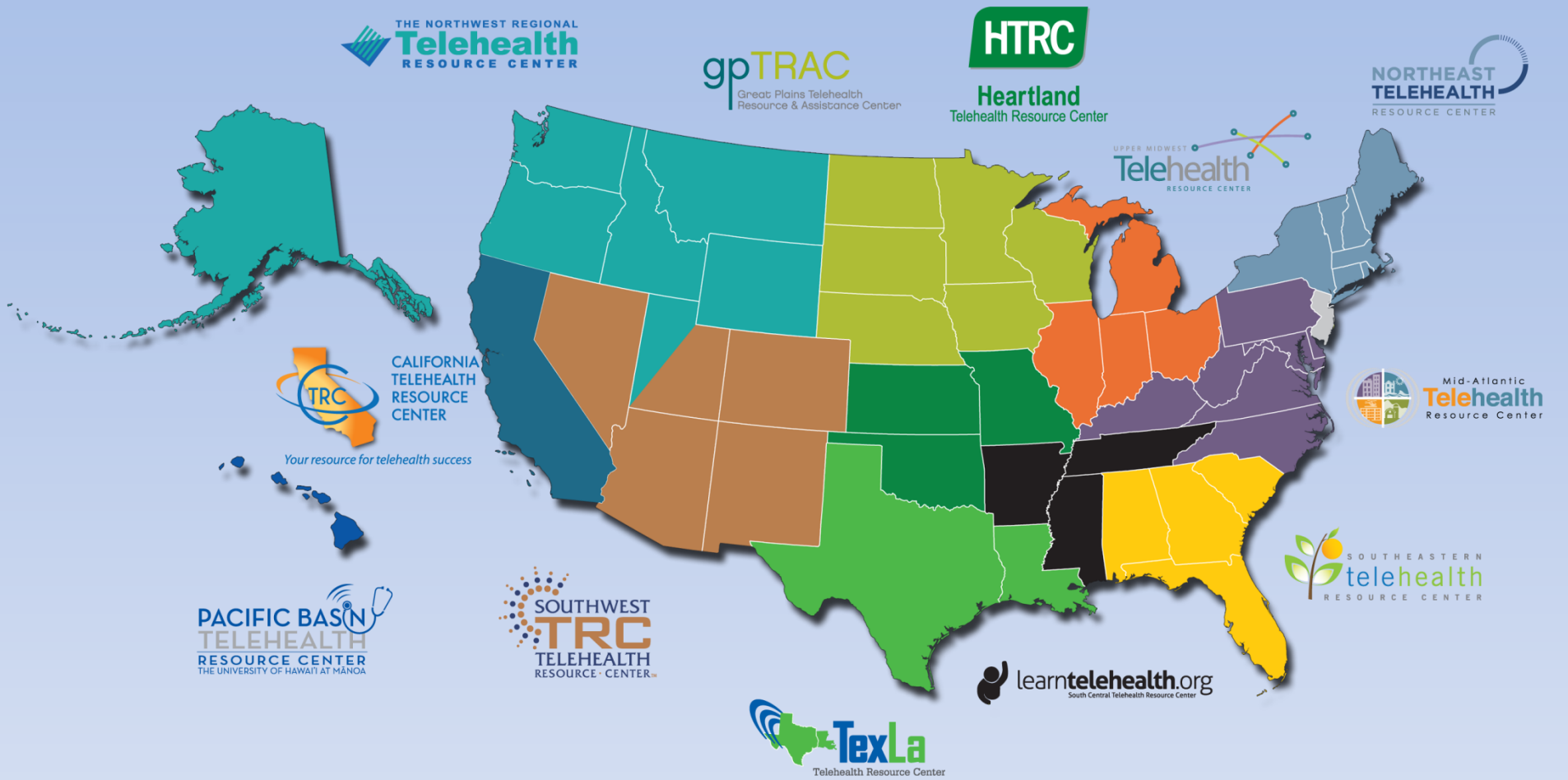

# The National Telehealth Webinar Series

Presented by
The National Network of
Telehealth Resource Centers

# TelehealthResourceCenters.org




TTAC TelehealthTechnology.org National Telehealth Technology Assessment Resource Center

Center for Connected Health Policy

2 National Resource Centers


| | | |
|---|---|---|
| NRTRC | gpTRAC | NETRC |
| CTRC | HTRC | UMTRC |
| SWTRC | SCTRC | MATRC |
| PBTRC | TexLa | SETRC |

12 Regional Resource Centers

Telehealth
Resource Centers

# Understanding and Managing the Risks of Cloud-Based Services

**Garret Spargo**
**National Telehealth Technology Assessment Resource Center**

19 December 2013

(9:00AM HST, 10:00AM AKST, 11:00AM PST, 12:00PM MST, 1:00PM CST, 2:00PM EST)

C:\> Shall we play a game?

zk8NJgAOqc4=

g+/hUkh3HrbSPm/keox4fA==

C:\> Shall we play a game?

