Redesigning Boston College's information security awareness program based on current research

Boston University Security Camp

Julie Gillis & David Millar

August 21, 2014

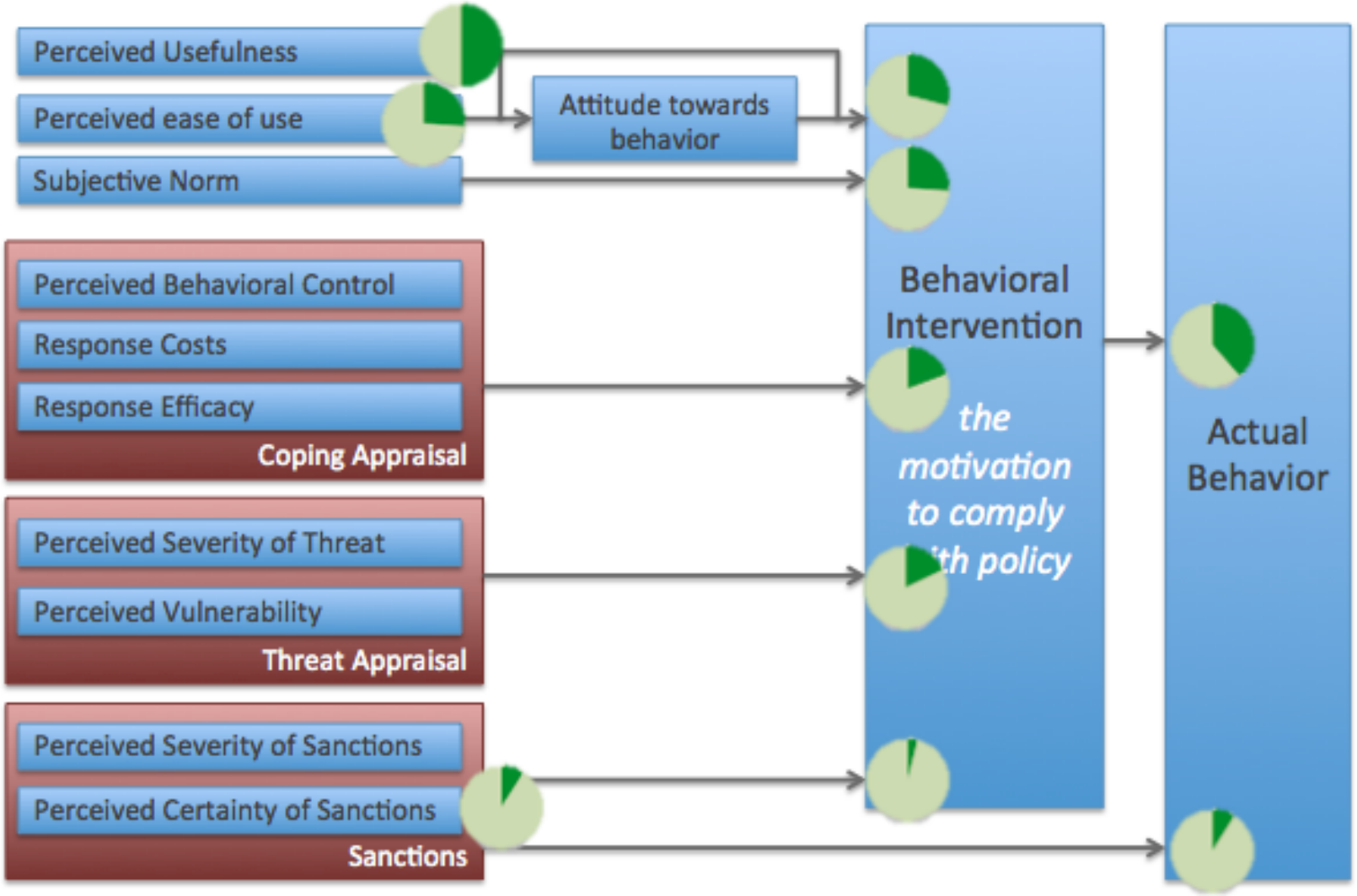
Agenda

- Motivation
- Review of literature
- BC’s planned approach

Dave's experience doing SETA

- Developed SETA based only on intuition
- Brochures, lectures, websites
- No fundamental improvement
- I must be doing it wrong
- Bigger brochures, bigger websites, more lectures
- No fundamental improvement
- Bigger brochures, etc.,etc,…..

