Behavioral Security Modeling

Eliminating Vulnerabilities by Building Predictable Systems

TRANSVASIVE

Transparent and Pervasive Security

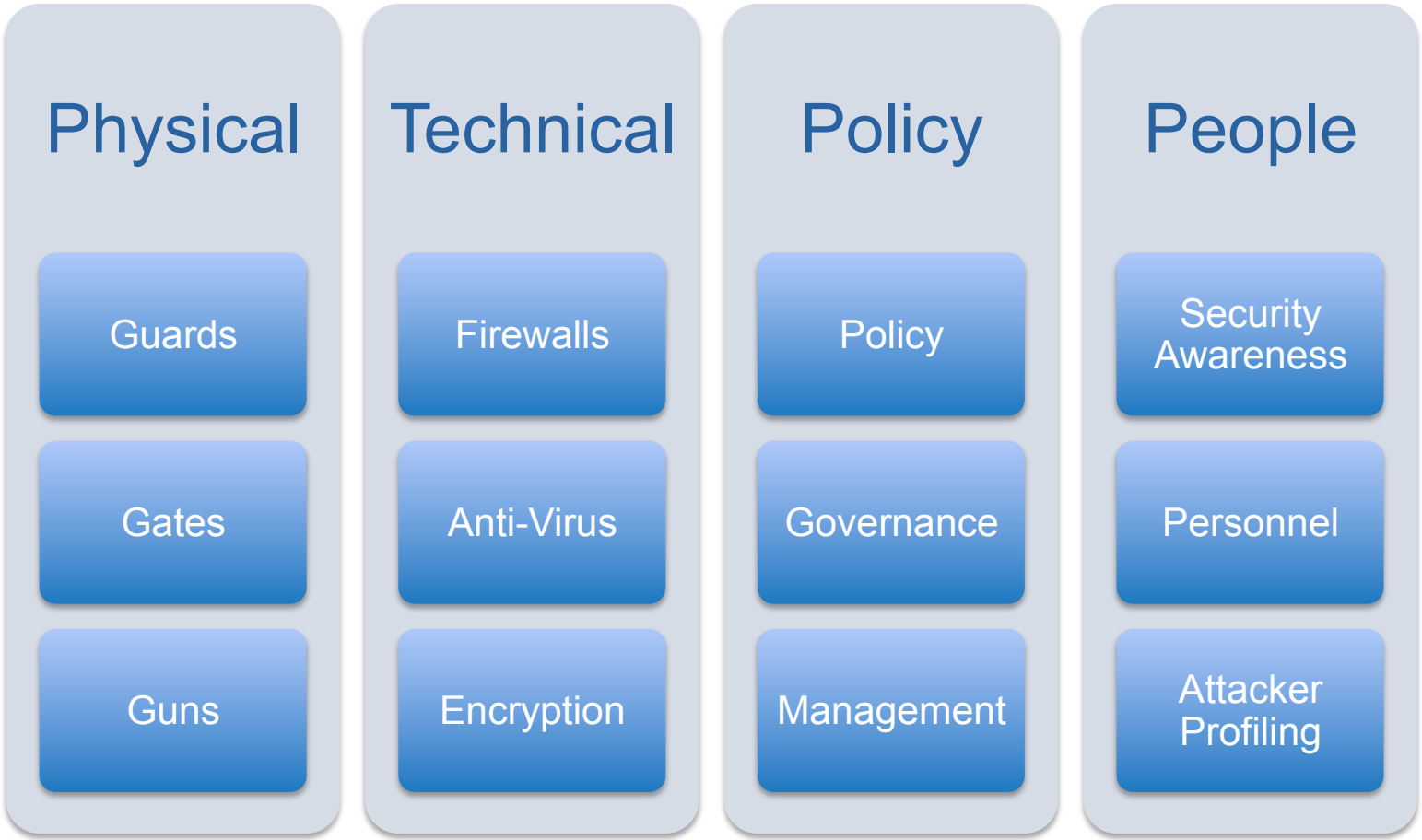
Behavioral Information Security

… the story so far …

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.

