

# Behavioral Information Security

An Introduction



*Transparent and Pervasive Security*

# Behavioral Information Security

- A new philosophy of Information Security, based on work begun in 2009
- Acknowledgements
  - Janet Wilth, who taught me the difference between IT Security and Information Security
  - Miles Edmundson, whose presentation on Homeostatic Risk Theory got me started
  - Jeff Stanton, who I found by searching for “Behavioral Information Security”

# The Pillars of Information Security



# The Pillars of Information Security

How proficient are we?

- Physical: Excellent. We've been doing it as long as there have been things to steal.
- Technical: Good. We've been doing it as long as there have been computers.
- Policy: OK. Established industry standards (ISO 27000), practices.
- People: Poor. "People are the problem."

# “People are the problem.”

- InfoSec perception of people
  - “You can’t fix stupid.”
  - “People should know better.”
  - CVE-0 (<http://isc.sans.org/diary.html?storyid=10933>)
- Security Awareness Training
  - POSTERS!
  - “Do good things”
  - “Security is everyone’s business”

# InfoSec perception of people

“I have observed in my fieldwork that many IT and infosec professionals have a somewhat rigid and Skinnerian view of human motivation, and this adversely influences the creativity of their ideas about how to get people on board with positive patterns of action.”

- Jeffrey M. Stanton, PhD

# Design is the problem.

- Failure to design for people
  - Classic example: “Why Johnny Can’t Encrypt,” Whitten and Tygar, 1999
  - PGP 5.0 vs. educated professionals: 9-3
  - “...simple to use for those *who already understand the basic models of public key cryptography and digital signature-based trust.*”

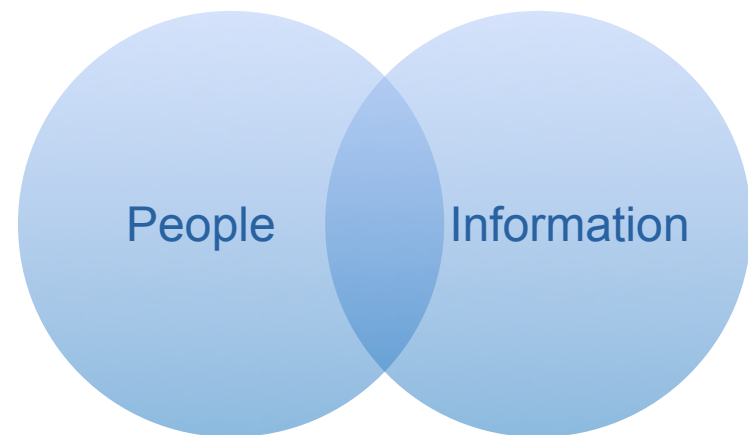
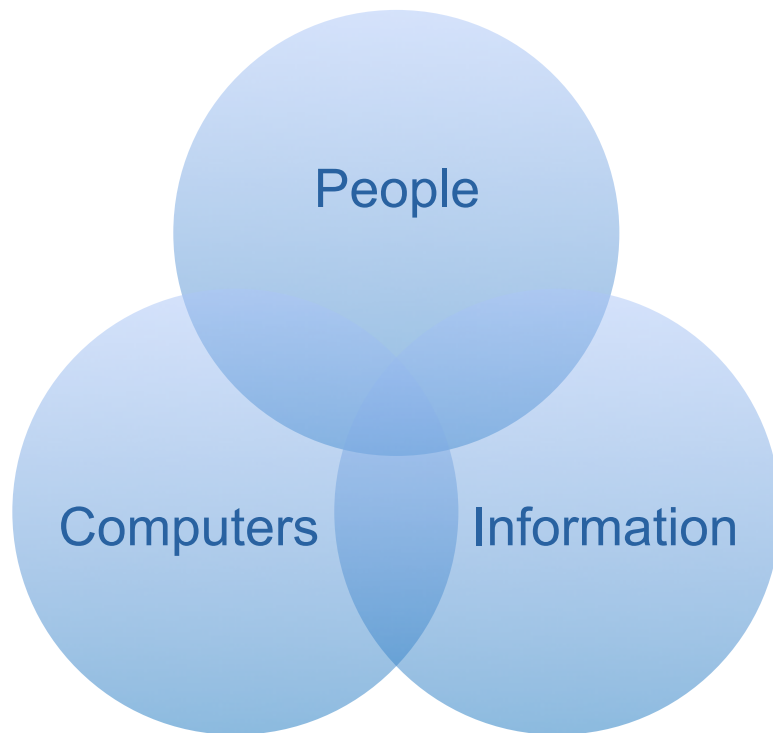
# Our expectations are the problem.

