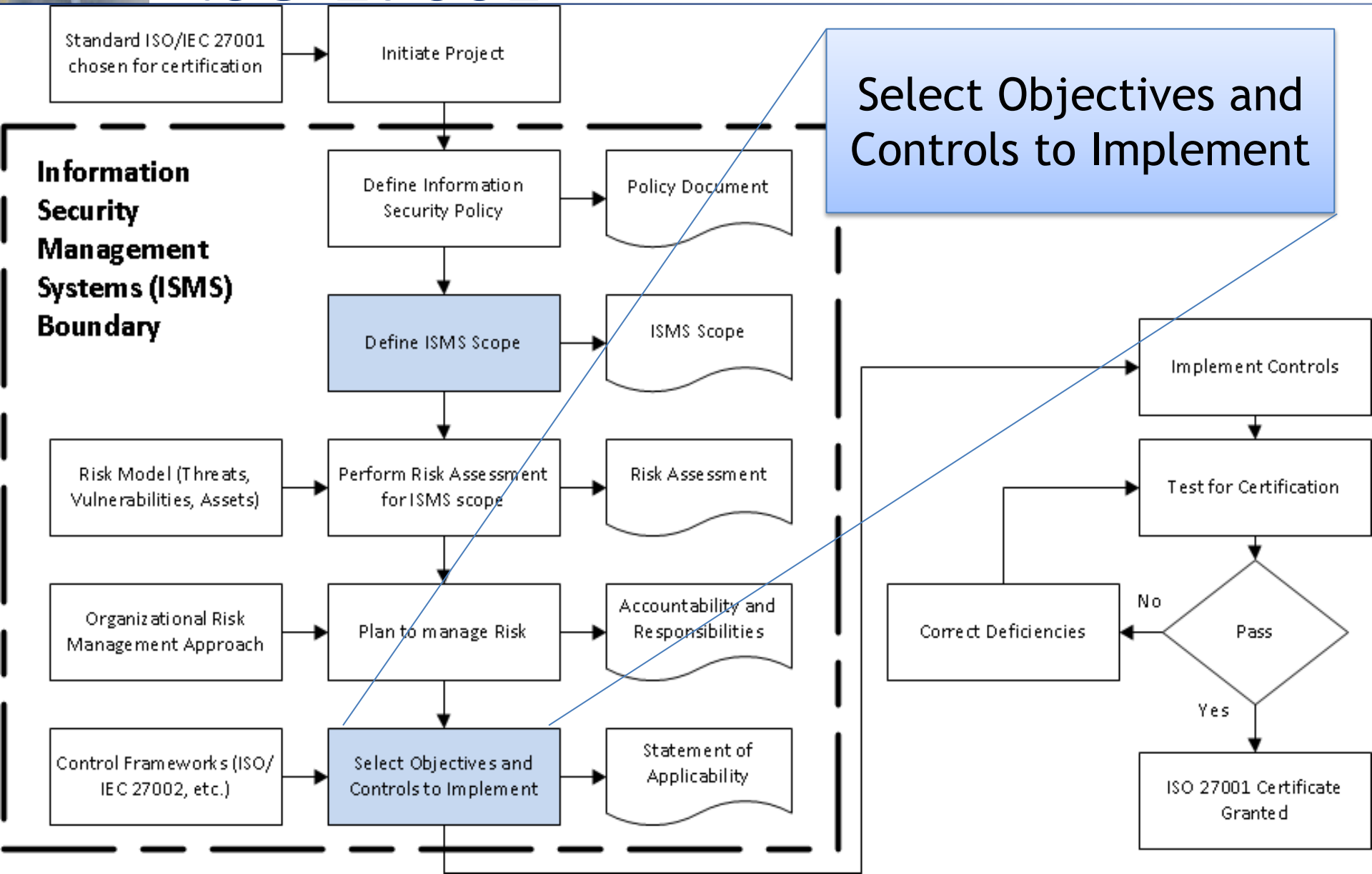
- Remove Data
- Define Boundary
- Secure Access (Apps)
- Monitor
- Protect Stored Data

Control Objectives

- Checklists
  - Architecture / system review
  - Detailed control list

- Standards
  - ISO 27002 (ISO 27001 Certification)
  - AICPA Service Organization Control (SOC) 2
  - FISMA NIST 800-53

ISO 27001


Standard ISO/IEC 27001 chosen for certification
Initiate Project
Information Security Management Systems (ISMS) Boundary
Define Information Security Policy
Policy Document
Define ISMS Scope
ISMS Scope
Risk Model (Threats, Vulnerabilities, Assets)
Perform Risk Assessment for ISMS scope
Risk Assessment
Organizational Risk Management Approach
Plan to manage Risk
Accountability and Responsibilities
Control Frameworks (ISO/IEC 27002, etc.)
Select Objectives and Controls to Implement
Statement of Applicability
Select Objectives and Controls to Implement
Implement Controls
Test for Certification
Pass
No
Correct Deficiencies
Yes
ISO 27001 Certificate Granted

Regulatory Control Objectives

ISO 27002	NIST	PCI DSS	SOX	HIPAA
4. Risk Assessment and Treatment	✓	✓		
5. Security Policy	✓	✓		
6. Organization of Information Security	✓			
7. Asset Management	✓			✓
8. Human Resources Management	✓			✓
9. Physical and Environmental Security	✓	✓	✓	✓
10. Communications and Operations Management	✓	✓	✓	✓
11. Access Controls	✓	✓	✓	✓
12. Information Systems Acquisition, Development and Maintenance	✓	✓	✓	✓
13. Information Security Incident Management	✓	✓	✓	✓
14. Business Continuity Management	✓		✓	✓
15. Compliance	✓		✓	✓

TAKEOFF

1. Pitot heat
2. CABIN PRESS mode
3. Windshield heat
4. Cross connection
5. Both pitot
6. Radios/SAV AHRS/IFF
7. Shoulder harnesses
8. Ejection seats
9. Oxygen
10. FLIR/radar
11. INCOS trays
12. Brake selection switch
13. Winds/fin
14. Flaps
15. Speedbrakes

NIST Special Publications (SP)

