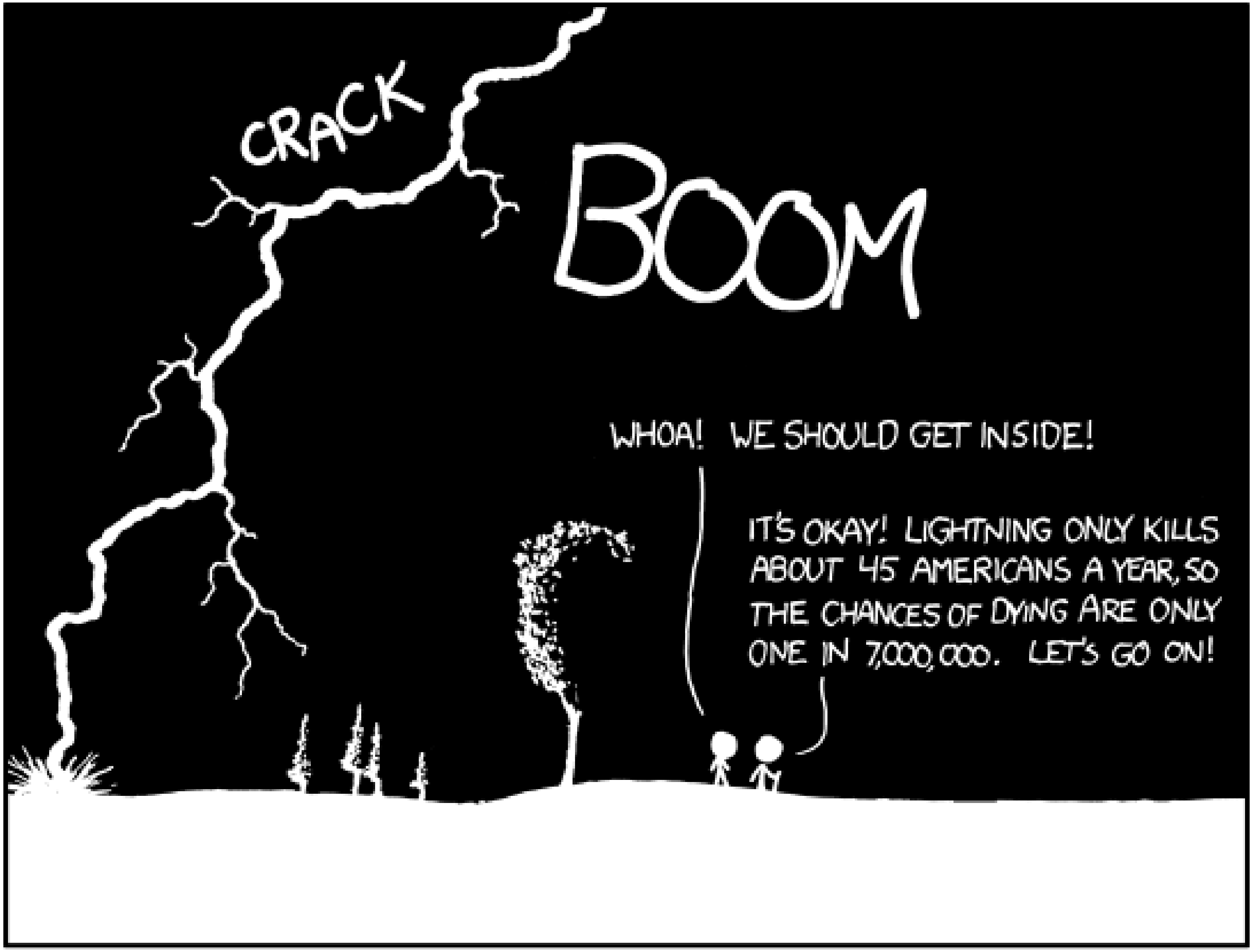

CRACK
BOOM
WHOA! WE SHOULD GET INSIDE!
IT'S OKAY! LIGHTNING ONLY KILLS ABOUT 45 AMERICANS A YEAR, SO THE CHANCES OF DYING ARE ONLY ONE IN 7,000,000. LET'S GO ON!

THE ANNUAL DEATH RATE AMONG PEOPLE
WHO KNOW THAT STATISTIC IS ONE IN SIX.

http://xkcd.com/795/

Risky Business: Click-Throughs & You

Janine Roeth, UC Santa Cruz
Isaac Straley, UC Irvine

TODAY

- Context
- UC Workgroup - “Where is the risk?”
- Examples from vendor terms & real-life
- Actions to address risk
  - Institutional & individual
- References

[WARNING]

POLL

Have you accepted click-through agreements for your University (professional) use?

ABOUT UNIVERSITY OF CALIFORNIA

Ten campuses

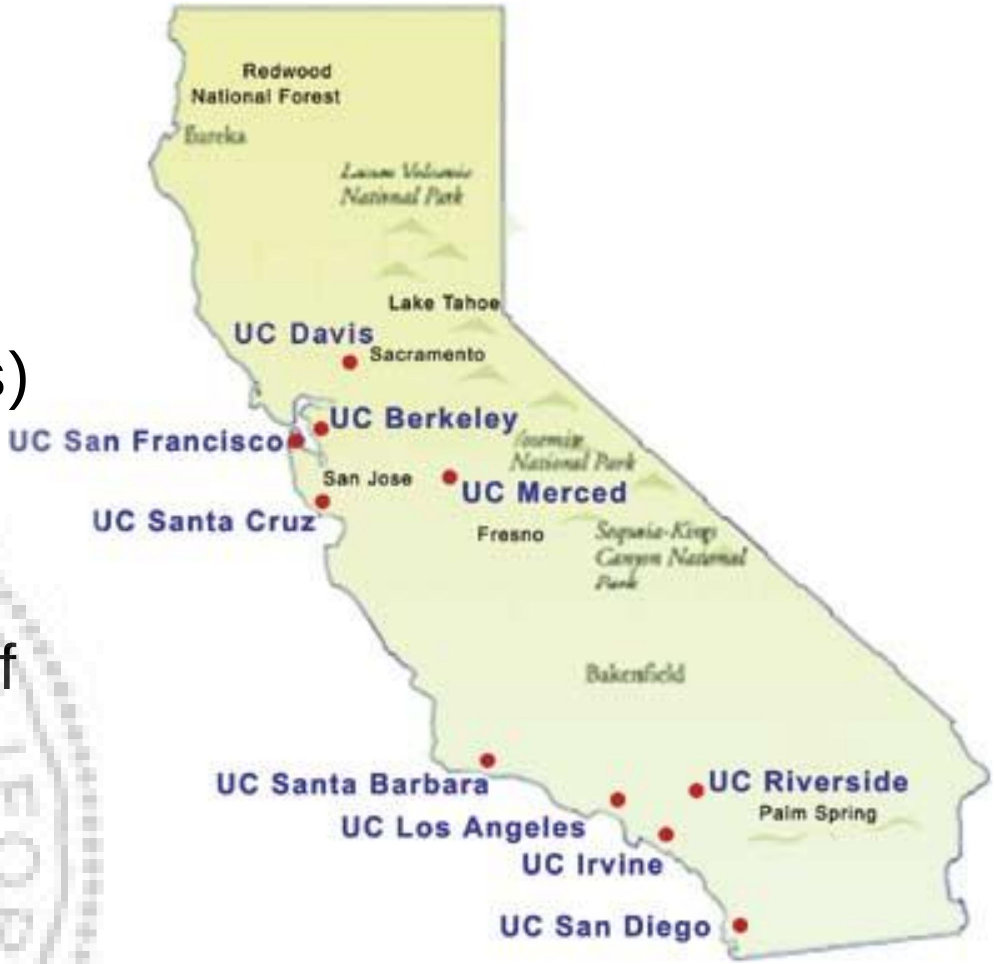
Five medical centers

Dept. of Energy lab(s)

220,000+ students

180,000+ faculty/staff

Public Research University



ABOUT UNIVERSITY OF CALIFORNIA

Systemwide, Common Mission:
Research, Teaching & Public Service

CONTEXT

- University departments & employees use services to broad institutional benefit
- Faculty and staff are agreeing to terms without knowing/considering potential risks

Ease of "click-through" enables bypass of Procurement

UC Workgroup:

Where is the Risk?

POLL

What is your primary concern about click-throughs?

- If I actually read every word of the terms, would I actually understand it?
- Terms violate University policies
- Who has the authority to agree / “sign”
- Data security or privacy risk
- My data being sold to advertisers
- I have no concerns

WORKGROUP GOAL

Risk-based view to inform choices, streamline acquisition and better protect the university

“Where is the risk and what should we do about it?”

WORKGROUP APPROACH

- Examine vendor’s default terms and conditions
- Identify higher and lower risk
- Identify actions to address the risk or provide guidance to the University community

Mar-Aug 2013

Terms and Conditions May Apply

“If you were to read everything you agreed to, it would take one full month ….out of every year. That’s 180 hours …every year.”

Cullen Hoback,
producer and director

VENDOR TCS REVIEWED

Examples of…

- Cloud storage, collaboration, social media
- Used by individuals and institution
- Popular or pervasive
- Multi-platform, i.e. web, mobile

Dropbox
You Tube
Google Analytics
iCloud

AREAS EXAMINED

- Acceptable Use Policy
- Clarify Rights and License (University & End User Data)
- Credit Card Information
- Data Access/Retention/Transfer
- Data Location/Residency/ Export Controls
- Data Privacy
- Data Security & Integrity
- Fees
- FERPA Designation
- Governing law
- Health Information
- Indemnification
- Insurance
- Limitation of Liability
- Representations & Warranties
- Response to Legal Orders & Demands for Data
- Supplier Outsourcing/ Subcontractors
- Vendor Modifications (Terms & Service)

WORKGROUP FINDINGS

Higher Risk:

Conflicts that arise under specific conditions

Lower Risk:

Conflicts with business practices or showed disadvantage

LOWER RISK

Click-through terms disadvantaged or were out of alignment with higher ed practices - not favorable

e.g. Governing law, Insurance, Limitation of liability, Service level agreements, Acceptable

HIGHER RISK

Clickthrough terms did not address the following conditions

sensitive data

or

critical business functions

RISK CONDITION: SENSITIVE DATA

Social Security Numbers

Credit Cards

Health Information

Insurance Information

Student Records

Human Subjects Data

Unpublished Research

Investigations

May be subject to:

- State Security Breach Notification Laws
- HIPAA, FERPA, Export Control
- PCI-DSS Regulations
- Agency Requirements

RISK CONDITION: SENSITIVE DATA

Personnel feeds

Conferences & events

Older student records

Research

Environmental Health & Safety

Investigations

Marketing/Sales

Sports, clubs, intramurals

Impact of a Breach:

Financial

Reputational

Strategic

RISK CONDITION: BUSINESS CRITICALITY

Availability – ability to do "business"

- Research, teaching and public service

What are your

Continuity Planning

- How long can you do without the service?
- Do you have backout plan or alternative way to work?

