# Awareness, Training & Education

## Comparative Framework

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Awareness</th>
<th>Training</th>
<th>Education</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level</strong></td>
<td>Information</td>
<td>Knowledge</td>
<td>Insight</td>
</tr>
<tr>
<td><strong>Learning Objective</strong></td>
<td>Recognition &amp; Retention</td>
<td>Skill</td>
<td>Understanding</td>
</tr>
<tr>
<td><strong>Example Teaching Method</strong></td>
<td>Media</td>
<td>Practical Instruction</td>
<td>Theoretical Instruction</td>
</tr>
<tr>
<td></td>
<td>-Videos</td>
<td>-Lecture and/or demo</td>
<td>-Seminar and discussion</td>
</tr>
<tr>
<td></td>
<td>-Newsletters</td>
<td>-Case study</td>
<td>-Reading and study</td>
</tr>
<tr>
<td></td>
<td>-Posters</td>
<td>-Hands-on practice</td>
<td>-Research</td>
</tr>
<tr>
<td><strong>Test Measure</strong></td>
<td>True/False</td>
<td>Problem Solving Recognition &amp; Resolution</td>
<td>Essay</td>
</tr>
<tr>
<td></td>
<td>Multiple Choice</td>
<td>(apply learning)</td>
<td>(interpret learning)</td>
</tr>
<tr>
<td><strong>Impact Timeframe</strong></td>
<td>Short-Term</td>
<td>Intermediate</td>
<td>Long-Term</td>
</tr>
</tbody>
</table>

"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.
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.

Two Questions

• What is normal for my organization?

• What should I do if I detect abnormal activity?
Annually Review the Plan

Understand Current Culture

Get Leadership Involved

Plan for Success

Norms Community

Awareness Training Education

Two Questions

Annually Review
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 Inspection Sheet

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD-AWARE</td>
<td>Installed?</td>
<td>-30</td>
</tr>
<tr>
<td></td>
<td>Check Updates</td>
<td>-05</td>
</tr>
<tr>
<td></td>
<td>&gt;= 1 Week Old</td>
<td>-10</td>
</tr>
<tr>
<td></td>
<td>&gt;= 3 Weeks,</td>
<td>-20</td>
</tr>
<tr>
<td></td>
<td>Last System Scan</td>
<td>-05</td>
</tr>
<tr>
<td></td>
<td>&gt;= 1 Week Old</td>
<td>-10</td>
</tr>
<tr>
<td></td>
<td>&gt;= 3 Weeks,</td>
<td>-20</td>
</tr>
<tr>
<td></td>
<td>Scan Results</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For each process</td>
<td>-10</td>
</tr>
<tr>
<td></td>
<td>For every 20 additional items</td>
<td>-05</td>
</tr>
<tr>
<td></td>
<td>Defragment Analyze</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Suggested?</td>
<td>-10</td>
</tr>
<tr>
<td></td>
<td>Add/Remove Program List</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wild Tangent</td>
<td>-10</td>
</tr>
<tr>
<td></td>
<td>Weather Bug</td>
<td>-10</td>
</tr>
<tr>
<td></td>
<td>Well Known File Sharing</td>
<td>-20/item</td>
</tr>
<tr>
<td></td>
<td>Browser Health</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Search Bar Other Than Google</td>
<td>-10</td>
</tr>
<tr>
<td></td>
<td>Viruses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Definition Files</td>
<td>-5</td>
</tr>
<tr>
<td></td>
<td>&gt;= 1 Week Old</td>
<td>-10</td>
</tr>
<tr>
<td></td>
<td>&gt;= 3 Weeks,</td>
<td>-20</td>
</tr>
<tr>
<td></td>
<td>System Data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Space Remaining on C-Drive</td>
<td>-10</td>
</tr>
<tr>
<td></td>
<td>Majority of Academic Data</td>
<td>-10</td>
</tr>
<tr>
<td></td>
<td>Stored on C-Drive</td>
<td>-20</td>
</tr>
</tbody>
</table>

## Best in BDE

- **Best Regiment:** 86.13
- **Best Company:** 95.00
- **Worst Reg:** 75.00
- **Worst Company:** 53.50
• 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

<table>
<thead>
<tr>
<th>Class</th>
<th>Embedded</th>
<th>%</th>
<th>Attachment</th>
<th>%</th>
<th>Sensitive</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freshmen</td>
<td>82</td>
<td>8%</td>
<td>129</td>
<td>13%</td>
<td>117</td>
<td>12%</td>
</tr>
<tr>
<td>Sophomores</td>
<td>70</td>
<td>7%</td>
<td>126</td>
<td>12%</td>
<td>110</td>
<td>11%</td>
</tr>
<tr>
<td>Juniors</td>
<td>86</td>
<td>9%</td>
<td>117</td>
<td>12%</td>
<td>115</td>
<td>12%</td>
</tr>
<tr>
<td>Seniors</td>
<td>58</td>
<td>6%</td>
<td>114</td>
<td>11%</td>
<td>114</td>
<td>11%</td>
</tr>
<tr>
<td>Total</td>
<td>296</td>
<td>29%</td>
<td>486</td>
<td>48%</td>
<td>456</td>
<td>46%</td>
</tr>
<tr>
<td>Total sent</td>
<td>1010</td>
<td></td>
<td>1014</td>
<td></td>
<td>999</td>
<td></td>
</tr>
</tbody>
</table>
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 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

4/21/2006 1:15 PM
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