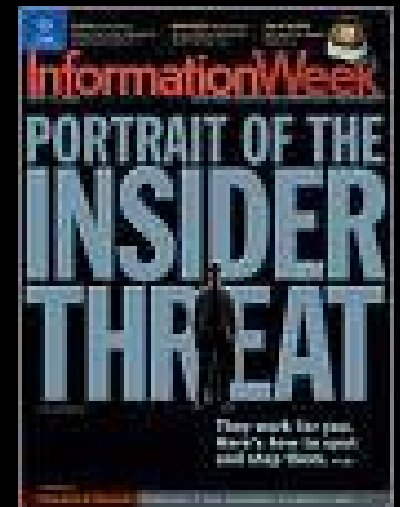




INFRASTRUCTURE, SAFETY,  
AND ENVIRONMENT

# *Insiders Behaving Badly*

Shari Lawrence Pfleeger  
RAND Corporation  
pfleeger@rand.org



# How Can We Tell When Something's Not Right?



# Project Partners



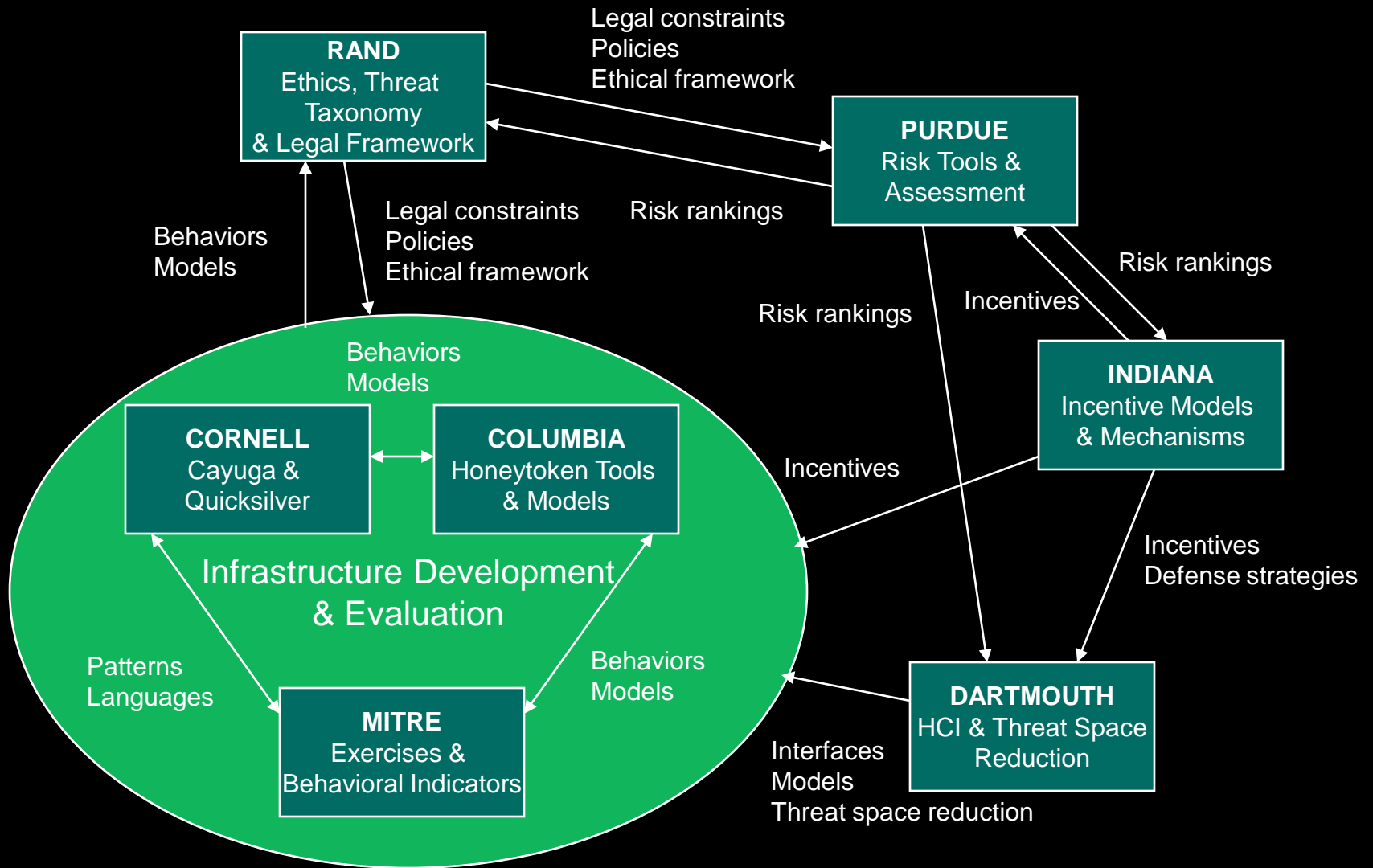
# ***Project Funding & Stakeholders***

- **The project is a 24+ month, \$3+ million effort by a seven-institution multidisciplinary team.**
- **Project duration: 1 April 2007 to 31 July 2009**
- **Stakeholders include industry, government, and the research community.**
- **Information, presentations, and publications can be found at [www.thei3p.org](http://www.thei3p.org).**

# *Two Thrusts*

- **Technology Exploration**
  - How can technology help us recognize and understand insider behavior?
  - How can technology prevent or mitigate inappropriate insider behavior?
- **Environmental Constraints**
  - What incentives can keep insiders from performing inappropriate actions?
  - How can authorizations and user interfaces be improved to encourage secure behaviors?
  - What are the legal and ethical constraints on implementing proposed technologies? How can they influence incentives and policy choices?
  - How do we quantify and manage the risk of inappropriate insider behavior?

# Collaboration



# ***Strong Project Focus on Nature of Problem***

- **MITRE looked at motivation, typical action with volunteers**
- **Dartmouth characterizing threat to be able to reduce it**
- **Columbia and Cornell examined actions with real-life situations**
- **Indiana looking at student behaviors**
- **Purdue identified and characterizing risks**
- **RAND defined insider threat and created taxonomy**