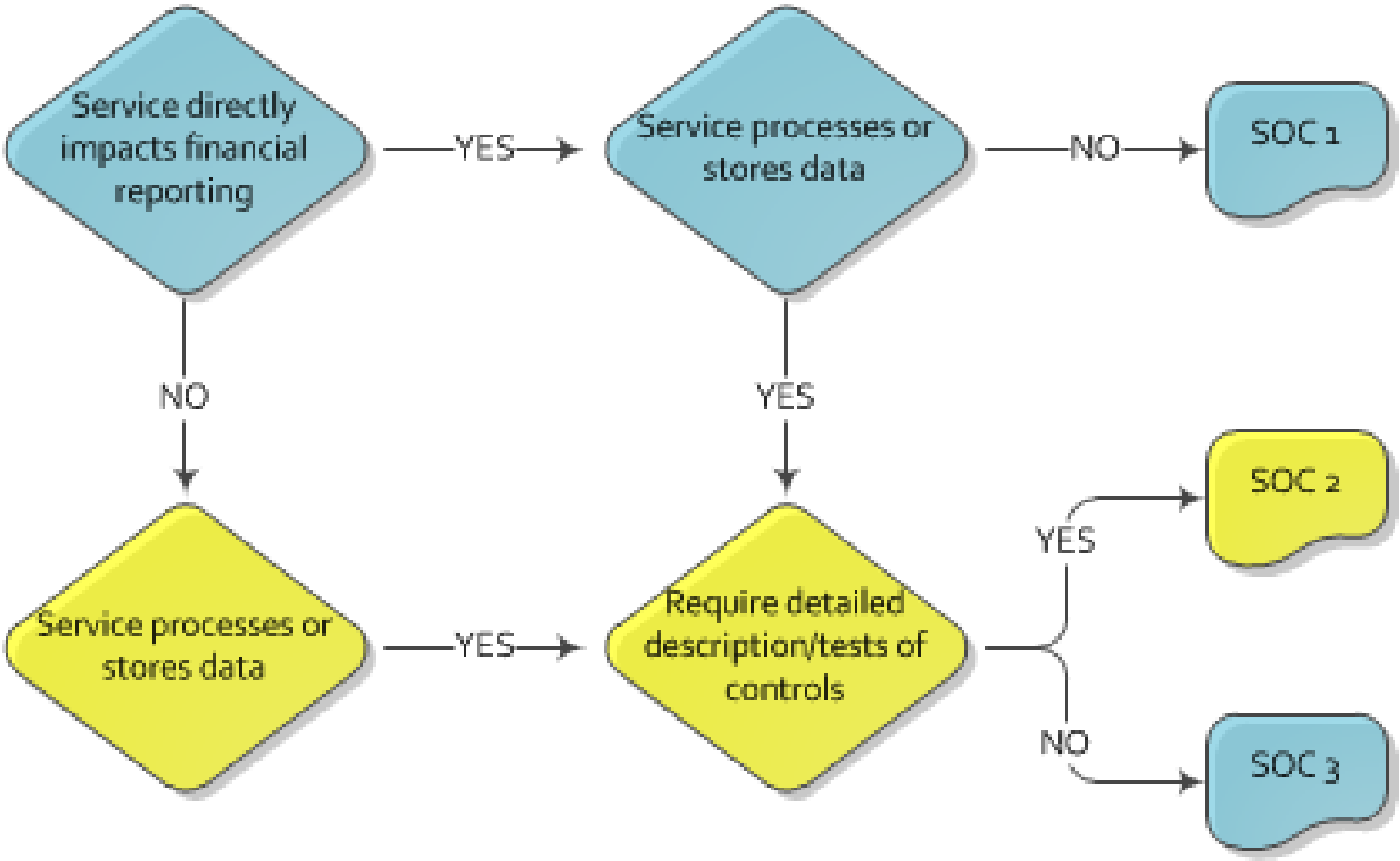
- 800-146: DRAFT Cloud Computing Synopsis and Recommendations
- 800-145: A NIST Definition of Cloud Computing
- 800-144: DRAFT Guidelines on Security and Privacy in Public Cloud Computing

NIST Cloud Roadmap SP 500-293

Volume I, High-Priority Requirements

1. Portability
2. Security
3. Service Levels Agreements
4. Services
5. Federation
6. Security Assessments
7. Government Requirements
8. Future Development (Nation-size cloud)
9. Reliability
10. Metrics

SOC 2


Service directly impacts financial reporting
YES
Service processes or stores data
NO
SOC 1
NO
YES
Service processes or stores data
YES
Require detailed description/tests of controls
YES
SOC 2
NO
SOC 3

SOC 2

- Trust Services Principles and Criteria
  - Availability Principle and Criteria
    - 3.0 Procedures in place to achieve documented system availability objectives in accordance with defined policies

#	Criteria	Illustrative Controls
3.15	Procedures exist to maintain system components, including configurations consistent with the **defined system availability and related security policies**.	• 3rd Party Opinion • Inventory List • Change management

HIPAA

US Code, Title 45, Part 164 Security and Privacy

Control	Description
164.310(d)(2)(iii) Accountability	Implement procedures to **maintain a record of the movements** of hardware and electronic media and any person responsible therefore.
164.312(a)(1) Access	Implement technical policies and procedures for electronic information systems that maintain ePHI to allow **access only to those persons or software programs that have been granted access rights** as specified in Sec 164.308(a)(4)
164.312(b) Audit	Implement hardware, software, and/or procedural mechanisms that **record and examine activity** in information systems **that contain or use ePHI.**

PCI DSS 2.0

- Risk-based Approach…
- PCI SSC July Guidance and August Paper
  1. Do not generalize – each case differs
  2. Rely on other assessors at your own risk

"5 Mistakes Auditing Virtual Environments (That You Don't Want to Make)"

http://info.hytrust.com/pci_top_5.html

PCI Security Standards Council™

QUALIFIED SECURITY ASSESSOR

Risk-Based Approach

Risk-Based Approach

Assets

1. Process Type: Development, Test and/or Production
2. Data Type: Public, Restricted and/or Sensitive

Vulnerabilities

1. Change
2. File Access
3. Remote Management

Threats

1. Motive
2. Means
3. Opportunity

epsilon

Heartland PAYMENT SYSTEMS®
The Highest Standards | The Most Trusted Transactions

ChoicePoint

DNP
Dai Nippon Printing Co.,Ltd.

cardsystems
the power of the right solution

Risk-Based Approach

Example of how scope and responsibility may differ* by type of cloud service:

Cloud customer responsibility	
Cloud service provider responsibility	

PCI DSS Virtualization SIG GIS

Area of Responsibility	*Type of Cloud Service* IAAS	PAAS	SAAS
Data			
Software, user applications			
Operating systems, databases			
Virtual infrastructure (hypervisor, virtual appliances, VMs, virtual networks etc)			
Computer and network hardware (processor, memory, storage, cabling, etc.)			
Data center (physical facility)			

