



# Security Considerations When Moving to the Cloud

February 6, 2013  
Delaware Cyber Workshop 2013

Presented by Jim Garrity

# Agenda

- Lets look at data security concerns
  - Consumer perspective
  - Company/executive perspective
- Where are the hidden risks?
  - Data leaks
  - Social engineering
  - Big data and how it is used/handled
- How the cloud provides a better solution
- Q&A

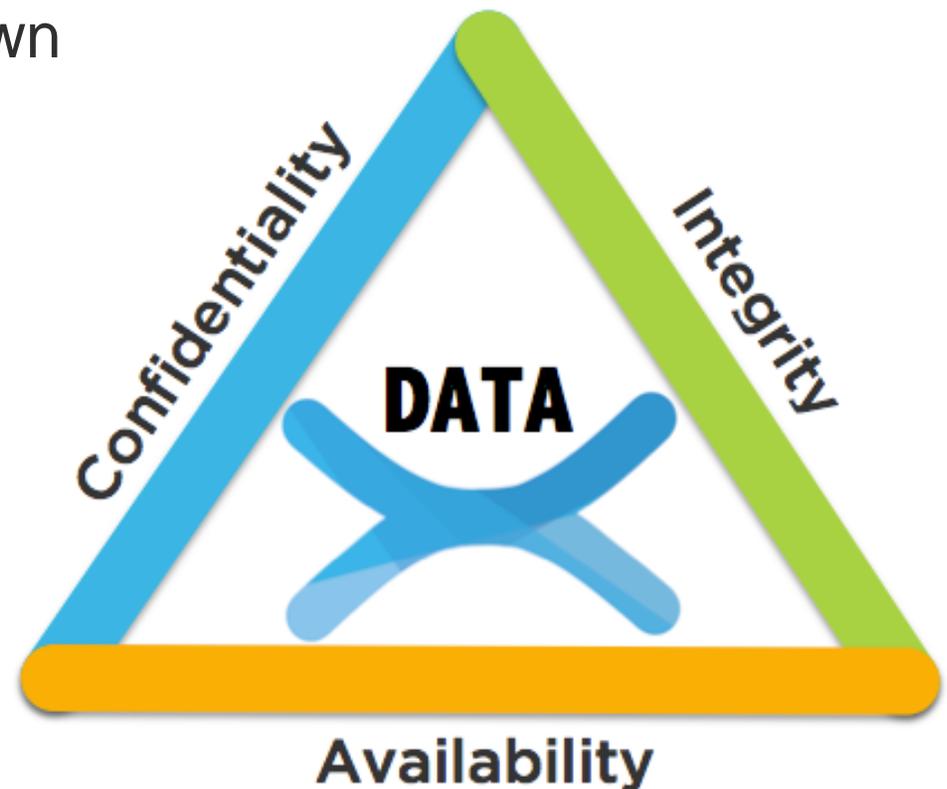


# Cloud Security Concerns

What should I be focused on?

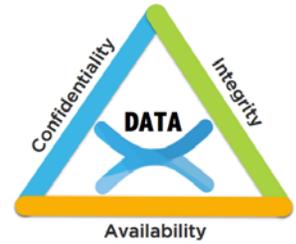
Cloud security concerns boil down to three areas of risk:

1. Confidentiality
2. Integrity
3. Availability



# Cloud Security Concerns

## Area of Risk: Confidentiality



Consider your **medical** and **financial** data...



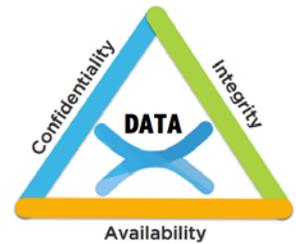
- Does anyone outside of me and my primary care provider have access to my detailed medical history?
- What does my insurance company have access to?
- What does IT have access to? Everything?



- Banking and investment data – browser attacks provide data
- Credit scores – what does my employer do with my data?
- Purchase history – spender or saver? Impact to employer?