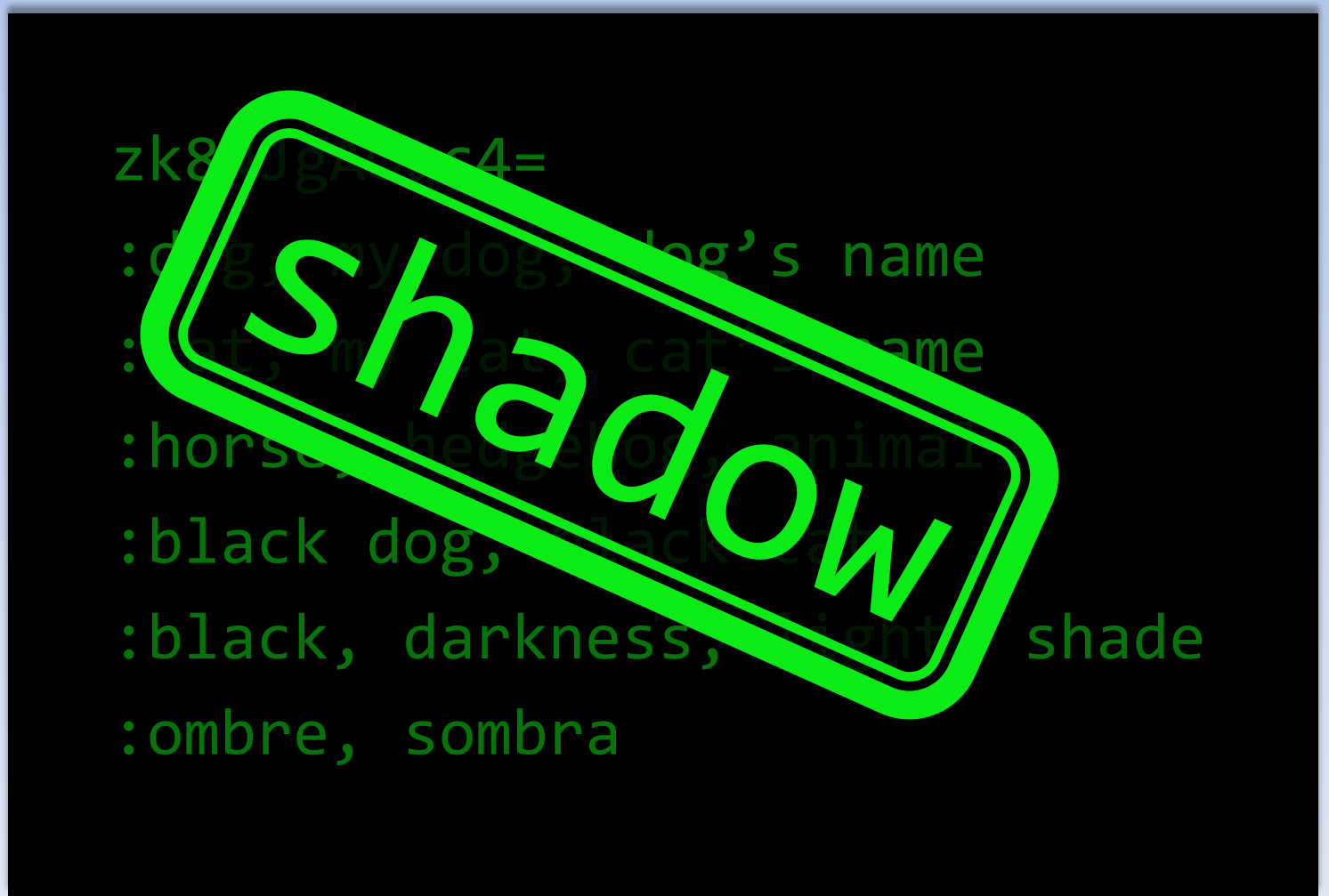
```
zk8NJgAOqc4=
:car

g+/hUkh3HrbSPm/keox4fA==
:school
```

# C:\> Shall we play a game?

```
zk8NJgAOqc4=
:dog, my dog, dog’s name
:cat, my cat, cat’s name
:horse, hedgehog, animal
:black dog, black cat
:black, darkness, light, shade
:ombre, sombra
```

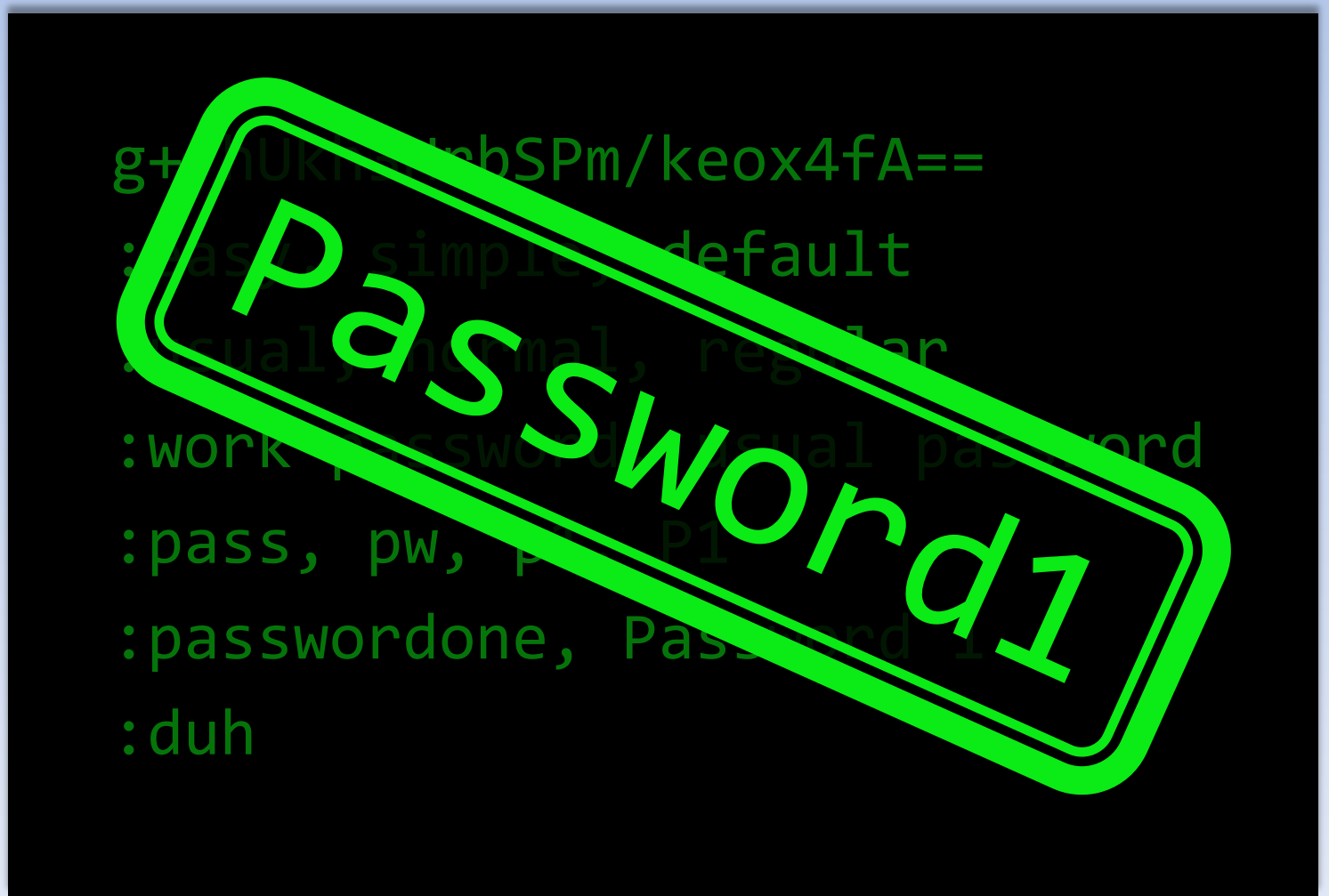
C:\> Shall we play a game?



