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.
Risky Business: Click-Throughs & You

Janine Roeth, UC Santa Cruz
Isaac Straley, UC Irvine

© 2014 Regents of the University of California
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
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
“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
Examples of...
- Cloud storage, collaboration, social media
- Used by individuals and institution
- Popular or pervasive
- Multi-platform, i.e. web, mobile
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
Clickthrough terms did not address the following conditions:

- sensitive data
- 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
Availability – ability to do “business”
- Research, teaching and public service

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

What are your critical functions?
Vendor Terms:

What The Terms Say and Real-Life Events
We protect [your data] on our servers using a combination of administrative, physical and logical security safeguards“
Security

“[We take] precautions... to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction”
“We work hard to protect [us and you] from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold”
We have a team dedicated to keeping your information secure and testing for vulnerabilities"
Security

“We do our best to keep your information secure, but we need your help…..”
The massive data breach was a result of keylogging software maliciously installed on computers around the world.
Apple CEO Denies a Lax Attitude Toward Security...

...hackers correctly answered security questions...[or used] a phishing scam to obtain user IDs and passwords
Evernote hacked - almost 50 million passwords reset after security breach

Two-Step Verification Available to All Users
[May 5, 2014]

Web vulnerability affecting shared links

[May 6, 2014]

Dropbox told about vulnerability in November 2013, only fixed it when the media showed interest
The vulnerabilities earned the security researcher...a $30,000 bug bounty from Google...
We're hiring the best practically-minded security researchers and contributing 100% of their time toward improving security across the Internet.
“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
“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.”
“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”
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”
“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.”
“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”
How to Transfer Files Between Dropbox, Google Drive and Other Online Data Storage Services

Your account is ready. Get started.

Download the free mover.

Customize an account.

DON'T LET YOUR DATA ...

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 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 limited in its ability to protect the data.
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
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

*UC Cloud Services Workgroup & Center of Excellence*
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.
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.

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>On-Premise</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Management and Ownership</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Discuss</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Discuss</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td>Discuss</td>
<td></td>
</tr>
<tr>
<td>Incident Management</td>
<td>Discuss</td>
<td></td>
</tr>
<tr>
<td>Data Recovery</td>
<td>Discuss</td>
<td></td>
</tr>
</tbody>
</table>

**EMAIL / CALENDAR SOLUTION: ASSESSMENT MATRIX**

This matrix was one tool used in our assessment and was designed and written by the opinion of the assessment team.

**MICROSOFT VS GOOGLE ASSESSMENT MATRIX**

- Category: Google Apps for Education
  - Issue: Office 365
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

+ Customer

- Operating System
- Applications
- Security Groups
- Firewalls
- Network Configuration
- Account Management

Amazon Web Services

[Logos for various compliance and security standards]
INDIVIDUAL
GOALS

- Improve education & self-service tools so end-users can:
  - Consider risks of data sensitivity & business criticality
  - Determine appropriateness
“What kinds of data do I have?”

Tie to University-wide information classification

- Risk-based
- Indicates data sensitivity
Maps each Data Class, aka Protection levels 0 to 3 to Adverse Business Impact

Includes Sample Data

<table>
<thead>
<tr>
<th>Data Class</th>
<th>Adverse Business Impact*</th>
<th>Sample Data (not an exhaustive list)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection Level 3</td>
<td>Extreme</td>
<td>-</td>
</tr>
<tr>
<td>Protection Level 2</td>
<td>High</td>
<td>-</td>
</tr>
<tr>
<td>Protection Level 1</td>
<td>Moderate</td>
<td>-</td>
</tr>
</tbody>
</table>

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
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.
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 stored in various cloud services. Please contact cloud-services@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.

