Strategies for Improving Workers Cyber Security Engagement

- Is there a need?
- What can be done?
This Country "will fall victim to a devastating cyber attack within the next few years"
(National Intelligence Director Mike McConnell , 2010)

“Former intel chief predicts ‘devastating’ cyber attack - FederalTimes.com,”
http://www.federaltimes.com/article/20100224/IT01/2240307/1035/IT01.
http://www.federaltimes.com/article/20100224/IT01/2240307/1035/IT01.
Guidance and examples of leading edge cyber security policy development and deployment strategies

Supported by current research and practice.

A practical formula for policy development. Examples and other resources for agencies are provided that break away from the traditional parochial prevention focused approaches of the past.
Multidimensional Approach

for cyber security policy that incorporates

promotional (positive reinforcement), and

proscriptive / prevention focused means
(including sanctions)
What you get

- Introduction to current thinking and practice in this area and will have
- Tools for assessing, creating and implementing cyber security policy within
- Your organization suitable to their specific environments and needs.
Non Static Policy
Developed by end users & managers
Positive tone
Set Example
Monitor and React
Transparency
Problems: Common Threats

- Viruses
- Spyware
- Trojans
- Zombies
- Damage
- Error
## Problems: Insider Threats

<table>
<thead>
<tr>
<th>Category</th>
<th>Breaches</th>
<th>Breaches</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking/Credit/Financial</td>
<td>4</td>
<td>3.0 %</td>
<td>288</td>
</tr>
<tr>
<td>Business</td>
<td>14</td>
<td>10.5 %</td>
<td>703</td>
</tr>
<tr>
<td>Educational</td>
<td>2</td>
<td>1.5 %</td>
<td>150</td>
</tr>
<tr>
<td>Gov’t/Military</td>
<td>3</td>
<td>2.3 %</td>
<td>80,000</td>
</tr>
<tr>
<td>Medical/Healthcare</td>
<td>1</td>
<td>0.8 %</td>
<td>0</td>
</tr>
<tr>
<td>Insider Theft</td>
<td>24</td>
<td>18.0 %</td>
<td>81,141</td>
</tr>
<tr>
<td><strong>TOTALS</strong></td>
<td>133</td>
<td></td>
<td>1,552,955</td>
</tr>
</tbody>
</table>

2009 Data Breach Insider Threat Category
Solution?

- Monitor everyone & everything
- Implement a Policy

Perhaps – but it a different way
Current literature, Survey & Interviews of:

- Managers
- IT Professionals
- Employees


<table>
<thead>
<tr>
<th>Item</th>
<th>Would Not Do This</th>
<th>Not Sure</th>
<th>Would Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>~ If company implemented a system to track computer activities I would change my settings to prevent this.</td>
<td>14%</td>
<td>38%</td>
<td>48%</td>
</tr>
<tr>
<td>~ If I knew how to change settings to prevent monitoring I would show co-workers how to do so.</td>
<td>24%</td>
<td>37%</td>
<td>39%</td>
</tr>
</tbody>
</table>
Evidence from Survey

- Non Technical Employees & Managers often have **poor grasp of vulnerabilities**
- Are **difficulties communicating** across technical and non-technical boundaries
- **Majority** of insecure actions are honest mistakes from lack of motivation or negligence and **not malicious**
People within organizations are the implementers of cyber and information security practices.
Motivating People to Adopt Information Security Practices

Tools and technology are available which can stop cyber attacks and malicious incidents within agencies and also reduce losses and speed recovery. The greatest failure of these systems lies in the human elements.
Motivating People to Adopt Information Security Practices

Strategies and processes have been identified that improve the human performance and acceptance of security related activities.
Motivating People to Adopt Information Security Practices

This session will highlight the current work in this area so that agencies may implement policies and practices that will more likely be adopted by the people within the organizations. We also identify managerial activities that promote integrity and policy compliance within the workforce.
Behavior is a function of the person and his or her environment

System

People

Technology

Process/Procedures

Environment
Change Processes (Lewin)

Kurt Lewin (founder of Social Psychology, 1890-1947)


**Force field analysis**: provides a framework for looking at factors influencing a situation.

**Driving Forces and Restraining Forces**

**Change Management**: 3 Stage process for humans

Unfreeze – Change – Refreeze
Change Processes (Lewin)

Change Management:

Unfreeze → Change → Refreeze
Motivation and Attention

(Osterloh & Frey)
Organizational Communication & Motivation
Message to be received and understood:

1. Be ready to hear message
2. Have a reason for listening

To have effect must then also:

Garner attention of the individual
People/User perspective

“users appreciate security to the extent that it enhances their productive activities or protects others whom they care about.”