# C:\> Shall we play a game?

```
g+/hUkh3HrbSPm/keox4fA==
:easy, simple, default
:usual, normal, regular
:work password, usual password
:pass, pw, p1, P1
:passwordone, Password 1
:duh
```

C:\> Shall we play a game?



# Overview

Cumulus: The fluffy white cloud

- What is the cloud, and why do we like it?

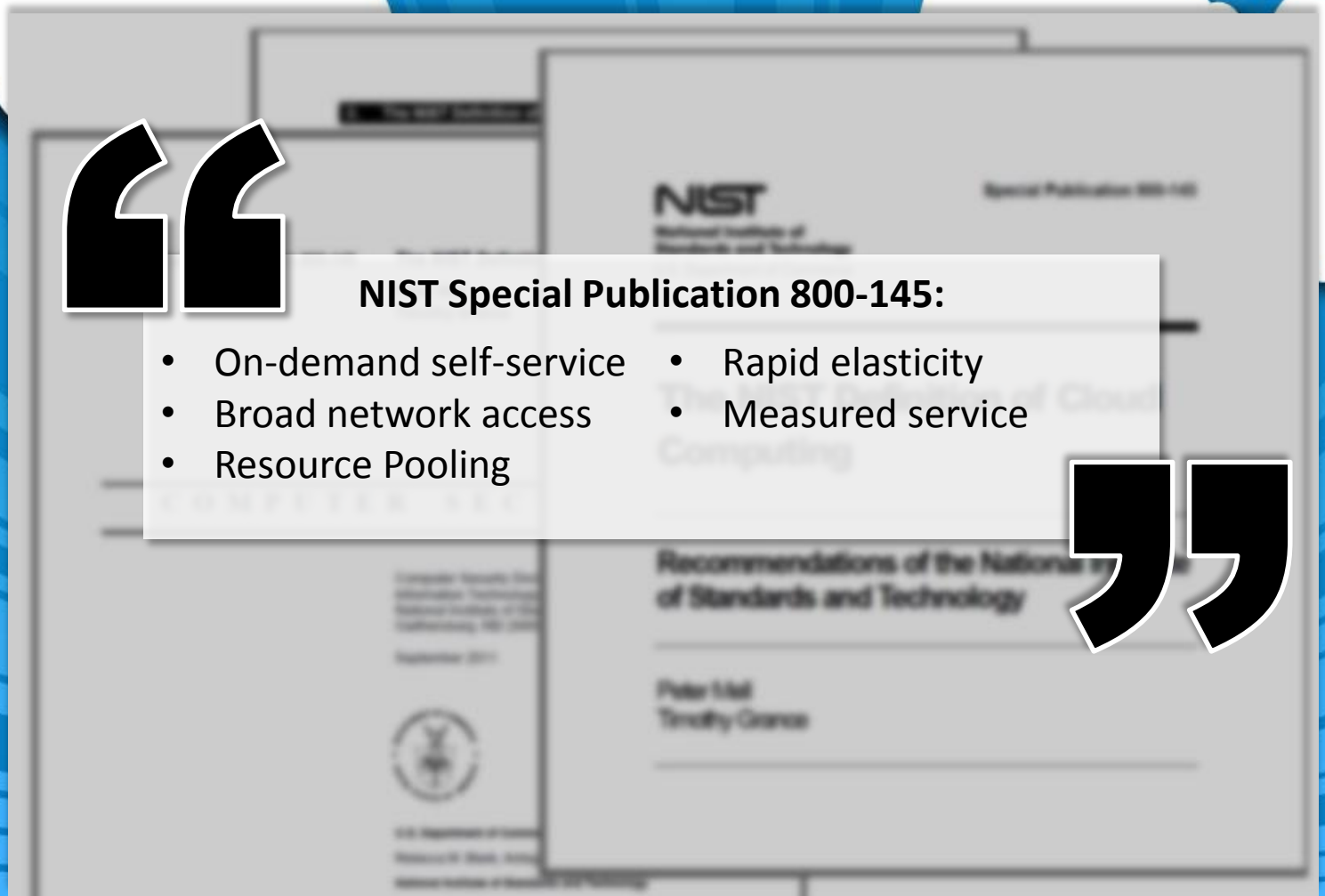
Nimbostratus: Rain on the horizon

- The downsides to cloud services.

Cumulonimbus: When lightning strikes

- Cloud safety and risk management.

