



*Information
Security*



**Advice
Strategy
Solutions
Consulting**

"That Will Never Happen To Us": Five Ways to Make Security Risks Relevant to Your Organization

Todd Brasel, PMP, CSM Principal Consultant
Vince Hannon, CISM Senior Consultant
NYSTEC Information Security Team

500 Avery Lane
Rome, NY 13441
315.338.5818
www.nystec.com

Contact Information



Vince Hannon

518-768-1156

vhannon@nystec.com

Todd Brasel

518-418-5669

tbrasel@nystec.com

*Bringing Clarity
To Complex Technology Projects*



About this Presentation

- Selecting a Risk Management Framework
- Performing a Risk Assessment
- (Five ways to) Build a Risk-Aware Culture
- Additional Resources



Anthem Breach

- Second-largest health insurer in the US
- 78.8 Million Records stolen
- More than populations of CA, TX, and NY - *Combined*

The screenshot shows an email or letter from Anthem. The header includes the Anthem logo and navigation links: Home, FAQ, A Letter from our CEO, and En Español. The main heading is "How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services". The body text explains that Anthem is working with AllClear ID to provide identity theft repair and credit monitoring services to affected members. It lists eligible states: California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, and Wisconsin. The letter includes a return address for Anthem, Inc. in Monroe, WI, and a QR code. At the bottom, there is a barcode and the date "February 25, 2015".

Anthem Home FAQ A Letter from our CEO En Español

Anthem 1-01
Anthem, Inc.
P.O. Box 260
Monroe, WI 53566 - 0260

How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services

Anthem is working with AllClear ID, a leading and trusted identity protection provider, to provide months of identity theft repair and credit monitoring services to current or former members affected by the Anthem breach dating back to 2004.

This includes customers of Anthem, Inc. companies Amerigroup, Anthem and Empire Blue Cross and Blue Shield companies, Caremore, and Unicare. Additionally customers of Blue Cross and Blue Shield insurance in one of fourteen states where Anthem, Inc. operates may be impacted and are also eligible: California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, and Wisconsin.

<NAME>
<STREET ADDRESS>
<CITY, ST ZIP>

0000001 01 SP 0.480 **SNGLP T1 1 2227 00727-235849 _-C01-P00001-I

February 25, 2015

Healthcare Breaches



https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

<http://www.databreaches.net/>

Office of Inadequate Security
Your info, their screw-ups.

Home | About | Breach Laws | Privacy Policy | Transparency Reports

Home » Breach Types » Hack » Anthem's notification letter to affected members

Feb 14 2015 Anthem's notification letter to affected members
Hack, Health Data, U.S.

A template of Anthem's letter to affected members has been submitted to the General's Office. You can read it [here](#) (pdf).

Related Posts:

- California settles with Anthem Blue Cross over data breach
- A preview of SCDOR's breach notification letter to...
- Credit union notifying customers after drive with personal...
- U.S. states say Anthem too slow to inform customers about...
- Senators blast Anthem for 'unacceptable'...

U. S. Department of Health & Human Services
Office for Civil Rights

File a Breach | HHS | Office for Civil Rights | Contact Us

Breach Portal

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

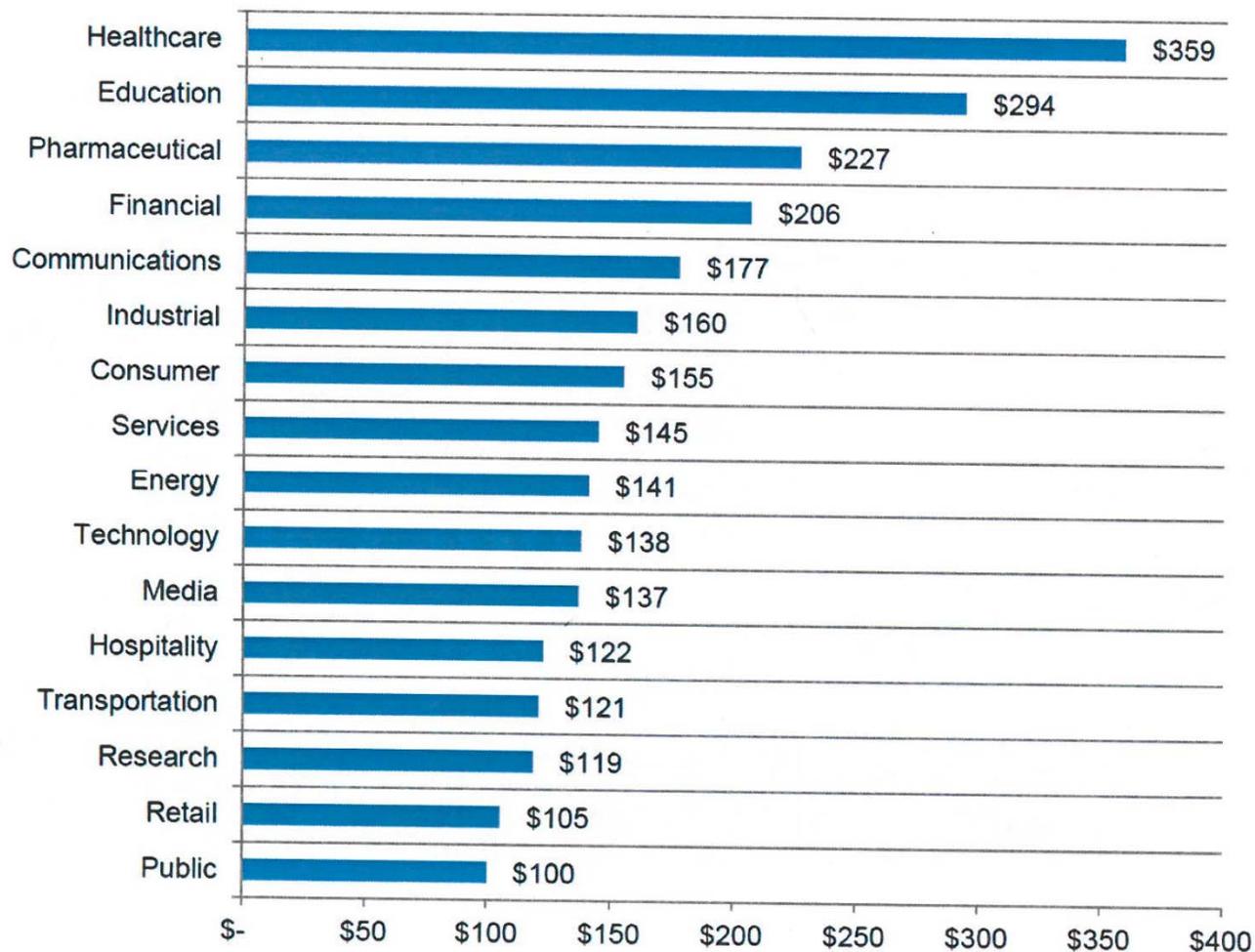
[Show Advanced Options](#)