“are people who have to get the basic productive task done.”

“wary of changes that interfere with productivity”
Perception of Importance

Humans – optimistic (Fischhoff, 1978)
Event with beneficial outcome more likely
Event with adverse outcome less likely

Overconfidence Bias (Kruger & Dunning, 1999)
don’t know enough to know you don’t know
Motivation for Security Compliance

“People need a reason to care about security before they will take time to listen to information or warnings about it.”

Organizations that can get employees motivated to pay attention to security will have greater success in getting generating positive security behaviors.
Security and Accountability

Two measures connected with security:

1. monitoring user behavior
2. policy enforcement

Make employees accountable seems to work
Want to avoid excessive control (who’s def?)

“When workers see it as excessive or unfair or when trust is eroded” (still all perspective)

Abrupt changes to policy may cause concern
“Employees take their cues about what is important from managers”

How managers transmit their interests:
1. Not setting example of right behaviors
2. Leave monitoring to IT
3. Monitor employees not management
4. Under fund/under resource training
5. Tell employees to work around controls to get job done if necessary
Organizational Insecurity Cycle

- Perceptions of Risk → Investment in Protection

- Monitoring Capabilities

- Detected Problems

- Investment in Protection

+ Detected Problems

+ Monitoring Capabilities

Least Protection

Organizational Insecurity Cycle

Most Protection

Security or Privacy Failure
Organizational Memory

Knowledge Loss

1.5 % labor force quit/month
4 years – 1/2 gone
6 years – 2/3 gone
10 - ?
Policy - Findings

Few aware of policies
Where they are
Non-existent
Not disseminated
Not enforced
Not updated

= why bother to follow them
IT creates policy and throws it “over the transom” to managers.

Managers create policy and throw it “over the transom” to IT or others.
Trust can substitute for rigid contract in governance of employee behavior.

Low trust ⇔ Rigid & detailed contract & rules

High trust ⇔ Lesser defined rules & regs
Policy - Influence

It is about “right behavior”
It is based on Mission & Values

Most managers did not match policy with view of it as motivational mechanism.
What Works

- Non Static Policy
- Developed by end users & managers
- Positive tone
- Set Example
- Monitor and React
- Transparency
Promoting Positive Security Behaviors

Transparent Security Governance

- Remove Communication Barriers
- Provide Consultative Leadership
- 3D Security Governance: Devise, Document, Dissemination
- Community Based Monitoring and Compliance
- Collective Memory and Librarian
Transparent Security Governance

Remove Communication Barriers

- Specialized knowledge
- Rapid Change
- Jargon

- FIX
  - Get all Speaking Same Language
  - Technology translators – Bridge Tech & Users
    - Train
    - Hire
    - Cross train

(not just technology – contacts & culture)
Transparent Security Governance

Provide Consultative Leadership

- Management, IT & Users – Meet
- Ask them what and how
- Develop Translators
3D Security Governance:
Devise, Document, Dissemination

- Leader - devise policy and charts course
- Constituency – wording, details, structure
  (works best with 2 – IT Savy & User Popular)
- Make it real – write what you mean and enforce it
  Too harsh is not realistic
  If it is ok for some personal use say so.

* Do not allow development to be killed by committee
Community Based Monitoring and Compliance*

- True Transparency
- Publicize:
  What is monitored & By whom & For what. Techniques, Results & Enforcement Outcomes.

*Employees, IT & Management jointly created these for a reason.
Transparent Security Governance

Collective Memory and Librarian

Reinforce/Recognize Positives
Retain learning
Memo
Annual Reports
Newsletter
Wikki or Blog
Conclusion - What Works

- Non Static Policy
- Developed by end users & managers
- Positive tone
- Set Example
- Monitor and React
- Transparency


Web Links

► Cryptography Ban Laws & Map http://rechten.uvt.nl/koops/cryptolaw/
► Federal Trade Commission http://www.ftc.gov/sentinel/
► Information Systems Audit & Control Association http://www.isaca.org/
► Tech Soup – technology info for nonprofits http://www.techsoup.org/
► Syracuse Info Systems Evaluation (SISE) Project Papers http://sise.syr.edu/archive.htm
► SANS Info Sec Reading Room http://www.sans.org/reading_room/

(*you know that the rest of the world has access to this as well….*)