* ***Note:*** *This is an example only. Cloud service offerings should be individually reviewed to determine how responsibilities* between *the cloud provider and cloud customer are assigned.*

Risk-Based Approach

Liability to customers?
- choose non-persistent state
- decline backup services

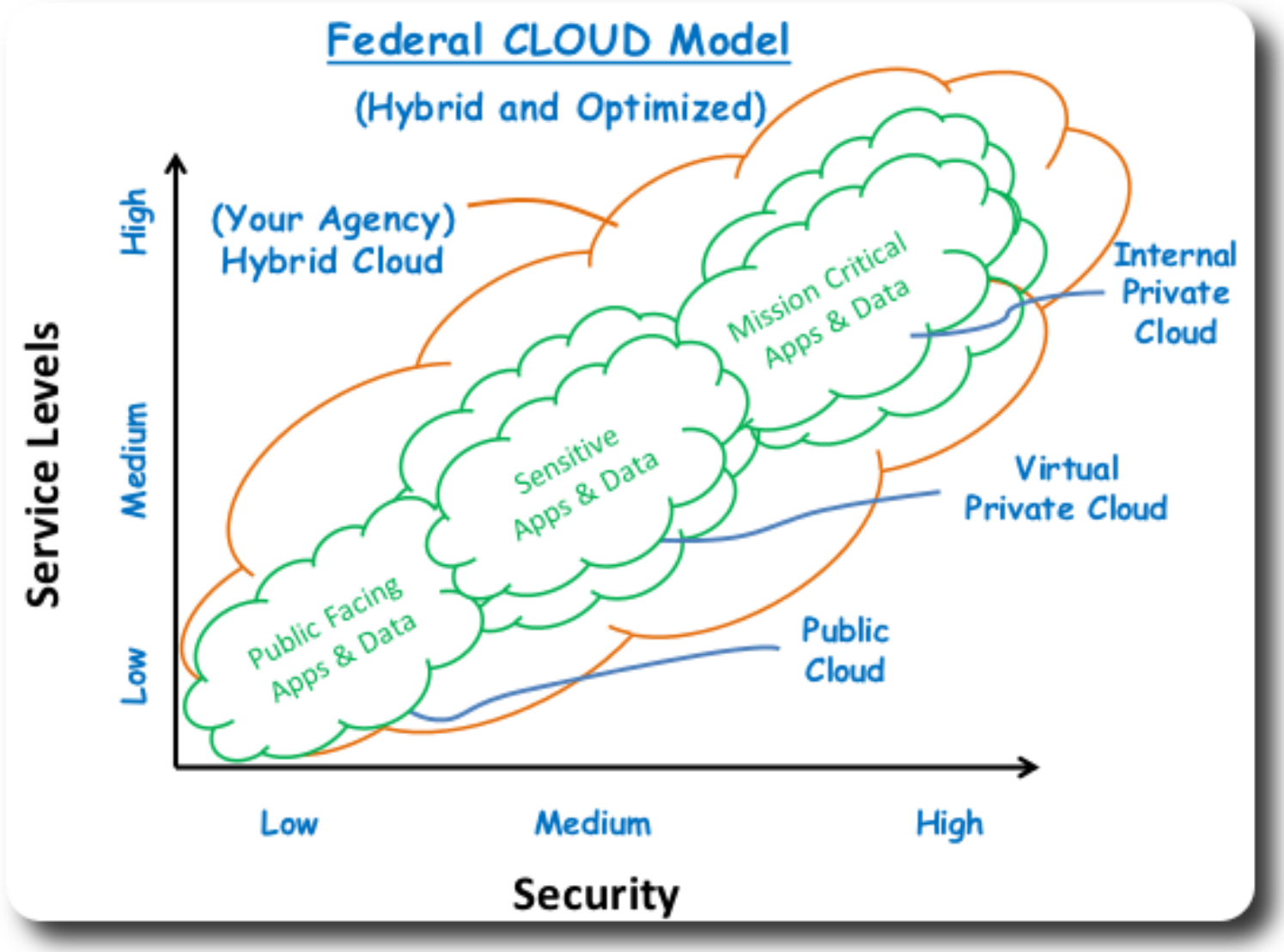
EU Directive 2002/58/EC (ePrivacy)

1. French Data Protection Act of 1978
2. French Postal and Electronic Communications Code
3. French Consumer Protection Code

Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques

1. Personal data services provided to the public
2. Security breach = accidental or unlawful **destruction, loss, alteration**, disclosure or unauthorized access
3. Breach description, impact and remediation