Vendor Terms:

What The Terms Say and Real-Life Events

Security

“We protect [your data] on our servers using a combination of administrative, physical and logical security safeguards”

Mar-Aug 2013

Security

“[We take] precautions…to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction”

Mar-Aug 2013

Security

"We work hard to protect [us and you] from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold"

Mar-Aug 2013

Security

“We have a team dedicated to keeping your information secure and testing for vulnerabilities”

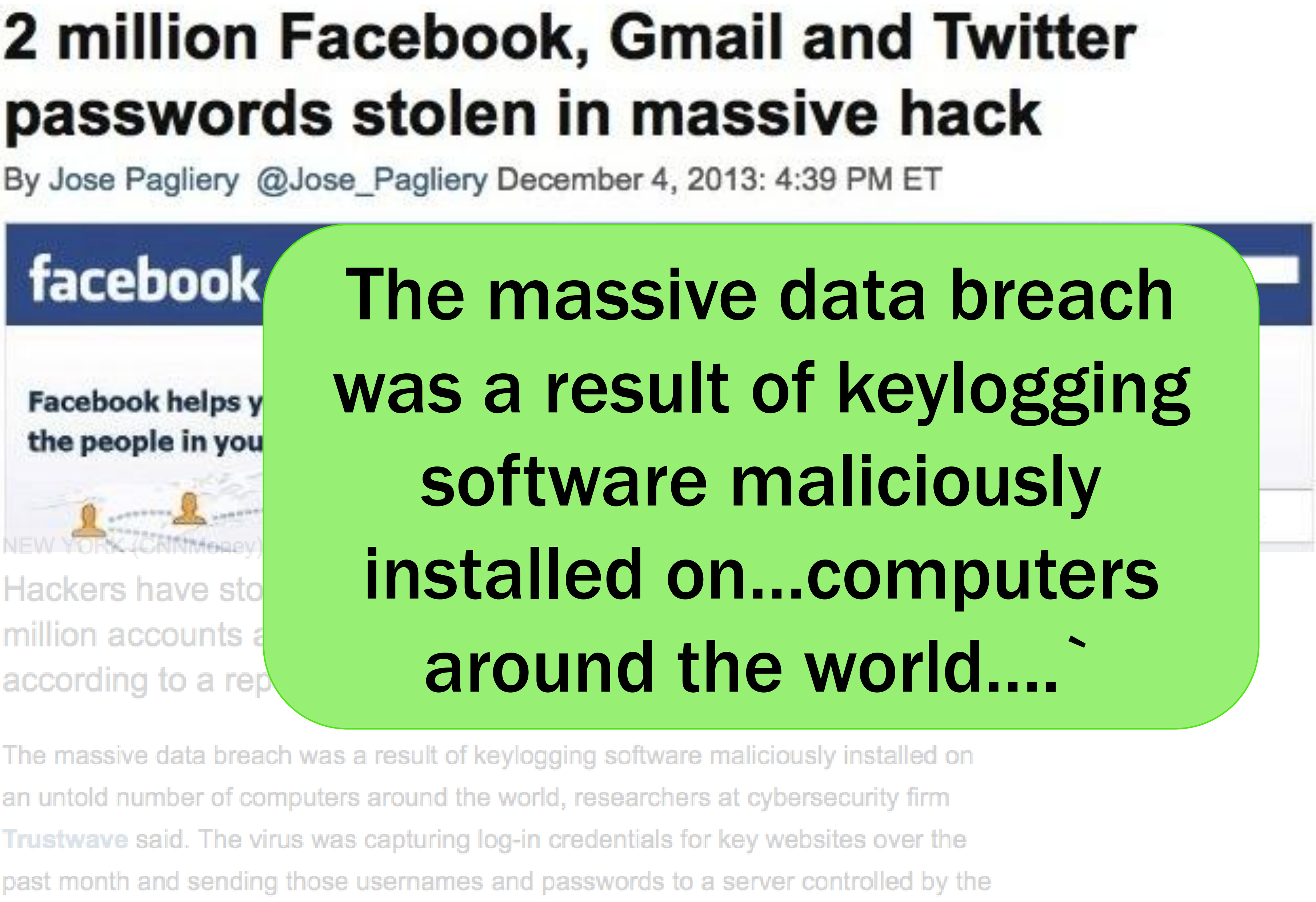
Mar-Aug 2013

Security

“We do our best to keep your information secure, but we need your help…..”

Mar-Aug 2013

CNN Money



2 million Facebook, Gmail and Twitter passwords stolen in massive hack

By Jose Pagliery @Jose_Pagliery December 4, 2013: 4:39 PM ET

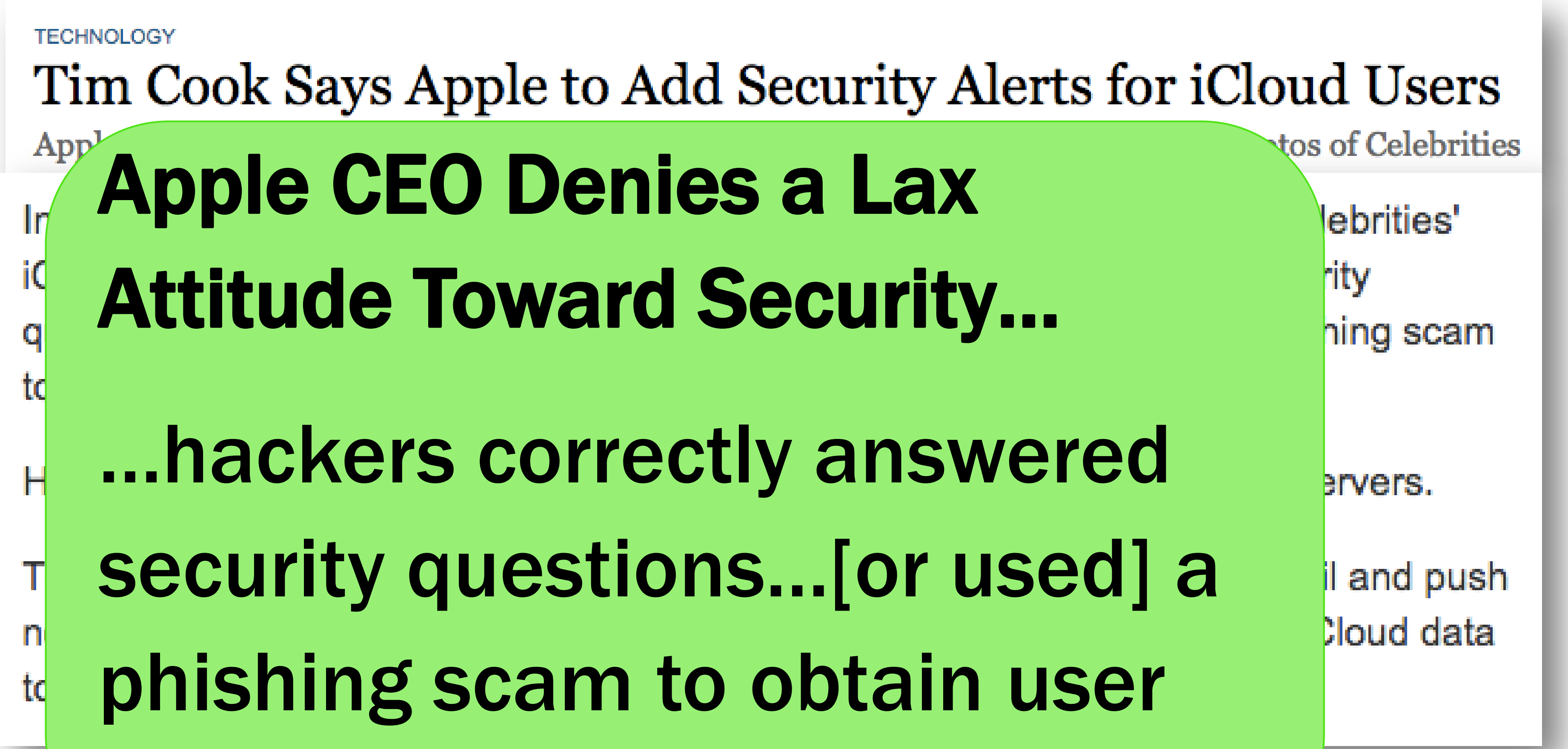
NEW YORK (CNNMoney)

Hackers have sto
million accounts a
according to a rep

The massive data breach was a result of keylogging software maliciously installed on an untold number of computers around the world, researchers at cybersecurity firm Trustwave said. The virus was capturing log-in credentials for key websites over the past month and sending those usernames and passwords to a server controlled by the

The massive data breach was a result of keylogging software maliciously installed on...computers around the world....`

THE WALL STREET JOURNAL.



TECHNOLOGY

Tim Cook Says Apple to Add Security Alerts for iCloud Users

Appl tos of Celebrities

In lebrities'
iC rity
q ning scam
to

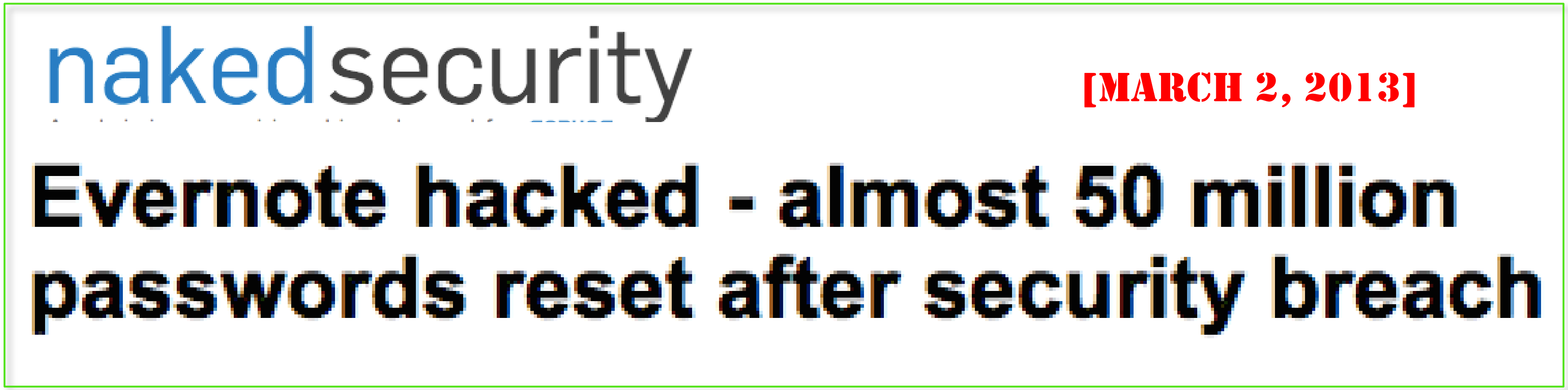
H ervers.