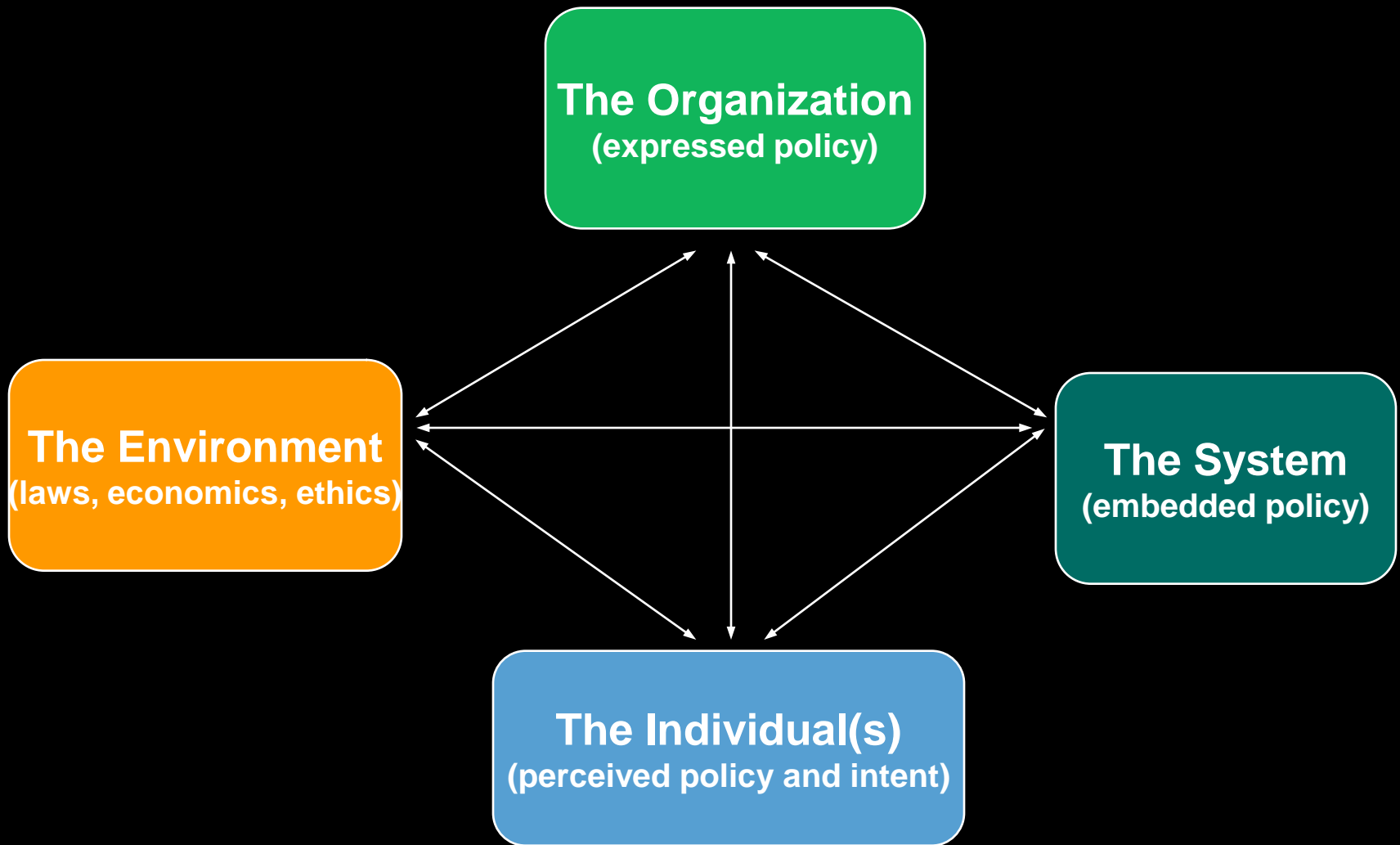
# ***Three-Plus-One Workshops***

- **11-12 June 2007 in Washington, DC**
  - **Invited stakeholders, including financial sector, government, academics**
  - **Listened to stakeholder experiences with insider actions**
- **15-16 April 2008 in Durham, North Carolina**
  - **Engaged industry to focus on economic impacts of insider actions, plus legal constraints and taxonomy of insiders/actions**
- **20-25 July 2008 at Schloss Dagstuhl, Germany**
  - **Some team members in week-long discussion of insider threat research**
- **4-5 May 2009 in Washington, DC**
  - **Reported findings to stakeholders, policy-makers, others**
- **Plus face to face meetings and periodic teleconferences**
- **Special issue of *IEEE Security & Privacy* on insider threat (Nov/Dec 09)**