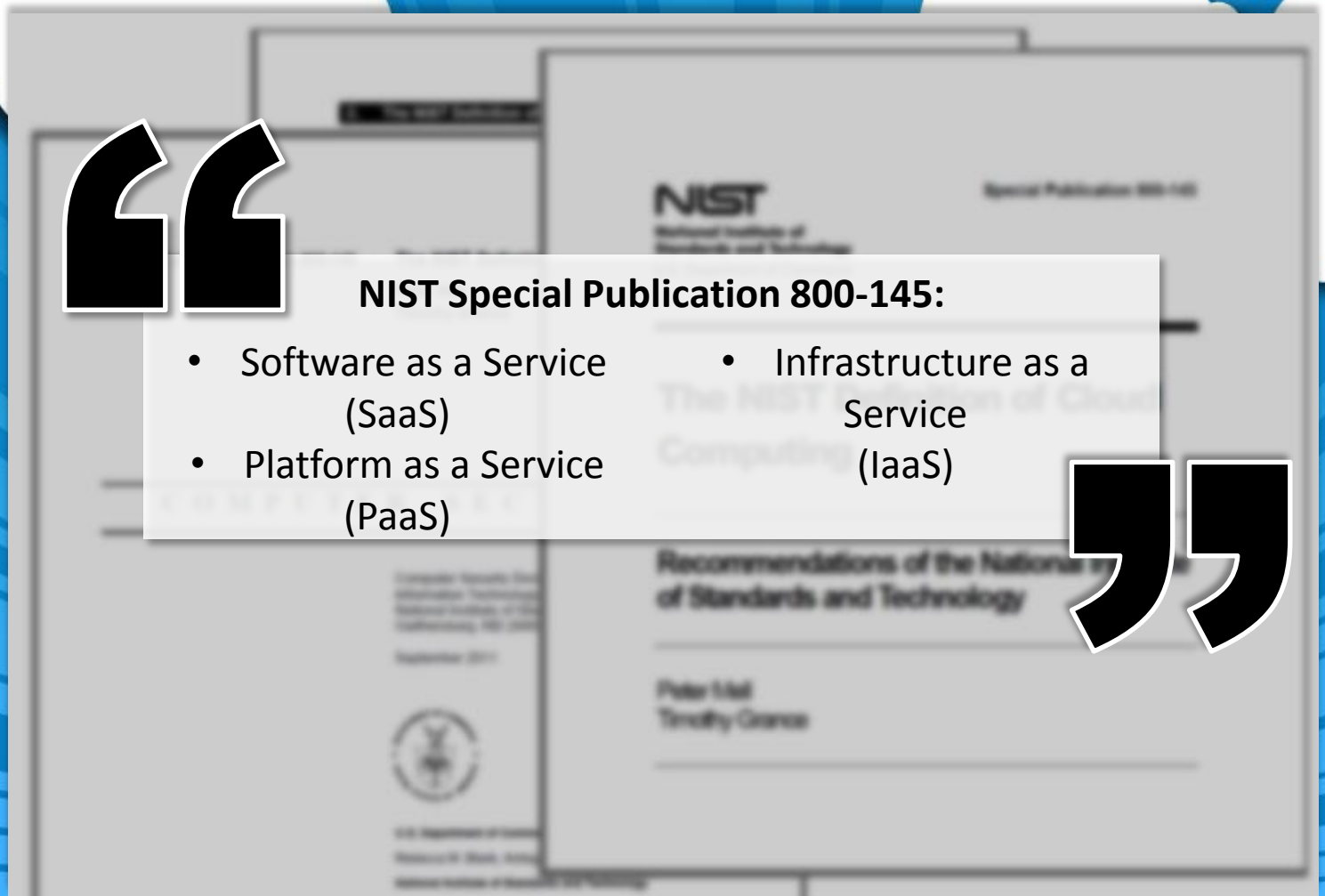
# Cumulus: What is the cloud?



**NIST Special Publication 800-145:**

- On-demand self-service
- Broad network access
- Resource Pooling
- Rapid elasticity
- Measured service

# Cumulus: What is the cloud?




**NIST Special Publication 800-145:**

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

# Cumulus: What is the cloud?

- Web-based applications and services
  - Salesforce.com, Google Apps
  - Email, social media & networking
  - mHealth and wellness portals
  - ArcGIS (resource-intensive application)

# Cumulus: What is the cloud?

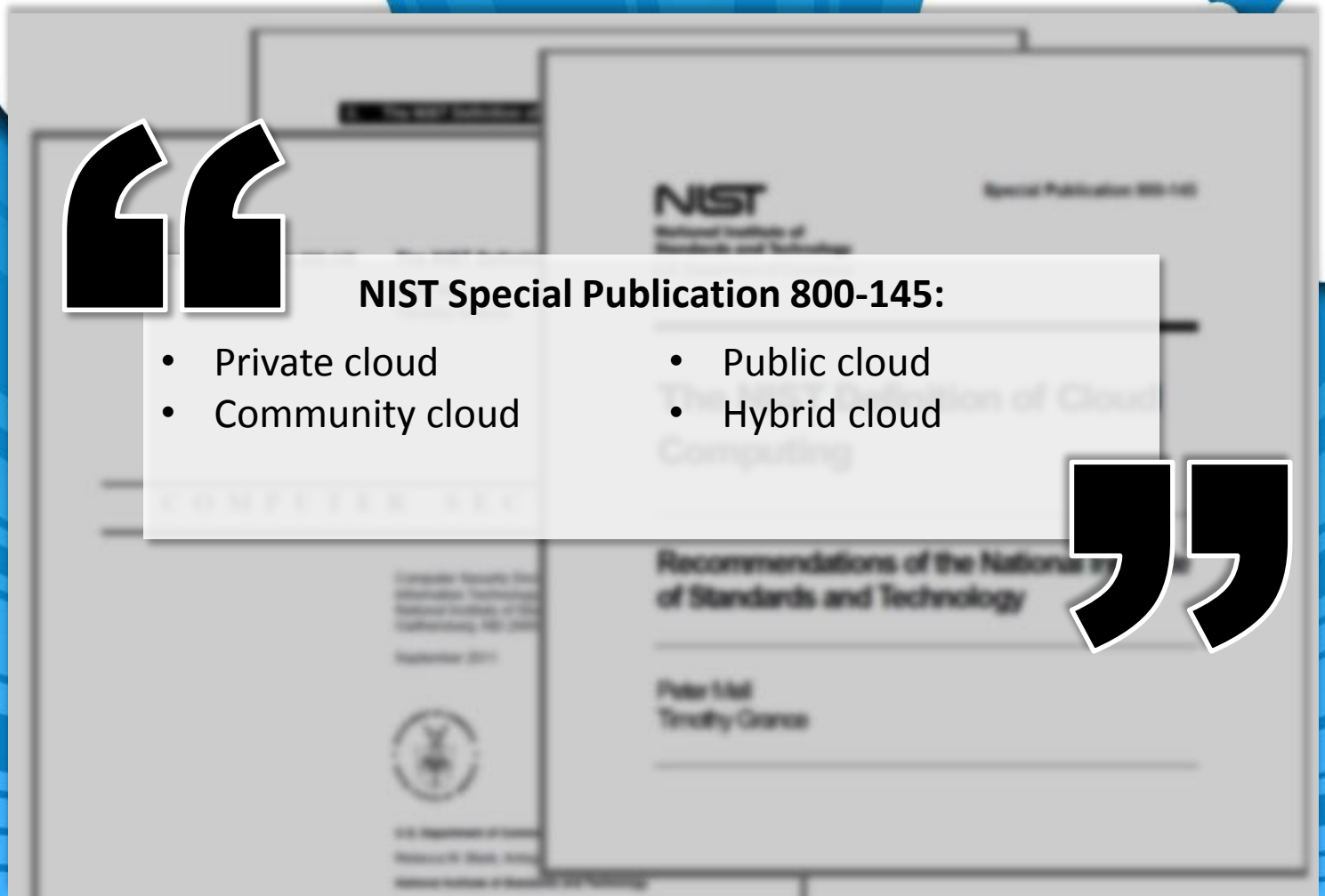
- Personal “content lockers”
  - SkyDrive, Google Drive, DropBox, Amazon Cloud Drive, iCloud, etc.
  - Will grow from 1.7 EB in 2012 to 20 EB in 2017 (1 Exabyte = 1,000,000 Terabytes)
- Corporate “remote data storage”