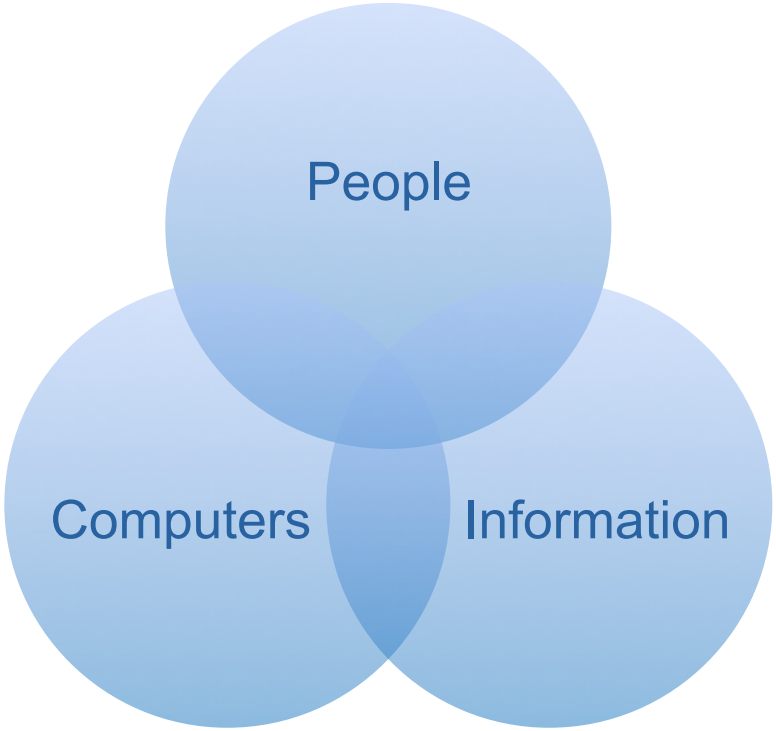
- Failure to design for people
  - Classic example: “Why Johnny Can’t Encrypt,” Whitten and Tygar, 1999
  - PGP 5.0 vs. educated professionals: 9-3
  - “…simple to use for those *who already understand the basic models of public key cryptography and digital signature-based trust.”*

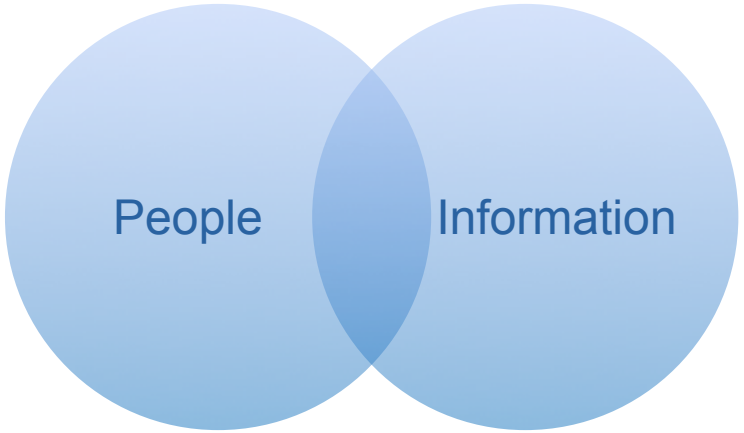
Our expectations are the problem.

- 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?

