Awareness, Training & Education

Comparative Framework			
	Awareness	**Training**	**Education**
Attribute	What	How	Why
Level	Information	Knowledge	Insight
Learning Objective	Recognition & Retention	Skill	Understanding
Example Teaching Method	*Media* -Videos -Newsletters -Posters	*Practical Instruction* -Lecture and/or demo -Case study -Hands-on practice	*Theoretical Instruction* -Seminar and discussion -Reading and study -Research
Test Measure	True/False Multiple Choice (identify learning)	Problem Solving Recognition & Resolution (apply learning)	Essay (interpret learning)
Impact Timeframe	Short-Term	Intermediate	Long-Term

"The Human Factor in Training Strategies" by Dorothea de Zafra, Nov. 1991 as quoted in NIST SP 800-16

Changing Security Culture

1. Understand the current security culture.
2. Get leadership involved.
3. Plan for success.
4. Offer active awareness, training, and education opportunities.
5. Build norms and community.
6. Ensure everyone can answer two questions.
    i. What is normal in my organization?
    ii. What should I do if I detect abnormal activity?
7. Annually review and revise your plan.

Understand the Current Security Culture

- **Type**: academy, baseball team, club, fortress, tough guy/macho, work hard/play hard, bet your company, process?
- **Assumptions, values, norms, and behaviors?**
  - Security is someone else's job.
  - I am too busy to bother with security.
  - It is too complicated to understand.
- **Sense of Community?**

Get Leadership Involved

- Changing organizational security culture is HARD and requires lots of resources.
- If your leadership is not going to set the example and be actively involved, stop now and save everyone a lot of time and effort.

Plan for Success

- Vision
- Values
- Behavior
- Training
- Education
- Community
- Carrots and sticks

Offer Active Awareness, Training, and Education Opportunities

The key word is ACTIVE. You have to actively engage every employee so that they are aware, trained, and educated.

Users remember:

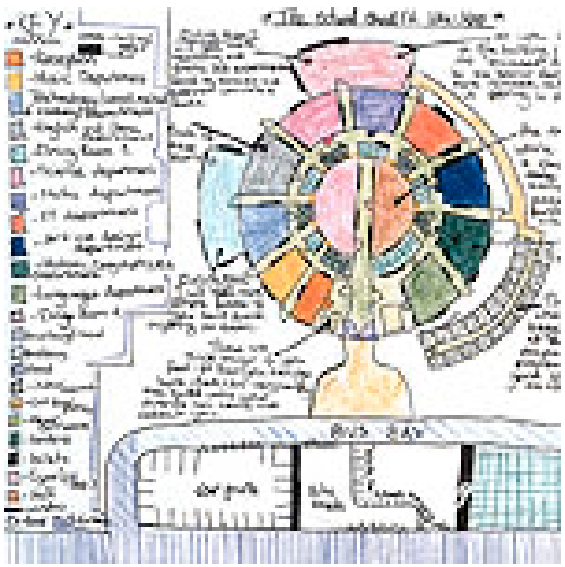
30% of what they hear

40% of what they see and hear

70% of what they do

Build Norms and Community

- Norms are accepted by policy, policy enforcement, and rewards.
- It takes a village to build an employee.