Typical academic research circa 2005



Literature reviewed

- Search scholar.google.com for
  - “information security” AND (education OR training OR awareness)
- Search Gartner Group for
  - “information security” AND (education OR training OR awareness)
- Not reviewed, but recommended:
  - *Measuring the Effectiveness of Security Awareness Programs,* Educause/ECAR 2013

Academic Research in Information Security

Terminology

SETA Security Education Training and Awareness

Academic approach to SETA

- SETA is viewed as the process of ensuring compliance with the organization's security policy
- Tacit assumption is that if employee complies with the policy, there can be no security incident

The problem

- Estimated > 50% of data breaches are due directly or indirectly to poor IS security compliance [1]
- SETA programs are developed based on “tradition, personal judgment and whim” [2]
- Most SETA programs lack an underlying theory [3]
- These programs are not working well:
  - < 12% believe awareness programs are effective [4]
  - 24% didn’t know if their university had a security policy [5]
  - 18% had read it [5]
  - “Most people just eat the chocolate and throw away the brochure”

1. Stanton, Stam, Mastrangelo, 2005
2. Walls (Gartner), 2013
3. Karjalainen & Siponen, 2011
4. Albrechtsen, 2007
5. SanNicolas-Rocca, 2014

Gartner on current state of SETA

"..most enterprises have assumed that a ***set of undefined objectives*** exist for their security awareness program, but have not actually documented these objectives. ...The end result is a costly, unproven awareness program ***based on tradition, personal judgment and whim.*** This approach is not tolerated in any other phase of IT security operations and should not be tolerated in the realm of security awareness." [1]

"Gartner clients report that many employees regard the content, structure and delivery method of security awareness programs to be outmoded and symptomatic of a security program that is out of touch with the modern work environment." [1]

"User guides and policies are filled with statements that are non-specific and require users to take security actions that are beyond their capabilities." [2]

1. Walls (Gartner), 2013

2. Gartner, 2013

Research on sanctions

- Employees' compliance with security policies is not always best explained by fear of sanctions, because…
- Employees use neutralization techniques - rationalizations to justify non-compliance
  - "Nobody could possibly understand this policy"
  - "Nobody has time to comply with these policies"
  - "My compliance with policy X offsets non-compliance with Y"
- Bottom line: no consensus on the value of sanctions

Siponen & Vance, 2010

A qualitative study of users' view on information security (1)

- 2007 survey of bank and customer service center
  - "Of course, there are rules and guidelines for information security behaviour. Nevertheless, I haven't heard about them or seen them. ... I don't believe that everyone has read them… I believe my behaviour is approximately the same as the documented expected behaviour, although I don't know what is written. "
  - "One should know that there are rules on how to behave. I believe the documentation is huge – it is not possible to read it all or to act in compliance with all the demands. "

Albrechtsen, 2007

A qualitative study of users' view on information security (2)

- "IT-rules – they're boring. I don't know them word-for-word, but I know the essence. I don't believe my colleagues know the essence, they don't possess the necessary knowledge to understand it. "

Albrechtsen, 2007

SETA in higher education

- 3 Phases
  I. Survey the university
  II. Assemble faculty and staff to design SETA for the campus
    - Voluntary participation
    - 90 minutes – lunch provided
    - Instant poll on knowledge of policy and threats
    - Small groups spend 30 min. preparing SETA proposals
    - Teams formed to expand on most promising ideas

  III. Survey attendees afterward
- Conclusion: Including end users in planning SETA :
  - Is an effective method to train on policies and procedures and
  - Motivates users to comply.

SanNicolas-Rocca, 2014

2 Requirements for SETA

1. SETA must be
   - Persuasive
   - Non-cognitive
2. Focus on the essential features of SETA
   - Mandatory / voluntary participation
   - Intangible threats

Cognitive arguments and pedagogies are not successful at changing behaviors.

Normative methods are better at that.