http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.html
http://www.cisco.com/en/US/netsol/ns1175/networking_solutions_solution_category.html
http://www.vmware.com/files/pdf/cloud/eight-key-ingredients-building-internal-cloud.pdf

# Cumulus: What is the cloud?

- Runtime, development, and cloud computing platforms
  - Provide access to a range of applications and system configurations for temporary or long-term use
- Hosting infrastructure
  - Provide physical or virtual devices
- Amazon EC2, OpSource Cloud, GoGrid and Rackspace, Azure
- Web hosts, service providers, and virtualized data centers

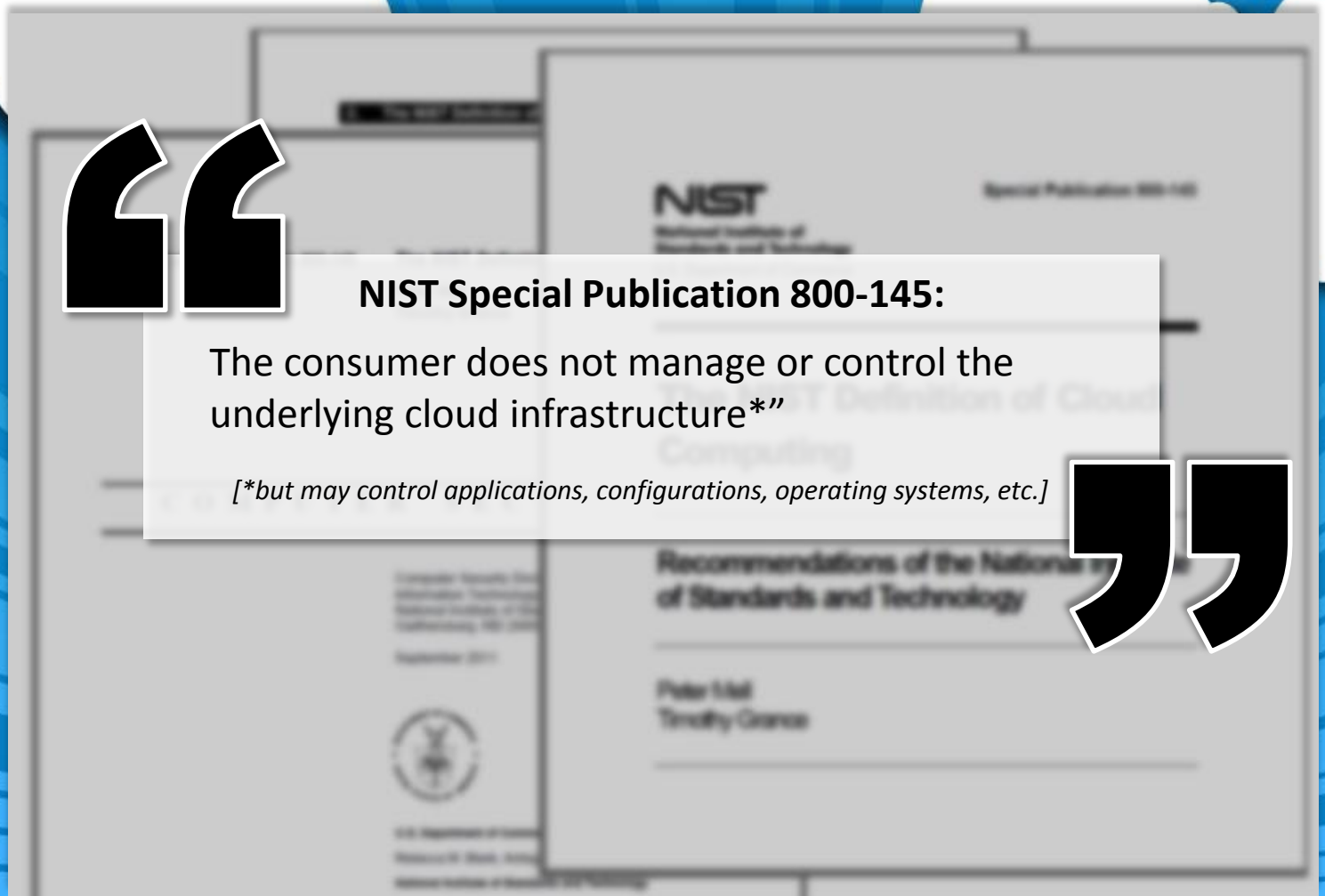
# Cumulus: What is the cloud?