Breach Report Results							
	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
1	Brooke Army Medical Center	TX	Healthcare Provider	1000	10/21/2009	Theft	Paper/Films
2	Mid America Kidney Stone Association, LLC	MO	Healthcare Provider	1000	10/28/2009	Theft	Network Server
3	Alaska Department of Health and Social Services	AK	Healthcare Provider	501	10/30/2009	Theft	Other, Other Portable Electronic Device
4	Health Services for Children with Special Needs, Inc.	DC	Health Plan	3800	11/17/2009	Loss	Laptop
5	L. Douglas Carlson, M.D.	CA	Healthcare Provider	5257	11/20/2009	Theft	Desktop Computer

Bringing Clarity
To Complex Technology Projects



Cost of Data Breaches Per Capita, By Industry

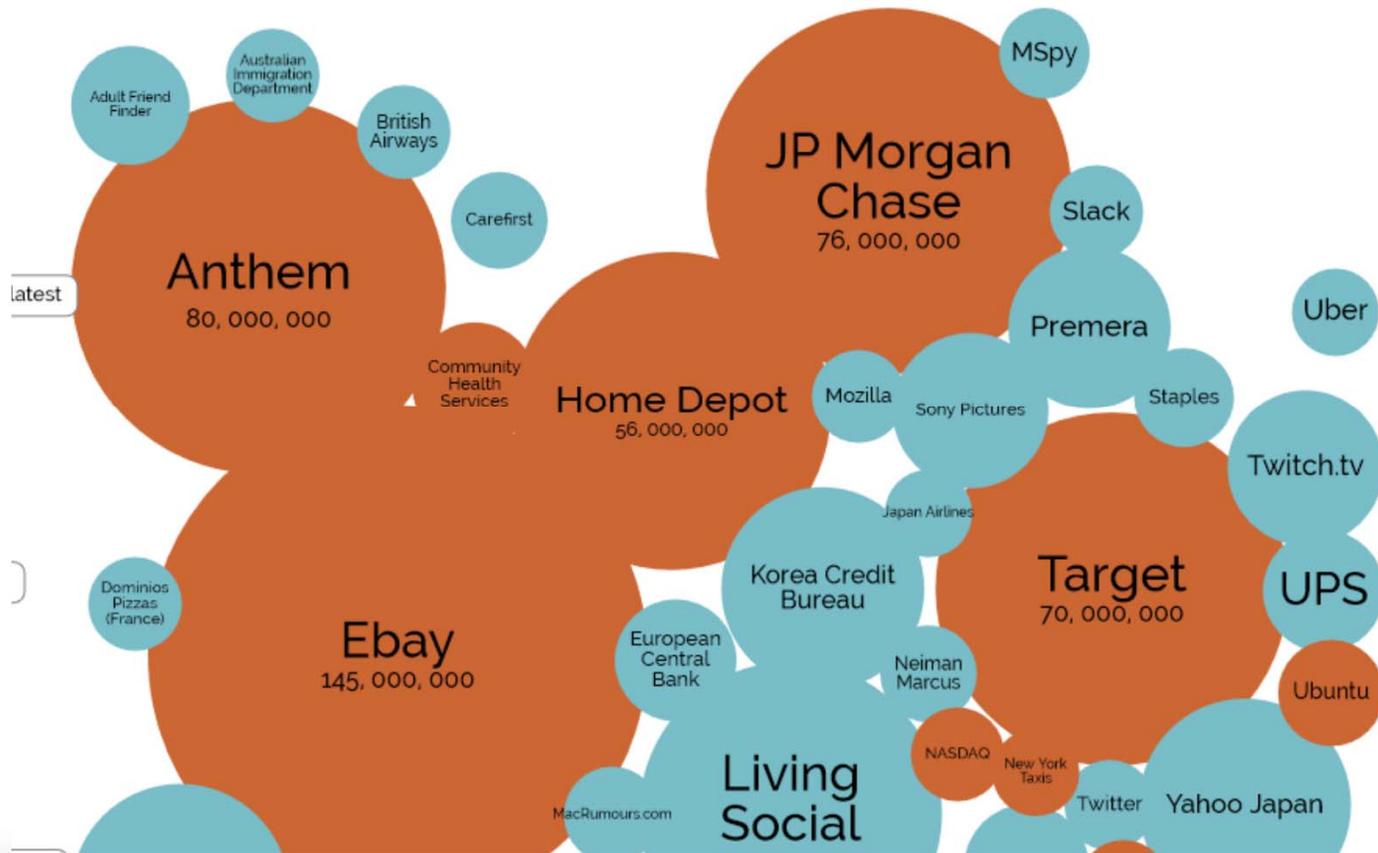


Source: Ponemon Institute, LLC. "2014 Cost of Data Breach Study".



Recent Data Breaches

<http://www.informationisbeautiful.net/visualizations/world-s-biggest-data-breaches-hacks/>



Bringing Clarity
To Complex Technology Projects



Selecting a Risk Management Framework

A *risk management framework* is a strategy for prioritizing and sharing information about the security risks to an information technology (IT) infrastructure.

- Organizes and presents information in a way that both technical and non-technical personnel can understand.
- Provides a common view and a method to measure an organization's security risk
- It has three important components: a *shared vocabulary*, *consistent assessment methods* and a *reporting system*.