Karjalainen & Siponen, 2011

Terminology

- Pedagogy: methods and practices of teaching, e.g.
  - *Behaviorism:* reinforce or reward desired behavior, punish undesired behavior
  - *Instructivism*: instructor explains the topic
  - *Constructivism*: learners communicate with each other
  - *Social constructivism*: groups construct knowledge for one another collaboratively creating a ***culture***

ORIENTATIONS OF PEDAGOGIES

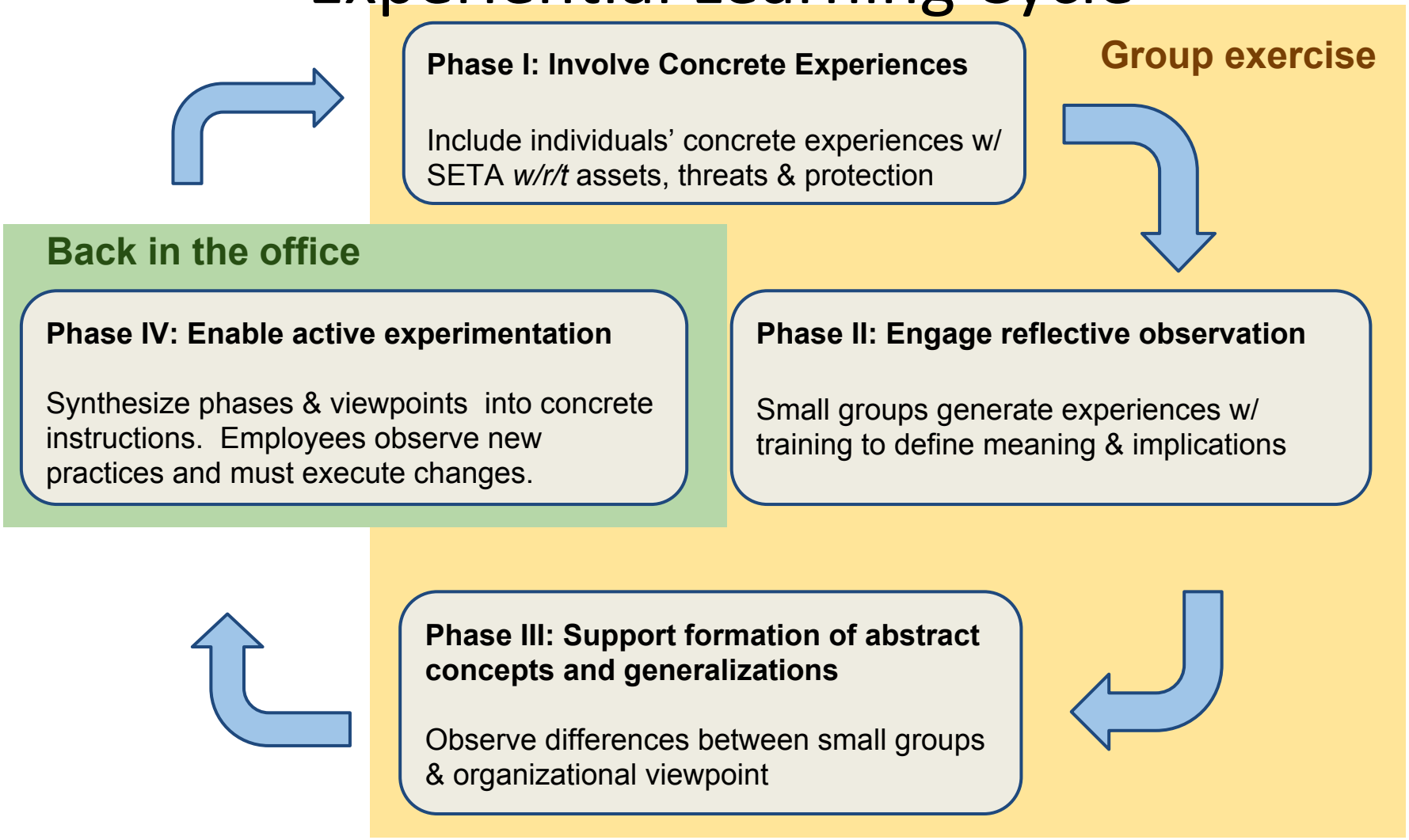
Today

The goal

	Transmission	Transaction	Transformation	
Learning paradigm	Behaviorism	Cognitivism	Constructivism	Social Constructivism
General aims	Mastery of knowledge	Cognitive abilities	Change beliefs and actions, personal change	Change beliefs and actions, communal change
Content	Subject-centered	Problem-centered	Learner-centered	Community-centered
Teaching methods	Instructor led	Cognitive problem solving	Personal knowledge through collaboration	Communal knowledge through collaboration
Evaluation of learning	Tests	Acquired intellectual skills	Conversational forms of evaluation for individuals	Conversational forms of evaluation for groups