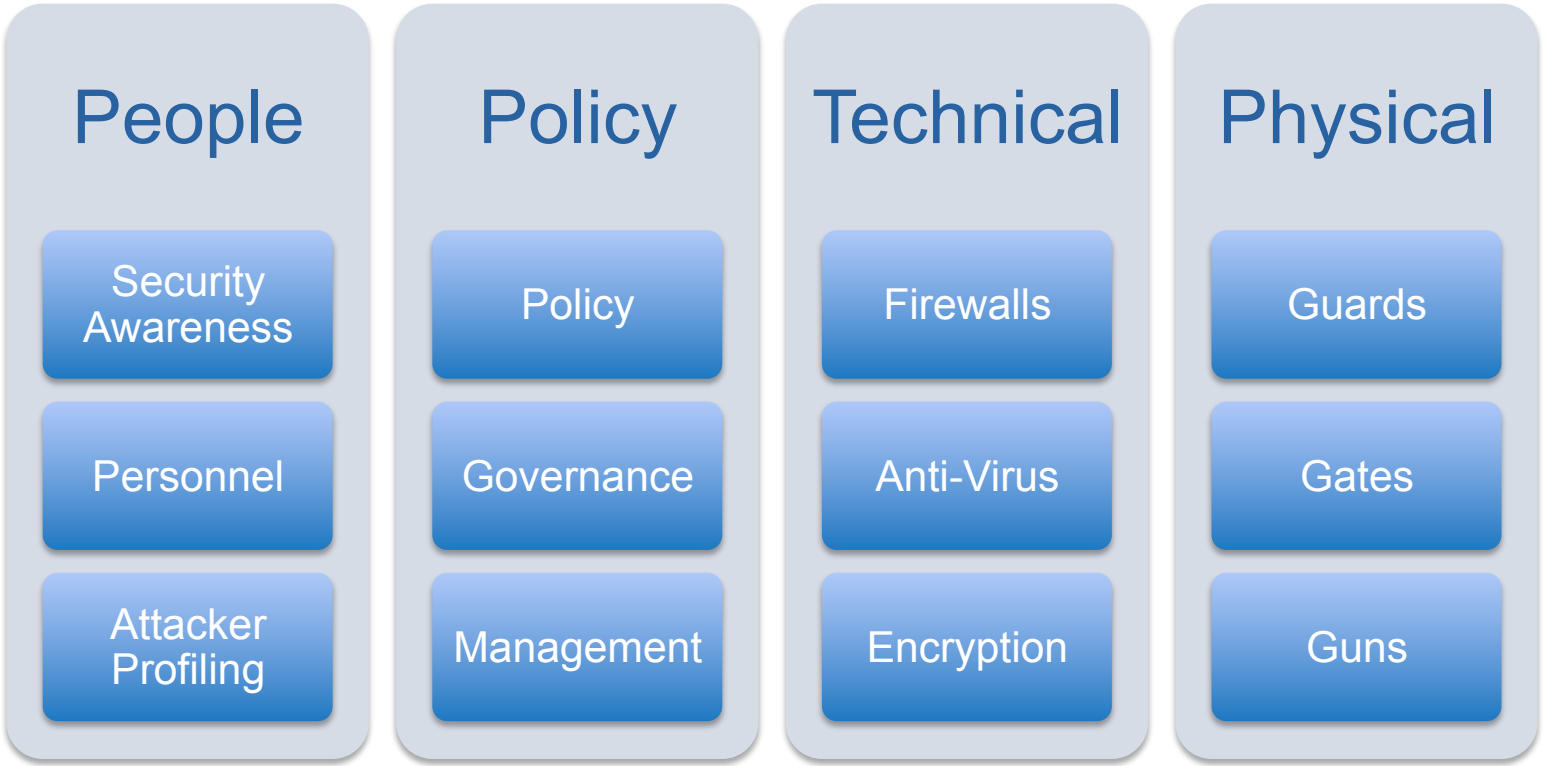
- Information Security Started as IT Security
- With change to Information Security, we need to change our focus from technology to people





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

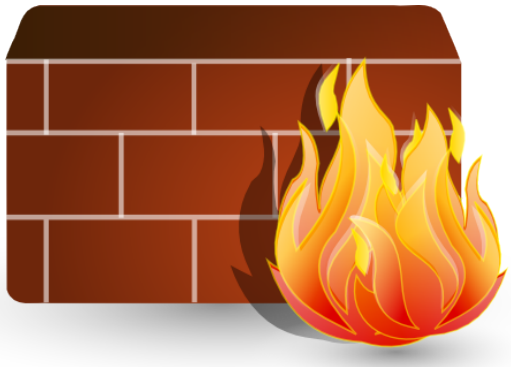
- My definition:
  - A formal methodology to manage information risk, derived from knowledge of how humans behave and interact with information
- Design and implementation of security architectures and controls based on our understanding of people
  - “Human Interface Design” for InfoSec

Why BIS?

- Develop new tools for information security
- Address the “people problem”
- Help modernize our profession

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

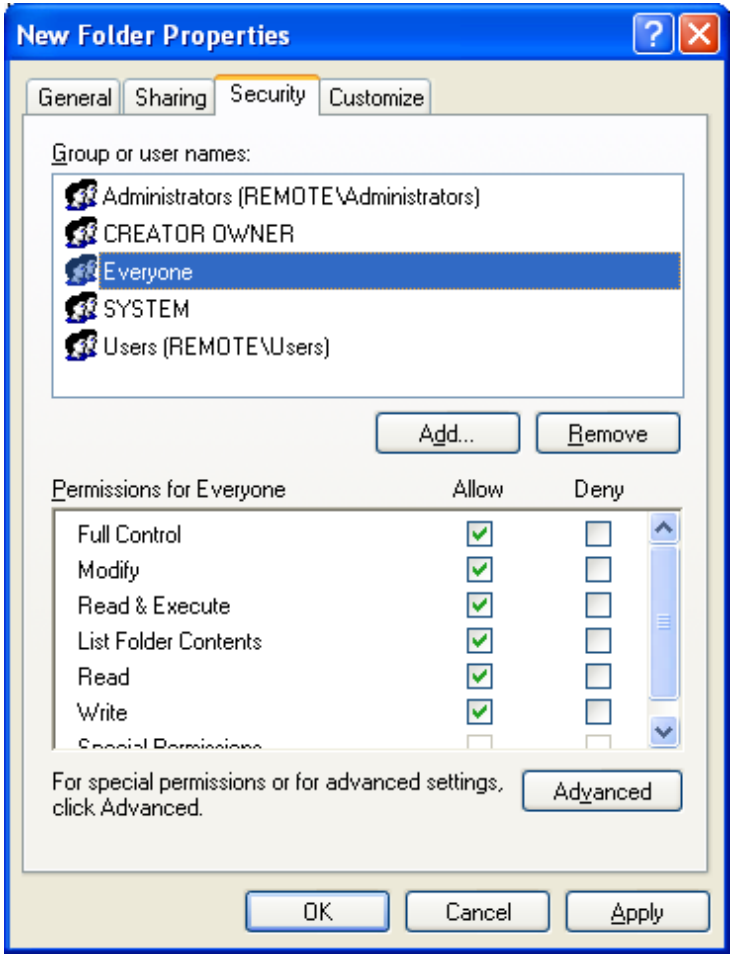
Don't be too proud of this technological terror you've constructed. The ability to DROP PACKETS is insignificant next to the potential of UNDERSTANDING HUMAN BEHAVIOR.