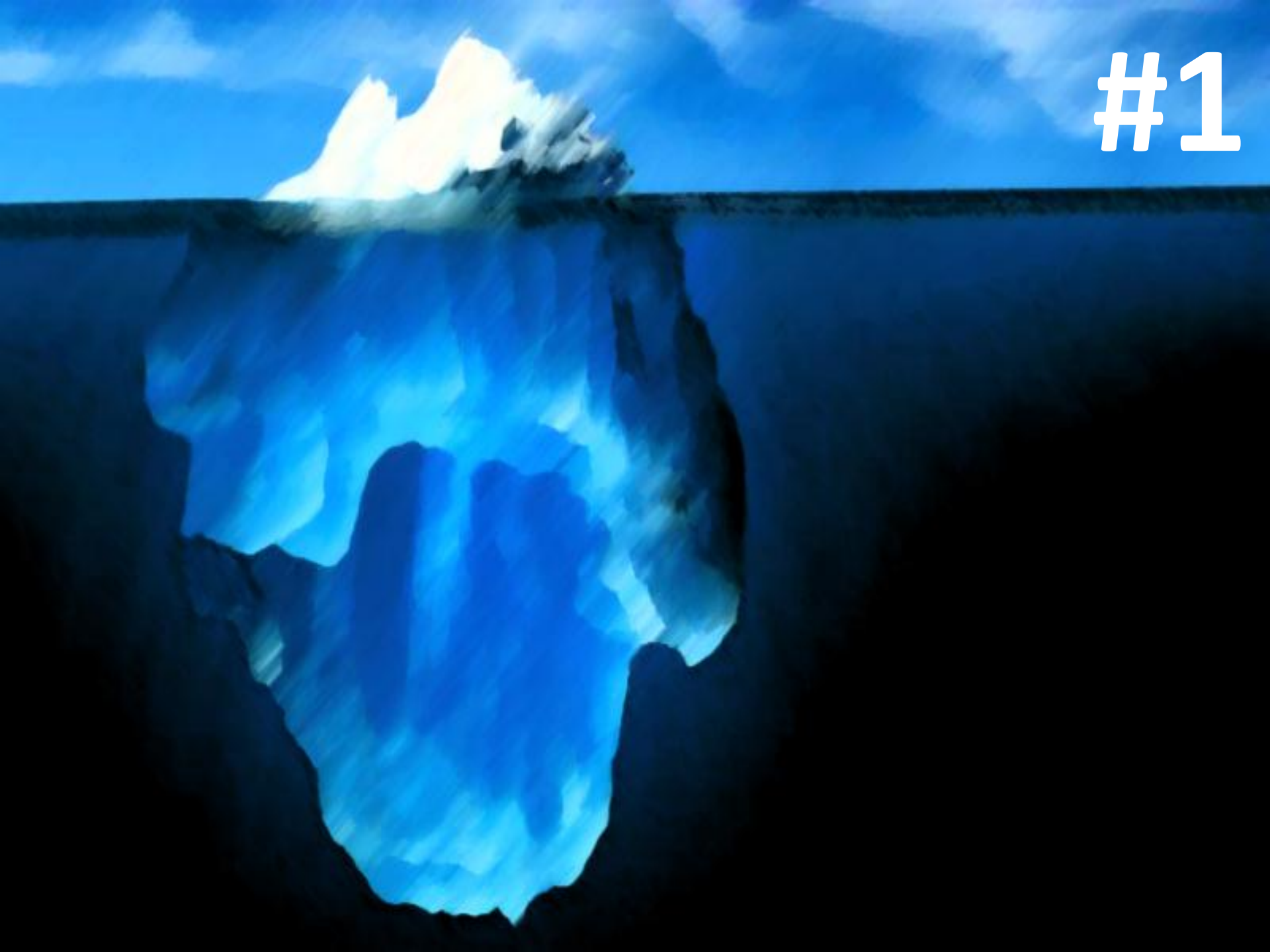
Cloud Risk Model



http://vmwaredoug.com/?p=66

Threats

1. The Iceberg
2. The Vindictive Admin
3. Change Control
4. The Barn Door


#1

CardSystems

THE ICEBERG: 2005

1. Unnecessary risk from stored data
2. Vulnerabilities not adequately assessed
3. “Simple, low-cost, and readily available” controls

“ Failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations.

http://www.ftc.gov/os/caselist/0523148/0523148.shtm

Sony

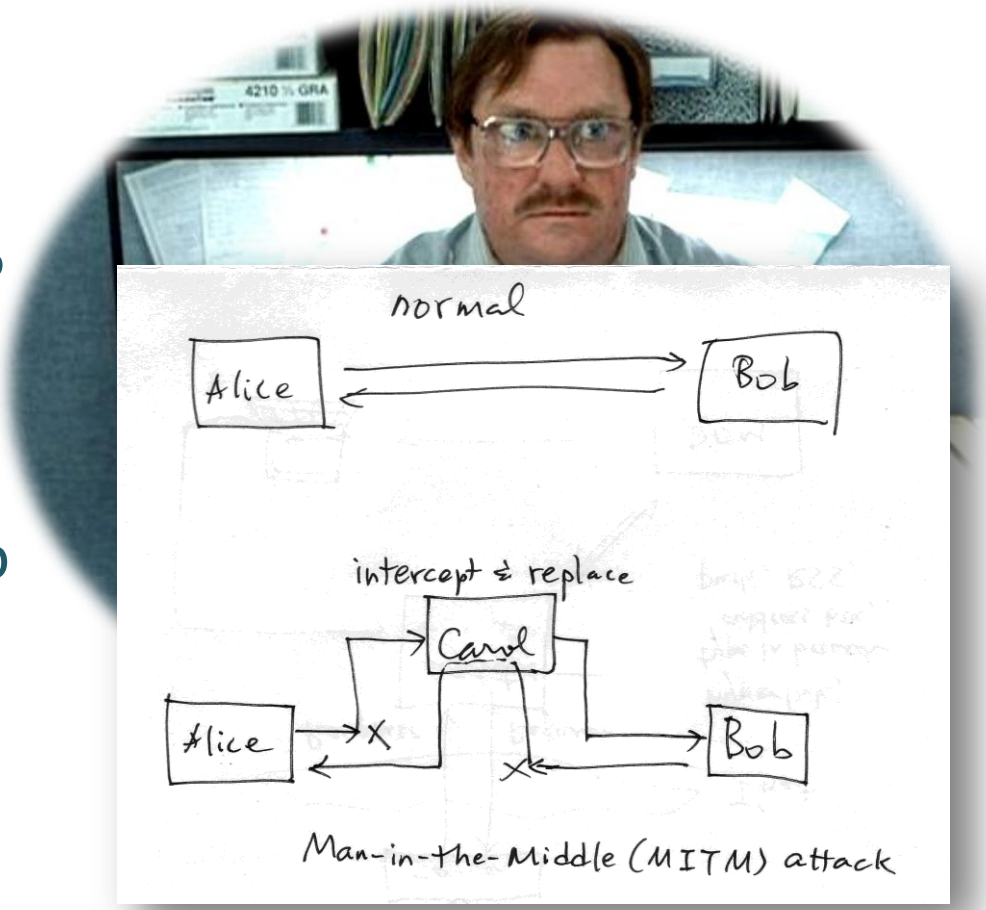
> Nobody is secure. Sony is just the tip of this thing.
>
> There's nothing from the government or regulatory industry that says anything about how to run a shop.
>
> You would have thought a big time reputable company like Sony would be running up-to-date, patched software with an appropriate firewall. If Sony didn't do this, which other big, reputable companies aren't doing this?

http://www.wallstreetandtech.com/articles/229403047?cid=nl_wallstreettech_daily


#2

City of San Francisco

"…not only was Childs the only admin, he was always on call, 24 hours a day, 7 days a week, 365 days a year. As the only admin with the knowledge and access to the FiberWAN, he had no help…keeping the city dependent on a sole admin for its core network."



THE VINDICTIVE ADMIN

http://www.pcworld.com/businesscenter/article/149159/sorting_facts_from_fiction_in_the_terry_childs_case.html

Shionogi

"Cornish then [deleted] the contents of each of 15 'virtual hosts' on Shionogi's computer network. These 15 virtual hosts (subdivisions on a computer designed to make it function like several computers) housed the equivalent of 88 different computer servers."

