

# New York State Cyber Security Conference 2013

Strategies for  
Improving Workers  
Cyber Security Engagement

Joseph Treglia, PhD  
Syracuse University

School of Information Studies  
Whitman School of Management  
June 2013

INSIDERS  
SCAMS

CYBER CRIMES  
SCADA

MOBILITY

SQL INJECTION  
PHISHING  
TOD

PHISHING  
CREDENTIALS  
STOLEN

# Strategies for Improving Workers Cyber Security Engagement

- ▣ Is there a need ?
- ▣ What can be done ?

# Not IF but WHEN

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)

[http://www.federaltimes.com/article/20100224/IT01/2240307/1035/IT01.](http://www.federaltimes.com/article/20100224/IT01/2240307/1035/IT01)

# This session

- ▣ 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.

# Shortcut - What Works

- ▣ 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

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

**INSIDERS**

To April 1, 2009

133 Breaches

1,552,955 Records



2009 Data Breach Insider Threat Category

ITRC – Identity Theft Resource Center - <http://www.idtheftcenter.org>

# Solution?

- ▣ Monitor everyone & everything
- ▣ Implement a Policy

Perhaps – but it a different way

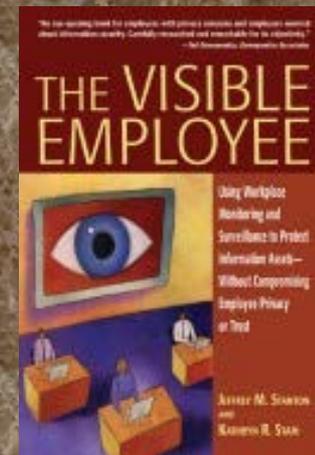
# Study

## Current literature, Survey & Interviews of:

- ▣ Managers
- ▣ IT Professionals
- ▣ Employees

Jeffrey M. Stanton and Kathryn R. Stam, *The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets-Without Compromising Employee Privacy or Trust* (Information Today, Inc., 2006).

S.J. Marcinkowski and J.M. Stanton, "Motivational aspects of information security policies," IEEE, vol. 3, 2003,



# Employee take on monitoring

(Stanton & Stam survey)

Item	Would Not Do This	Not Sure	Would Do This
~ If company implemented a system to track computer activities I would change my settings to prevent this.	14%	38%	48%
~ If I knew how to change settings to prevent monitoring I would show co-workers how to do so.	24%	37%	39%

# 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**

# Motivating People to Adopt Information Security Practices

People within organizations are the implementers of cyber and information security practices.



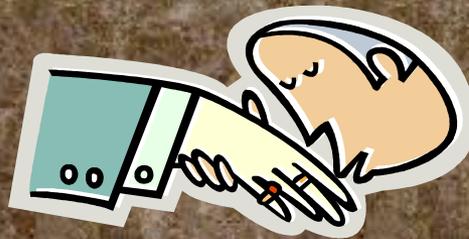
# Motivating People to Adopt Information Security Practices

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.