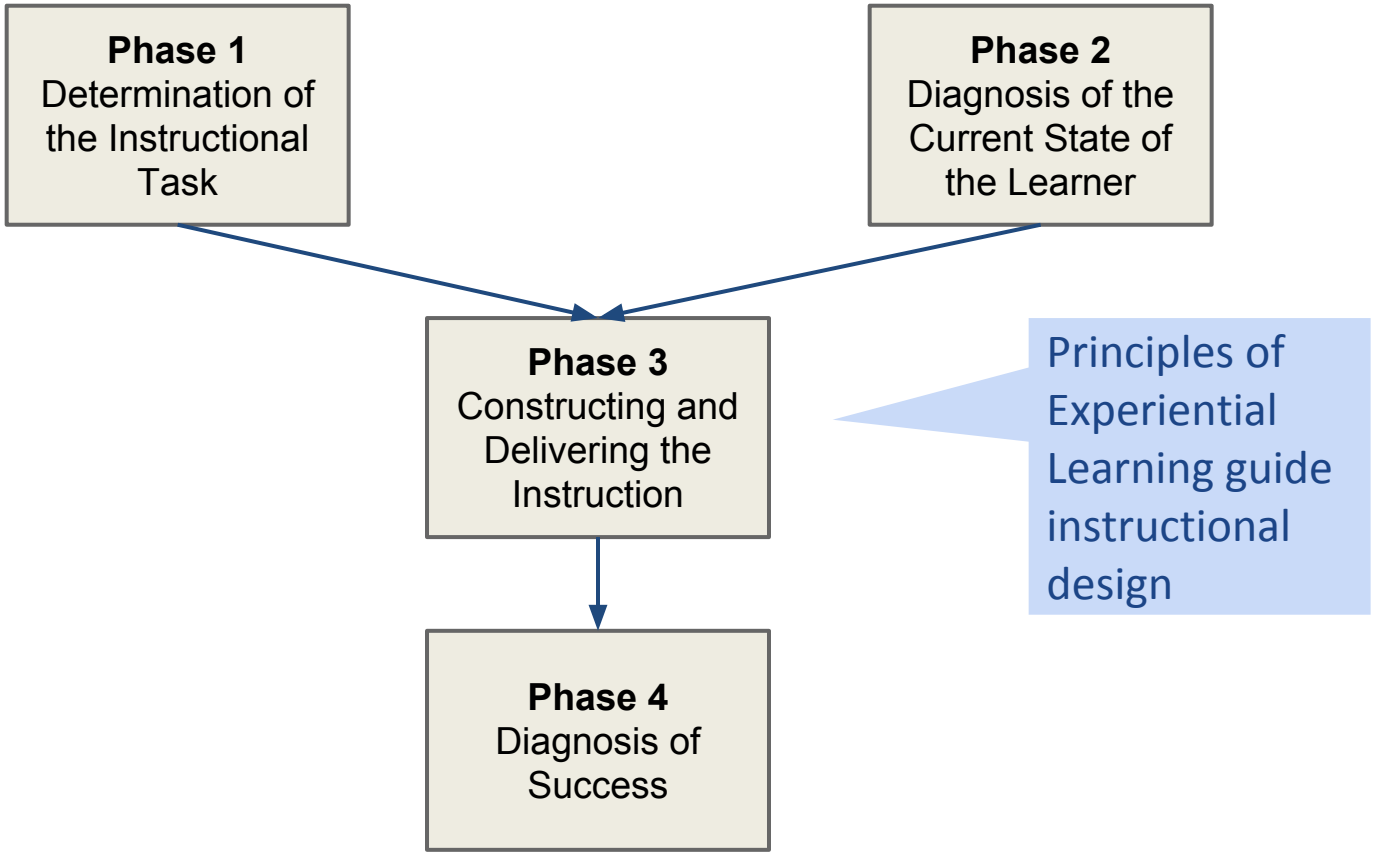
Karjalainen & Siponen, 2011

Experiential Learning Cycle



Karjalainen & Siponen, 2011

Universal Constructivist Instructional Theory



Puhakainen & Siponen, 2010

Worked example (1)

Problem: *Tech firm employees not complying with policy that requires intellectual property be encrypted (7zip) when sent in email*

1. Anonymous survey revealed:
    a. Users generally knew there was a policy
    b. Non-technical staff had trouble using encryption tools
    c. Some employees found the data classification rules confusing
    d. Others found the security manual cumbersome and confusing
2. Interviews revealed:
    a. Management didn't always follow the policy
    b. Sales team often didn't follow the policy
    c. Sometimes receiving party could not decrypt email

Puhakainen & Siponen, 2010

Worked example (2)

3. IS Security manual was revised to address complaints about confusion
4. Two training sessions were held:
    a. All users
        i. Group discussion of risks (activate existing knowledge)
        ii. Learners submit their own chosen documents and group processes how to classify them (activate cognitive processing)
        iii. Learners analyze possible consequences for company, team and learners themselves if intellectual property were leaked. (make the subject matter relevant)
    b. Non-technical users
        i. Enable them to use the encryption software
        ii. Explain how to send the password through another channel

Puhakainen & Siponen, 2010

Worked example (3)

5. Results
    a. Learners realized they had sent considerable intellectual property unencrypted
    b. Non-technical users complained in the training session that 7Zip's lack of support for S/MIME made it hard to correspond with customers
6. Instructors facilitated confidential discussions with CEO re:
    a. CEO's uneven use of encryption
    b. Sales refusal to use encryption
7. Follow up actions
    a. Security department agreed to look for S/MIME compliant crypto tool
    b. Sometimes receiving party could not decrypt email