# *Five Perspectives on Insiders and Their Behavior*

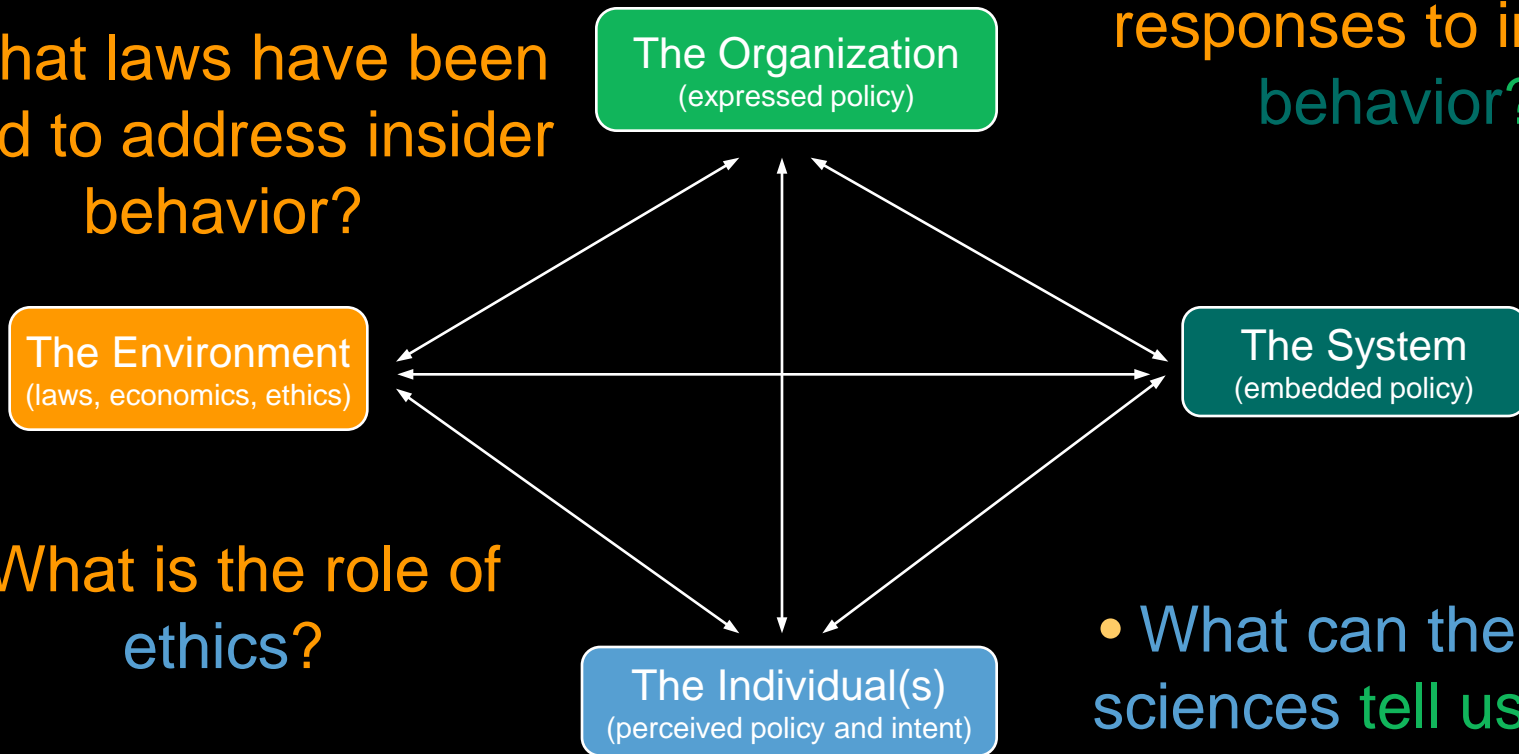
- **Who are “insiders” and what kinds of behaviors do we care about?**
  - Led to insider taxonomy
- **What can we learn from those who study human behavior?**
  - Leading to research agenda WRT behavioral decision theory
- **What is the role of ethics?**
  - Led to guidelines for research on insiders
- **What are appropriate responses to unwelcome insider behaviors?**
  - Leading to framework for response space
- **What is the role of the law?**
  - Led to preliminary database of legal actions against insiders

# *A Taxonomy of Insiders and Their Actions*



# Mapping Onto Taxonomy of Insiders

- What laws have been used to address insider behavior?



- What are appropriate responses to insider behavior?

- What is the role of ethics?

- What can the social sciences tell us about appropriate responses?