Helpful for addressing potential threats pro-actively, planning budgets and creating a culture in which the value of data is understood and appreciated.



Risk Management Framework Examples

COSO - Committee of Sponsoring Organizations of the Treadway Commission - The COSO "Enterprise Risk Management-Integrated Framework" published in 2004 has eight Components and four objectives categories.

ISO - International Standards Organization - The purpose of ISO 31000:2009 is to be applicable and adaptable for any public, private or community enterprise, association, group or individual.

COBIT - Control Objectives for IT (COBIT) – ISACA - COBIT is a generic and useful governance framework for enterprises of all sizes, whether commercial, not-for-profit or in public sector.

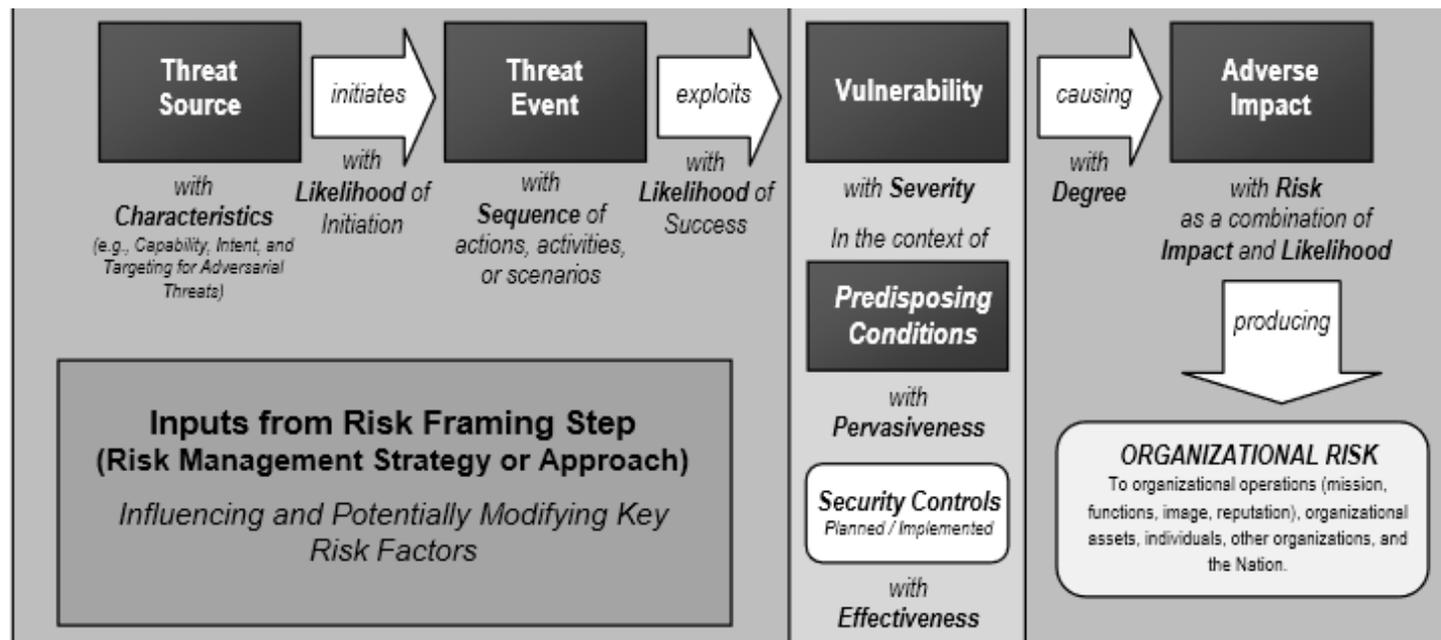
NIST - National Institute of Standards and Technology (NIST) Risk Management Framework – The Risk Management Framework (RMF) is the “common information security framework” for the federal government and its contractors.



Understanding and Assessing Risk

It is important to select and use a standardized approach to assessing information security risk for your organization.

NIST Special Publication 800-30 Revision 1 provides a comprehensive approach to assessing risk



Risk Assessment Results

Risk Report

Assessed risks are rated and recommendations made, which become part of the remediation plan.

Lack of an Active <Agency Name> Incident Response Program Leads to Increased Impact and Risk

Attribute	Score	Risk Summary
Risk Identifier	Adv-26	Because it is impossible to prevent all breaches, organizations must be prepared to handle breaches with a documented and rehearsed
Likelihood	High	

Impact	<p>Compliance Overview</p> <p>Requirements - Required</p> <p>Fully Compliant: 60 % Partially Compliant: 20 % Total of Required: 80 %</p>  <p>Notes</p> <p>% of Required items for which full compliance was achieved % of Required items that were only partially complied with % of Required items in total that were at least partially complied with</p>	
Risk Score	<p>Requirements - Addressable</p> <p>Fully Compliant: 67 % Partially Compliant: 12 % Total of Addressable: 78 %</p>  <p>Notes</p> <p>% of Addressable items for which full compliance was achieved % of Addressable items that were only partially complied with</p>	
Recommendations	<p>Requirements - No Mandate</p> <p>Fully Compliant: 56 % Partially Compliant: 27 % Total of No Mandate: 83 %</p> <p>Total (Required & Addressable)</p> <p>Fully Compliant: 64 % Partially Compliant: 16 % Total: 79 %</p> <p>Total (Required, Addressable, No-Mandate)</p> <p>Fully Compliant: 59 % Partially Compliant: 23 % Total: 82 %</p>	

#	Recommendation	Risk #	Risk Score
1	Develop a plan to manage identified security issues and to reduce the impact of associated security risks.	1	Moderate
2	Continue regular communications to advance security awareness through interactive meetings, visits, and distributed materials.	1	Moderate
3	Develop procedures to detect and address compliance lapses that arise due to the human component of security at both the headquarters and remote offices.	2	Moderate
4	Ensure operations managers and staff are aware of applicable regulations and that staff are following them to the best of their ability.	3	High

Assessing Risk

- Being on The Bad List isn't a good thing
Managing risk should be proactive, not reactive
- Identify a suitable risk management framework
Provides common vocabulary, assessment methodology, and reporting standards
- Use the framework's risk assessment methodology
Standardized and consistent measurement of risk
- Use the risk assessment to develop a remediation plan