THE VINDICTIVE ADMIN

http://www.flyingpenguin.com/?p=13259

Google

"…we are significantly increasing the amount of time we spend auditing our logs to ensure those controls are effective. That said, a limited number of people will always need to access these systems if we are to operate them properly...."

THE VINDICTIVE ADMIN

http://gawker.com/5637234/

35

Salesforce

CHANGE CONTROL

2:46 am PDT : NA1/NA5/NA6/CS0,CS3,CS1,CS12 salesforce.com System Status

The salesforce.com NA1/NA5/NA6/CS0,CS3,CS1,CS12 instances are continuing to experience a service disruption. Power issues were detected but our technician onsite has confirmed this has been fixed. We are currently working to restore the service. Please check the status of trust.salesforce.com frequently for updates regarding this issue.

http://www.zdnet.com/salesforce-com-suffers-worldwide-disruption-after-power-outage-7000000581/
http://www.informationweek.com/cloud-computing/software/salesforce-outage-follows-data-center-po/240003577
http://www.wired.com/cloudline/2012/07/salesforce-outage/


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CRISC
CGEIT
CISM
CISA

#4

38

LinkedIn

THE BARN DOOR

"What has surprised customers and security experts alike is that a company that collects and profits from vast amounts of data had taken a bare-bones approach to protecting it. The breach highlights a disturbing truth about LinkedIn's computer security: there isn't much."

-- NYT 2012/06/11

"LinkedIn spent nearly $1 million investigating and unraveling the theft of 6.5 million passwords in June and plans to spend up to $3 million more updating security on its social networking site."

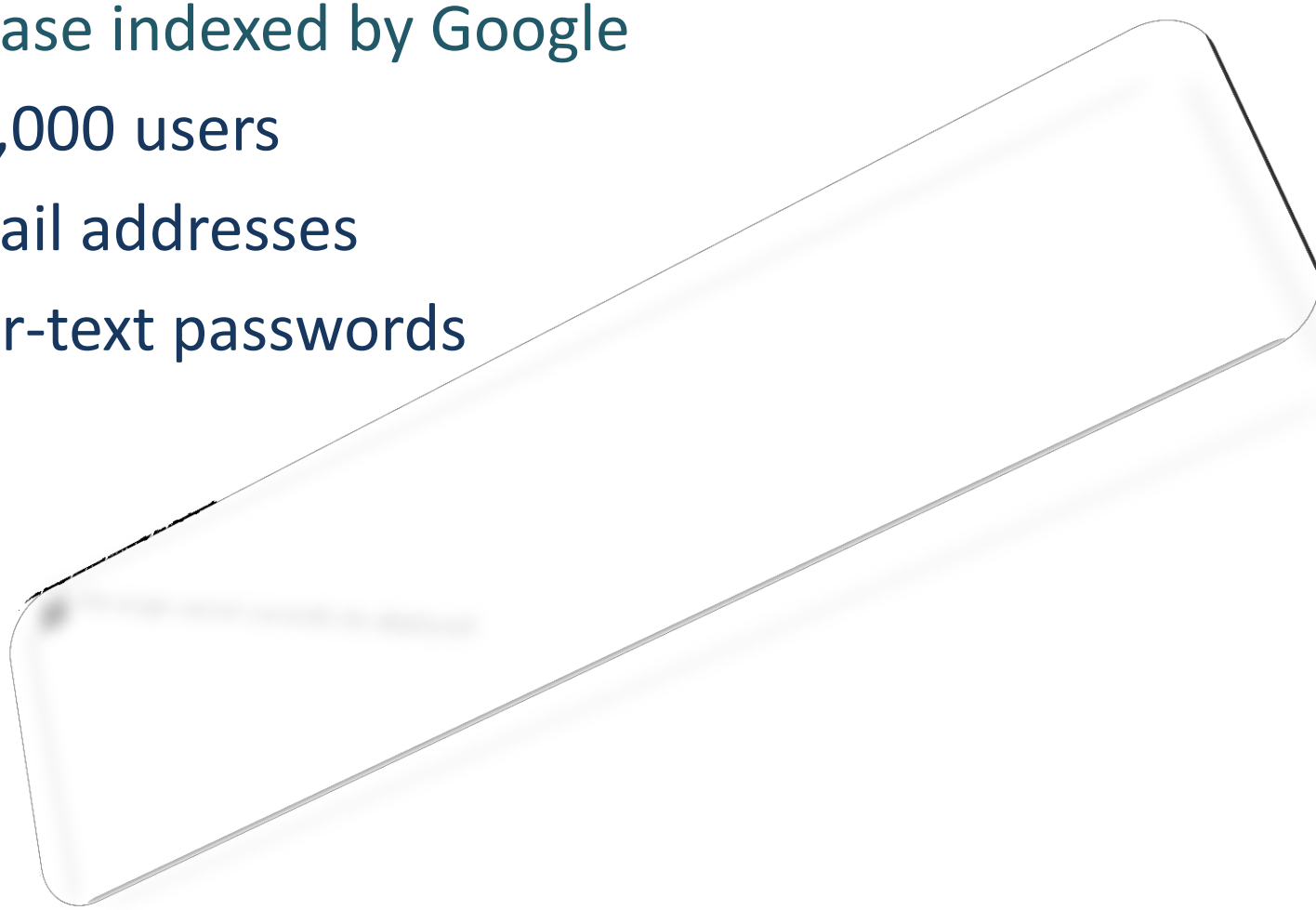
-- ZDNet 2012/08/03

http://www.nytimes.com/2012/06/11/technology/linkedin-breach-exposes-light-security-even-at-data-companies.html
http://www.zdnet.com/breach-clean-up-cost-linkedin-nearly-1-million-another-2-3-million-in-upgrades-7000002115/

Groupon

THE BARN DOOR

1. Indian subsidiary Sosasta, acquired Jan 2011
2. Database indexed by Google
   - 300,000 users
   - e-mail addresses
   - clear-text passwords



http://risky.biz/sosasta

Dropbox

THE BARN DOOR

- Marketing
  - Crypto Strength (e.g. AES 256 bit)
  - Process - Always Encrypted
- Reality
  - Keys managed by Dropbox
  - No external review
  - No confidentiality or integrity validation

Lessons Learned

42

Lessons Learned

1. Remove (Regulated) Data
   - World
   - Large
   - Named
2. Define Boundary
   - Services, Ports, Listeners, Interfaces
   - Privileges, Processes and Patterns
3. Secure Access
4. Monitor Change, “Breaches” and HR
5. Protect Data