Puhakainen & Siponen, 2010

Worked example (4)

7. Follow-up (cont.)
    a. Follow up surveys, group and individual interviews
8. Actual results
    a. Sales team continued to not use encryption
    b. Six users complained that the CEO didn't actively enough champion security

Puhakainen & Siponen, 2010

Literature takeaways (1)

- Consider taking a more analytical approach: “Ready. Aim. Fire.” vs. “Ready. Fire. Aim.”
  - Focus on just a few, key priorities
  - Survey and interview users to identify where the breakdown is occurring - i.e. identify the learning task
  - Develop training materials *collaboratively* with users
- “Norms” seems like an opportunity area
  - Thus the value of group exercises/processes
  - Also consider posters profiling security practices of campus thought leaders

Literature takeaways (2)

- Group workshops appear to be effective
  1. Focused on high-risk groups
  2. To improve the quality of learning materials
- Most or all of the literature treats “policy” and “procedures” as the definitive reference for employee behavior.
- Similarly, most of the literature assumes there are sanctions for non-compliance

Literature takeaways (3)

Reframe our model of SETA from..

….a one way transmission of facts

to…

- Focus on a few key priorities
- Identify the learning tasks
- Identify the knowledge gap (surveys, focus groups)
- Look for opportunities to
  - clarify policies, procedures
  - trouble-shoot current processes

Discussion

- Generally, we all probably apply sanctions for things like theft, embezzlement, harassment, plagiarism, etc
- Does your institution prohibit in policy
  - Divulging credentials in reply to a phishing message?
  - Not applying security patches?
- Does your institution apply sanctions for any of these activities?

Discussion

- Conversely, what has been your experience with positive rewards:
  - What about simple rankings by School or Department
    - Fewest compromises as a percentage of hosts managed
    - Lowest rate of response to phishing attacks

Upcoming SETA Plans at Boston College...

