



# Data Security

## Addressing Your Fears of Hosted eCapture & eReview

Presented By: Megan Wilcox

May 2009





Data Security:

## Addressing Your Fears of Hosted eCapture & eReview

- 2009 SaaSCon conference; ~500 attendees; top concerns include **Security** and integration.
- 2007 Forrester Research survey; 8 reason why companies say “No Thanks” to SaaS; 50% **Security** Concerns.
- Rackspace Managed Hosting survey sites **Security** among SaaS customers’ top technical concerns.

# Three Layers of Security

 **Physical Security**

 **Application Security**

 **User Security**





# Physical Security: Controlled Back End Access

- ✓ Back end – used by SaaS provider for maintenance and management

## SOLUTION TO THE FEAR = TOP TIER SAS-70 II DATA CENTER

Common Fear = No control over:

- Where the servers are at
- Who can get to the servers
- What security measures in place for building access
- How the equipment and running processes are protected against natural disaster



# Physical Security: Controlled Back End Access

## Building Access

- Security Gate
- 24-hour security guards/video surveillance
- Authorized access list/Photo ID verification

## Equipment Access

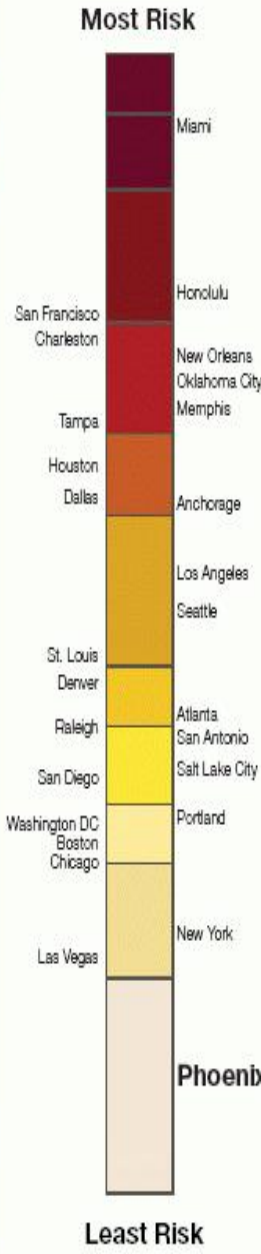
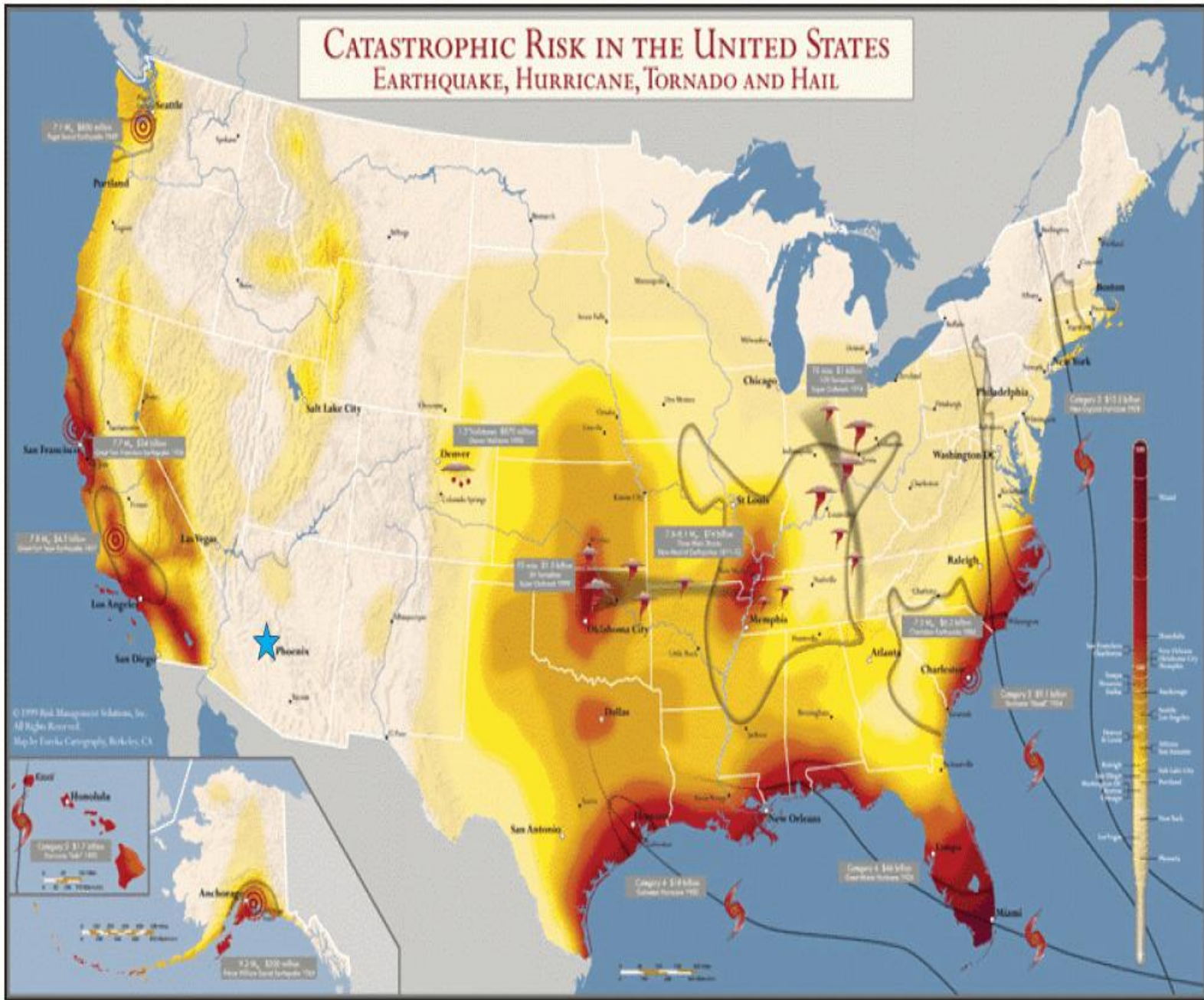
- Electronic Access Control
- Biometric Security
- Locked rack/cages