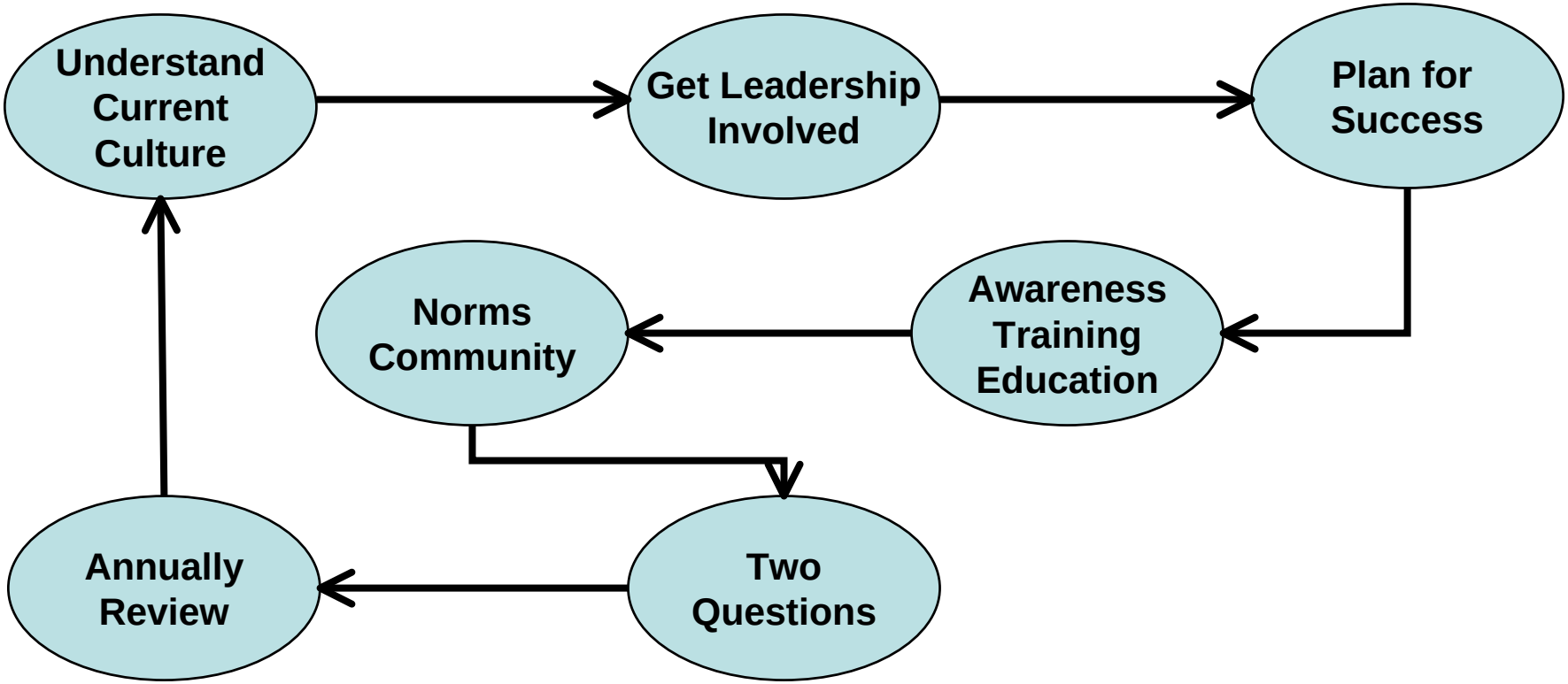


http://www.architectureweek.com/2004/1201/culture_1-1.html

Two Questions

- What is normal for my organization?
- What should I do if I detect abnormal activity?

Annually Review the Plan



West Point Examples

- Cadet Information Security Officers (ISOs)
- Carronade
- CDX
- CERT
- MAADNET

Cadet Information Security Officers

- Empower **students** to administer their companies, fix problems locally, conduct training, conduct exercises, and lead.
- Results
  - Increased notification of outages
  - ISO Empowerment through Active Roles
  - New User Training led by students
  - IT SAMI
  - Carronade Exercise