T il and push
n Cloud data
to

Apple CEO Denies a Lax Attitude Toward Security…

…hackers correctly answered security questions…[or used] a phishing scam to obtain user IDs and passwords

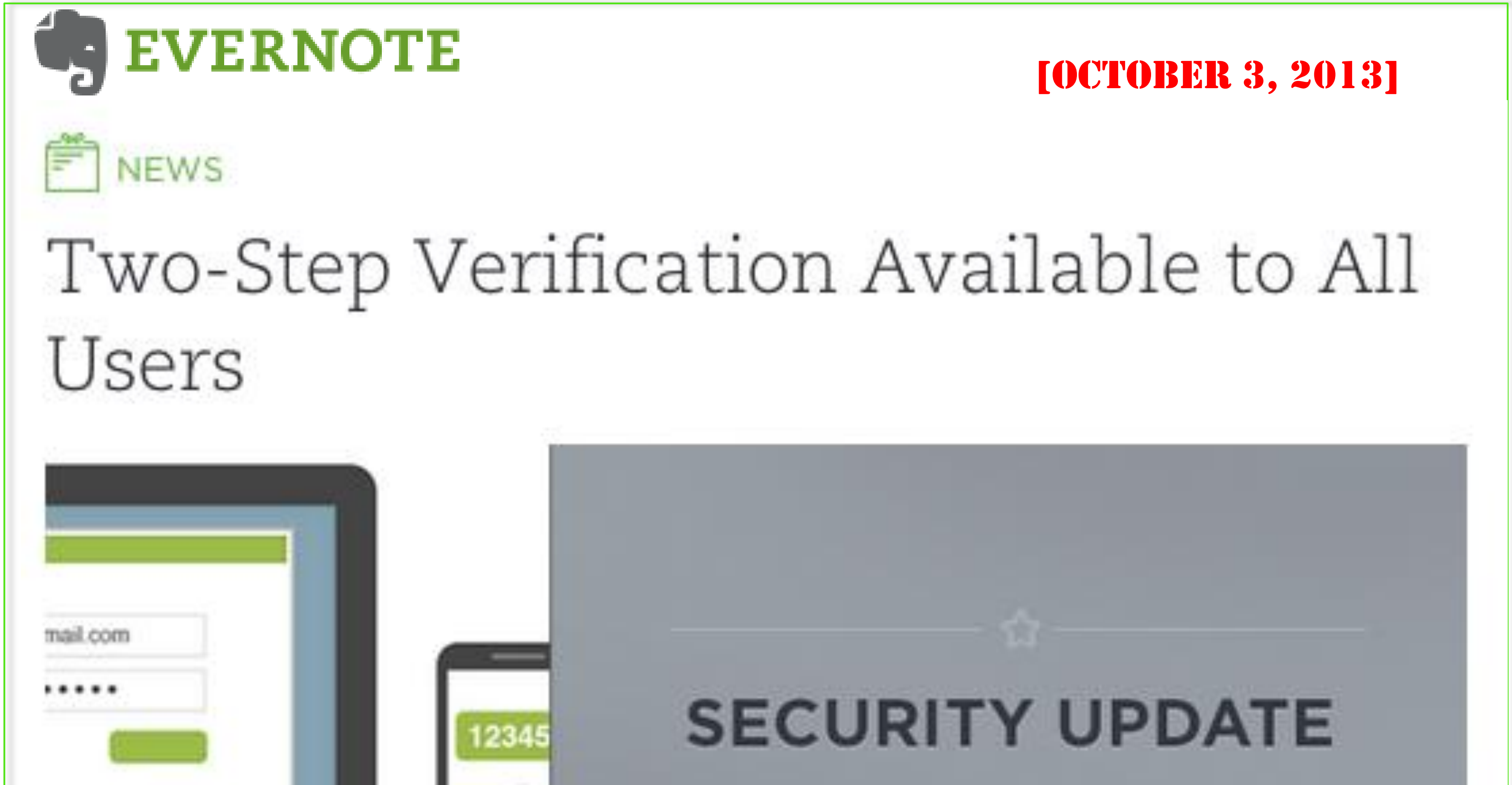
Sept 2014



nakedsecurity

[MARCH 2, 2013]

Evernote hacked - almost 50 million passwords reset after security breach

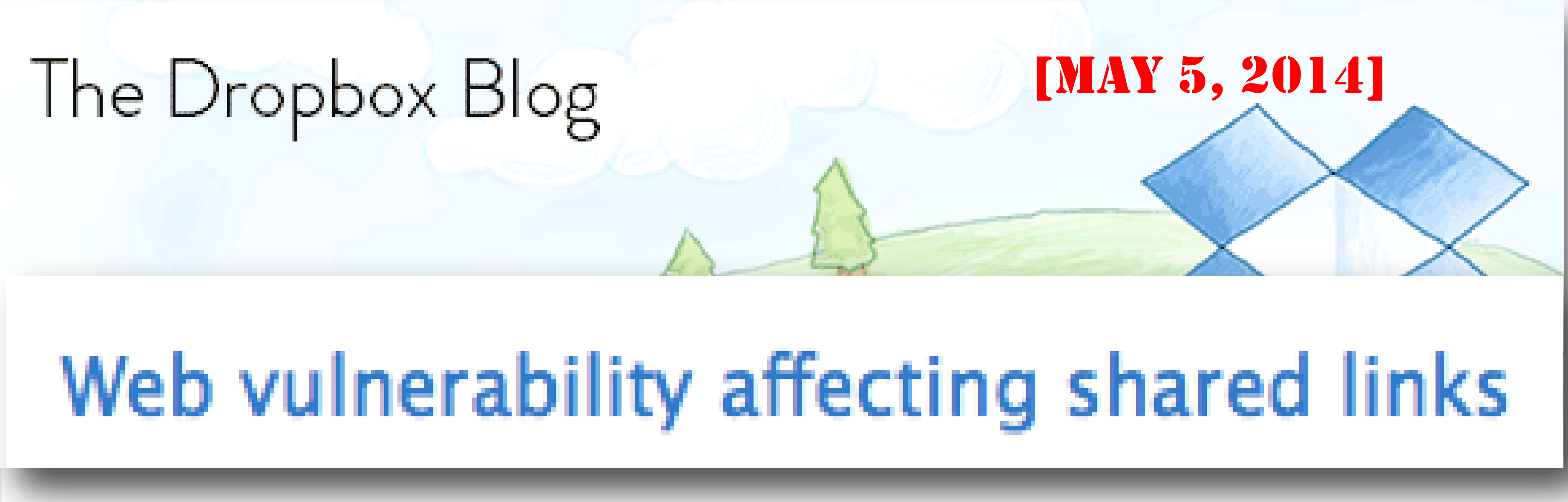


EVERNOTE

[OCTOBER 3, 2013]

NEWS

Two-Step Verification Available to All Users



The Dropbox Blog

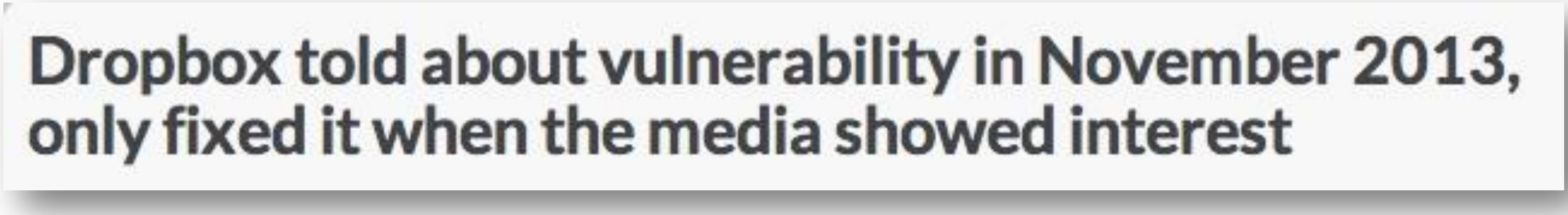
Web vulnerability affecting shared links

[MAY 5, 2014]