<table>
<thead>
<tr>
<th>Teaching files (e.g., course content, syllabi)</th>
<th>Box.com</th>
<th>Google Apps (Drive, Docs, etc.)</th>
<th>Microsoft Office 365 (SkyDrive)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research files (e.g., papers, data files)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>N/A</td>
</tr>
<tr>
<td>Administrative contracts, reports</td>
<td>✔️</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>Protected health to HIPAA</td>
<td>✔️</td>
<td></td>
<td></td>
<td>HIPAA guideli</td>
</tr>
<tr>
<td>Student records</td>
<td>✔️</td>
<td></td>
<td></td>
<td>Under Review by the CISO</td>
</tr>
<tr>
<td>Credit cards</td>
<td>✔️</td>
<td></td>
<td></td>
<td>PCI Data Se Standards</td>
</tr>
<tr>
<td>Human resources</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personnel records</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Venues</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee records</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 1. Data use requirements for UCLA cloud storage services

<table>
<thead>
<tr>
<th>Box</th>
<th>Permitted</th>
<th>Contact Client Support</th>
<th>Prohibited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any information already publicly available</td>
<td>Data relating to human subjects or animal research</td>
<td>Storage of UCLA Logon, OASIS Logon, MedNet AD, and EMAD passwords</td>
<td></td>
</tr>
<tr>
<td>Student records not related to health</td>
<td>Export controlled data</td>
<td>Credit card</td>
<td></td>
</tr>
<tr>
<td>Personnel records</td>
<td>Use of 3rd-party Box apps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
Promoting Two-Step Verification aka Two-Factor Authentication
A guide to staying safe and secure online

Stay safe and secure online

Good to know

Simply Secure

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
<table>
<thead>
<tr>
<th></th>
<th>Requires a warrant for content</th>
<th>Tells users about government data requests</th>
<th>Publishes transparency reports</th>
<th>Publishes law enforcement guidelines</th>
<th>Fights for users' privacy rights in courts</th>
<th>Fights for users' privacy rights in Congress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Apple</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Dropbox</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Facebook</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Google</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
</tbody>
</table>

2013

https://www.eff.org/who-has-your-back-2013
## WHO HAS YOUR BACK? 2014

<table>
<thead>
<tr>
<th>Company</th>
<th>Requires a warrant for content</th>
<th>Tells users about government data requests</th>
<th>Publishes transparency reports</th>
<th>Publishes law enforcement guidelines</th>
<th>Fights for users' privacy rights in courts</th>
<th>Fights for users' privacy rights in Congress</th>
</tr>
</thead>
<tbody>
<tr>
<td>amazon.com</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
<tr>
<td>Apple</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
<tr>
<td>Dropbox</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
<tr>
<td>facebook</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
<tr>
<td>Google</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
</tbody>
</table>
PRIVACY

- UC Privacy Initiative: [http://ucop.edu/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/](http://www.internet2.edu/cloud-services/)

Risk Assessment:

[http://bconnected.berkeley.edu/using-bconnected/about-bconnected/choosing-google-apps-berkeley](http://bconnected.berkeley.edu/using-bconnected/about-bconnected/choosing-google-apps-berkeley)


Information Classification:

[https://security.berkeley.edu/data-classification](https://security.berkeley.edu/data-classification)


Allowable Data Use/Data Use Agreements:

[http://cloud.ucdavis.edu/privacy_security.html](http://cloud.ucdavis.edu/privacy_security.html)


Cyber Security Awareness:

[http://its.ucsc.edu/security/ncsam.html](http://its.ucsc.edu/security/ncsam.html)


Privacy: [http://ucop.edu/privacy-initiative](http://ucop.edu/privacy-initiative)
Terms and Conditions May Apply: [http://tacma.net/](http://tacma.net/)

Vendor Examples:


[https://blog.evernote.com/blog/2013/10/04/two-step-verification-available-to-all-users/](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/](https://blog.dropbox.com/2014/05/web-vulnerability-affecting-shared-links/)

[http://grahamcluley.com/2014/05/dropbox-vulnerability-privacy/](http://grahamcluley.com/2014/05/dropbox-vulnerability-privacy/)

[http://threatpost.com/50-security-flaws-fixed-in-google-chrome](http://threatpost.com/50-security-flaws-fixed-in-google-chrome)

[http://googleonlinesecurity.blogspot.com/2014/07/announcing-project-zero.html](http://googleonlinesecurity.blogspot.com/2014/07/announcing-project-zero.html)

Vendor Supported Security Awareness:

[https://simplysecure.org/](https://simplysecure.org/)


[https://www.facebook.com/security](https://www.facebook.com/security)