**NIST Special Publication 800-145:**

- Private cloud
- Community cloud
- Public cloud
- Hybrid cloud

# Cumulus: What is the cloud?




**NIST Special Publication 800-145:**

The consumer does not manage or control the underlying cloud infrastructure*”

*[*but may control applications, configurations, operating systems, etc.]*

# Cumulus: What is the cloud?

- Need to balance costs, controls, and convenience when implementing a cloud-based solution
- Do you want it fast, easy, cheap, or reliable?

# Cumulus: Why use the cloud?

- Resources on demand
  - Account for peak utilization
  - Don’t have machines idly sitting
  - Ability to quickly stand up complex environments

# Cumulus: Why use the cloud?

- Redundancy and reliability
  - Possibility of geographic redundancy for disaster management / recovery
  - Localized problems may be circumvented
  - Access to support personnel and assets that might be underutilized if locally managed (and thus more expensive)

# Cumulus: Why use the cloud?

- Economic incentives
  - Economy of scale - a supercomputer at your fingertips
  - Switch from capital expenses to operational expenses
  - Reduce support cost of upgrading software on end-user machines

# Cumulus: Who uses the cloud?

- Large and small businesses, banks, law firms, recruiting offices, hospitals, schools, municipal, state, and national governments, research institutions, entrepreneurs, children, adults, parents, grandparents, the person sitting in your chair watching this (cloud-based) webinar.

# Cumulus: Who uses the cloud?

- Your customers and your employees are using the cloud
- Your organization – willingly or not – is supporting cloud-based applications and services
- By 2017, nearly two-thirds of all workloads will be processed in the cloud

http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.html

# Nimbostratus: What could possibly go wrong?

- Remember the Adobe game?
  - Was turned into a crossword puzzle
  - They emailed affected users – “it was an old system set to be decommissioned” – the new system is a salted hash
  - They only mentioned the loss of IDs and encrypted passwords (even though more data was lost)

zed0.co.uk/crossword

# Nimbostratus: What could possibly go wrong?

- Remember the Adobe game?
  - Adobe lost plaintext email addresses, password hints, and encrypted passwords
  - Sony lost plaintext email addresses and passwords in a separate incident
  - Secure passwords (with no other matches) that were safe with Adobe were exposed (with context) through Sony
    - Adobe Hint: SSNDOB
    - Sony Password: 5551234561351
    - Matched by email address

http://www.troyhunt.com/2013/11/adobe-credentials-and-serious.html

# Nimbostratus: What could possibly go wrong?

- The power of large numbers
  - Millions of records lost
  - Multiple breaches across multiple organizations and data sets
  - People are lazy
  - 1 + 1 > 2

# Nimbostratus: What could possibly go wrong?

- Where are your keys?
  - Public-key infrastructure (PKI) commonly used when encrypting data
  - As Adobe show, old systems and old data doesn't necessarily die
  - Even encrypted data can be recorded
    - Stays secure, no one can read it
    - What if the key gets leaked in the future?
  - NSA, etc. are fine examples … but …

# Nimbostratus: What could possibly go wrong?

- Border Gateway Protocol vulnerability
  - Reroute traffic without the end-user knowing
  - Data can be recorded while rerouted
  - Data can be modified while rerouted

http://www.wired.com/threatlevel/2008/08/revealed-the-in/
http://www.wired.com/threatlevel/2013/12/bgp-hijacking-belarus-iceland/
http://www.ietf.org/rfc/rfc4272.txt

# Nimbostratus: What could possibly go wrong?

- Innocuous leaks: the service provider loses non-critical data
  - What if all that is lost is a username or email address?
  - Maybe not a problem for something like Adobe – I have nothing to hide.
  - What if I am using a service like “members.livingwithHIV.com” and the username leaks?
  - Who controls your data?

# Nimbostratus: What could possibly go wrong?

- Innocuous leaks: the digital traces of services used on your network
  - What cloud-based services are being used, and in what ways?
  - What security breaches exist in these other services?

# Nimbostratus: What could possibly go wrong?

- Spearphishing
  - Targeted efforts to get users to give up passwords, protected information, etc.
  - Does your traffic provide a new vector of attack for spearfishing – if they know what services you are using (and their company email address), they can target you with a more refined attack

# Nimbostratus: What could possibly go wrong?

- Loss of Access
  - What to do when the cloud is down
  - "The internet is broken"
    - At your organization, on the connection to your ISP, from the ISP to your cloud-based service provider, or internally within your provider's system
    - Major cloud-based providers have suffered substantial outages
      - Without an SLA (and utilizing typically "free" services), what can you do?

# Nimbostratus: What could possibly go wrong?

- Loss of Access
  - What to do when the service goes away and your data becomes stranded
    - Zeo Personal Sleep Manager
    - Google Reader
    - Geocities