- Everyone can't be a security expert.
  - Cognitive failure: what's obvious to security experts isn't necessarily obvious to someone without the same experience level
  - Training everyone to be experts isn't practical
  - Design systems to account for lack of expertise, taking over security decisions when possible



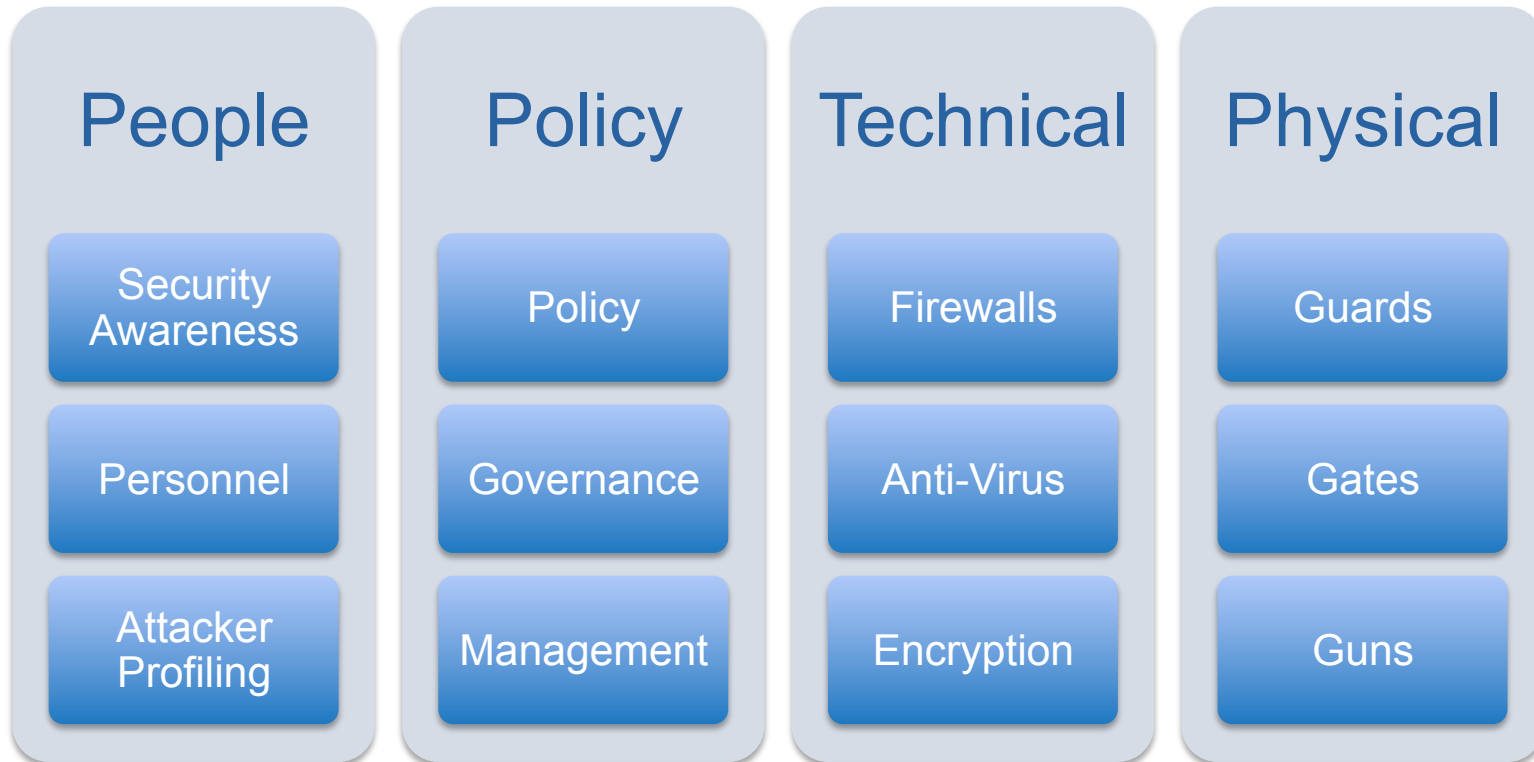
# Well, how did we get here?

- Information Security Started as IT Security
- With change to Information Security, we need to change our focus from technology to people



# Behavioral Information Security

- A philosophical shift, placing people first



# Behavioral Information Security

- From Jeffrey Stanton:
- Defined as:
  - complexes of human action within organizations that influence the availability, confidentiality, and integrity of information systems and resources
- Mindsets and motivations of individuals whose actions have positive and negative influences on information security

# Behavioral Information Security

- My definition:
  - A formal methodology to manage information risk, derived from knowledge of how humans behave and interact with information
- Design and implementation of security architectures and controls based on our understanding of people
  - “Human Interface Design” for InfoSec

# Why BIS?

- Develop new tools for information security
- Address the “people problem”
- Help modernize our profession
- **Reduce cost and improve effectiveness of Information Security**



Don't be too proud of this technological terror you've constructed. The ability to **DROP PACKETS** is insignificant next to the potential of **UNDERSTANDING HUMAN BEHAVIOR.**



# BIS Resources

- Leverage work from other academic and professional disciplines
  - Economics, especially Behavioral Economics
  - Cognitive Psychology
  - Organizational Theory
  - Sociology
  - Information Science
  - Behavioral Profiling (Israeli Security Authority)
  - Human-Computer Interaction