IT SAMI

IT-SAMI INSPECTION SHEET

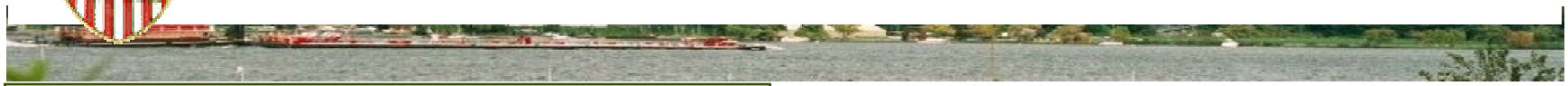
Cadet Name	Company	Year	Inspector Name	
Category				
ITEM		POINTS		
AD-AWARE				
INSTALLED?		NO,		-30
CHECK UPDATES		>= 1 WEEK OLD,	- 05	
		>=3 WEEKS,		-10
		>= 1 MONTH,		- 20
LAST SYSTEM SCAN		>= 1 WEEK OLD,	- 05	
		>=3 WEEKS,		-10
		>= 1 MONTH,		- 20
SCAN RESULTS				
	For each process		-10	
	For every 20 additional items,			-05
DEFRAGEMENT ANALYZE				
SYSTEM SUGGESTED?			YES,	-10
ADD/REMOVE PROGRAM LIST				
WILD TANGENT			YES,	-10
WEATHER BUG			YES,	-10
WELL KNOWN FILE SHARING		YES,	-20/item	
BROWSER HEALTH				
SEARCH BAR OTHER THAN GOOGLE			YES,	-10
VIRUSES				
DEFENITION FILES		>= 1 WEEK OLD,	- 5	
		>=3 WEEKS,		-10
		>= 1 MONTH,		- 20
SYSTEM DATA				
SPACE REMAINING ON C-DRIVE			< 20%,	-10
MAJORITY OF ACDEMIC DATA				
STORED ON C-DRIVE			YES,	-20

4/21/2006 1:15 PM

Best In BDE

Best Regiment:	86.13
Best Company:	95.00
Worst Reg:	75.00
Worst Company:	53.50

Carronade



- Active learning phishing exercise.
- Student controlled, student initiated.
- Four messages
- Leadership and IT infrastructure aware of concept but not deployment date

From: sr1770@usma.edu [mailto:sr1770@usma.edu]
Sent: Tuesday, June 22, 2004 4:57 PM
To: cadet@usma.edu
Subject: Grade Report Problem

There was a problem with your last grade report. You need to:

Select this link Grade Report and follow the instructions to make sure that your information is correct; and report any problems to me.

Robert Melville
COL, USCC
sr1770@usma.edu
Washington Hall, 7th Floor, Room 7206

Carronade Results

	Email Scheme					
	Embedded		Attachment		Sensitive	
Class	**open**	**%**	**open**	**%**	**open**	**%**
Freshmen	82	8%	129	13%	117	12%
Sophomores	70	7%	126	12%	110	11%
Juniors	86	9%	117	12%	115	12%
Seniors	58	6%	114	11%	114	11%
Total	296	29%	486	48%	456	46%
Total sent	1010		1014		999	

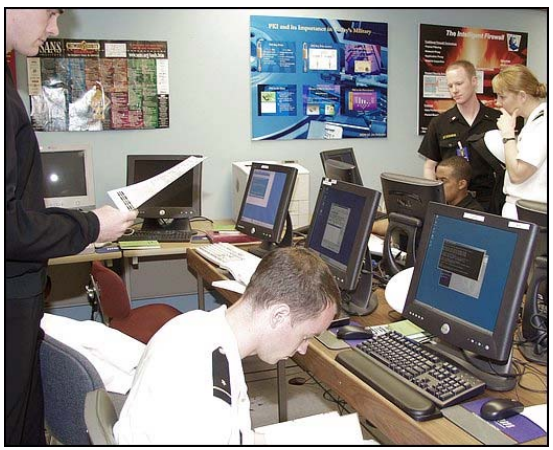
CDX

- Active learning competition between Army, Navy, Air Force, Coast Guard, Merchant Marine, and Air Force Institute of Technology.
- Cadets take onsite pass for the exercise and man the site 24 hours a day.
- NSA attacks through VPN channels. The sites defend and offer a standard suite of services.

CDX

Principal benefit is leadership and education.