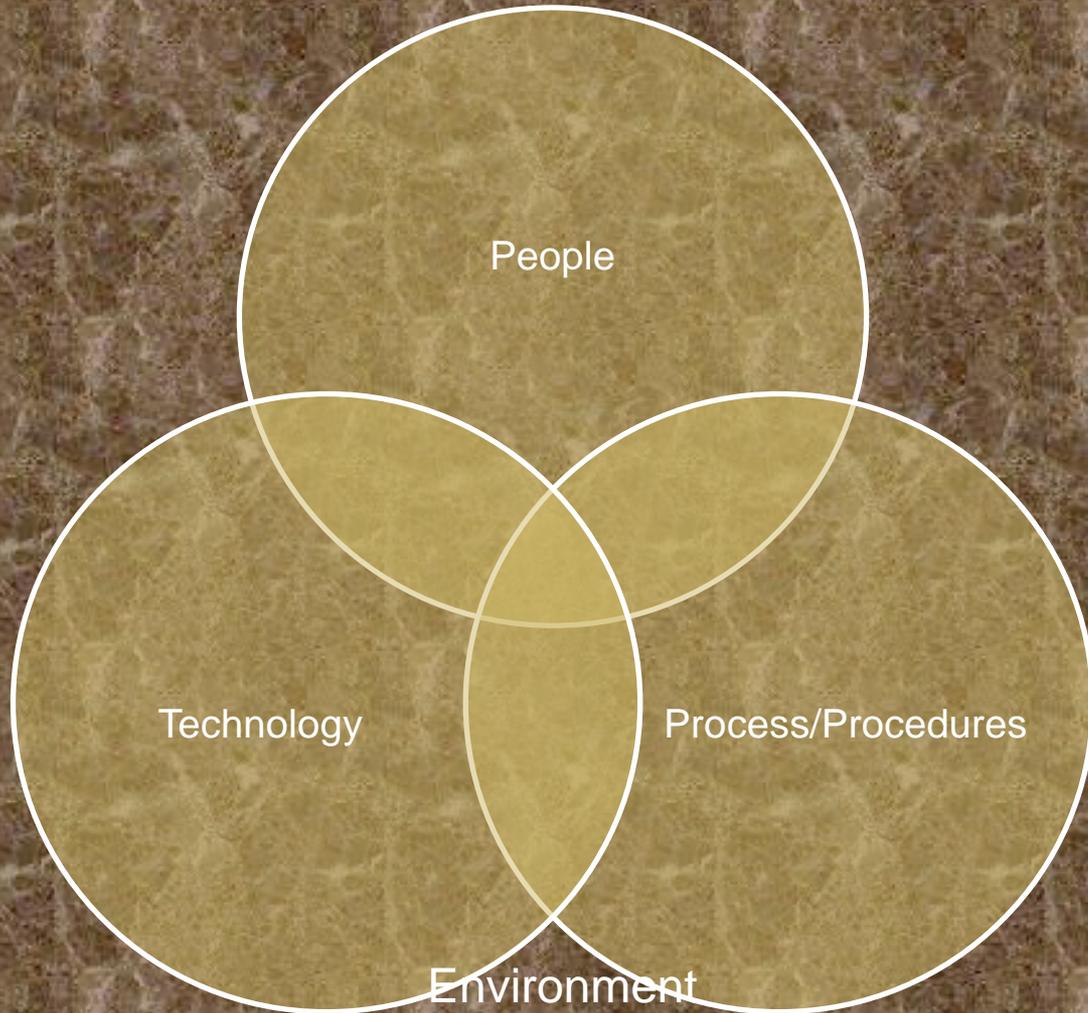


# Change Processes

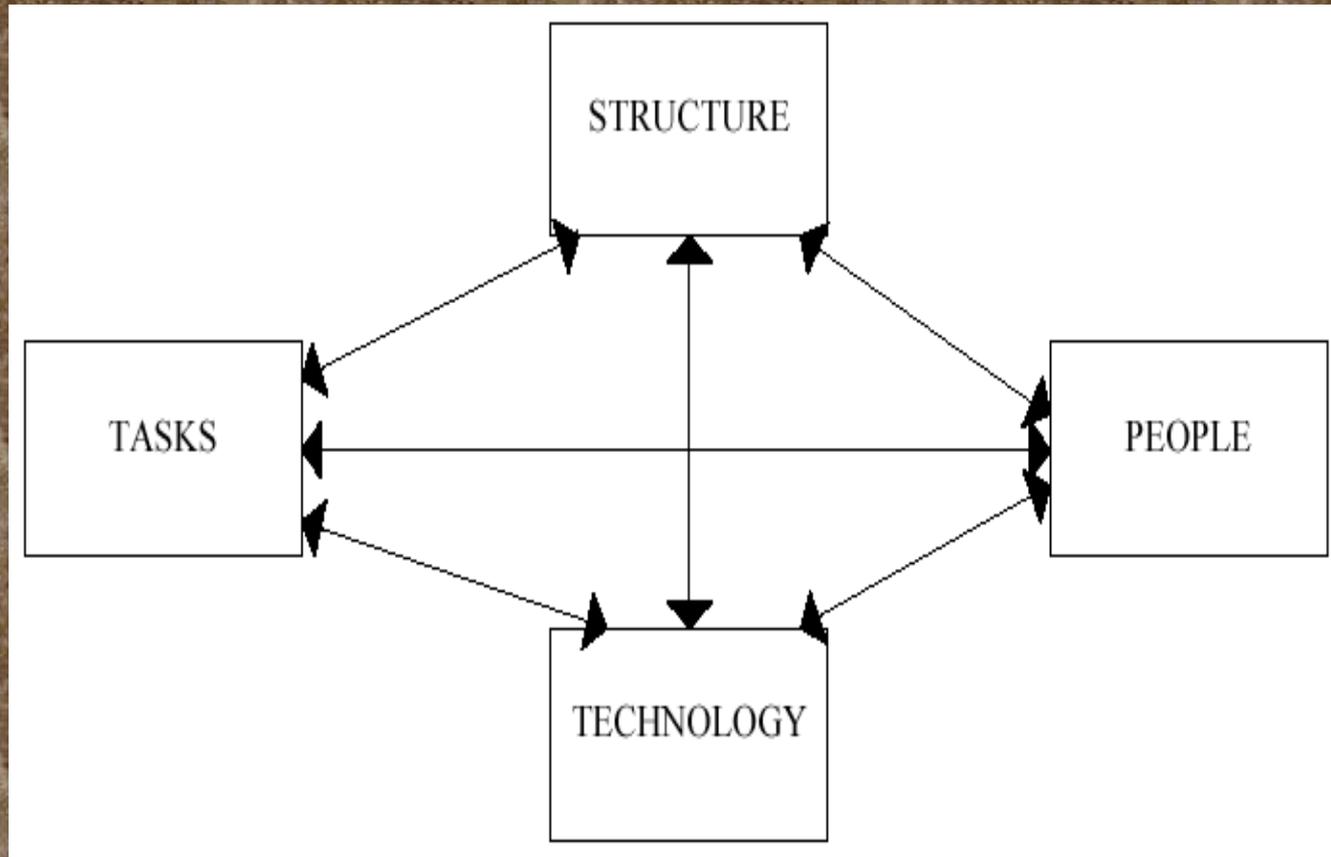
**Behavior is a function of the person and his or her environment**

(Sansone, C.; C. C. Morf, A. T. Panter (2003). *The Sage Handbook of Methods in Social Psychology*. Sage. ISBN 076192535X.)

# System



# Leavitt – “Diamond” model for organizational change



Leavitt, H.J. (1964). Applied organizational change in industry: structural, technical and human approaches

# Change Processes (Lewin)

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

**Leadership Climates: (1) authoritarian, (2) democratic and (3) laissez-faire work environments.** (Miner 2005: 39-40) (Miner, J. B. (2005).

*Organizational Behavior: Behavior 1: Essential Theories of Motivation and Leadership*. Armonk: M.E. Sharpe)