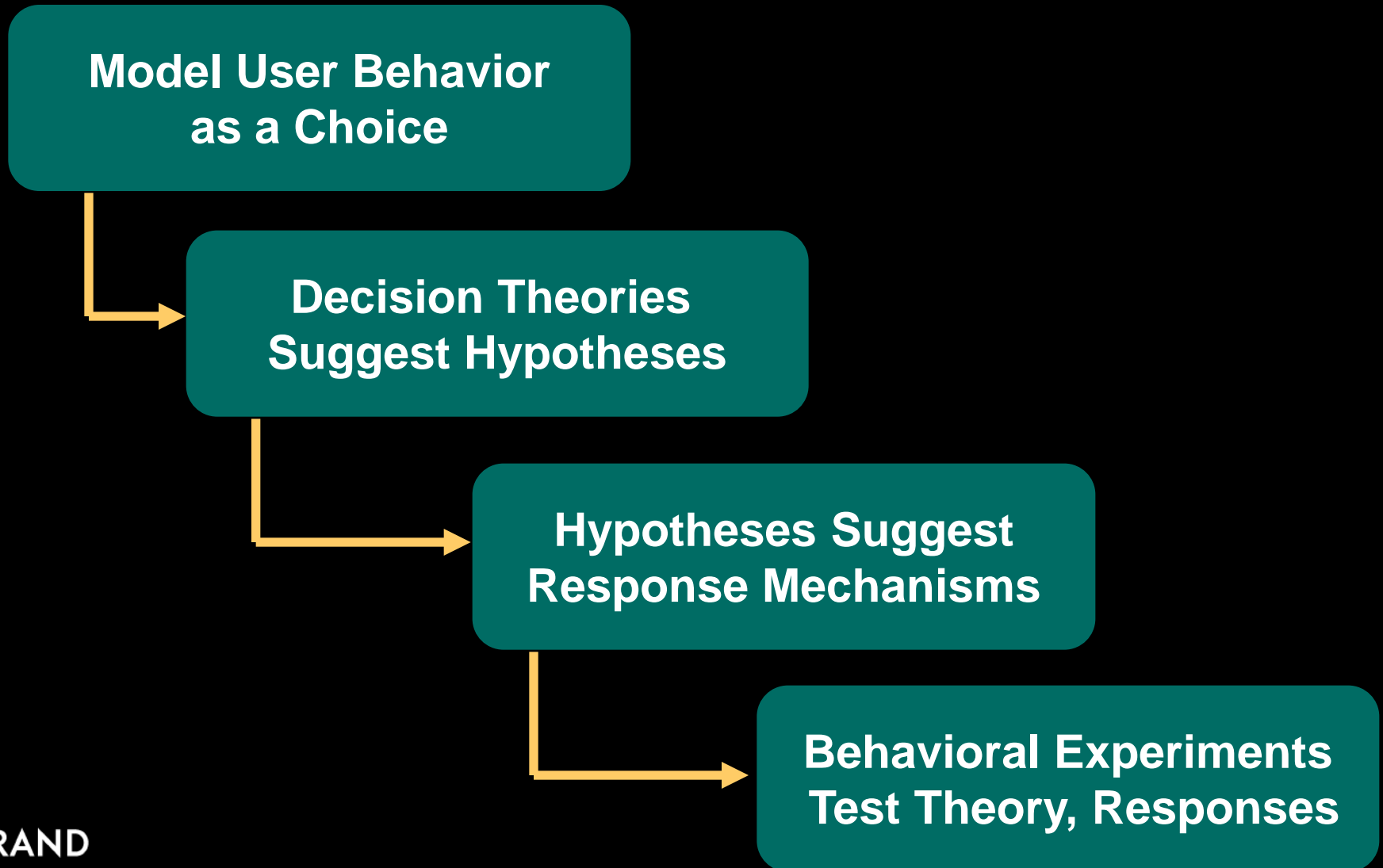
# *Five Perspectives on Insiders and Their Behavior*

- **Who are “insiders” and what kinds of behaviors do we care about?**
  - Led to insider taxonomy
- **What can we learn from those who study human behavior?**
  - Leading to research agenda WRT behavioral decision theory
- **What is the role of ethics?**
  - Led to guidelines for research on insiders
- **What are appropriate responses to unwelcome insider behaviors?**
  - Leading to framework for response space
- **What is the role of the law?**
  - Led to database of legal actions

# ***Three Research Questions Arose From Insider Workshops***

- **How do individuals deal with conflicts among goals (such as security and productivity)?**
- **What role should organizational codes of ethics play in individual actions and an organization's response to insider threat?**
- **Is there a relationship between an individual's and an organization's value systems that is predictive of threatening individual behavior?**

# *Complements Usability Research: Focuses on User Decision-making*



# *Hypotheses About How Users Decide*

1. Users will choose stronger passwords when perceived compromise is more likely or consequential.
  2. Users will choose stronger passwords when perceived security risks are more tangible and less abstract.