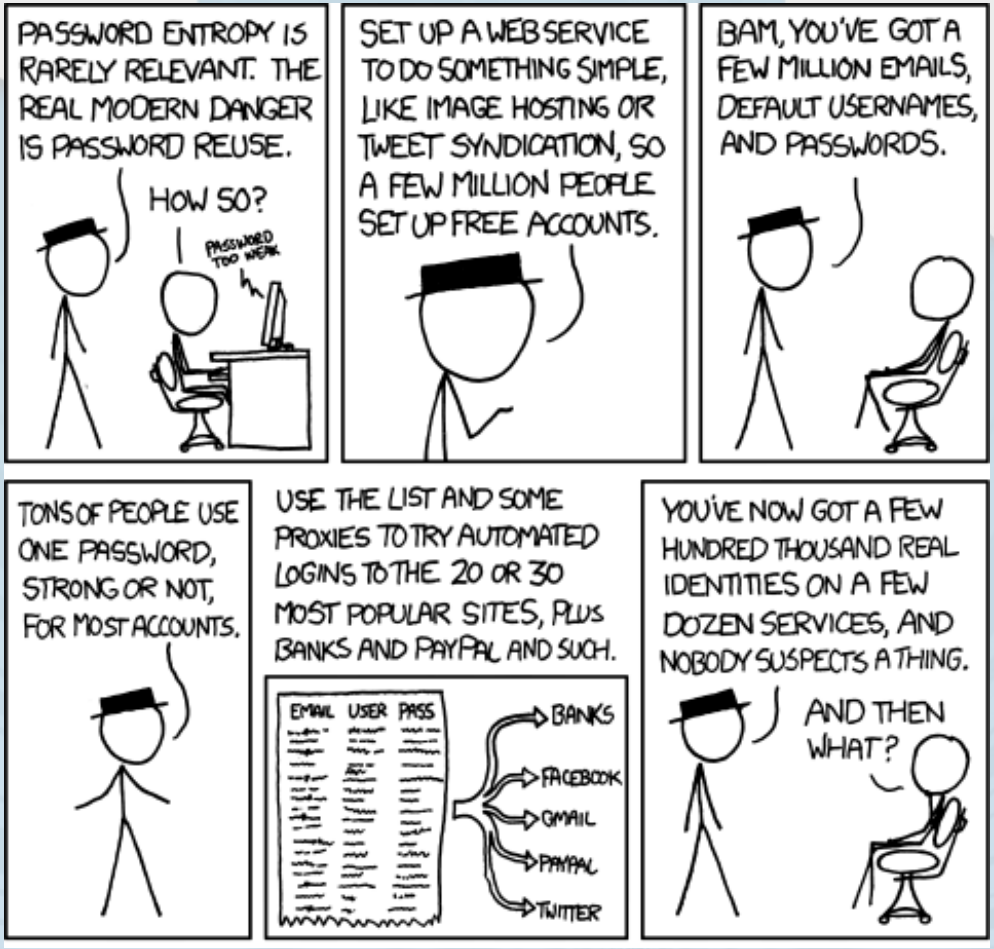
# Nimbostratus: What could possibly go wrong?

- Poor implementation on “your” side
  - Is your WAN properly configured to securely support, audit, and control cloud-based applications?
  - How is “backhauling” impacting traffic on your network?
  - You need to plan for traffic/packet shaping, ensuring Quality of Service (QoS), etc.

# Nimbostratus: What could possibly go wrong?

- Poor implementation on “their” side
  - Cisco forecasts that by 2017, 7.7 Zettabytes of data will be sent to, between, and within data centers
    - In terms of 4 TB hard drives, you could circumscribe Earth 4.4 times with that data
  - What if an application you select is poorly designed?
    - “Chatty” applications
    - Supporting insecure protocols
    - Poorly implementing secure protocols

# Nimbostratus: What could possibly go wrong?




xkcd.com/792/

# Nimbostratus: What could possibly go wrong?

- Loss of Data
  - Data at rest, in motion, in use
  - HIPAA  Breach Notifications
    - 720 recorded events, with 27,771,823 individuals affected
    - Note that reporting is inconsistent
    - 198 events were categorized as a hacking / unauthorized access / IT incident
    - 357 events (~50%) involved theft, often of a laptop, mobile device, server, or disk drive

# Nimbostratus: What could possibly go wrong?

- Loss of Data
  - Physical access to a device with saved passwords, automatic sign-on for accounts, etc. is bad.  Very, very bad.
  - The tools to crack passwords are getting smarter and easier to use
    - Using YouTube, Twitter, Wikipedia, Project Gutenberg for better dictionary attacks
    - Rainbow tables (pre-computed table of hashed passwords) are growing

# Cumulonimbus: Before lightning strikes

- Tools to manage your data
  - Data Loss Prevention
    - Network, endpoint, and file DLP
    - Identify critical / sensitive data and protect it
  - Firewalls
    - Stop traffic to (and from) your network
    - Administering this can be onerous
  - Encryption
    - Use for data in motion and data at rest
    - Remember  Adobe – even encrypted data can pose a risk when retained for a long enough span of time

$$\text{Risk} = \text{Impact} * \frac{\text{Time}}{\text{Probability of Incident}}$$