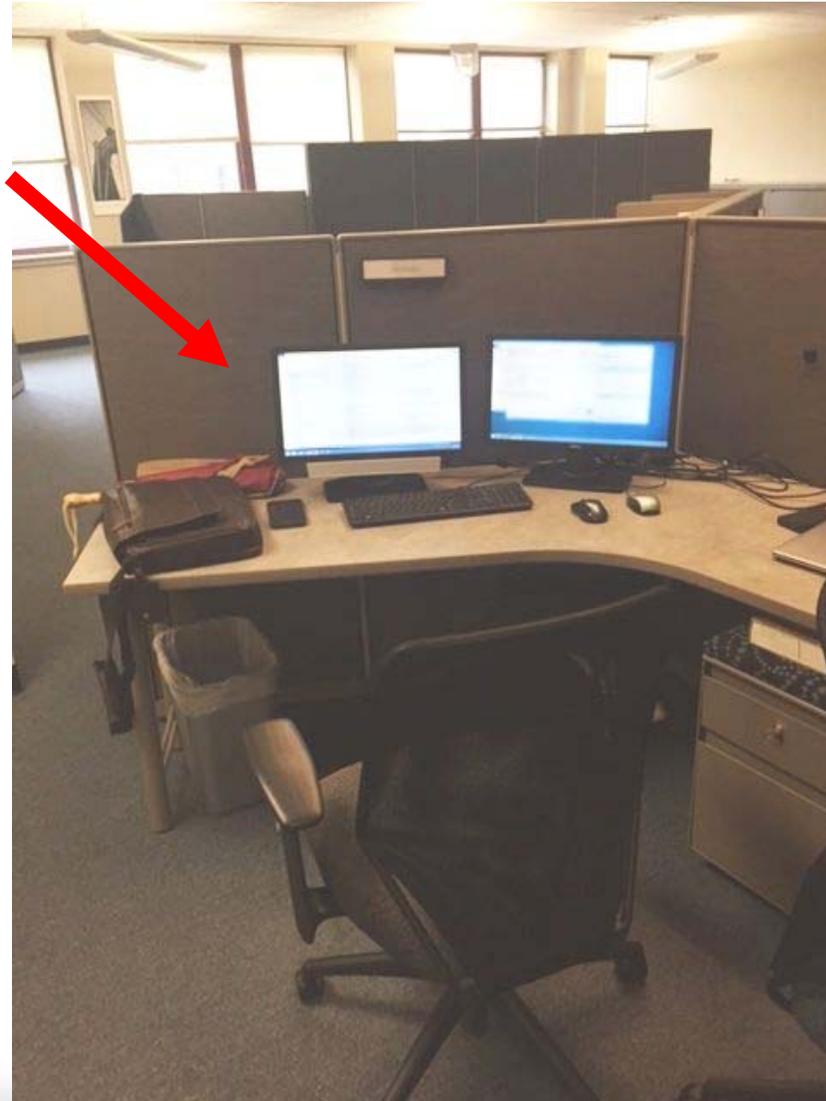
Put the Risk Assessment to Work



*Bringing Clarity
To Complex Technology Projects*



Is Your Risk Assessment Working?