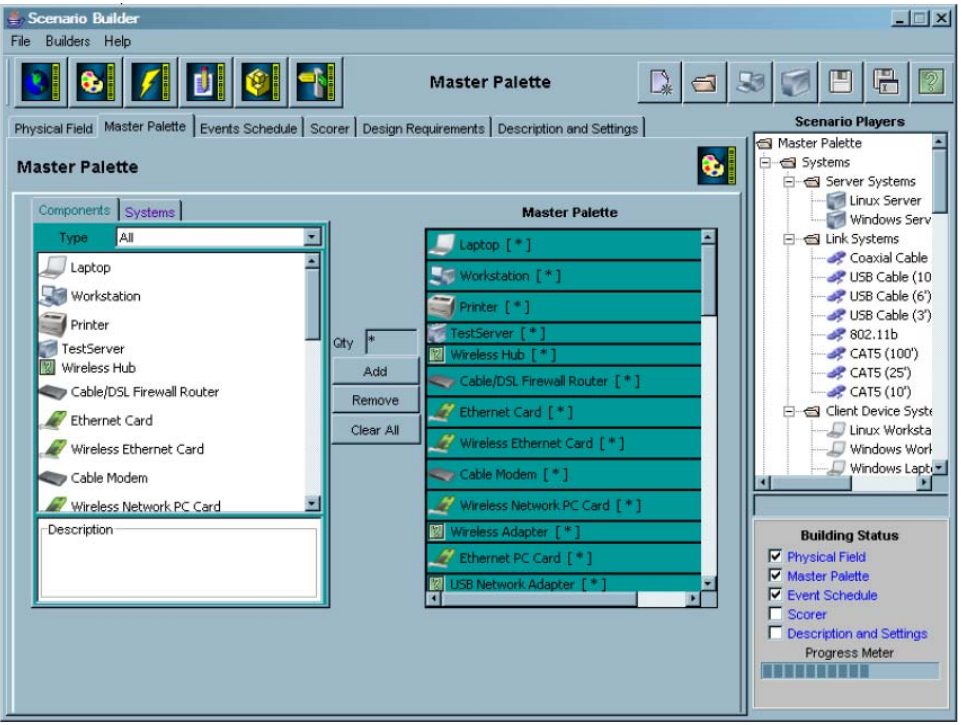
Capt. Allen Harper of the U.S. Marine Corps, a student at the Naval Postgraduate School and head of the blue team, begins analyzing the red team's attack.



CERT

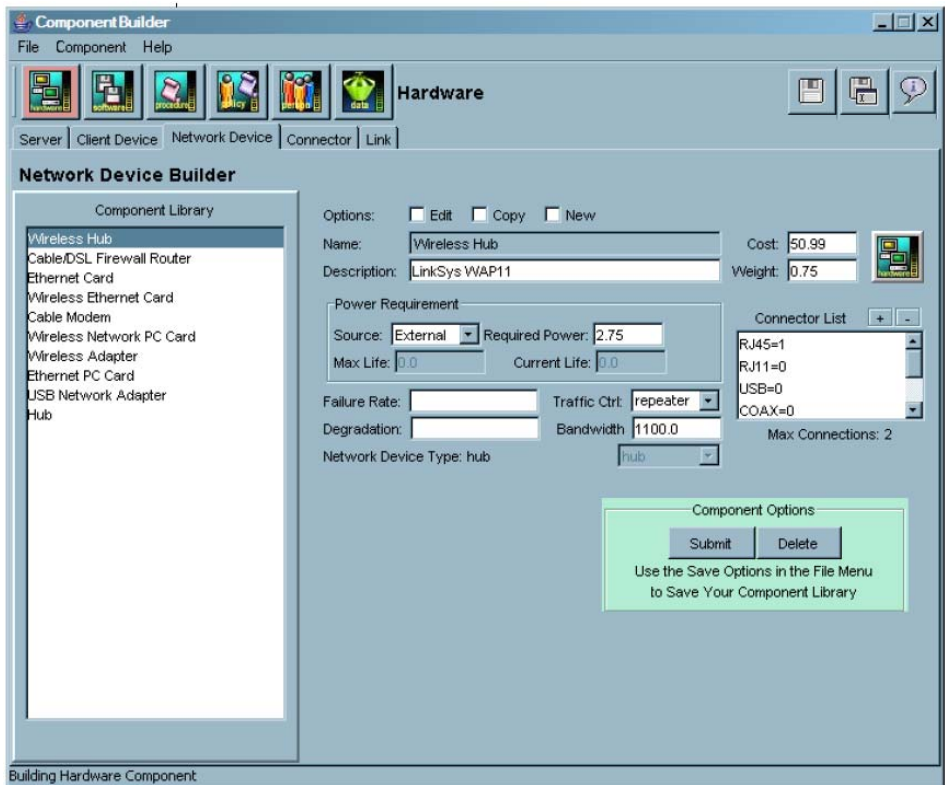
- Computer Emergency Response Team
- Meets weekly (Tuesday 3:30-4:30)
- Open to everyone
- CERT is a component of technical governance.
  - All security policies are staffed through the CERT.
  - Incidents are investigated by the CERT.
  - Vibrant community of practice with vigorous discussion.