Behavioral Security Modeling

a method for describing security requirements using BIS principles

Everyone



"I just set up this new folder, and want to give everyone access"

Everyone…

- on my team?
- in IT?
- in the company?
- who is able to access this directory, even anonymously?

The “Everyone” Problem

- Desired (intended) outcome:
  I authorize all IT employees and contractors to view (read) the contents of my folder.
- Actual outcome:
  I authorize all employees, contractors, vendors, partners, anyone with an account.
- Difference between intended and actual outcomes introduces a vulnerability; employees outside IT, vendors and partners have unauthorized access to my folder.

Behavioral Security Modeling

- Standard methodology for describing desired / intended outcome
- Useful to describe user intent
- Useful to describe system functionality
- Allows analysis to identify gaps between intent and functionality = vulnerabilities

Behavioral Security Modeling

- Improves precision of security requirements to prevent introduction of vulnerabilities in the first place by building systems that behave as people expect (predictable)

Components

- Actors (People)
  - Individuals (Roles, Specific People)
  - Groups (Social Groups within Organization)
- Objects (Information)
- Actions
  - Functional Actions
    - Simple Actions (Read, Write)
    - Complex Actions (Purchase Book, Create Account, etc.)
  - Security Actions (Identify, Authenticate, Authorize, Delegate, etc.)

Components

- Constraints (Limitations)
  - Time (Business Hours)
  - Location (In Office)
- Hidden Constraints
  - Implied, assumed, or unstated constraints
  - “Give access to Bob in Accounting (only as long as he’s working here, and it’s appropriate for his job)”

Scenario 1: SharePoint

“I want everyone working for my company to have access to my SharePoint site.”

- Actor: Me (Site Owner)
- Actor: All employees and contractors
- Security Action: Authorize [Functional Action]
- Functional Action: Read
- Object: My SharePoint site
- Constraints: Only at work (or when using VPN)
- Hidden Constrains: Only for current employees and contractors

Scenario 1: SharePoint

How do I set this up?

“Hmm. Why don’t I just use this ‘authenticated users’ group, that will include everyone!”

Gap: Authenticated Users includes more people than “all employees and contractors”

Possible Fix: Present a list of organizationally appropriate groups

What group would you like to be able to view the site?

- My team
- My department
- All employees
- All employees and contractors
- *All employees, contractors, vendors, and partners*

Scenario 2: SharePoint II

Alice, a marketing employee I'm working with on a six month project requests access to my site.

- Actor: Me (Site Owner)
- Actor: Alice (specific person)
- Security Action: Authorize [Functional Action]
- Functional Action: Read
- Object: My SharePoint site
- Constraints: Only at work (or when using VPN)
- Hidden Constraints: Only for duration of the project, only if Alice is still an employee, and in her current position.

Scenario 2: SharePoint II

What happens?

SharePoint sends me an email and I click on "give Alice read access." (not what I really want)

Gap: No time limit placed on access.

Possible Fix: Present a list of options for time limited access.

How long would you like Alice to have access?