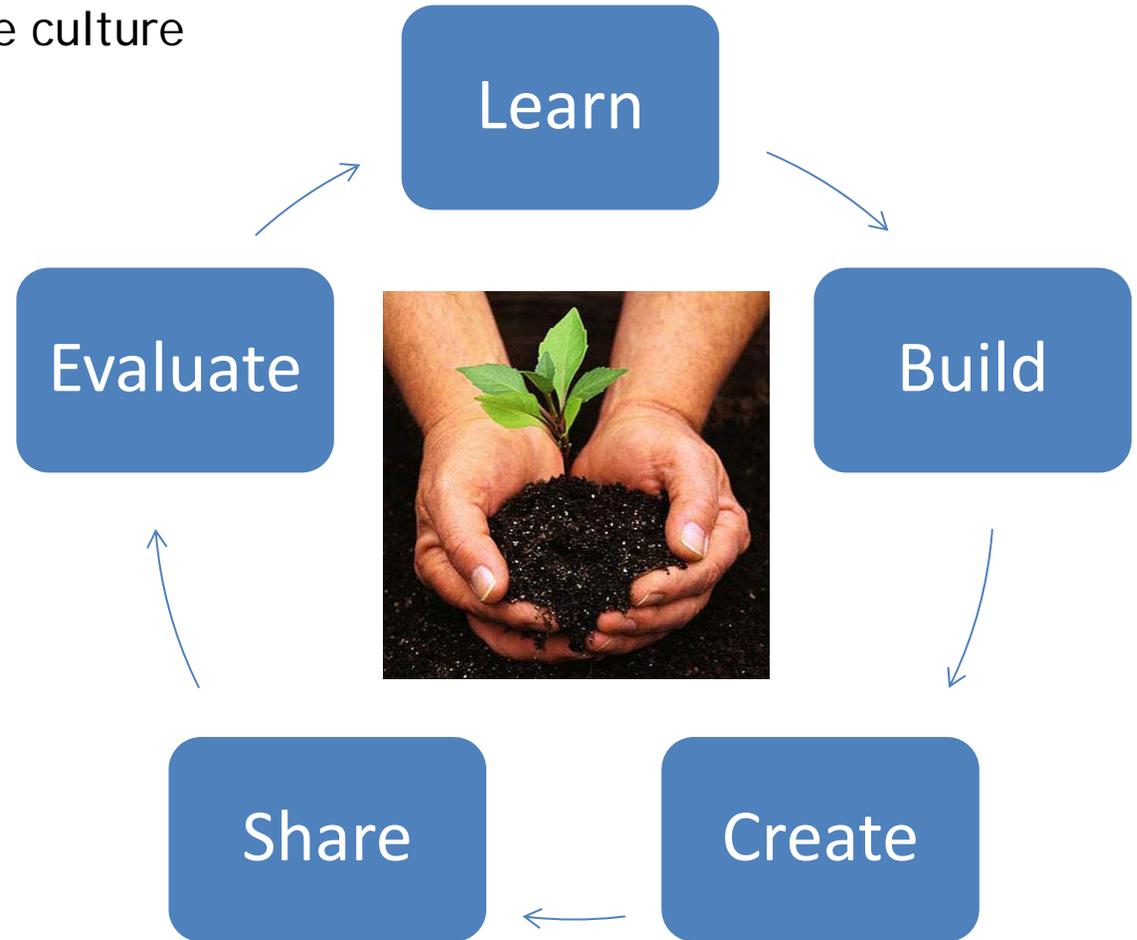


*Bringing Clarity
To Complex Technology Projects*



Strategy and Plan

Strategy: Build a risk-aware culture

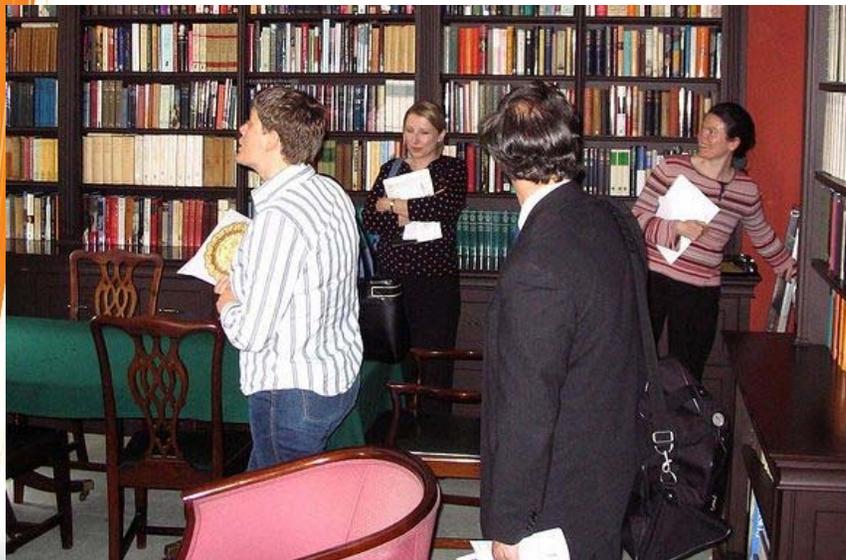


Plan: Make small, meaningful and cumulative changes to your organization

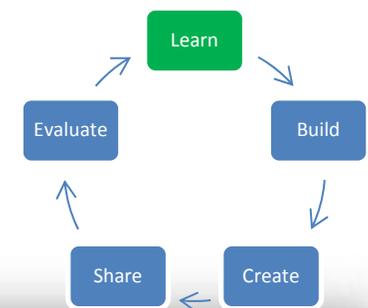


Learn... About Your Organization

Environment
influences...



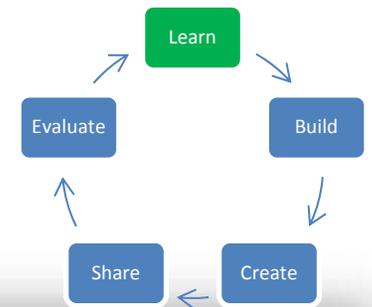
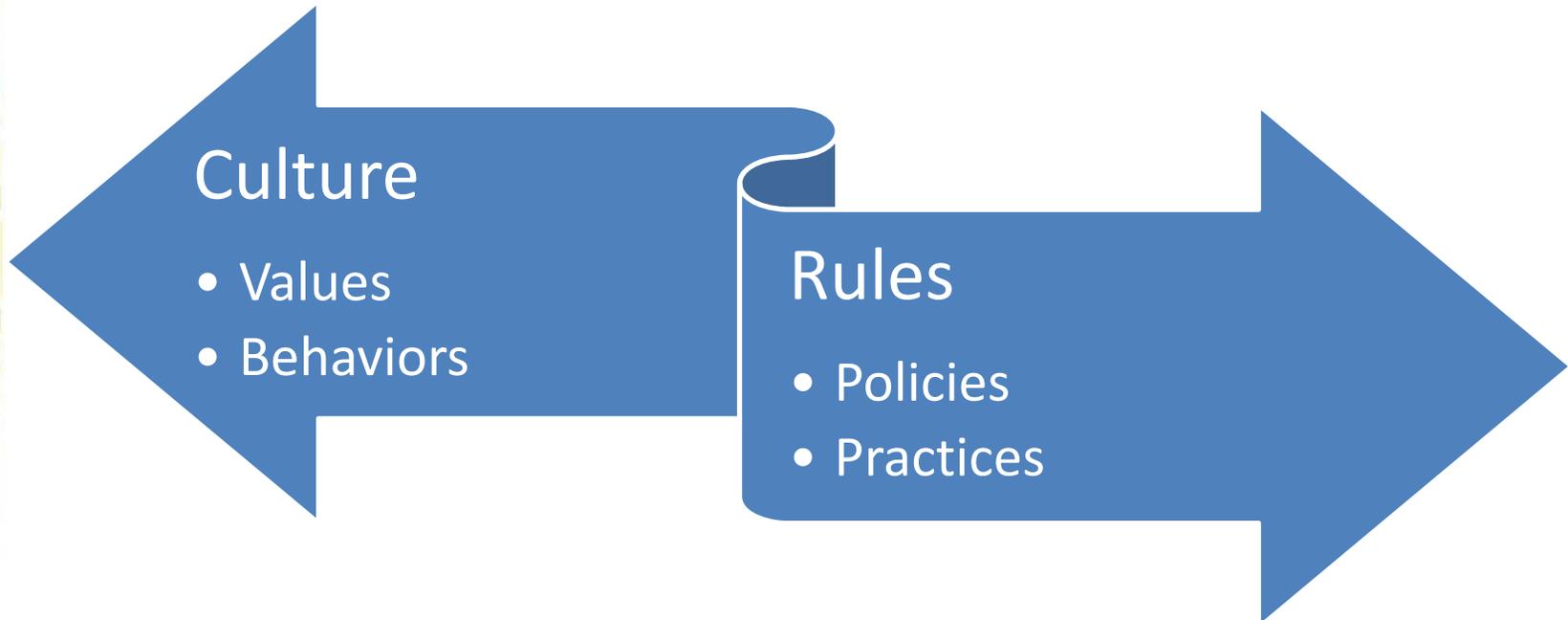
... and reinforces
behavior