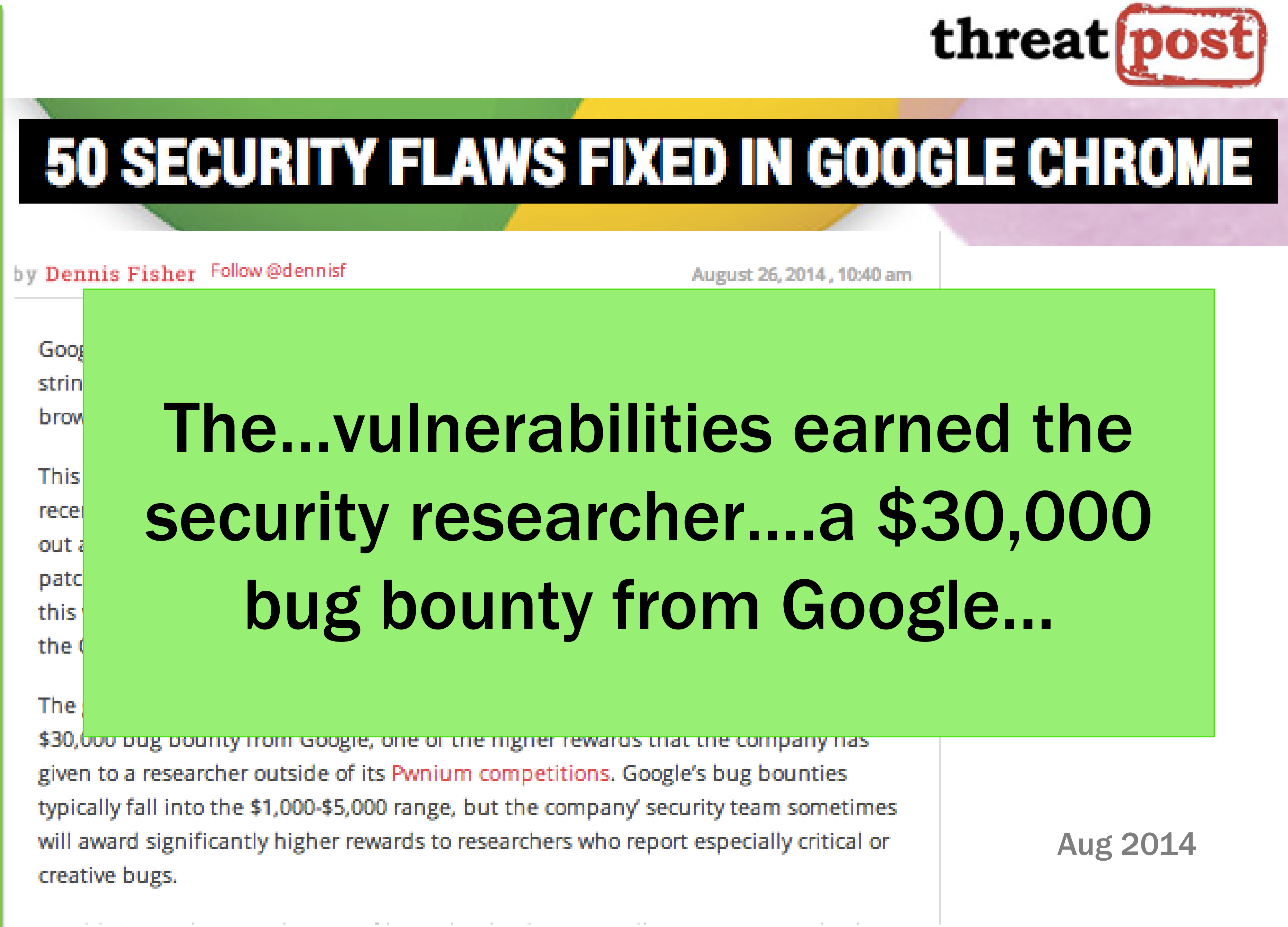
Graham Cluley

The latest computer security news, advice and opinion

[MAY 6, 2014]



Dropbox told about vulnerability in November 2013, only fixed it when the media showed interest



threatpost

50 SECURITY FLAWS FIXED IN GOOGLE CHROME

by Dennis Fisher Follow @dennisf August 26, 2014, 10:40 am

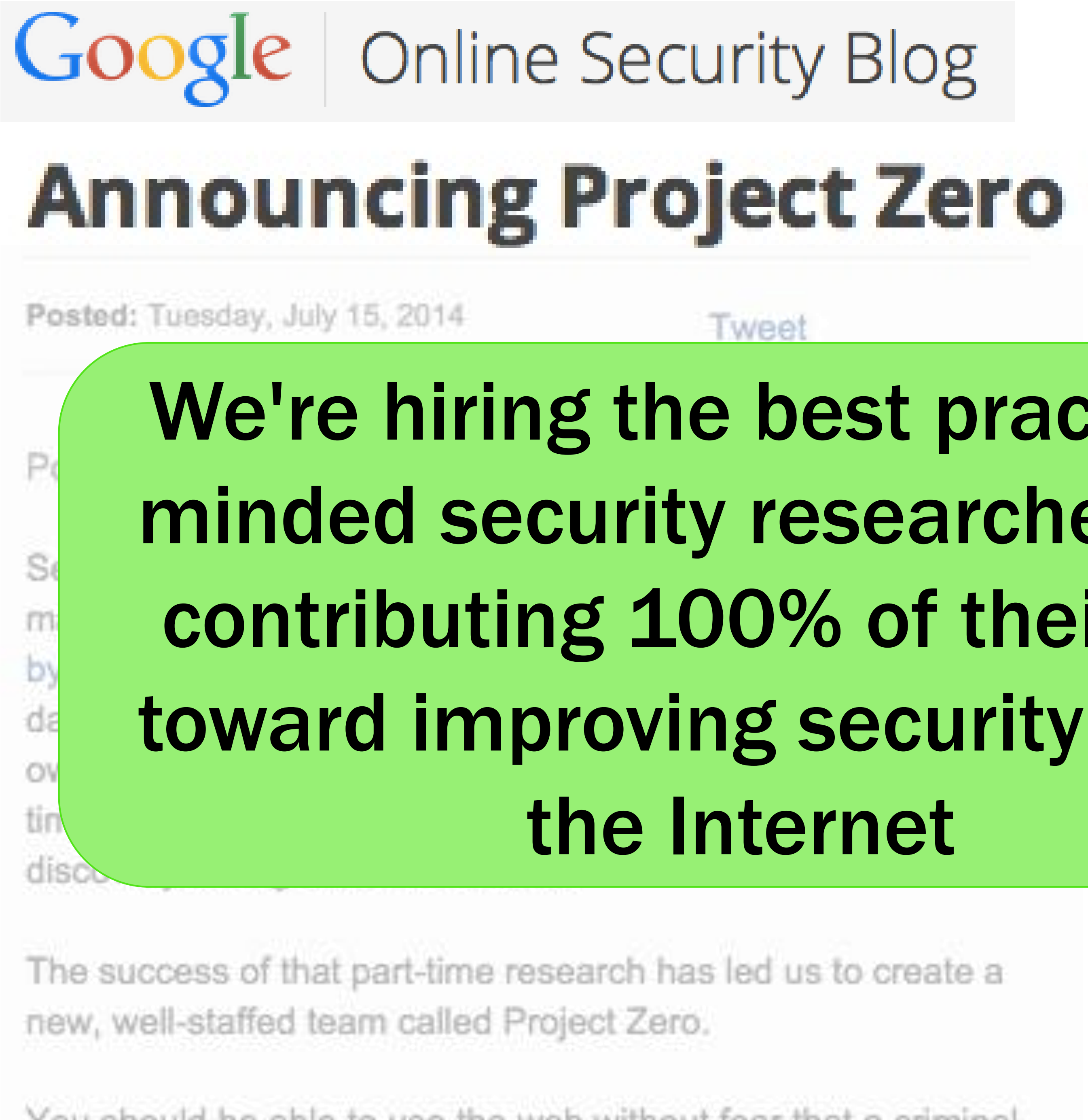
Goog
strin
brow

This
rece
out a
patc
this
the

The
$30,000 bug bounty from Google, one of the higher rewards that the company has given to a researcher outside of its Pwnium competitions. Google's bug bounties typically fall into the $1,000-$5,000 range, but the company' security team sometimes will award significantly higher rewards to researchers who report especially critical or creative bugs.

The…vulnerabilities earned the security researcher….a $30,000 bug bounty from Google…

Aug 2014



Google | Online Security Blog

Announcing Project Zero

Posted: Tuesday, July 15, 2014

Tweet

The success of that part-time research has led us to create a new, well-staffed team called Project Zero.

You should be able to use the web without fear that a criminal

We're hiring the best practically-minded security researchers and contributing 100% of their time toward improving security across the Internet

July 2014

Modifications to Terms & Service

"We may revise these Terms from time to time… If you do not agree to the new terms, please stop using the Services"

Mar-Aug 2013

Modifications to Fees

“Dropbox may change the fees and charges…, or add new fees and charges…, but we will give you advance notice of these changes by email. ”

Mar-Aug 2013

Modifications to Terms & Service

“Unless we make a change for legal or administrative reasons, or to correct an inaccurate statement, we will provide you with seven (7) days notice…and an opportunity to comment”

Mar-Aug 2013

Data Retention and Access

“If you wish to cancel your account or request that we no longer use your information to provide you services, you may delete your account here”

Data Retention and Access

“We may retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements”

Data Retention and Access

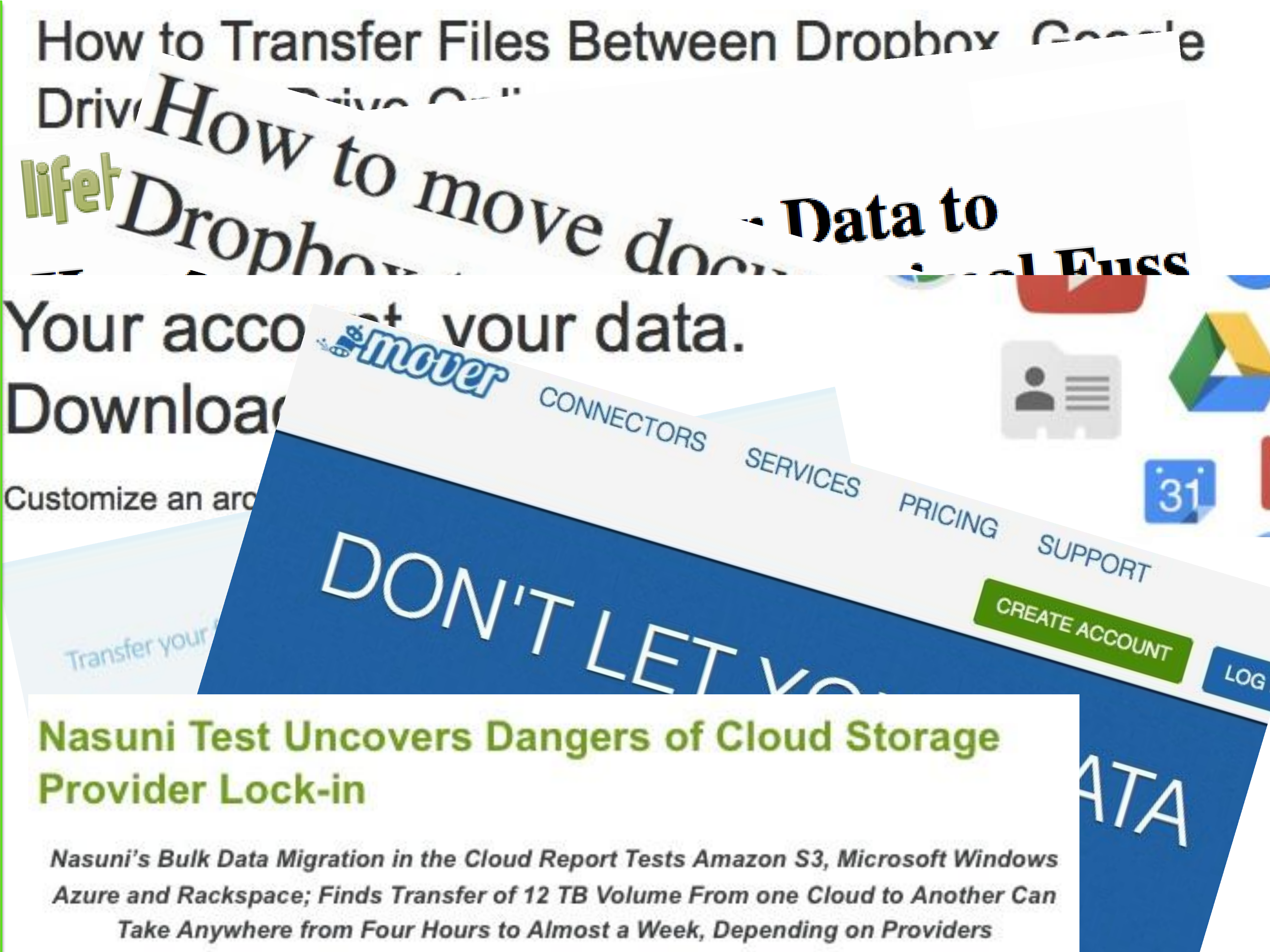
“If you cancel your account, the Content in your account will not be deleted unless you purposely delete that information, and sync your account before you cancel your account.”