Social Media

Control Objectives

Control Objectives	Cloud Marketing
1. Remove Data	Spread Data
2. Define Boundary	Overcome Boundaries
3. Secure Access (Apps)	Access Anywhere and APIs
4. Monitor	Always Up
5. Protect Stored Data	Always Up

Control Objectives

Control Objectives
1. Remove Data
2. Define Boundary
3. Secure Access (Apps)
4. Monitor
5. Protect Stored Data


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CRISC
CGEIT
CISM
CISA

2. Define Boundary

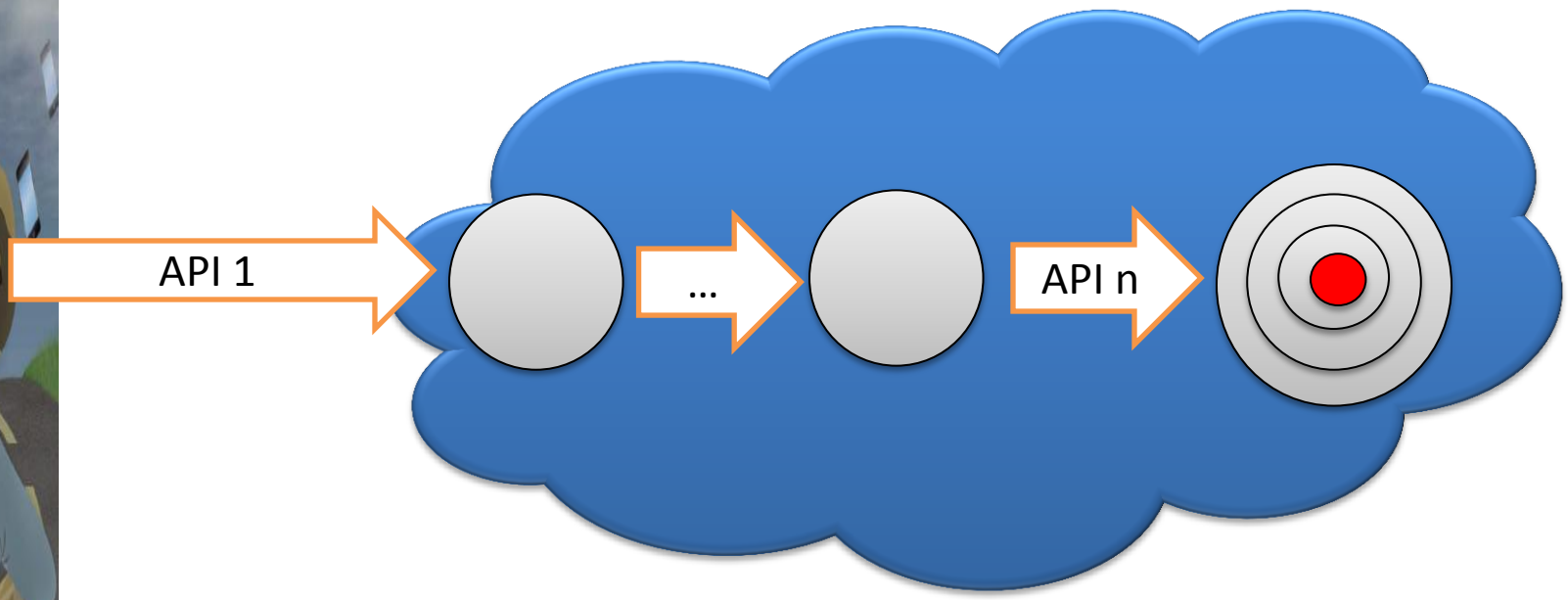
3. Define Boundary

- …directory traversal allows remote retrieval of any file from host
- Attacker needs access to network on which host resides

http://www.vmware.com/security/advisories/VMSA-2009-0015.html
http://www.metasploit.com/modules/auxiliary/scanner/http/vmware_server_dir_trav