  3. Users will choose stronger passwords when they have done so in the past.
  4. Users will choose passwords based on the first examples that come to mind.
  5. Users' password choices are subject to how choice is framed.
- **Normative decision theories** (e.g., utility maximization)
  - **Identifiable victim effect** (e.g., Jenni & Loewenstein 1997 )
  - **Recent decision bias** (e.g., Kahneman & Tversky 1979)
  - **Default bias** (e.g., Samuelson & Zeckhauser 1988)
  - **Framing effects** (Kahneman & Tversky 1979)

## *Hypotheses Suggest Potential Response Mechanisms*

- **Change actual and perceived probability and values**
- **Decrease abstraction of security outcomes**
- **Increase abstraction of memorability outcomes**
- **Provide opportunities for “recent decisions”**
- **Provide strong default choices**
- **Assume control of choice framing**

# *Five Perspectives on Insiders and Their Behavior*

- **Who are “insiders” and what kinds of behaviors do we care about?**
  - Led to insider taxonomy
- **What can we learn from those who study human behavior?**
  - Leading to research agenda WRT behavioral decision theory
- **What is the role of ethics?**
  - Led to guidelines for research on insiders
- **What are appropriate responses to unwelcome insider behaviors?**
  - Leading to framework for response space
- **What is the role of the law?**
  - Led to database of legal actions