*Bringing Clarity
To Complex Technology Projects*



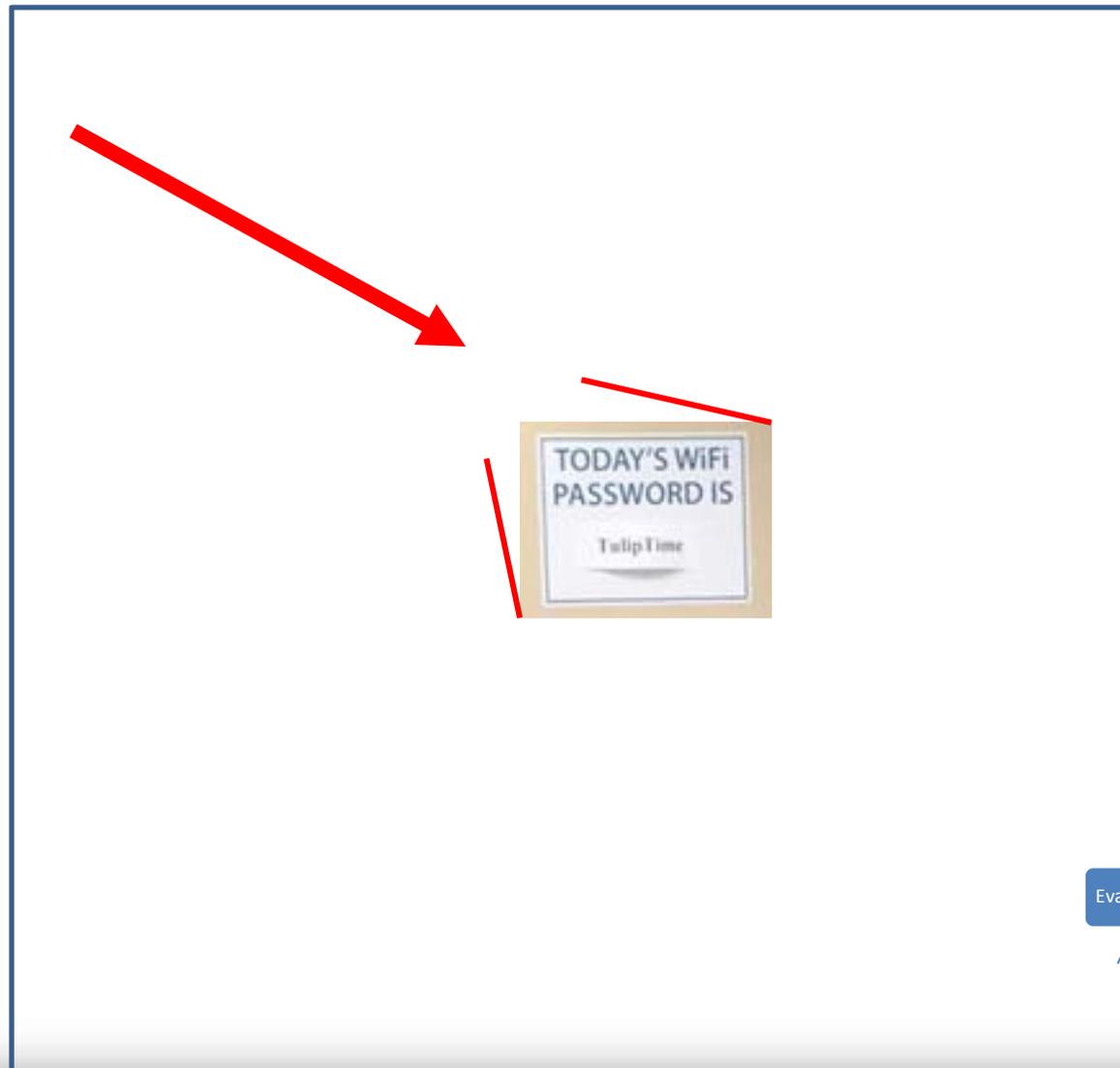
Learn... About Conflicts



*Bringing Clarity
To Complex Technology Projects*



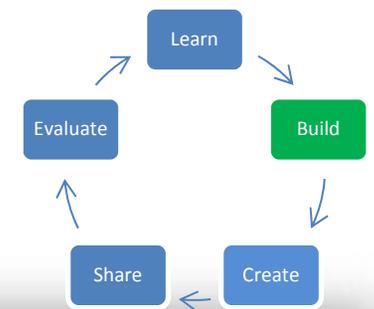
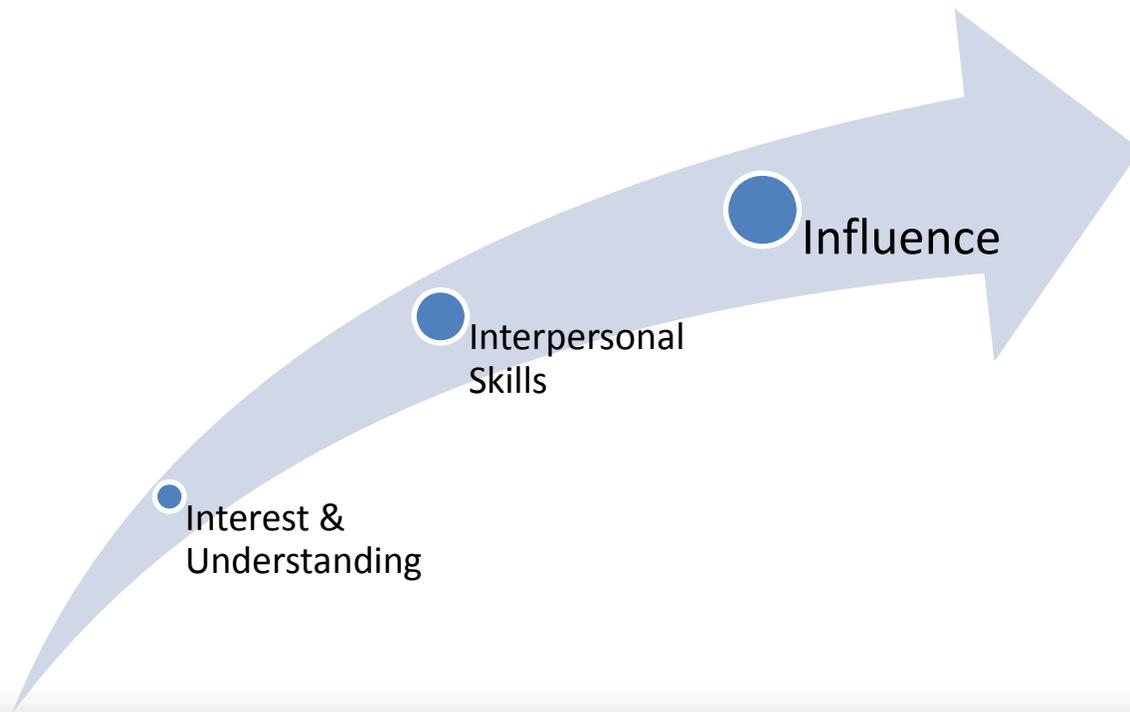
Learn... By Observation