History of SETA at BC

Approach used to-date:
intuition
tradition
loosely-defined obj.
cognitive approach

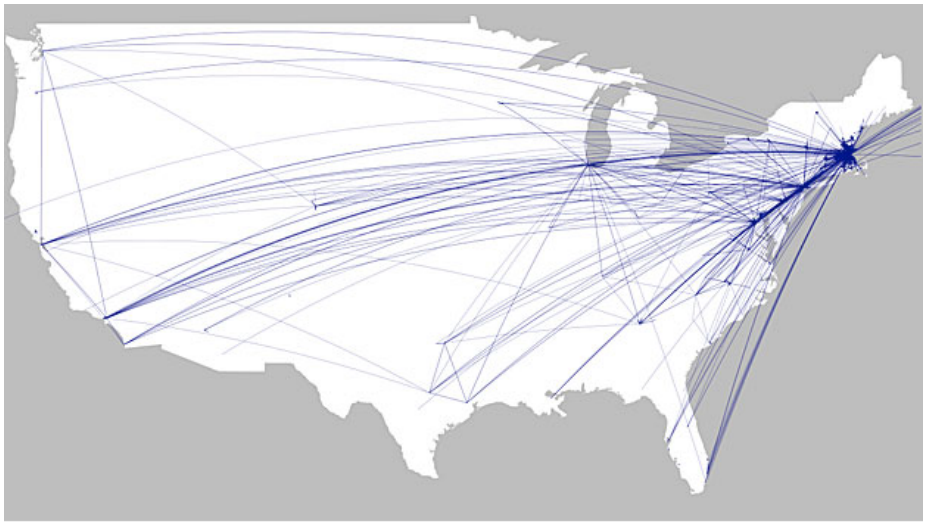
YouTube

Bb
Blackboard

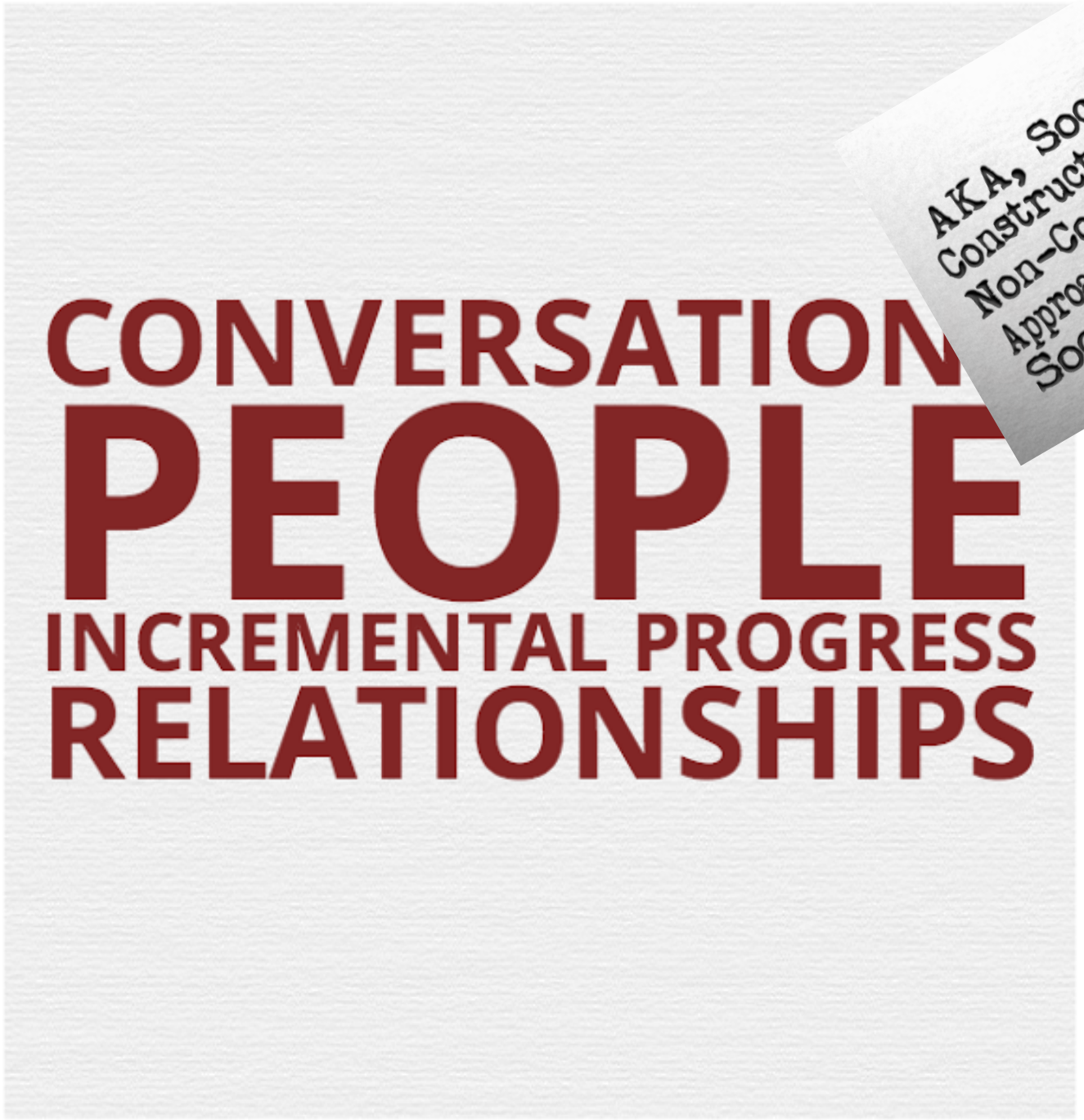
StaySafeOnline.org
Powered by National Cyber Security Alliance