MAADNET

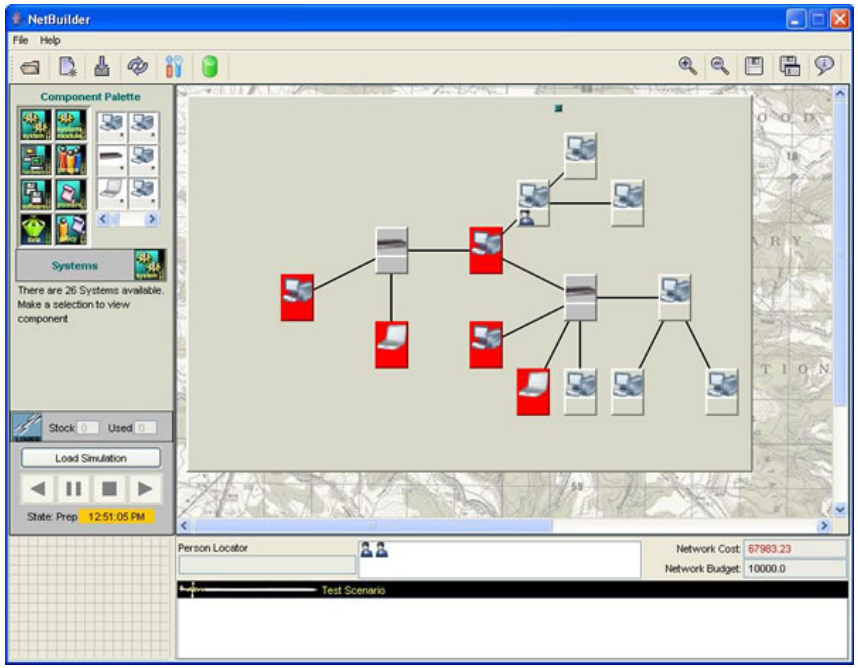


Game that incorporates people, procedures, data, hardware, and software into a realistic simulation.

Build components, systems, Networks, and then scenarios.



MAADNET



MAADNET will support nationwide competitions as teams compete to design the most productive and best defended networks.

USMA Team

- COL Curt Carver
- **LTC Ron Dodge**
- Dr Aaron Ferguson
- LTC John Hill
- Dr John James
- MAJ Fernando Maymi
- COL Dan Ragsdale
- COL Gene Ressler

Thing to Take Away

- The situation is getting worst.
- Perimeter defenses are not working.
- Centralized management is not working.
- Passive approaches to awareness and training are not working.
- Active approaches are necessary to build an **effective organizational security culture**.

Questions, Queries, Comments, A Conversation

Class of 2009 Computing System

- Dell Precision M70 Laptop
  - 15.4” Screen/256MB Video w/PCI-E
  - 2.0 GHz PM(Dothan) CPU
  - 1 GB DDR2 Memory
  - 60 GB 7200 rpm Hard Drive
  - CD-RW/DVD Drive
  - Docking Station
  - WindowsXP, Office 2003
- Iomega External HD
  - 160 GB HD
  - USB 2.0/Firewire
  - Backup Software
- DELL A922 Printer
  - Color Printer
  - Copier/Scanner
- 1GB Thumb Drive