Bringing Clarity
To Complex Technology Projects



Build... A Community of Interest



Bringing Clarity
To Complex Technology Projects

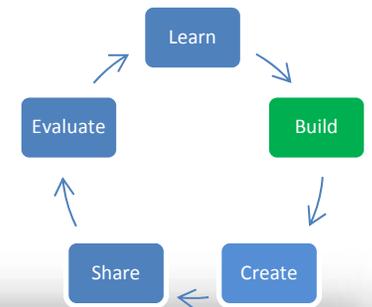


Engaging Your Community

Listen to the people in your community...



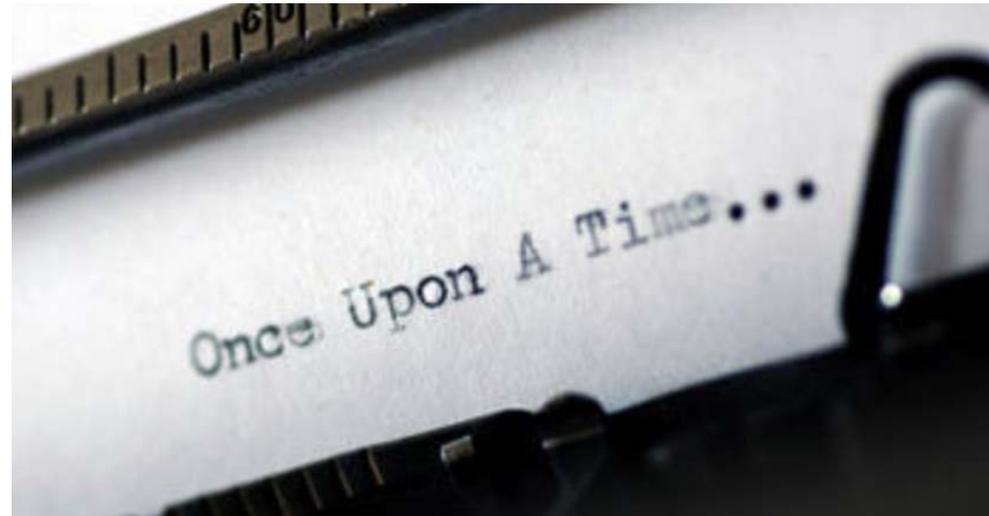
... instead of ***lecturing*** to them



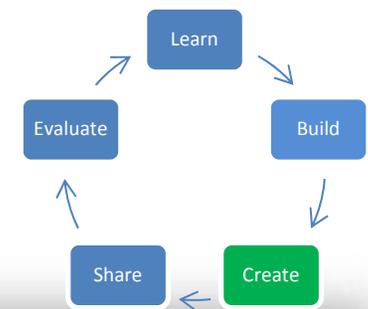
Bringing Clarity
To Complex Technology Projects



Create... Stories About Risk



- Speak to values
- Include facts and data
- Empower the listener

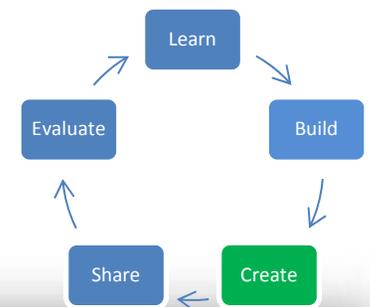


Use Appropriate Language



Focus on the problem and not the person

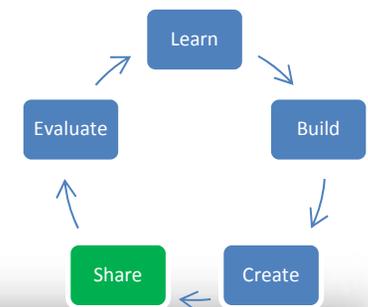
Be aware of the contextual meaning of terms



Share... The Stories About Risk



- Communicate where conflicts occur
- Vary the modes of communication



*Bringing Clarity
To Complex Technology Projects*



Promoting Risk Awareness Online



Carefully select your online presence to fit your needs.



Home Safety Tips & Advice News & Views Parents' Guides Media Library Res

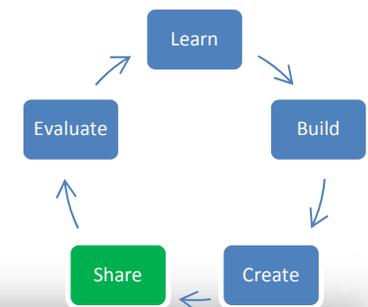
Home » Featured » Tips for Strong, Secure Passwords

Tips for Strong, Secure Passwords

Posted on August 6, 2014 by ConnectSafely in Featured, Safety Tips

A strong password is your first line of defense against intruders and imposters. **Never give out your password to anyone.*** Never give it to friends, even if they're really good friends. A friend can – maybe even accidentally – pass your password along to others or even become an ex-friend and abuse it. **Don't just use one password.** It's possible that someone working at a site where you use that password could pass it on or use it to break into your accounts at other sites. **Create passwords that are easy to remember but hard for others to guess.** When possible, use a phrase such as "I started 7th grade at Lincoln Middle School in 2004" and use the initial of each word like this: "I57gaLMSI2004." And make them at least a little different (by adding a couple of unique