Why is BC taking a more formal approach to SETA now?

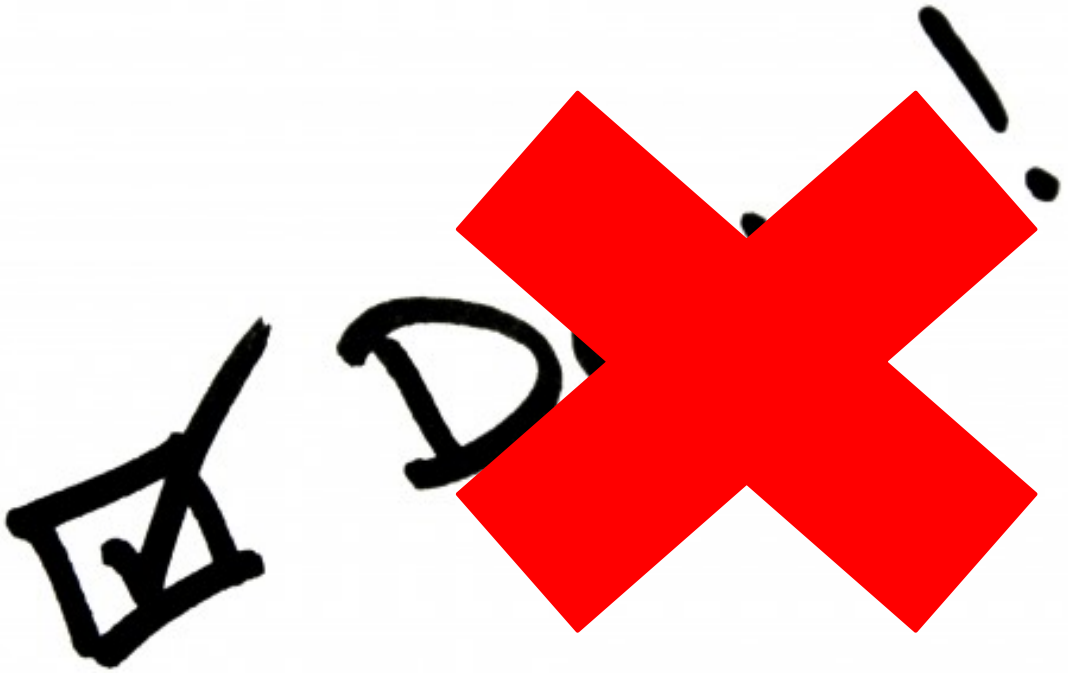
April 22, 1970



- $40 million so far for ALS research.
- Viral Activity - June 1 and August 17.
- 28 million users talking about
- 2.4 million Ice Bucket Challenge videos were shared on Facebook.