Mar-Aug 2013

Modifications to Terms and Service

“Apple reserves the right at any time to …impose new or additional terms or conditions... If you do not agree…, stop using the Service and contact iCloud Support to retrieve your Content”

Mar-Aug 2013



How to Transfer Files Between Dropbox, Google Drive

lifeh

How to move documents from Dropbox

Data to

Fuss

Your account, your data.

Download

Customize an arc

Transfer your

Nasuni Test Uncovers Dangers of Cloud Storage Provider Lock-in

Nasuni's Bulk Data Migration in the Cloud Report Tests Amazon S3, Microsoft Windows Azure and Rackspace; Finds Transfer of 12 TB Volume From one Cloud to Another Can Take Anywhere from Four Hours to Almost a Week, Depending on Providers

VENDOR TC SUMMARY

- Vendor terms designed to protect themselves

  Vendors transfer risk to the user, leaving those they must legally accept

- Examples: General security statements are very general; terms and fees can change at any time, with limited options for moving or deleting data

- If anything goes “wrong”, the University is

POLL

How do you feel about click-throughs?

- We are in trouble, time to give up
- We can improve how we address the risk, but I’m not sure how
- We can improve how we address the risk, and I have ideas
- I’m not worried, we’ve addressed the risks.

Actions

Addressing the risk of Click-Throughs

ACTIONS

Address the risk at two levels:

Institution

Individual

INSTITUTIONAL GOALS

- Increase services covered by negotiated terms to tip the balance in favor of University
- Enable campuses to make risk-based choice for adoption
- Highlight areas of shared responsibility and action for implementation

PROCUREMENT

- Capitalize on partner agreements (Internet2, CENIC)
- Prioritize areas of need (e.g. instruction, file sharing, collaboration)
- Jump start other conversations with a cloud computing contract template

box

LastPass ****

INTERNET 2®

fuze™

CRASHPLANPRO e

canvas
BY INSTRUCTURE

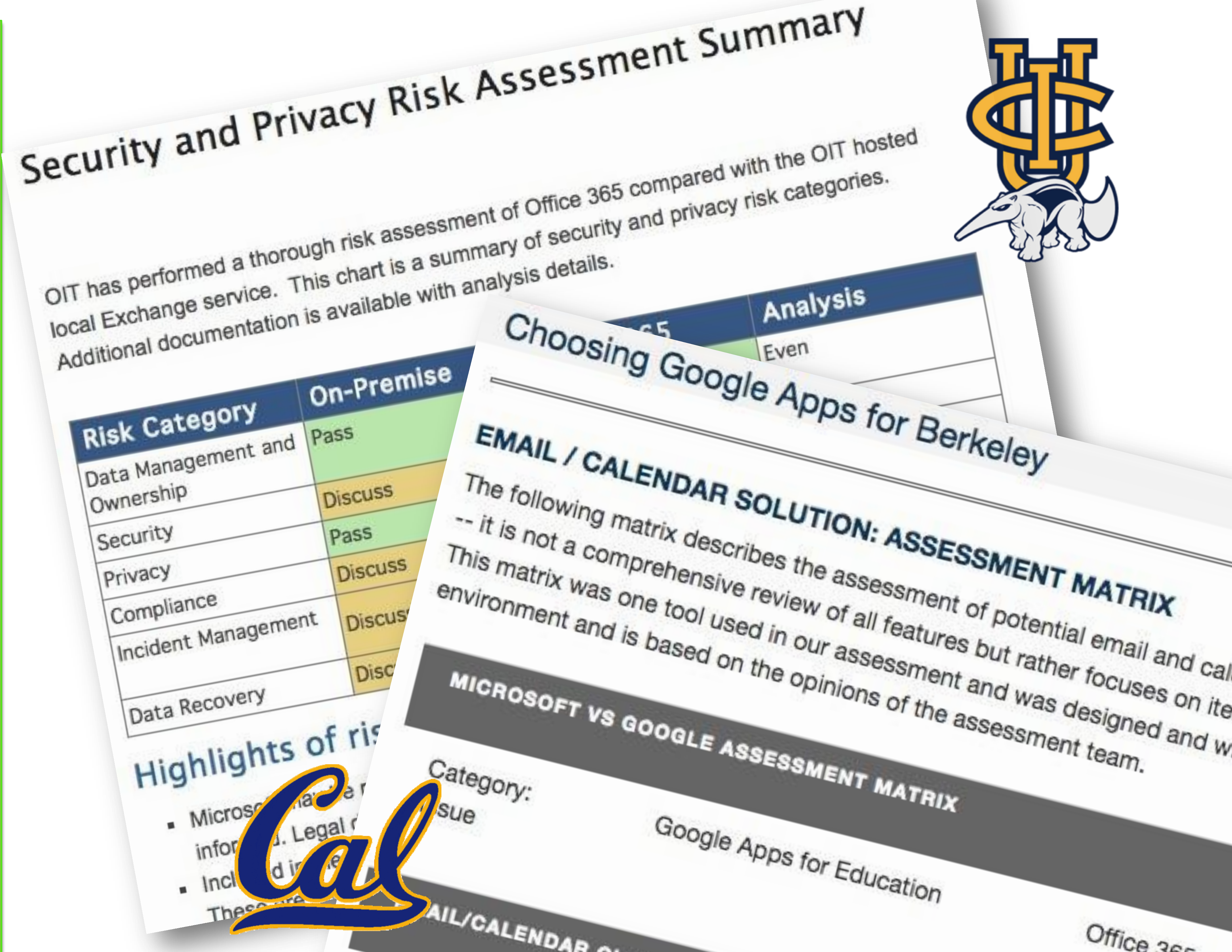
Windows Azure ★

amazon web services ★

Office 365 ★

RISK ASSESSMENT

- Develop tools to assess risk in adopting cloud services
- Campus/schools/units still determine if specific use is acceptable
- Share vendor assessments, review audits, etc.



Security and Privacy Risk Assessment Summary

OIT has performed a thorough risk assessment of Office 365 compared with the OIT hosted local Exchange service. This chart is a summary of security and privacy risk categories. Additional documentation is available with analysis details.

Risk Category	On-Premise	365	Analysis
Data Management and Ownership	Pass		Even
Security	Discuss		
Privacy	Pass		
Compliance	Discuss		
Incident Management	Discus		
Data Recovery	Disc		

Highlights of ris

- Micros nage d. Legal infor
- Incl d i e

These are

Choosing Google Apps for Berkeley

EMAIL / CALENDAR SOLUTION: ASSESSMENT MATRIX

The following matrix describes the assessment of potential email and cal
-- it is not a comprehensive review of all features but rather focuses on ite
This matrix was one tool used in our assessment and was designed and w
environment and is based on the opinions of the assessment team.

MICROSOFT VS GOOGLE ASSESSMENT MATRIX

Category:

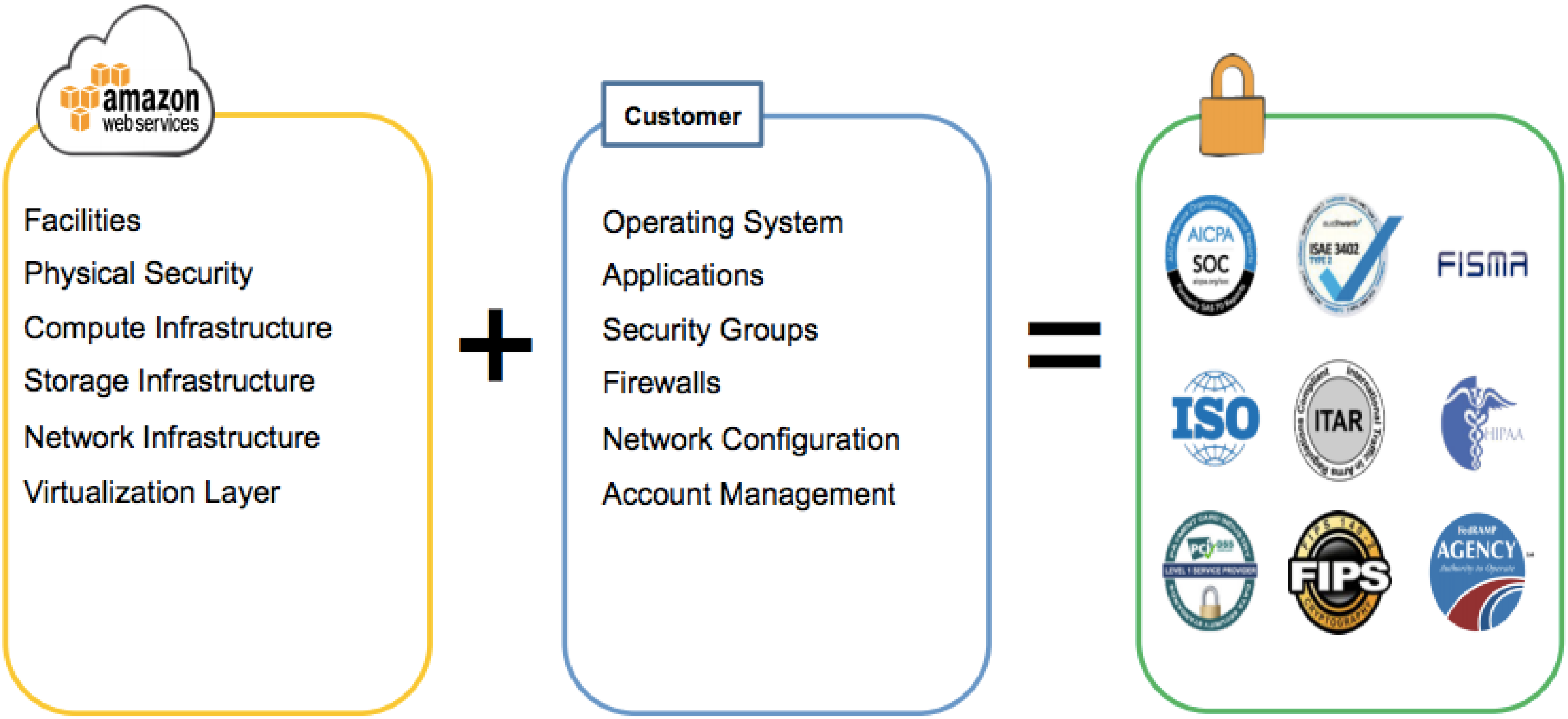
Issue	Google Apps for Education	Office 365