# Cloud Security Concerns

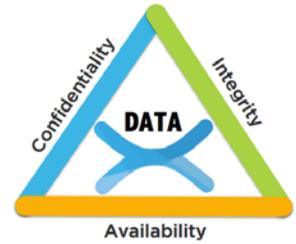
## Area of Risk: Confidentiality



- Confidentiality – limiting information access and disclosure to authorized users (“the right people”) and preventing access by or disclosure to unauthorized ones (“the wrong people”)
- Authentication – ability to uniquely identify a data system’s users, and supporting controls that limit each identified user’s access to the data system's resources
- Protection – needed against injection attacks, cross-site scripting attacks, phishing, spyware, and other attacks
- Data privacy – limiting access to individuals’ personal information

# Cloud Security Concerns

Area of Risk: Confidentiality

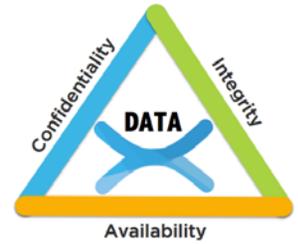


Cyber-attack at South Carolina tax collection agency

- Exposure: **387,000** credit cards, **3.6 million** social security numbers, **657,000** businesses
- Caused by: phishing email, clicked by one employee, which unleashed malware
- Cost to fix: **\$14+ million** and growing (informing tax payers; one year free credit monitoring; PR; legal; and updating technology security systems)

# Cloud Security Concerns

Confidentiality of data – Have you thought about the following?



Personnel issues – 73% of the issue



Virtual perimeter security



Privileged and end-user access



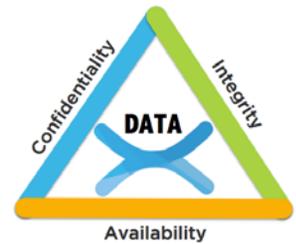
Investigative support



Backup and recovery – usually not secure

# Cloud Security Concerns

## Areas of Risk: Integrity



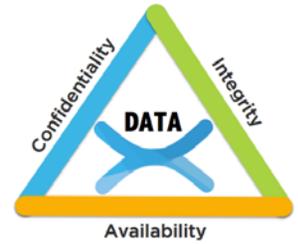
Is my data going to be used in the right way when it is not in my possession?

Is the data going to be manipulated or changed on my behalf?

Recent issues in banking industry where an end-user sees a different set of transactions and balance vs. a hacker.

# Cloud Security Concerns

## Areas of Risk: Integrity

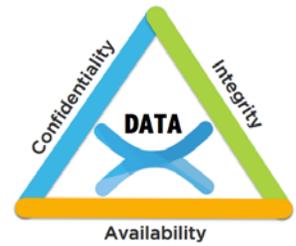


When data is provided to a consumer, the data is provided in a way that allows no manipulation of the original source data.

Integrity in IT is ensuring that data is preserved in its original state without being compromised by a technology or person and is provided to the consumer in its native form.

# Cloud Security Concerns

Areas of Risk: Accessibility or Availability



Recent outages affect sites:

**NETFLIX**



tumblr.

woot!

skype™

Pinterest

zynga

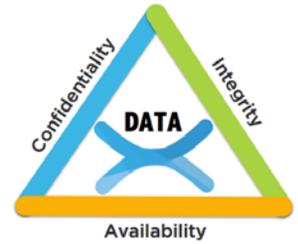
Data and applications are no good if they are not available.

Is the data set up in such a way that it cannot be easily lost?

What is the IT person's responsibility related to High Availability?

# Cloud Security Concerns

## Availability of Data



Web applications that provide critical data to consumers must always be available.

How do we go about building these highly available structures from the following perspectives?