CVE-2009-3733

3. Define Boundary



3. Secure Access - Authentication

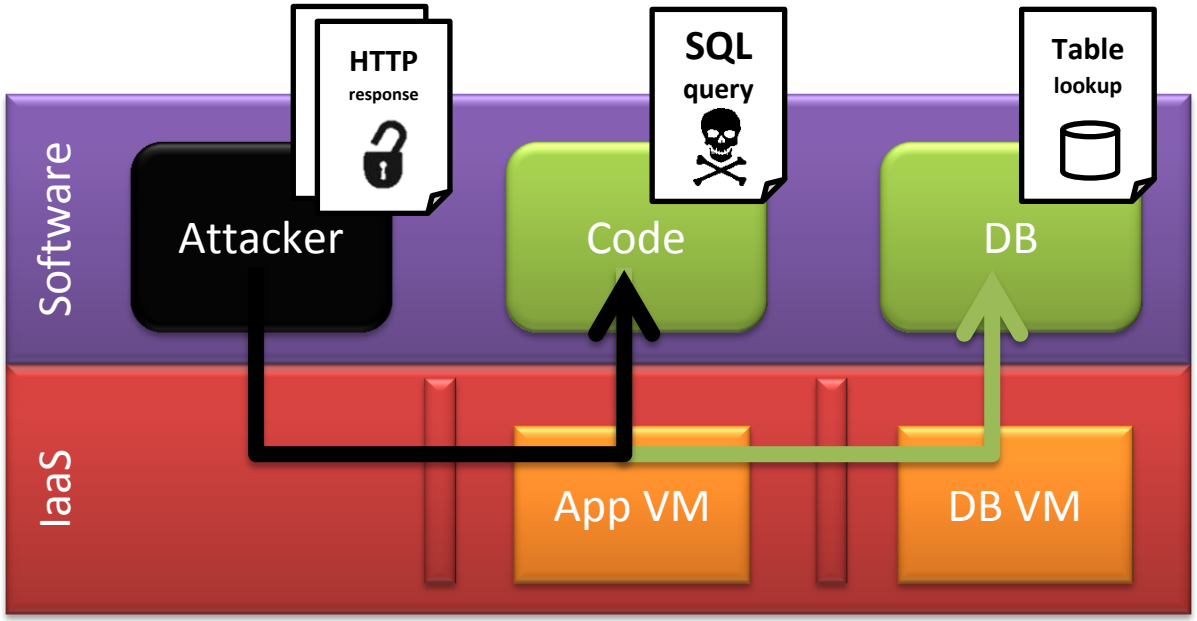
Choke Point

3. Secure Access - Authentication

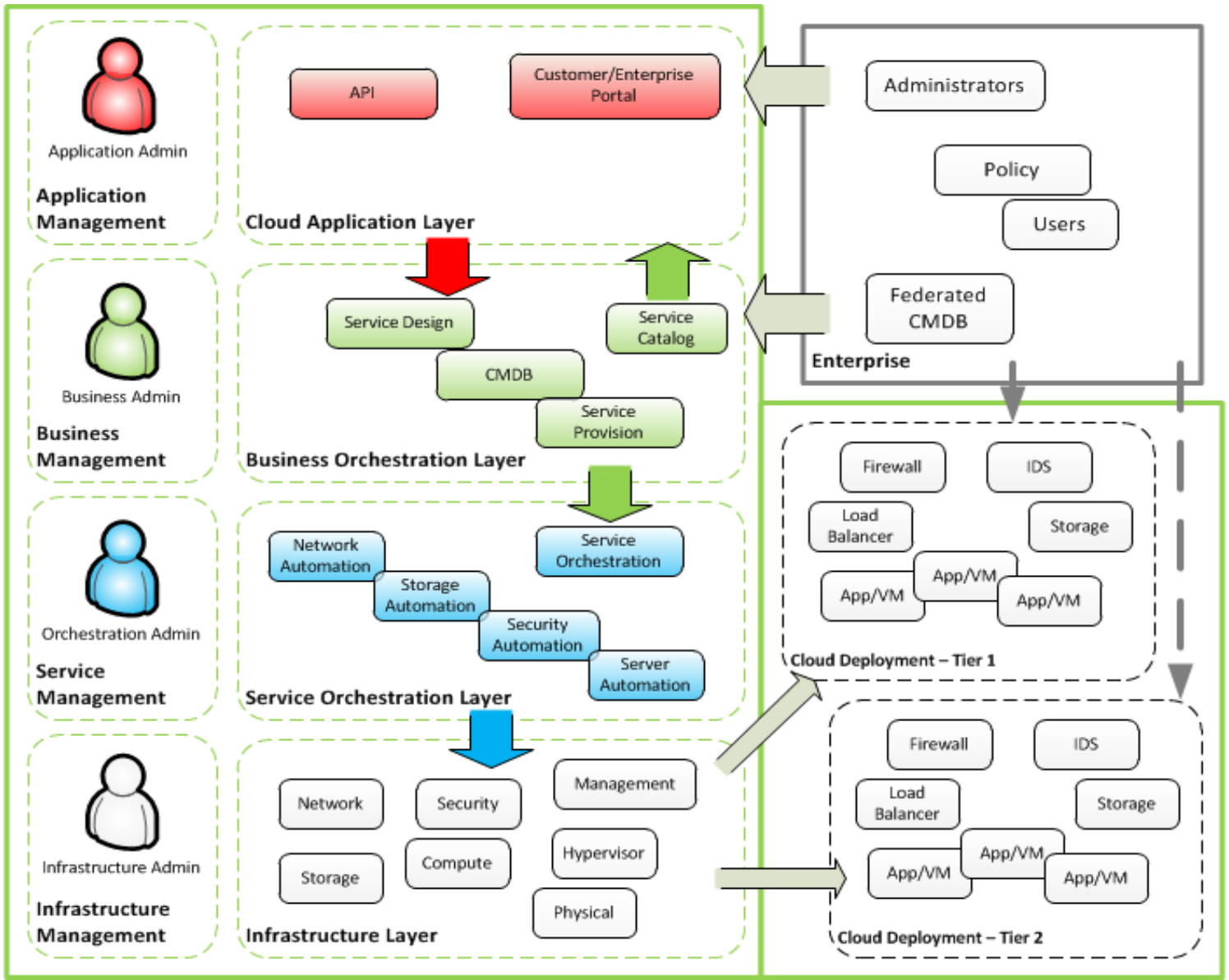
1) SQL injection instead of login
2) App converts data to SQL query
3) DB runs query, returns encrypted data
4) Application decrypts data and displays

Users

Username: Kermit Frog
Username: Rolph Dog
Username: Fozzie Bear



3. Secure Access - Authorization



4. Monitor - File Integrity

- Dormant
- Hibernated
- Template
- Move
- Copy

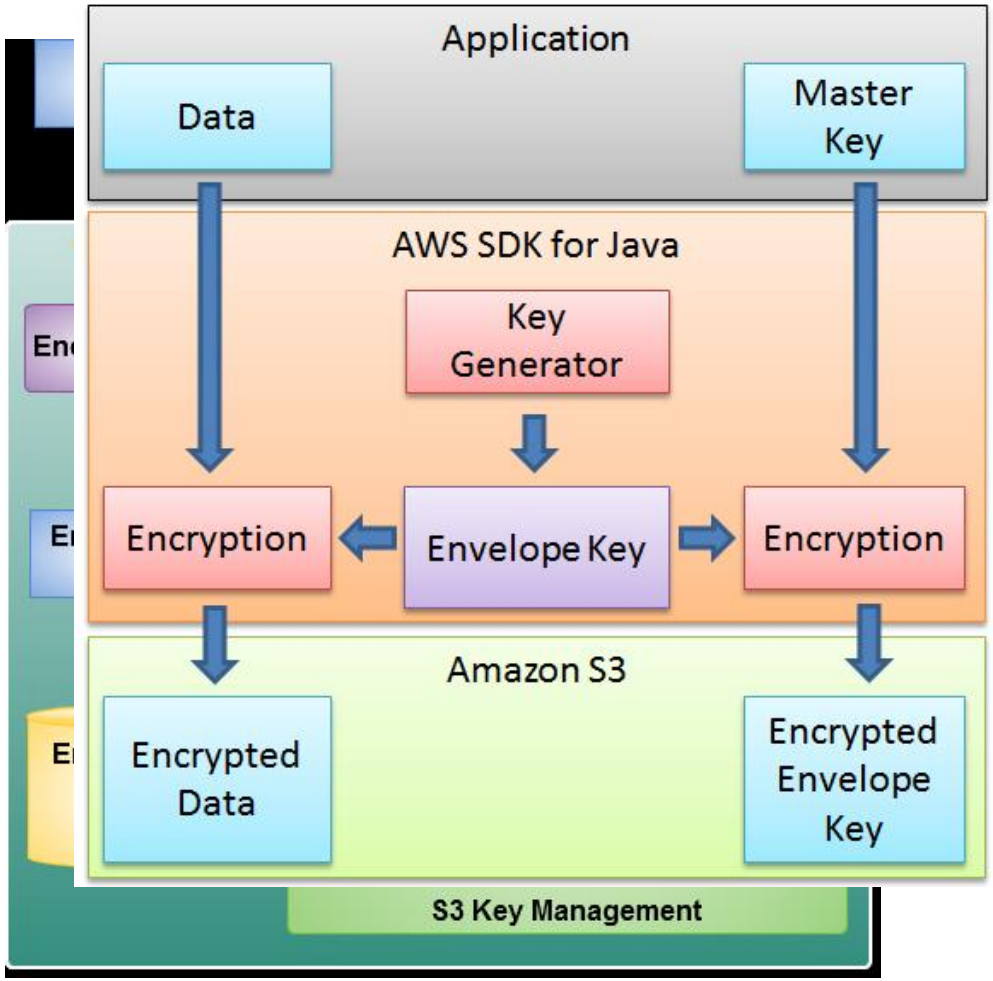
WINDOWS	UNIX
Access time	Access time
Creation time	Change time
Write time	Modify time