AIL/CALENDAR

IMPLEMENTATION SUPPORT

- Include implementation guidance along with contracts
- Highlight gaps for campus action
- Identify shared responsibilities, especially with security

Security & Compliance Shared Responsibility



Facilities
Physical Security
Compute Infrastructure
Storage Infrastructure
Network Infrastructure
Virtualization Layer

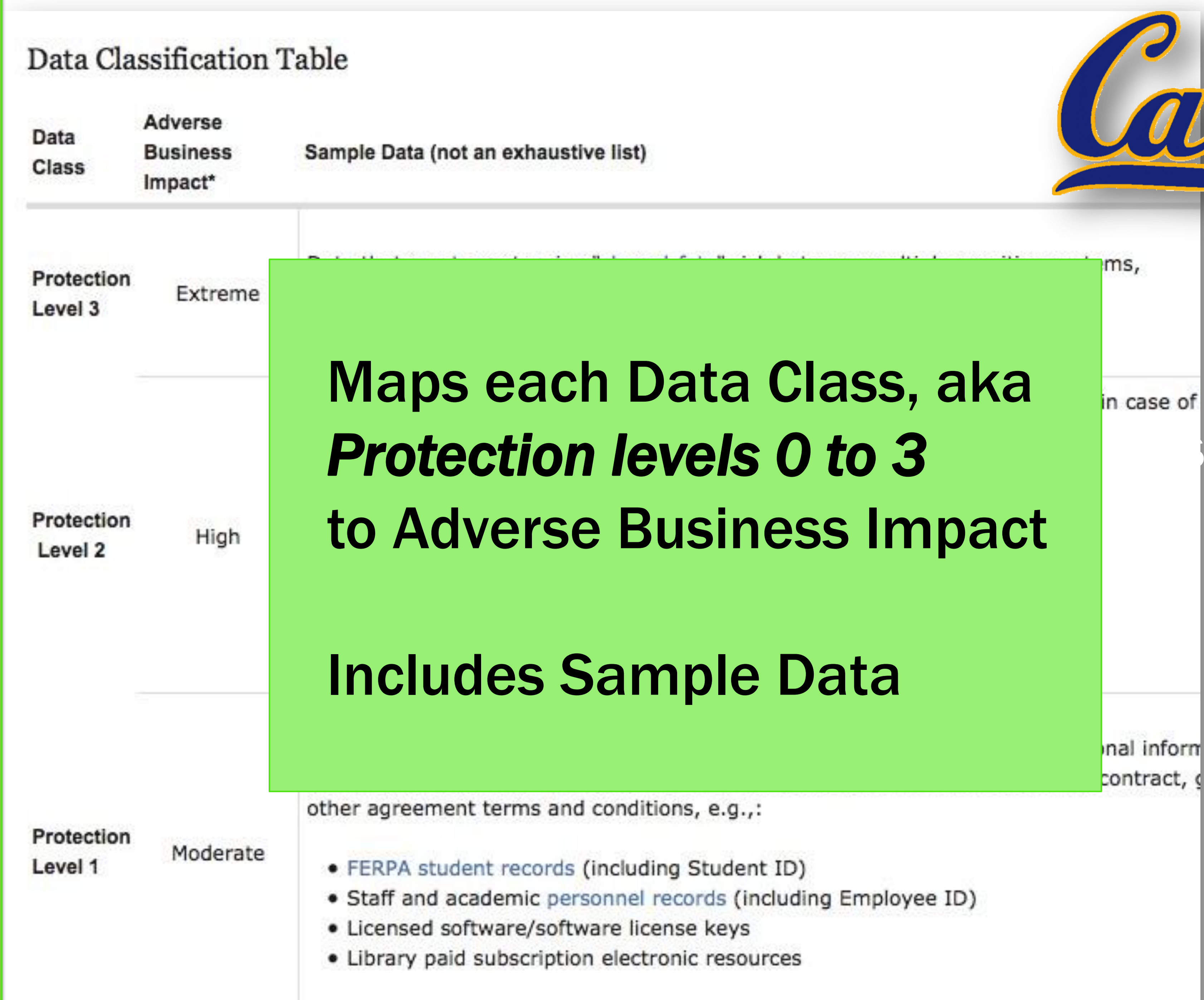
Operating System
Applications
Security Groups
Firewalls
Network Configuration
Account Management

INDIVIDUAL GOALS

- Improve education & self-service tools so end-users can:
  - Consider risks of data sensitivity & business criticality
  - Determine appropriateness

INFORMATION CLASSIFICATION

- “What kinds of data do I have?”
- Tie to University-wide *information classification*
  - Risk-based
  - Indicates data sensitivity

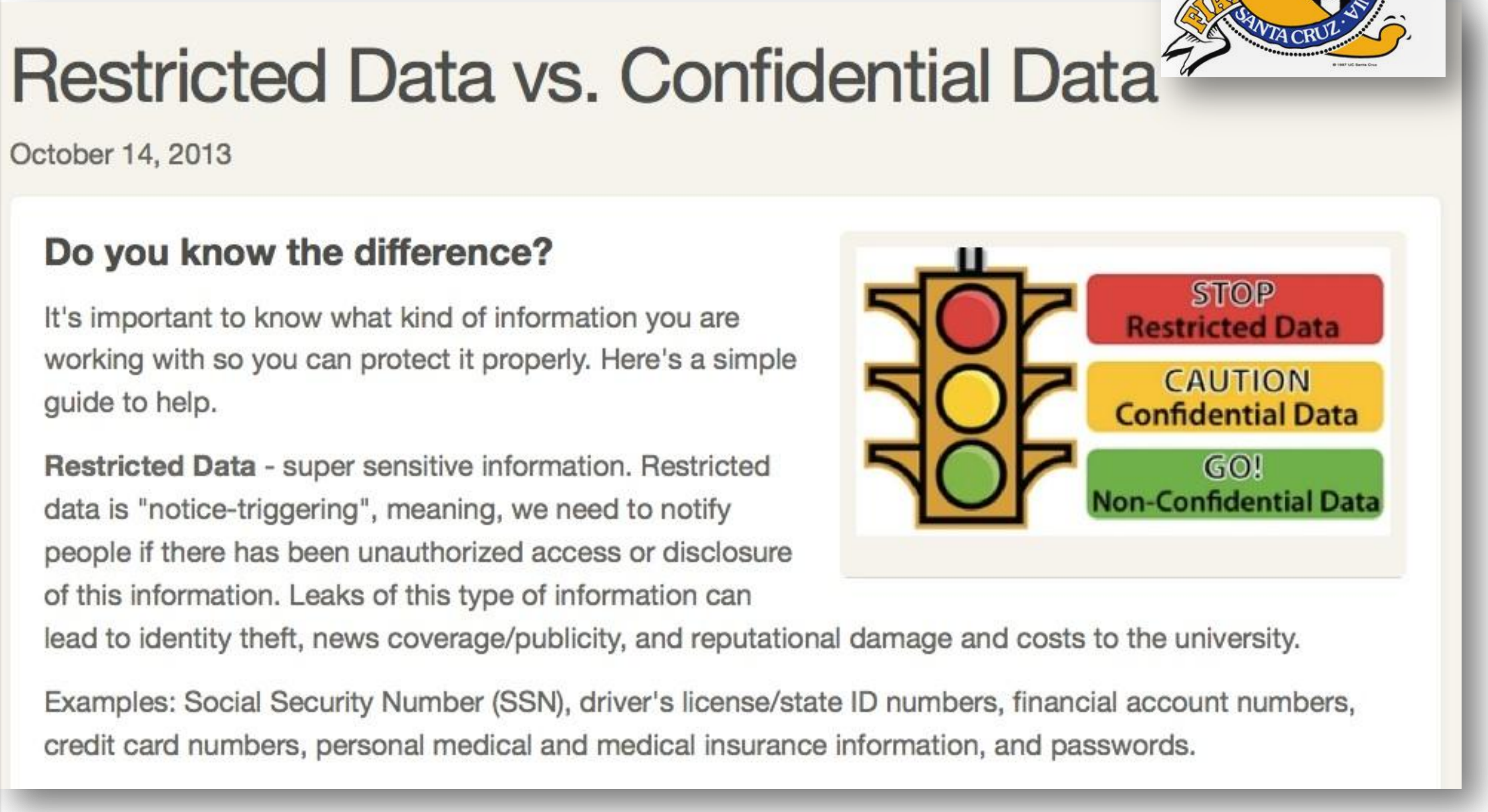


Data Classification Table

Data Class	Adverse Business Impact*	Sample Data (not an exhaustive list)
Protection Level 3	Extreme	ms,
Protection Level 2	High	in case of
Protection Level 1	Moderate	nal inform contract, g other agreement terms and conditions, e.g.,: • FERPA student records (including Student ID) • Staff and academic personnel records (including Employee ID) • Licensed software/software license keys • Library paid subscription electronic resources

Maps each Data Class, aka *Protection levels 0 to 3* to Adverse Business Impact

Includes Sample Data



Restricted Data vs. Confidential Data

October 14, 2013

Do you know the difference?