## Environment/ Disaster Security

- Disaster Free geographical area
- VESDA and pre-action fire suppression
- Diesel generator backup

# CATASTROPHIC RISK IN THE UNITED STATES

## EARTHQUAKE, HURRICANE, TORNADO AND HAIL



© 1999 Risk Management Solutions, Inc.  
 All Rights Reserved.  
 Maps by Florida Cartography, Berkeley, CA

# Application Security

Directly Associated With

- ✓ Role based access permissions; how do users get into the application/environment.

Common Fear =

- a) How is access authenticated/private
- a) Separation from other users of the environment



# Application Security



## Hybrid SaaS

- Dedicated Application Servers for each function
- Multi-tenant backend

## Encrypt Login

- Portal site hosted on HTTPS
- Active Directory User Authentication
- Server Access via VPN tunnel

## Dedicated NAS Share

- Active Directory Authentication
- Full Access
- IPRO 'hands-off' policy



Hybrid  
SaaS

Encrypt  
Login

Dedicated  
NAS  
Share



# User Security

## Identity Management

- ✓ Clients using the IPRO solution
- ✓ Administrators/Support Technicians of the IPRO solution

Common Fear = More hands in the Cookie Jar:

- Customer access to data
- IPRO Personnel access to data
- Who is looking at the files?
- Who is touching the files?

# User Security

- Required for all IPRO personnel that interact with the SaaS environment for support, maintenance, or management

- Includes items such as:
  - Password Strength Requirements
  - Client data confidentiality
  - Data Access limitations

- Access Granted to only members of, IPRO executives, IPRO corporate IT or IRPO SaaS Dept.

SaaS Security Policy

Mandatory Background Checks

Data Center Access List

Custom Identity Management per Account

- Required for all IPRO personnel that have access to customer data or physical devices on the SaaS environment

- You control who gets the logins
- Password Resets granted
- Customize authorized personnel to make requests for environment



# Data Security:

## Addressing Your Fears of Hosted eCapture & eReview

1. Physical
2. Application
3. User

**Fear = No control over systems protections from people and nature.**

**Solution = Host with a top tier Data Center**

**Fear = Unsure on how access is private and encrypted.**

**Solution = Dedicated resources and multiple layers of authentication and encryption**

**Fear = More people managing systems and have access to data**

**Solution = Strict security and confidentiality clauses and accommodating custom requests.**





# Data Security

## Addressing Your Fears of Hosted eCapture & eReview

Presented By: Megan Wilcox

May 2009