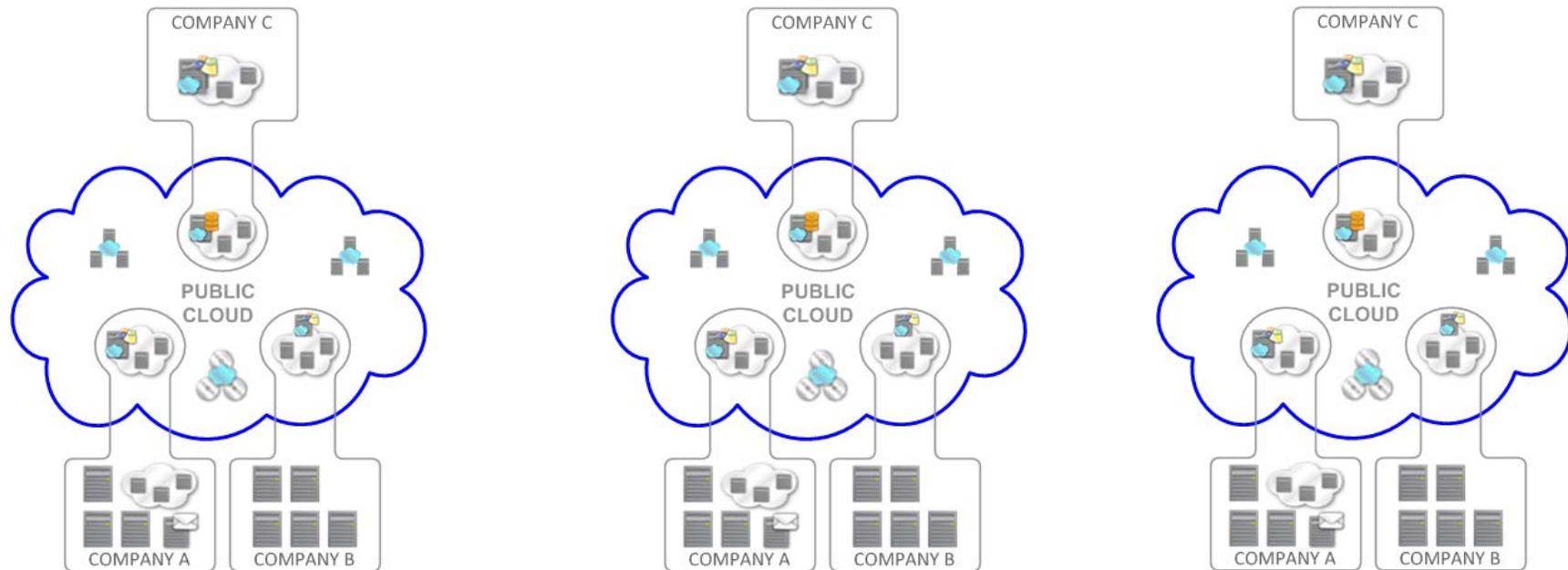
- Data center
- Network
- Cloud
- Storage

# How the Cloud Addresses Security

# The Cloud Addresses Security

$$S^2 + C^2 = B$$

The cloud is a smarter, stronger, more cost effective way to ensure that your data remains safe and compliant, running your business more effectively.



# The Cloud Addresses Security

## Start at the Data Center

A true cloud starts with the data center in mind:

- Tier 3 and 4 data centers
- Tier 1 networks (aggregate providers)
- Security that would rival most federal buildings

No cloud sits across one data center. Multiple data center approach is key.



# The Cloud Addresses Security

## Focus on the Networks

1. Networks should be diverse within the data center and across the globe
2. DDOS Mitigation Strategy must be in place to ensure availability
3. IDS/IPS must be in place
4. Data that traverses the network must be secured in transit