# BIS Resources

- Emerging ideas from others in the field
- Some talks I've attended 2009-2011:
  - Miles Edmundson, “Risk Homeostasis and What it Means for Info Security”
  - Rich Mogull and Mike Rothman, “Putting the Fun in Dysfunctional”
  - Pete Herzog, “Mastering Trust: Hacking People, Networks, Software, and Ideas”
  - Benjamin Tomhave, “Radical Thoughts on Security Reform”
  - Bruce Schneier, “The Dishonest Minority: Security's Role in Modern Society,” others



# BIS Resources

- Academic research and papers on Behavioral Information Security
  - Jeffrey Stanton and Kathryn Stam, “The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets-Without Compromising Employee Privacy or Trust”
  - Jose Gonzalez and Agata Sawicka

# Solutions

...because describing the  
problem is not enough

# A New Perspective

- The philosophical shift from technology to people
- Sometimes, a change in perspective (restating the problem) alone can help
- Case Study: Vulnerability Management

# Vulnerability Management

- Why do vulnerability management programs fail?
  - “Fix all the vulnerabilities!”
  - Buy a scanner...
  - Scan the network...
  - Send out the report...
  - A huge list of things to be fixed...
  - that is promptly ignored.

# Restate the Problem

- What problem is vulnerability management trying to solve?
  - “Keep the bad guys from breaking in”
  - (really, only some kinds of bad guys)
- How do we keep the bad guys out?
  - “Fix the vulnerabilities the bad guys use to break in”
  - Reduces cost without reducing risk reduction
- How do we fix the vulnerabilities?
  - “Find the vulnerabilities, and assign ownership”
  - Social consequences for not fixing them
  - Management reports (it affects my review)
  - Departmental reports (competition - NASA)

# BIS Research Results

- *The Visible Employee*, J Stanton, K Stam
  - 4 years of research (2001-2005)
  - Interviews with employees, managers, and IT professionals about their attitudes towards Information Security
  - Excellent raw data
  - Employee Survey Study
    - Compared to expected InfoSec success
    - Compared to independent external InfoSec audit

# Employee Survey Study

- Security Training and Awareness
  - “My company provides useful training to help employees improve their awareness of computer and information security issues.”
- Positive Security Culture
  - “The culture of my company encourages care and attention to information security issues.”
- Security Self-Efficacy
  - “There’s a lot I can do to keep the information I work with on my computer secure.”

# Employee Survey Study

- **Acceptable Use Policies**
  - “My company consistently enforces an acceptable use policy that governs what employees can and cannot do with their work computers.”
- **Monitoring Awareness**
  - “My company lets workers know how their computer activities are monitored.”
- **Expected Security Outcomes**
  - “My company will probably successfully avoid future problems due to information security breaches.”



# Predictors of Expected Success

- Statistical analysis of survey questions as a predictor of expected security outcomes
  - Survey predicted 64% of expected outcomes
  - Primary predictor: Training and Awareness
  - Secondary predictor: Positive Culture
- Interpretation: Employees with sufficient Security Awareness and Training feel confident in InfoSec success

# Predictors of Audit Success

- Compared survey to independent, expert review of company's security posture
  - Survey predicted 39% of “actual” outcomes
  - Primary predictor: Monitoring Awareness
  - Secondary predictor: Acceptable Use Policy
  - Self-Efficacy and Security Culture were *negatively* correlated with experts' ratings
  - Experts' opinions and employees' opinions were not correlated

# Survey Study Interpretation

- Companies may improve security by:
  - Establishing clear policies governing employee's behaviors affecting security
  - Consistently enforcing those policies
  - Transparently monitoring employee's behavior
- Self-sufficiency (strong culture and efficacy) may create overconfidence in the company's security
  - Negative correlation does not mean culture and efficacy negatively impact security

# Future Directions

- Improved taxonomy of user behaviors
  - Standardize/codify Stanton & Stam research
  - Common language for BIS practitioners
- BIS design principles: (some examples)
  - Restate the problem in terms of people
  - It's usually easier to change technology than change people
  - If you prevent people from doing their jobs, they **WILL** find a way around security

# Future Directions

- Behavioral Security Modeling
  - Describe security requirements using socially defined roles and desired / expected outcomes
  - Done: Presentation on BSM at OWASP AppSec USA 2011 ([appsecusa.org](http://appsecusa.org))
  - Soon: whitepaper on simple Behavioral Security Modeling methodology (*follow @transvasive or visit [transvasive.com](http://transvasive.com) for news on release*)
  - Planned: Training programs for BSM requirements gathering approach

# Future Directions

- BIS Risk Analysis
- Ultimate goal: development of a full BIS methodology
  - Toolkit for a complete security program (people, process, technology) using BIS principles

# Thank You!

Contact Information:

John Benninghoff

[john@transvasive.com](mailto:john@transvasive.com)

<http://transvasive.com/>

Twitter: @transvasive

 **TRANSVASIVE**

*Transparent and Pervasive Security*