# *Guidelines for Ethical Research*

- **Consent**
- **Deception and disguise**
- **Data handling**
  - **Data integrity**
  - **Data sharing**
- **Privacy, anonymity and confidentiality**
- **Bias**

# *Ethical Examples*

- **Consent:**
  - **Can we use subjects' data without consent? (Columbia research)**
- **Data sharing:**
  - **What if law enforcement requests data for which you have promised anonymity? (Cornell research)**
- **Deception:**
  - **How do we do rigorous empirical studies and provide the necessary “cover story”? (MITRE research)**
  - **When do we reveal the truth to subjects, if ever? (Columbia research)**

# ***Ethics Recommendations***

- **Approach potential study subjects with respect, convincing each one of the intrinsic value of the research.**
- **Balance the essential needs for consent and confidentiality with the justifications for deception and disguise.**
- **Plan in advance the ways in which the researchers will gather, store, manipulate and share data.**
- **Take care in presenting data and results so that consent and confidentiality agreements will not be breached.**
- **Plan in advance what options are available and desirable should data be unexpectedly revealed or legally requested by law enforcement.**
- **Think carefully about what options are available and desirable should information be revealed about past or upcoming malicious behavior.**
- **Make sure that the study design and results dissemination are consistent with institutional and organizational codes of ethics and guidelines for professional behavior.**

# *Five Perspectives on Insiders and Their Behavior*

- **Who are “insiders” and what kinds of behaviors do we care about?**
  - Led to insider taxonomy
- **What can we learn from those who study human behavior?**
  - Leading to research agenda WRT behavioral decision theory
- **What is the role of ethics?**
  - Led to guidelines for research on insiders
- **What are appropriate responses to unwelcome insider behaviors?**
  - Leading to framework for response space
- **What is the role of the law?**
  - Led to database of legal actions

# *How to Address the Response Space*



# *Laying Out the Response Space*

- **Start with the taxonomy categories:**
  - **Organization**
  - **System**
  - **Individual**
  - **Environment**
- **Add perspectives/points in time:**
  - **Detection**
  - **Prevention (keep it from happening)**
  - **Mitigation (when it's happening, moderate)**
  - **Punishment (taking action against actors)**
  - **Remediation (cleaning up afterward)**

# Example of Response Framework

	<b>Organization:</b>	<b>System:</b>	<b>Individual:</b>	<b>Environment:</b>
	No expressed policy	No embedded policy	No malicious intent	Laws, ethics apply
<b>Detection</b>		Embedded decoys; watchful monitoring		
<b>Prevention</b>	Create organizational policy	Embed organizational policy	User training, incentives, reminders, access control	Remind users of legal implications of their actions, and of costs to organization
<b>Mitigation</b>	Update related policies			
<b>Punishment</b>				Apply legal punishments
<b>Remediation</b>	Update related policies			

# *Five Perspectives on Insiders and Their Behavior*

- **Who are “insiders” and what kinds of behaviors do we care about?**
  - Led to insider taxonomy
- **What can we learn from those who study human behavior?**
  - Leading to research agenda WRT behavioral decision theory
- **What is the role of ethics?**
  - Led to guidelines for research on insiders
- **What are appropriate responses to unwelcome insider behaviors?**
  - Leading to framework for response space
- **What is the role of the law?**
  - Led to database of legal actions

# Law Addresses Only Part of Taxonomy

Does X have legitimate access? Yes

Does the action violate de facto or de jure policy? Yes

Are the policies deficient? No

Was the action legal? No

Was the action ethical? Yes or No

Are the policies implemented correctly in the system?

What was the system's role? Yes  
Object of misuse  
or Essential enabler

What were X's intent and motive?

Intentionally malicious,  
Externally or Internally motivated

## ***Insiders and Their Actions***

- **New and Different**
  - Taxonomy of insider actions published in *IEEE Security & Privacy* in 2008. Full paper to become a RAND technical report.
  - Ethics guidelines in paper submitted to *IEEE Security and Privacy*.
  - Response options being outlined.
- **Useful Impact**
  - Guidelines for ethical considerations, distinguishing among insiders, applying behavioral decision theory, and differentiating the response space.