

Behavioral Information Security

An Introduction



Copyright © 2011 Transvasive Security. All Rights Reserved.

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
- Technical
- Policy
- People

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
- Security Awareness Training

Perception

“You can’t fix stupid.”

“People should know better.”

CVE-0

(<http://isc.sans.org/diary.html?storyid=10933>)

Awareness

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

Comments on IT/InfoSec views on behavior

Quote from an email exchange between Jeffrey and I regarding use of behavioral information security principles. Having studied psych, and having a warped sense of humor, I find this quite funny.

People are NOT the problem: People fail because of poorly designed systems, not because they're stupid.

Design is the problem.

- “Why Johnny Can’t Encrypt,” Whitten and Tygar, 1999
- “...simple to use for those *who already understand the basic models of public key cryptography and digital signature-based trust.*”

Failure to design for people:

Only 3 of 12 people were able to successfully send a PGP encrypted message.

If you understand how public key crypto and signature based trust work, PGP is a usable system. (Even most security professionals don’t understand this)

We can't expect everyone to
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

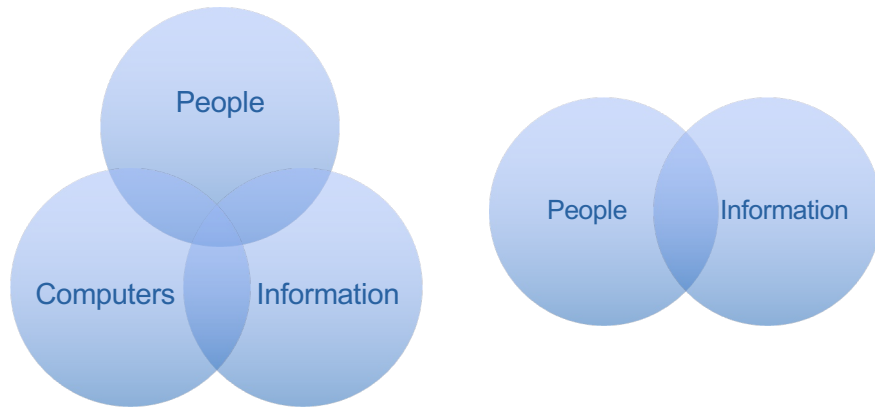
Solution: Design systems to account for lack of expertise, taking over security decisions when possible

A Framework for Reasoning About the Human in the Loop, Cranor, 2008:

With so many security failures attributed to humans, secure systems that do not rely on a "human in the loop" to perform security-critical functions are attractive.

Automated components are generally more accurate and predictable than humans, and automated components don't get tired or bored [14]. Indeed, in some areas we have seen significant progress towards secure systems that "just work" without human intervention. For example, while early anti-virus programs prompted users to make a decision about every detected virus, today many anti-virus programs automatically repair or quarantine infected files in their default mode of operation. Thus, anti-virus software no longer relies on inexperienced users to make security-critical judgments. When software is likely to be able to make a better security decision than a human, removing the human from the loop may be wise. Likewise, when a user is unlikely to have relevant insights into which configuration options to choose, well-chosen default settings may result in better security-configurations than most humans would achieve on their own.

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

Policy, Technical, and Physical flows from our knowledge and understanding of people.

Behavioral Information Security

- Jeffrey Stanton definition:
 - “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

Controlling the FAIR Probability of Action

Why BIS?

- **Reduce cost and improve effectiveness of Information Security**

We can use this to...

Develop new tools for information security

Address the “people problem”

Help modernize our profession

In the beginning there was only one computer, and many people who wanted to use it, so we could effectively dictate rules. We no longer have that leverage.

Solutions

How can BIS help us?

...because describing the problem is not enough

Stanton 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
 - Employee Survey Study
 - Compared to expected InfoSec success
 - Compared to independent external InfoSec audit

Excellent raw data

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

Multiple regression analysis, shows correlation

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

Assumes causation: Negative correlation does not mean culture and efficacy negatively impact security

My Research

- 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

Design principles: “rules of thumb” for a BIS approach to security design

BIS Program Design

- 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?
- How do we keep the bad guys out?
- How do we fix the vulnerabilities?

Problem:

“Keep the bad guys from breaking in”
(really, only some kinds of bad guys)

How to keep them out?

“Fix the vulnerabilities the bad guys use to break in”
Reduces cost without reducing risk reduction

How to fix?

“Find the vulnerabilities, and assign ownership”
Social consequences for not fixing them
Management reports (it affects my review)
Departmental reports (competition - NASA)

Behavioral Security Modeling

- A repeatable method for gathering accurate security requirements
- Done: Presentation on BSM at OWASP AppSec USA 2011 (appsecusa.org)
- Soon: whitepaper on simple Behavioral Security Modeling methodology, releasing at Secure360 (secure360.org)

Planned: Training programs for BSM requirements gathering approach

Modeling security requirements using BIS principles (define security needed in terms of people, expectations, etc.)

Formal BSM Modeling Uses/Extends Secure UML, “SecureUML: A UML-Based Modeling Language for Model-Driven Security,” Torsten Lodderstedt, David Basin, and Jürgen Doser, 2002. (Implementation; covered in forthcoming whitepaper – discussion point)

Future Research

- Improved taxonomy of user behaviors
 - Standardize/codify Stanton & Stam research
 - Common language for BIS practitioners
- BIS Risk Analysis
- Ultimate goal: development of a full BIS methodology

Toolkit for a complete security program (people, process, technology) using BIS principles

Resources: Disciplines

- Economics, especially Behavioral Economics
- Cognitive Psychology
- Organizational Theory
- Sociology
- Information Science
- Behavioral Profiling (Israeli Security Authority)
- Human-Computer Interaction

Leverage work from other academic and professional disciplines

Resources: Talks

- 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

Emerging ideas from others in the field
Some talks I’ve attended 2009-2011

Secure 360 2009, 2010, 2011, SecTor 2010

Resources: Research

- 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

Academic research and papers on Behavioral Information Security

Thank You!

Contact Information:

John Benninghoff

john@transvasive.com

<http://transvasive.com/>

Twitter: @transvasive