- For x months (pick a value 1-12)
- *Indefinitely (as long as Alice is in her current position)*
- *Indefinitely (as long as Alice is employed)*

Credit Card Payments

- Customer
  - Person/Group buying a product
- Merchant
  - Person/Group selling a product
- Processor
  - Person/Group clearing the payment

Credit Card Payments

- Customer:
  - Authorizes Merchant to take $149 in exchange for an iPod nano.
  - Provides *authorization token*: card number, expiration, name, address, phone, verification code (CVV2)

Detour: Security Tokens

- Security tokens (as used here) are bundles of information used to implement a security action in information systems
- Customer authorizes payment
- Token contains all data needed to confirm customer authorization
- Identification tokens (i.e. username)
- Authentication tokens (i.e. password)

Customer Model

- Actor: Customer
- Actor: Merchant
- Security Action: Authorize
- Functional Action: Receive payment
- Object: Customer’s account
- Constraints: $149, one transaction only, between Customer and Merchant
- Token: Card number + authorization data

Credit Card Payments

- Merchant:
  - Receives authorization token
  - Delegates transfer of $149 to Processor
  - Stores card number (as identification token) for marketing purposes
  - Provides authorization token to Processor
  - … and ships the product, of course.

Merchant Model (1)

- Actor: Merchant
- Actor: Processor
- Security Action: Delegate
- Functional Action: Transfer payment
- Object: Customer, Merchant accounts
- Constraints: $149, one transaction only, between Customer and Merchant
- Token: Card number + authorization data

Merchant Model (2)

- Actor: Merchant
- Actor: Customer
- Security Action: Identify
- Functional Action: Store object
- Object: Card number (token), transaction details
- Constraints: None
- Token: Card number

Credit Card Payments

- Processor:
  - Receives authentication token
  - Verifies authorization with Customer's bank
  - Transfers $149 from Customer to Merchant
  - *…and takes a $3 cut*
  - *…and pays Visa, of course.*

Gaps

- Authorization Token not constrained to fixed amount or to a specific transaction; (constraints not implemented) leaving token vulnerable to theft
- Merchant's identification token contains authorization data (re-use/misuse of security token) making token valuable and vulnerable to theft

Fixing Credit Cards

- Customer: Doesn’t really care, misuse (fraudulent charges) costs them nothing.
- Processor: Not discussed today, but one solution is to push for one-time-use card numbers, tied to a single transaction.
- Merchant: How can I constrain the authorization token for payment, and also use it as an identifier?

Payment Solutions

Typical Payment Gateway (Tokenization)

- Merchant sends authorization to Gateway OR Gateway gets authorization directly from Customer
- Gateway stores authorization returns a number (token) usable for remainder of transaction
- One-Time tokens or Multi-Use tokens

Payment Solutions

Payment Gateway (Tokenization)

- One-Time Tokens
  - Satisfies constraints … maybe
  - YES: One transaction only
  - YES: Between Customer and Merchant
  - Maybe: $149 (depends on implementation)
  - Doesn’t meet Merchant need to store identification token

Payment Solutions

Payment Gateway (Tokenization)

- Multi-Use Tokens
  - Partially satisfies constraints
  - No: One transaction only
  - YES: Between Customer and Merchant
  - No: $149
  - Meets Merchant need to store identification token

Payment Solutions

Payment Gateway (Tokenization)

- Gap: constraints not fully met
- Gap: identification number (usually) same as authorization number
- No known solution currently available that meets all requirements

Possible Solution

Model suggests a potential solution:

- Generate *two* tokens: one for authorization, one for identification
- One-time use authorization token (kept in payment system)
- Unique identification token (not valid for payment; non-reversible)

Possible Solution

- Two-Token Solution
  - Fully satisfies constraints
  - YES: One transaction only
  - YES: Between Customer and Merchant
  - YES: $149 (assume proper implementation)
  - Meets Merchant need to store identification

Behavioral Security Modeling

- A people-centric method for describing security requirements or implementations
- Removes ambiguity of social groups, makes unstated constraints explicit
- Allows us to build better systems using more precise security requirements
- Systems behave as expected = fewer vulnerabilities = better security

Future Directions - BSM

- Behavioral Security Modeling
  - Soon: whitepaper on simple Behavioral Security Modeling methodology *(follow @transvasive or visit transvasive.com for news on release)*
  - Expand, refine catalog of available actors, security/functional actions, constraints
  - Training programs for BSM requirements gathering approach
  - UML modeling template (based on Secure UML) for formal BSM modeling

Future Directions - BIS

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

Resources/References

- Some talks I've attended 2009-2011:
  - Miles Edumundson,"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

Resources/References

- 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,” others
  - Jose Gonzalez and Agata Sawicka

Thank You!

Contact Information:

John Benninghoff

john@transvasive.com

http://transvasive.com/

Twitter: @transvasive

TRANSVASIVE

Transparent and Pervasive Security