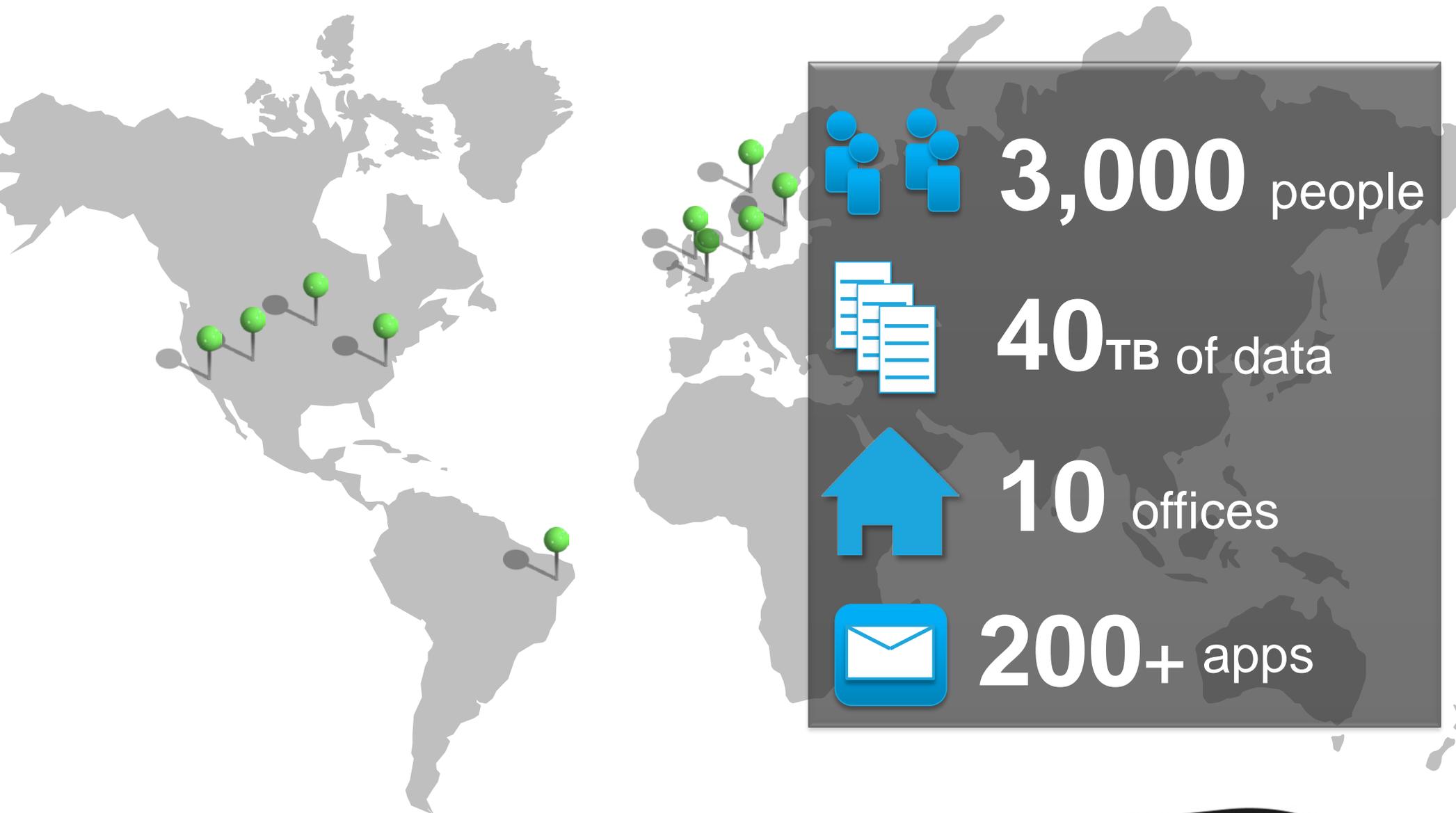
# The Cloud Addresses Security

## Bulletproof Cloud and Storage

1. Cloud has built-in redundancy at every level
  - Self healing nature of cloud
  - Redundant HA storage (controllers, disk)
  - I/O strategy
2. Virtual firewall strategy
3. Encrypted virtual network interfaces
4. Web application firewalls
  - CSSA
  - SQL injection
  - Mobility hacks
5. Storage
  - Data at rest
  - Data in transit
  - WORM technology
  - Audit

# Case Study

Payday loan company chooses the cloud to improve security



# The Cloud Addresses Security

Tell me something I do not know

Big data analytics and cloud provider services – the future of staying secure – WHY?

What does Quantum Computing have to do with anything?  
When will I go out of business when this technology hits?  
How does a hosting company help me with that?

# Discussion

Q & A

# Thank You

Jim Garrity

Vice President of Business Operations, Xtium

[Jim.garrity@xtium.com](mailto:Jim.garrity@xtium.com)