**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





# Monitoring – Employee Perceptions

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



# Cues

“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



# 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

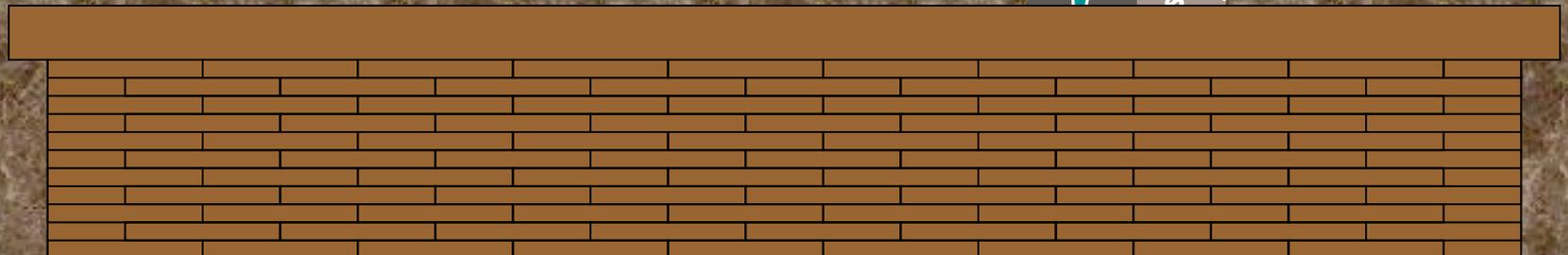


= why bother to follow them

# Policy – “Transom Technique”

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

Trust can substitute for rigid contract in governance of employee behavior

Low trust  $\Leftrightarrow$  Rigid & detailed contract & rules

High trust  $\Leftrightarrow$  Lesser defined rules & regs

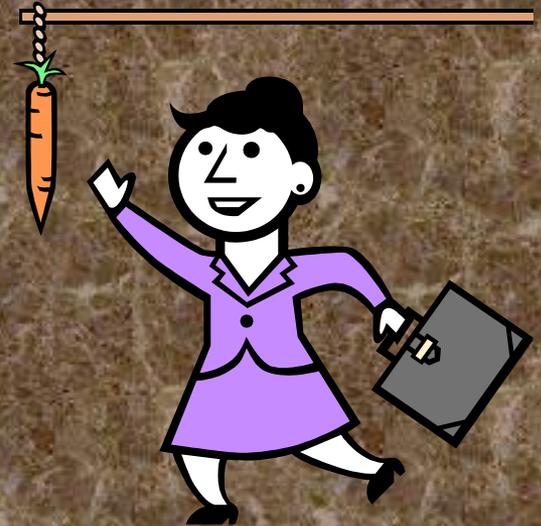


# Policy - Influence

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

# Transparent Security Governance

## 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

# Transparent Security Governance

## 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

# References

- Abawajy, J. (2012). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, (ahead-of-print), 1-12.
- Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29(4), 432-445.
- Berk, V. H., Cybenko, G., Souza, I. G. D., & Murphy, J. P. (2012, January). Managing Malicious Insider Risk through BANDIT. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 2422-2430). IEEE.
- Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach?. *Journal of Management Information Systems*, 29(3), 157-188.
- Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security*, 2010(3), 13-19.
- D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, 20(6), 643-658.
- Tamara Dinev and Quing Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *Journal of the Association for Information Systems* 8, no. 7 (July 2007): 386,22 pgs. Gardner, D., & Macky, K. (2012). Generational Differences: Something Old, Something New. In *Work and Quality of Life* (pp. 417-428). Springer Netherlands.
- Guo, K. H. (2012). Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis. *Computers & Security*.
- Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management*.
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95.
- Kumar, J. A. (2012). AN EFFICIENT AND ROBUST MODEL FOR DATA LEAKAGE DETECTION SYSTEM. *Journal of Global Research in Computer Science*, 3(6), 91-95.
- Labuschagne, W. A., Veerasamy, N., Burke, I., & Eloff, M. M. (2011, August). Design of cyber security awareness game utilizing a social media framework. In *Information Security South Africa (ISSA), 2011* (pp. 1-9). IEEE.
- Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012, May). Exploring game design for cybersecurity training. In *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on* (pp. 256-262). IEEE.
- Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48(7), 296-302.
- Jeffrey M. Stanton and Kathryn R. Stam, *The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets-Without Compromising Employee Privacy or Trust* (Information Today, Inc., 2006).
- S.J. Marcinkowski and J.M. Stanton, "Motivational aspects of information security policies," IEEE, vol. 3, 2003, 2527-2532
- Waly, N., Tassabehji, R., & Kamala, M. (2012). Measures for improving information security management in organisations: the impact of training and awareness programmes.
- Waly, N., Tassabehji, R., & Kamala, M. (2012, June). Improving Organisational Information Security Management: The Impact of Training and Awareness. In *High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICCESS), 2012 IEEE 14th International Conference on* (pp. 1270-1275). IEEE.
- Yang, X., Yue, W. T., & Sia, C. L. (2012). Cognitive Elaboration on Potential Outcomes and Its Effects on Employees' Information Security Policy Compliance Intention-Exploring the Key Antecedents. In *E-Life: Web-Enabled Convergence of Commerce, Work, and Social Life* (pp. 180-194). Springer Berlin Heidelberg.

# Web Links



- ▶ Cryptography Ban Laws & Map <http://rechten.uvt.nl/koops/cryptolaw/>
- ▶ Bureau of Industry & Security US Department of Commerce  
<http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm>
- ▶ Federal Trade Commission <http://www.ftc.gov/sentinel/>
- ▶ Identity Theft Resource Center  
[http://www.idtheftcenter.org/artman2/publish/lib\\_survey/index.shtml](http://www.idtheftcenter.org/artman2/publish/lib_survey/index.shtml)
- ▶ 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/](http://www.sans.org/reading_room/)

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