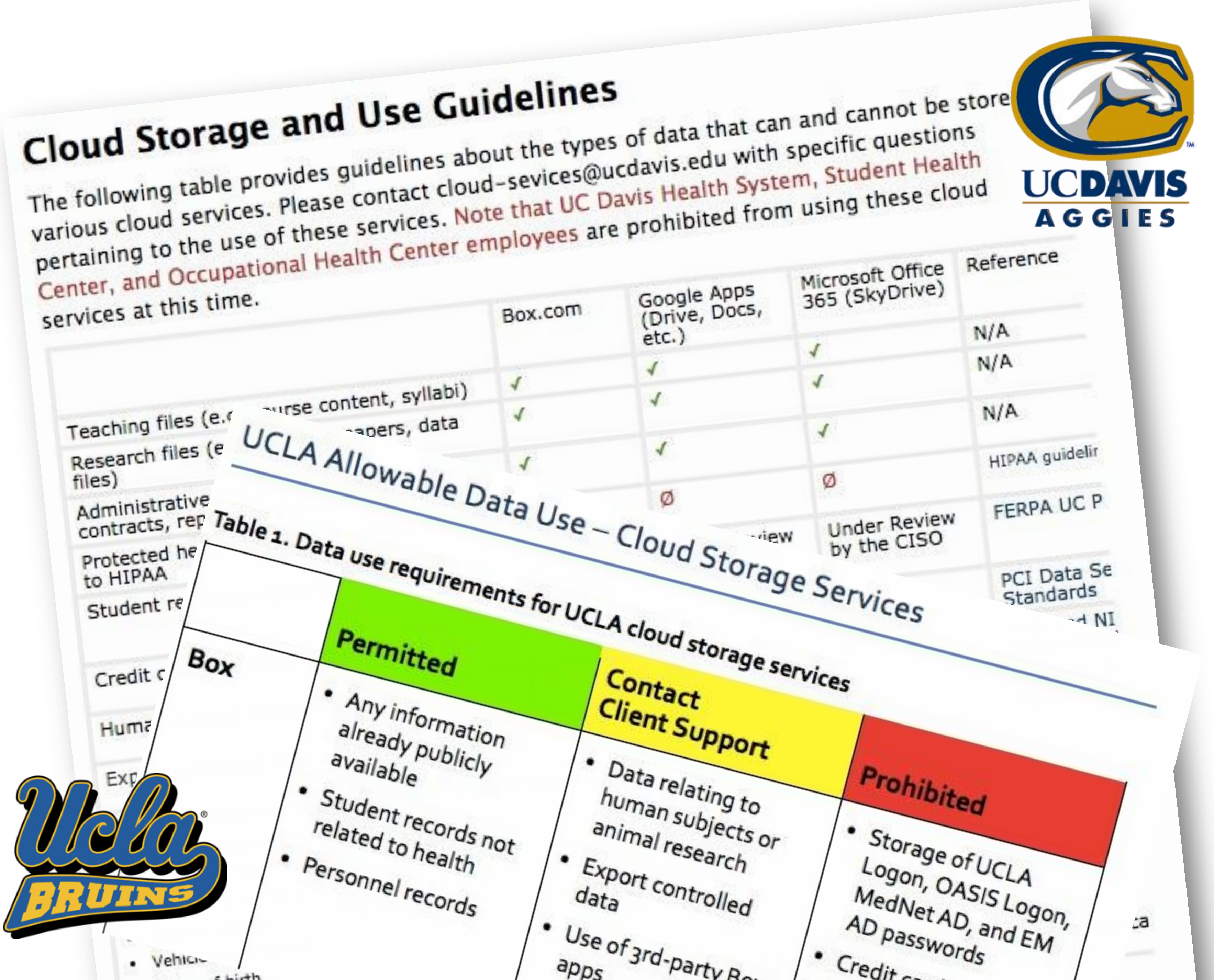
It's important to know what kind of information you are working with so you can protect it properly. Here's a simple guide to help.

Restricted Data - super sensitive information. Restricted data is "notice-triggering", meaning, we need to notify people if there has been unauthorized access or disclosure of this information. Leaks of this type of information can lead to identity theft, news coverage/publicity, and reputational damage and costs to the university.

Examples: Social Security Number (SSN), driver's license/state ID numbers, financial account numbers, credit card numbers, personal medical and medical insurance information, and passwords.

EDUCATION/AWARENESS

- Raise end-user awareness of risk conditions
- Help the end user make informed choices – “Should I use this service?”
- *Data Use Guidelines* show appropriateness by type of data



Cloud Storage and Use Guidelines

The following table provides guidelines about the types of data that can and cannot be store various cloud services. Please contact cloud-sevices@ucdavis.edu with specific questions pertaining to the use of these services. Note that UC Davis Health System, Student Health Center, and Occupational Health Center employees are prohibited from using these cloud services at this time.

	Box.com	Google Apps (Drive, Docs, etc.)	Microsoft Office 365 (SkyDrive)	Reference
Teaching files (e.g. ...urse content, syllabi)	✓	✓	✓	N/A
Research files (e... ...papers, data files)	✓	✓	✓	N/A
Administrative ... contracts, rep...	✓	✓	✓	N/A
Protected he... to HIPAA		Ø	Ø	HIPAA guidelir
Student re...		...view	Under Review by the CISO	FERPA UC P
Credit c...				PCI Data Se Standards
Huma...				...d NI
Exp...				
• Vehic... ...f birth				...a

UCLA Allowable Data Use – Cloud Storage Services

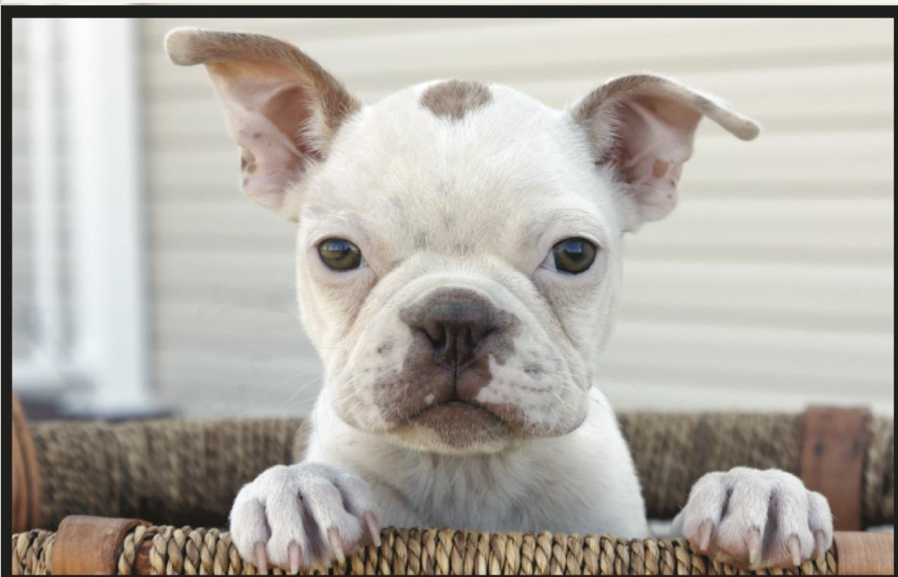
Table 1. Data use requirements for UCLA cloud storage services

	Permitted	Contact Client Support	Prohibited
Box	• Any information already publicly available • Student records not related to health • Personnel records	• Data relating to human subjects or animal research • Export controlled data • Use of 3rd-party Bo... apps	• Storage of UCLA Logon, OASIS Logon, MedNet AD, and EM AD passwords • Credit c...

DON’T FORGET THE BASICS

- Help end users adopt good security practices
- Vendors reinforcing key messages
- National Cyber Security Awareness Month – October!
    - Educause has lots of resources & examples

October is National Cyber Security Awareness Month!



Someone discovered my

PASSWORD.

Now I have to rename my dog.

Use strong passwords. A password such as your pet's name is not sufficient protection. Hackers systematically check every possible word to decipher passwords in no time.

Learn how to create safe passwords:

its.ucsc.edu/policies/password.html

STOP | THINK | CONNECT™

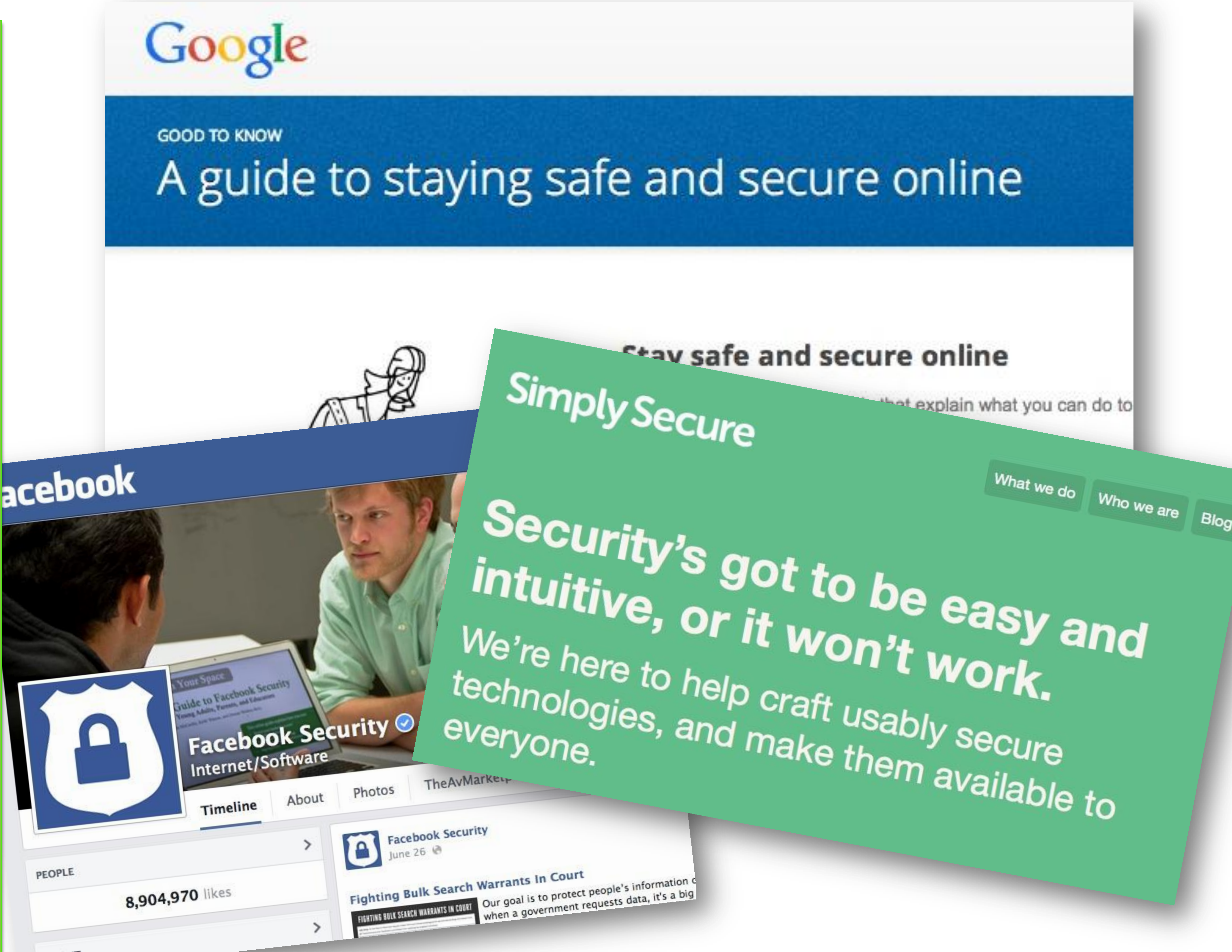
Two Steps Ahead Campaign

you acces
accounts.

These acc
falling into
accounted
your disposal to protect your account, such as two-factor authentication.

- What is Two-Factor Authentication?

Promoting Two-Step Verification aka Two-Factor Authentication



Google

GOOD TO KNOW

A guide to staying safe and secure online

Stay safe and secure online

that explain what you can do to

acebook

Guide to Facebook Security

Facebook Security

Internet/Software

Timeline

About

Photos

TheAvMarket

PEOPLE

8,904,970 likes

Facebook Security

June 26

Fighting Bulk Search Warrants In Court

FIGHTING BULK SEARCH WARRANTS IN COURT

Our goal is to protect people's information when a government requests data, it's a big

Simply Secure

What we do

Who we are

Blog

Security's got to be easy and intuitive, or it won't work.