Online - Pro:	Online - Con:
Support passive information sharing	Requires monitoring on a daily or hourly basis
Greater control over messages and content	Generating content can be time consuming
Provides a sense of organizational presence	Less control over messages and content



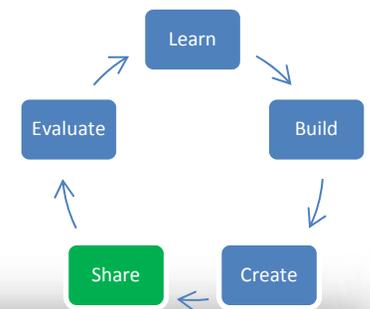
*Bringing Clarity
To Complex Technology Projects*



Keep Risk Communication Fresh

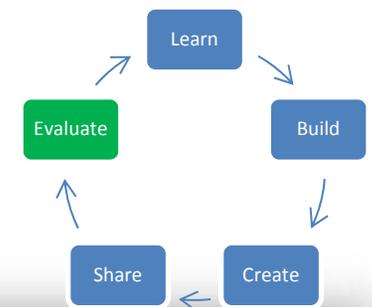


No matter which media you choose, keep your messages fresh – don't let them fade!

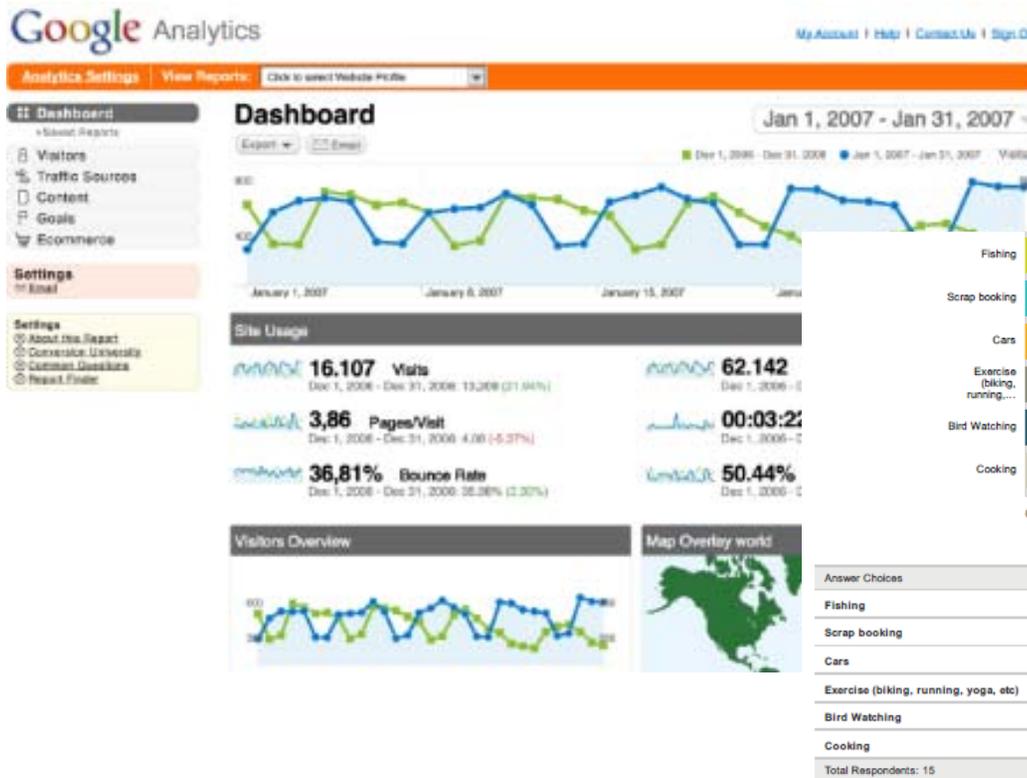


Evaluate... and Adjust

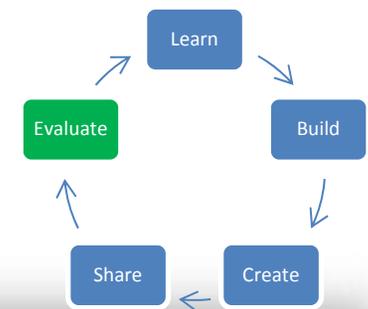
- Awareness surveys
- Community involvement
- Managerial support



Evaluate... With Data



Surveys and site metrics provide quantitative data about your risk communication



Bringing Clarity
To Complex Technology Projects



Remember:



Your Next 30 Days

Day	Goal
Week 1: Learn	Review your risk assessment and look for relevant weaknesses in your organization.
Week 2: Build	Reach out to several potential people who could form the core of your community of interest. Invite them to a group lunch on the topic of communicating about security. Share your story and get feedback.
Week 3: Create	Write a story that demonstrates how an ordinary person in your organization can take action to reduce the risk associated with the security weakness.
Week 4: Share	With feedback from your lunch meeting, plan the first communication and method of delivery. Determine how you will get quantitative feedback on the communication.
<i>Evaluate and Repeat!</i>	



Additional Resources

- NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST 800-30: Risk Management Guide for Information Technology Systems
- NIST 800-39: Managing Information Security Risk: Organization, Mission, and Information System View
- NIST 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems
- Ariely, Dan. *Predictably irrational: the hidden forces that shape our decisions*. 2010. Harper Perennial.
- Bruce Schneier's blog "Schneier on Security"
- Khaneman, D. & Tversky, A. *Prospect theory: an analysis of decision under risk*. 1979. *Econometrica*, 47(2), pp. 263-291.
- Yan, J., Blackwell, A., Anderson, R., & Grant, A. *The memorability and security of passwords - some empirical results*. 2000. University of Cambridge Technical Report #500 / UCAM-CL-TR-500
- Pfleeger, S. & Caputo, D. *Leveraging behavioral science to mitigate cyber-security risk*. 2012. MITRE.