CONVERSATION
PEOPLE
INCREMENTAL PROGRESS
RELATIONSHIPS
AKA, Social Constructivism, Non-Cognitive Approach, Effecting Social Norms.
ImageChef.com
UPLOADED AT PINWORDS.COM

We aren’t approaching this effort with any false belief that we will ever have the satisfaction of...



Approach

- Collaboration of ITS Security and ITS Communications and Training.
- Sponsored by ITS Sr. Mgmt.
- Project Management process - Charter, Project plan, etc.
- Per the literature:
  - Clearly defined objectives
  - Non-Cognitive

Goal of the project

Collaborate with a wide range of faculty and staff to create a Security Awareness program framework that will aid in the development of a culture of security at all levels within the BC employee community.


The process is as important as the product.
RECITE
Made with ♥ by recitethis.com

- Started evaluation in 2011
- Students moved summer 2013
- Faculty and staff moved summer 2014
- 280 Google Guides

ITS HOME
Vision, Mission & Values
Strategic Plan
Learning & Teaching
Research
Customer Service
Administrative Applications
Security
Infrastructure
Key Initiatives Timeline
News
Features
Office of the CIO
Departments
Tech Departments @ BC
Technology & Sustainability
Staff Directory
Where To Find Us
Students
Faculty

ITS Strategic Plan

VERSION 1.0, FALL 2013

Information Technology Services is pleased to present Version 1.0 of our strategic plan (PDF) (download Adobe Reader to view PDFs) for information technology in support of the University's mission and goals. The planning process is part of our efforts to align ITS priorities and to optimize our resources in ways that best support the outstanding teaching, learning, research, service, and student formation activities at Boston College.

On behalf of the entire ITS team of dedicated professionals, thank you for your interest and support!

Michael Bourque

Mike Bourque
Vice President, ITS

ITS STRATEGIC PLAN V. 1.0

KEY INITIATIVES TIMELI

APPROACH

The ITS Strategic Plan is focused

1. Learning and Teaching
2. Research
3. Customer Service

- Actively involved 150 members of the University community.
- Two years.

2 Parallel Tracks

Process as Important as Product

1) High-risk groups

- Custom workshops with two “high risk” groups -
  - HR and FVP

2) BC-wide representation (100-200 people) at a workshop aimed at gathering info, sharing info, and designing the SETA framework.

Planned Activities

- Determine invitee list for workshop.
- Design survey related to “what data goes where”
- Nov/December workshop, may include:
  - Interactive survey related to “what data goes where”
  - Group discussion and then wider sharing.
  - Security and C&T share info tying together table talks, and the facts of “what data goes where”, and the challenge of changing behavior.
  - Tables asked to brainstorm how to do educate and change.
  - Wider sharing
- January - April 2015
  - Implement ideas from the Fall workshop - may include web site, use of SANS videos, events, communication, etc.
- May - June 2015 - survey all faculty and staff (?)
- July 2015 - Review lessons learned and prepare for next campaign.

Questions?

Bibliography (1)

SanNicolas-Rocca, 2014

Designing Effective Knowledge Transfer Practices to Improve IS Security Awareness and Compliance, 2014 47th Hawaii International Conference on System Science

Educause/ECAR, 2013

Measuring the Effectiveness of Security Awareness Programs, 2013

Walls (Gartner), 2013

Effective Security Awareness Starts With Defined Objectives, Andrew Walls, Gartner Group, December 10, 2013

Gartner, 2013

User Behavior Can Improve Security, but Only With Development and Practice Gartner Group, December 10, 2013

Karjalainen & Siponen 2011

Toward a New Meta-Theory for Designing Information Systems Security Training, Journal of the Association for Information Systems, August, 2011

Puhakainen & Siponen, 2010

Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study, MIS Quarterly, December 2010

Bibliography (2)

Siponen & Vance, 2010

Neutralization, New Insights Into the Problem of Employee Information Systems Security Policy Violations MIS Quarterly, September 2010

Albrechtsen, 2007

A qualitative study of users' view on information security, Computers & Security, June 2007

Stanton, Stam, Mastrangelo, 2005

Analysis of end user security behaviors, Computers and Security, (24) 2 2005