We're here to help craft usably secure technologies, and make them available to everyone.

POLL

Which of the following do you have at your campus:

-Use of negotiated Internet2 Net+ services

-Vendor assessments

-Risk assessments

-Implementation guides

-Information classification

-End-user education/awareness campaigns

MORE WORK TO DO

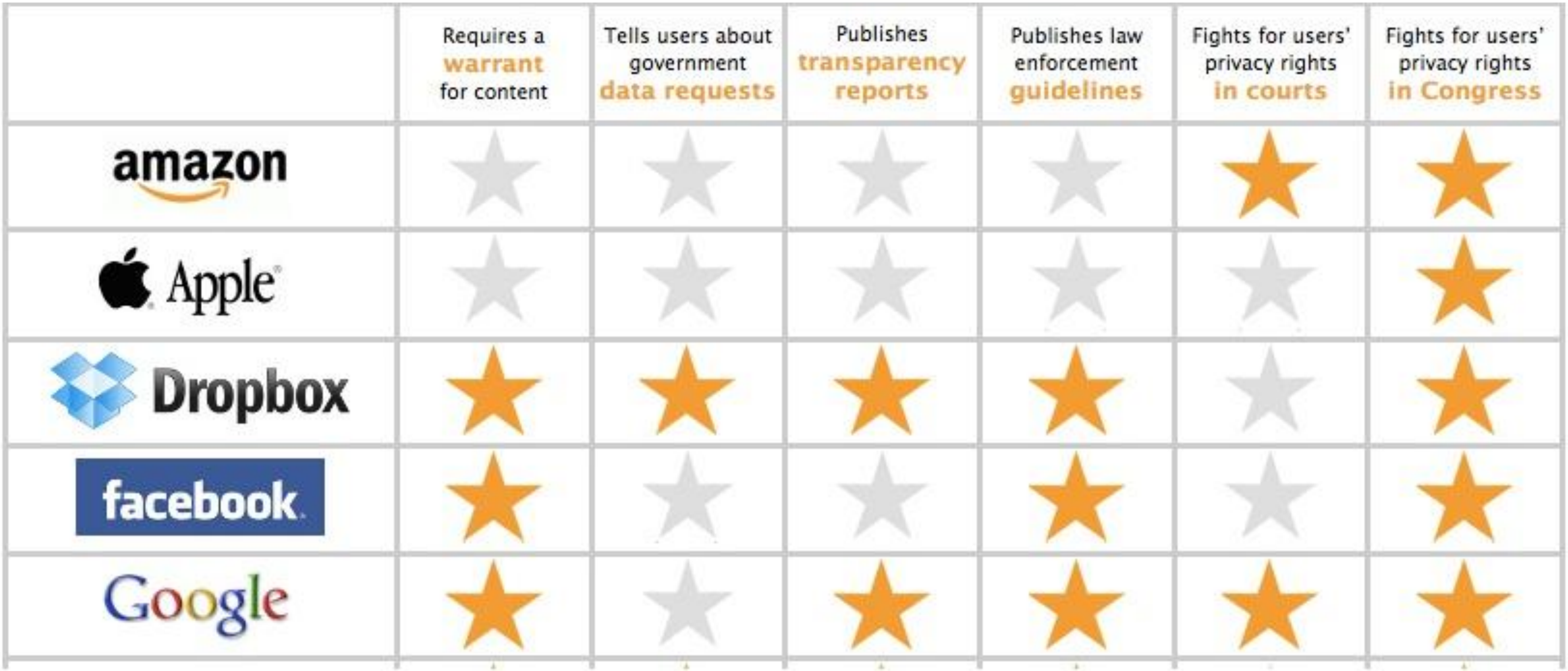
- Hard questions remain
  - Who is “authorized” to accept terms?
  - How about BYOD & personal use?
- BIG efforts
  - Risk assessments
  - Information classification
  - End-user education/awareness

Changing Landscape

Looking at privacy

CONTRACT
ACT
oth parties associate themselves as business ass
he formation of a joint venture, for the purpo
ess provided for by terms and provisio
The headings, titles a
and shall not co

WHO Has Your Back?

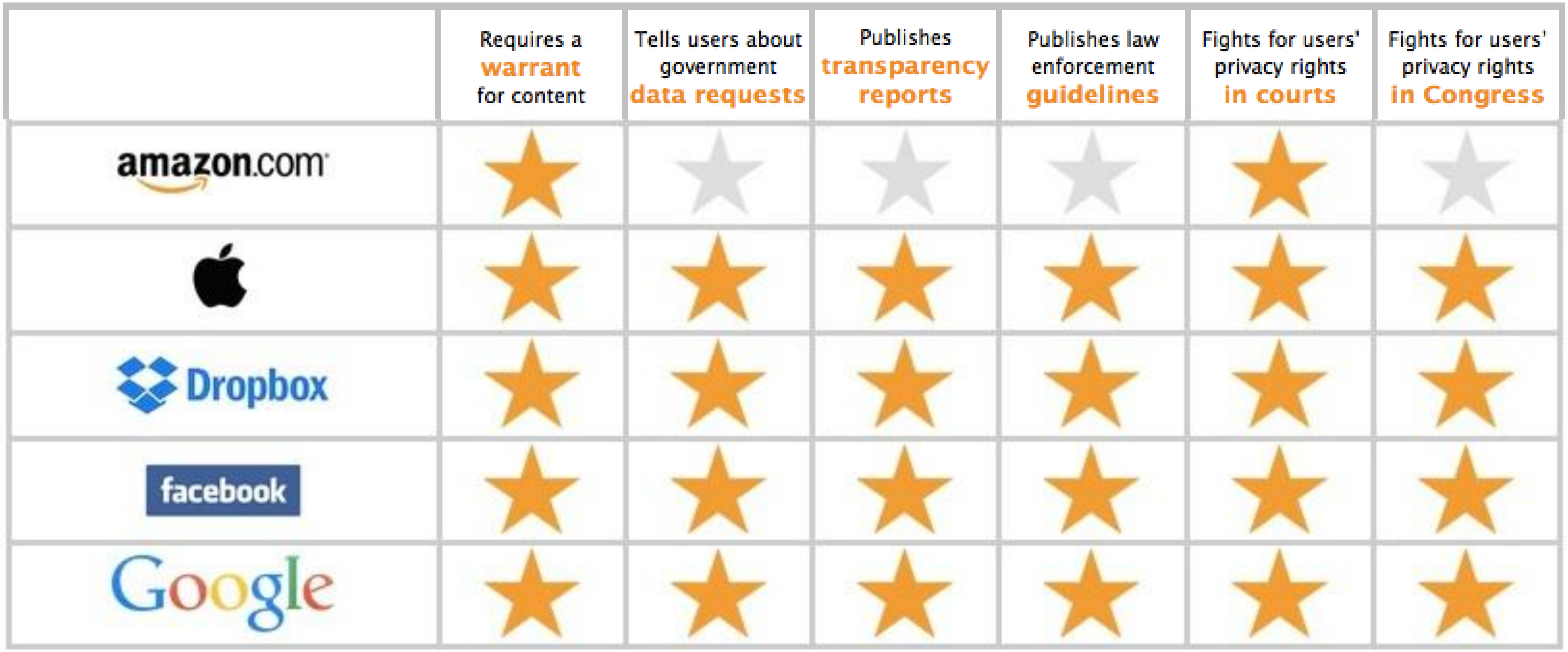


	Requires a warrant for content	Tells users about government data requests	Publishes transparency reports	Publishes law enforcement guidelines	Fights for users' privacy rights in courts	Fights for users' privacy rights in Congress
amazon	☆	☆	☆	☆	★	★
Apple	☆	☆	☆	☆	☆	★
Dropbox	★	★	★	★	☆	★
facebook	★	☆	☆	★	☆	★
Google	★	☆	★	★	★	★

[2013]

https://www.eff.org/who-has-your-back-2013

WHO HAS YOUR BACK?



	Requires a **warrant** for content	Tells users about government **data requests**	Publishes **transparency reports**	Publishes law enforcement **guidelines**	Fights for users' privacy rights **in courts**	Fights for users' privacy rights **in Congress**
amazon.com	★	☆	☆	☆	★	☆
	★	★	★	★	★	★
Dropbox	★	★	★	★	★	★
facebook	★	★	★	★	★	★
Google	★	★	★	★	★	★

[2014]

https://www.eff.org/who-has-your-back-2014

PRIVACY

- UC Privacy Initiative: http://ucop.edu/privacy-initiative
- Privacy Principles:
  - Autonomy Privacy
  - Information Privacy
- Training and Awareness

THANK YOU

What are you doing
to address
risk of click-throughs?

Janine Roeth, UC Santa Cruz, jar@ucsc.edu
Isaac Straley, UC Irvine, straley@uci.edu

Internet2 Net+ Cloud Services: http://www.internet2.edu/cloud-services/

Risk Assessment:

http://bconnected.berkeley.edu/using-bconnected/about-bconnected/choosing-google-apps-berkeley

http://www.oit.uci.edu/office365-project/risk-summary/Information Classification:

https://security.berkeley.edu/data-classification

http://its.ucsc.edu/news/security-news/restricted.html

Allowable Data Use/Data Use Agreements:

http://cloud.ucdavis.edu/privacy_security.html

http://www.cloud.ucla.edu/sites/default/files/box-data-use-agreement.pdf

Higher Ed

Cyber Security Awareness:

http://its.ucsc.edu/security/ncsam.html

http://www.stopthinkconnect.org/

Privacy: http://ucop.edu/privacy-initiative

Terms and Conditions May Apply: http://tacma.net/

Vendor Examples:

http://money.cnn.com/2013/12/04/technology/security/passwords-stolen/

http://online.wsj.com/articles/tim-cook-says-apple-to-add-security-alerts-for-icloud-users-1409880977

http://nakedsecurity.sophos.com/2013/03/02/evernote-hacked-almost-50-million-passwords-reset-after-security-breach/

https://blog.evernote.com/blog/2013/10/04/two-step-verification-available-to-all-users/

https://blog.dropbox.com/2014/05/web-vulnerability-affecting-shared-links/

http://grahamcluley.com/2014/05/dropbox-vulnerability-privacy/

http://threatpost.com/50-security-flaws-fixed-in-google-chrome

http://googleonlinesecurity.blogspot.com/2014/07/announcing-project-zero.html

Vendor Supported Security Awareness:

https://simplysecure.org/

https://www.google.com/intl/en_us/goodtoknow/

https://www.facebook.com/security

Vendor