



Office of the Chief Information Officer

Information Security Outreach: Conversations & Conversions

OHECC 2009

**Thursday
March 26, 2009**



Agenda

- Overview
- Modifying User Behavior
- Technology is [not] the Answer
- Targeted Dialogues
- Designing a Security Communication Plan
- Audiences
- Case Study
- References

Overview

- Different projects under various directors/areas
- Overlap of information security policy, procedure, standards development
- High risk environment with long-term solutions
- 2 Unrelated Security Incidents led to:
 - Consolidation of information security messages
 - Focused project/policy efforts
 - Reduce highest risk areas with short-term & long-term solutions

What We Did

- Motto became “Security is the responsibility of every member of the university”
 - Faculty
 - Staff
 - Technical Staff
 - Students
 - Deans & VPs

What We Did

- Inventoried related information security projects and determined priorities
 - Developed security standards
 - Focused SSN remediation efforts on highest risk areas
 - Purchased encryption technology for distribution by central IT to protect the university
 - “Beefed-up” education and awareness

... Where We're Going

“No plan survives contact with the enemy”

Helmuth von Moltke the Elder

- Deploying user education, training, and awareness
- Developed technical training to be delivered online and through instructor led training - Summer 2009
- Implemented first of four security standards - remaining standards in effect Q2-Q3 2009

Modifying User Behavior

- Make information security relevant to individuals' practices and role at university
 - Shredfest
 - Secwog (Technical Community)
 - Poster Campaigns (Students Faculty & Staff)
 - First Year Experience (Students)
 - Handouts and Special Events (Faculty & Staff)

Technology is [not] the Answer

- Education has the largest impact on liability - consider that most big security problems lately (VA, State of Ohio) had an element of user error involved.
- People need to understand the impact they have on security before removing their responsibility through technology
- Technology should be balanced with user responsibility

Getting the Point Across Through Targeted Dialogues

- Understand how the security message relates to the groups you approach. Consider the following questions:
 - What role does this group play?
 - What information do they handle?
 - What tasks do they perform?

Target your communications to match the audience and you get not only a better impact but better understanding of the people you are protecting

Designing a Security Communication Plan

<DNA Security Tools Portal>							
Project Team Communication Plan							
	Deliverable	Description	Delivery Method	Frequency	Owner	Audience	
1	Reports	Project status report	Regular update on critical project issues	E-mail	Weekly	Shawn	Security project Team
2	Presentations	SECWOG	Presentation of the tool to the security workign group	Meeting	1 time - April 2009	Shawn	Security Working Group
3	Project Announcements	DNA Tools Launch	Message declaring changes/usage availablility of the tools	Listserv	1 time - April 2009	Shawn	Distcons, DNA-Public, DNA-Private
4		CIO Quarterly IT Update	Article describing the crit server inventory process and how it supports ISO implementation	Newsletter	1 time - April 2009	Shawn	Deans/Administrators
5	Documentation	How-To Document	Walkthru/instructions on how to use the web interface to add/edit/modify server requests	Website/PDF	1 time - April 2009	Shawn	DNA/Technical Staff
6							
7							
8							
9							
10							
11							
12							

Designing a Security Communication Plan

- Target the right audience at the right time
 - Too much talk becomes noise to the audience
- Include someone who understands the business process

Designing a Security Communication Plan

- Long-term goals with short-term milestones
 - Example: BuckeyeSecure branding
- Look to public security resources before inventing your own
 - Educause, University Communicators, Federal Govt.

Audiences: Technical vs. Non-technical

- Communicators are not always technically minded
 - Use technical people to talk with technical people or risk losing credibility
- Technical people often can't speak plainly enough for the non-technical audience
 - Choose your approach and speakers carefully or risk being ignored.
- Offer help in translating techspeak

Audiences: Faculty vs. Student



- Faculty: Most see their job as teaching, writing and research. Many don't consider the security implications of that mission.
- Students: They are often uneducated about the impact of personal security. Unfortunately its hard to get and keep their attention.

Case Study: University Computer Security Standards

- Drafted Standards with community input
 - Chose 1 standard to begin process - the broadest applicable standard
- Communicated requirements to technology staff and got Dean/VP support

Case Study: University Computer Security Standards

- Established reporting process involving Administrative and Technical contacts
 - Monthly reporting by participants
 - Reminders/Follow-up
 - Quarterly analysis and progress reports to participants

Case Study: University Computer Security Standards

- Help documents, FAQs and supporting web tools
 - Modified documents quickly to support reporting process

References

- <http://buckeyesecure.osu.edu>
- <http://www.educause.edu/security/>
- <http://www.onguardonline.gov/>

Contact Info

- Shawn Sines, IT Security Outreach Specialist
- sines.22@osu.edu
- Kristina Torres, Communications Manager
– torres.103@osu.edu