System	Database	Network	IAM	Application
Audit Trail				
Configs Binaries Registry Permissions	Tables Indexes Stored Procedures Permissions	Routes Rules Configs ACLs	Users Groups Roles Passwords	Keys Binaries Configs


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CRISC
CGEIT
CISM
CISA

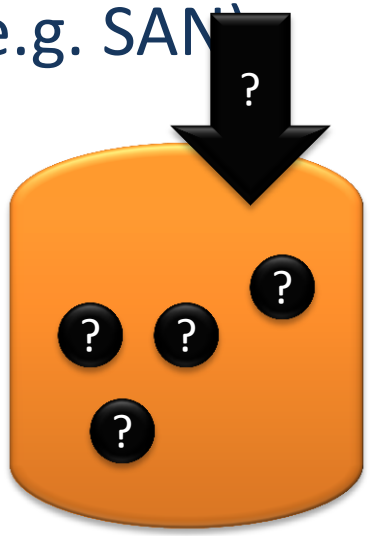
5. Protect Stored Data

- Encryption
  - Client Side
  - Server Side
- Residue
  - Suspend, Hibern
  - Swap
- Tokenization
  - Randomness



5. Protect Stored Data: AWS

- Instance Storage (C: Drive)
  - Dependent on Machine (Non-persistent)
- Elastic Block Storage (EBS)
  - Retained Independent of Server (e.g. SAN)
  - Encrypt Blocks
- Simple Storage Service (S3)
  - Independent, persistent
  - HTTP-based API
  - Encryption Library



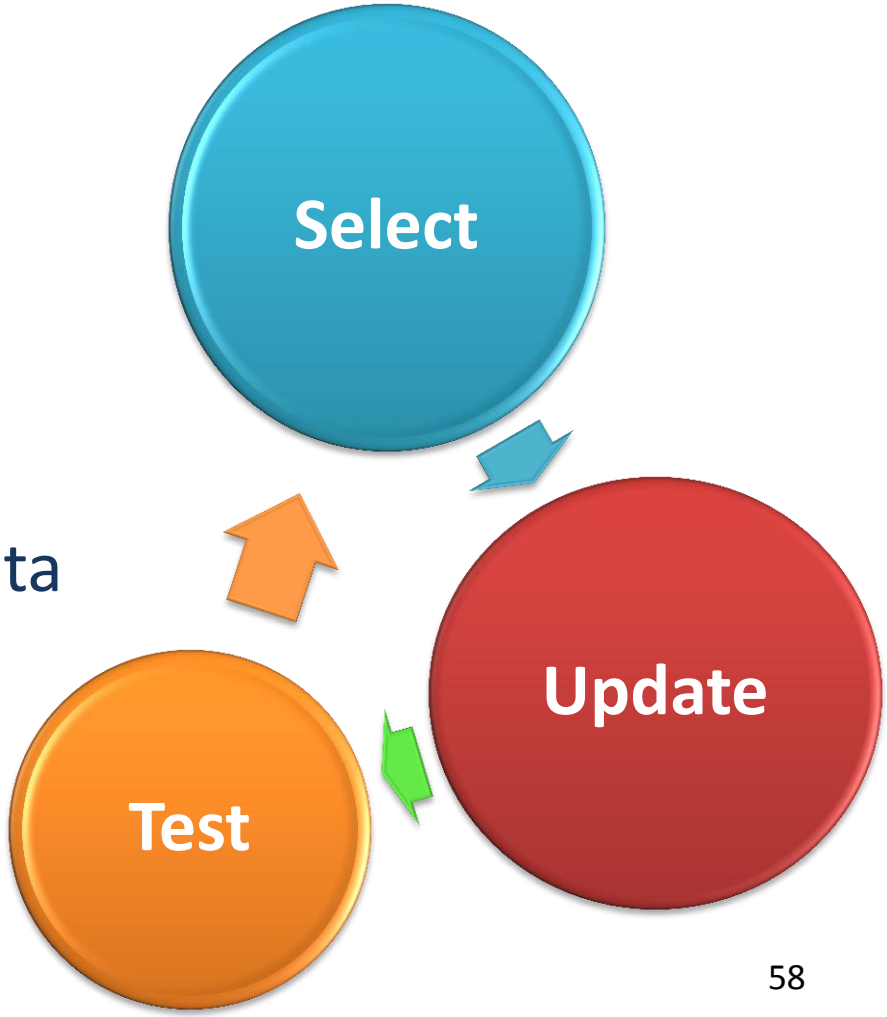
5. Protect Stored Data: VMware

- Virtualization files
  - .vxmf – teaming configuration (workstation groups)
  - .vmx – machine configurations
  - .vmsd – snapshot descriptor
  - .vmdk – disk geometry, layout, structure (VMFS-3 max 32 physical extents)
  - .vmem – paging file backup
  - .vswp – swap file
  - .vmss – suspended state
  - .vmsn – snapshot of running state of a machine
- Suspend leaves memory on physical disk
  - .vmss created
  - .vswp removed

http://communities.vmware.com/docs/DOC-13179

Apply Today's Presentation

- Select Controls
  1. Remove Data
  2. Define Boundary
  3. Secure Access
  4. Monitor
  5. Protect Stored Data
- Update Controls
- Test Controls



Thank you!

davi@flyingpenguin.com

@daviottenheimer