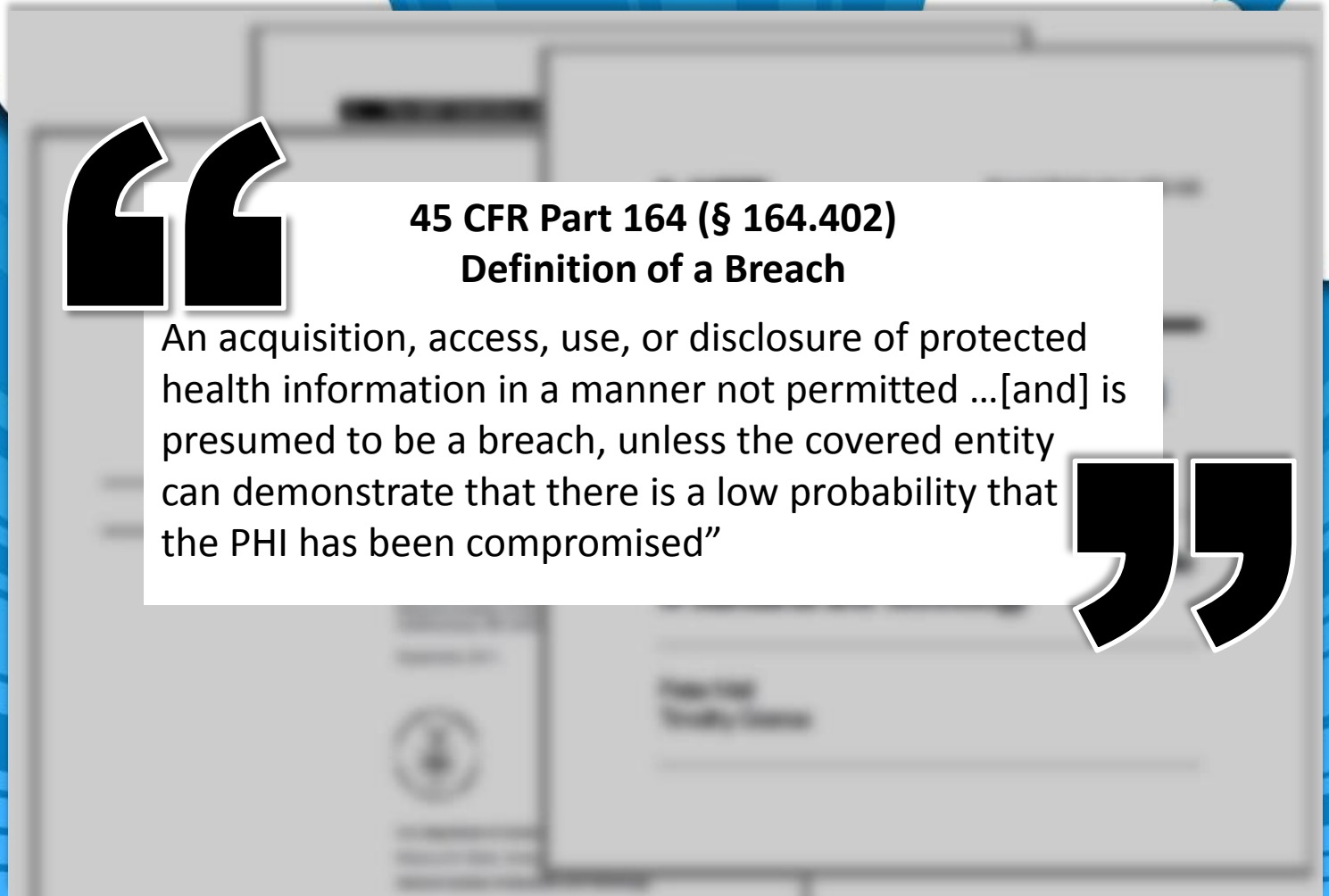
# Cumulonimbus: Before lightning strikes

- Tools to manage your users
  - Password requirements
    - Enforce password policies
    - Enable Single Sign-On
  - Permitted actions / usage policies
    - Determine who can perform which actions
    - Monitor what services are being used
  - Create and disable accounts
    - Fit cloud-based products into employee onboarding and exit procedures

# Cumulonimbus: Before lightning strikes

- Tools to manage your cloud
  - Configure your network
    - “Moving to the cloud” != “no hardware needed”
    - Add cloud-based applications to your QoS policy
  - Select your supported tools
    - Determine what you will and will not allow
    - Train your users on policies and tools
  - Backup your cloud-based systems and data
    - Prepare for the worst

# HIPAA Breach Notification



**45 CFR Part 164 (§ 164.402)**
**Definition of a Breach**

An acquisition, access, use, or disclosure of protected health information in a manner not permitted …[and] is presumed to be a breach, unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised”

# HIPAA Breach Notification

- According to the Final Rule
  - You can rebut if you can show:
    - It is unlikely that the data could be used for re-identification
    - The person accessing the data is not capable of re-identifying the information or otherwise poses a risk
    - The data was not actually acquired or viewed
    - The extent to which risks to PHI have been mitigated
  - Cloud-based service providers as “business associates” as identified in 45 CFR 160.103
  - Given how much data is out there, how little do you need to leak for it to be identifiable?

# So now what?

- Do your homework
  - Read up on standard practices
  - Perform a market review
  - Interview cloud-based service providers to assess your risks and determine their ability to mitigate them
    - Ask about encryption, HIPAA compliance audits, and policies and procedures for data protection, retention, and recovery
  - Use the tools that are available to manage your cloud-based services
  - Be aware that vendor-supplied whitepapers may be biased

# Some Resources

**HIPAA Information**

- HIPAA Final Ruling http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- Understanding HIPAA http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
- FAQ on HIPAA and "Cloud Computing" https://www.cdt.org/files/pdfs/FAQ-HIPAAandCloud.pdf

**NIST Publications and Programs**

- Cloud Computing: http://www.nist.gov/itl/cloud/index.cfm
- Computer Security: http://csrc.nist.gov/publications/PubsSPs.html

**Materials referenced in the presentation**

- http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.html
- http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1184/whitepaper_c11-706172.html
- http://www.cisco.com/en/US/netsol/ns1175/networking_solutions_solution_category.html
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
- http://www.ietf.org/rfc/rfc4272.txt
- http://www.sans.org/critical-security-controls/
- http://www.troyhunt.com/2013/11/adobe-credentials-and-serious.html
- http://www.wired.com/threatlevel/2008/08/revealed-the-in/
- http://www.wired.com/threatlevel/2013/12/bgp-hijacking-belarus-iceland/
- http://xkcd.com/792/
- http://www.vmware.com/files/pdf/cloud/eight-key-ingredients-building-internal-cloud.pdf
- http://zed0.co.uk/crossword

# Q & A

Please submit your questions via the Q&A text box on your screen or contact me after the presentation

**Garret Spargo**
TTAC Director
gspargo@anthc.org

Follow Us!

TTAC
TelehealthTechnology.org
National Telehealth Technology Assessment Resource Center

Telehealth
Resource Centers

# The National Telehealth Resource Center Webinar Series

## 3rd Thursday of every month

## Next Webinar:

**Telehealth Topic:** Telehealth Legislation: A Live Q&A

**Presenter:** U.S. Representative Gregg Harper (R-Miss.)

**Date:** Thursday, January 16, 2014

**Times:** 8:00AM HST, 9:00AM AKST, 10:00AM PST, 11:00AM MST, 12:00PM CST, 1:00PM EST


# Your opinion of this webinar is valuable to us.

Please participate in this brief perception survey:

**http://www.surveymonkey.com/s/NationalTRCWebinarSeries**

TRC activity is supported by grants from the Office for the Advancement of Telehealth, Office of Health Information Technology, Health Resources and Services Administration, DHHS