Future InfoSec Research (with a focus on METHODS)

Merrill Warkentin

Mississippi State University

http://misprofessor.us

Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Future directions for behavioral information security research

Robert E. Crossler [a,*], Allen C. Johnston [b], Paul Benjamin Lowry [c], Qing Hu [d], Merrill Warkentin [a], Richard Baskerville [e]

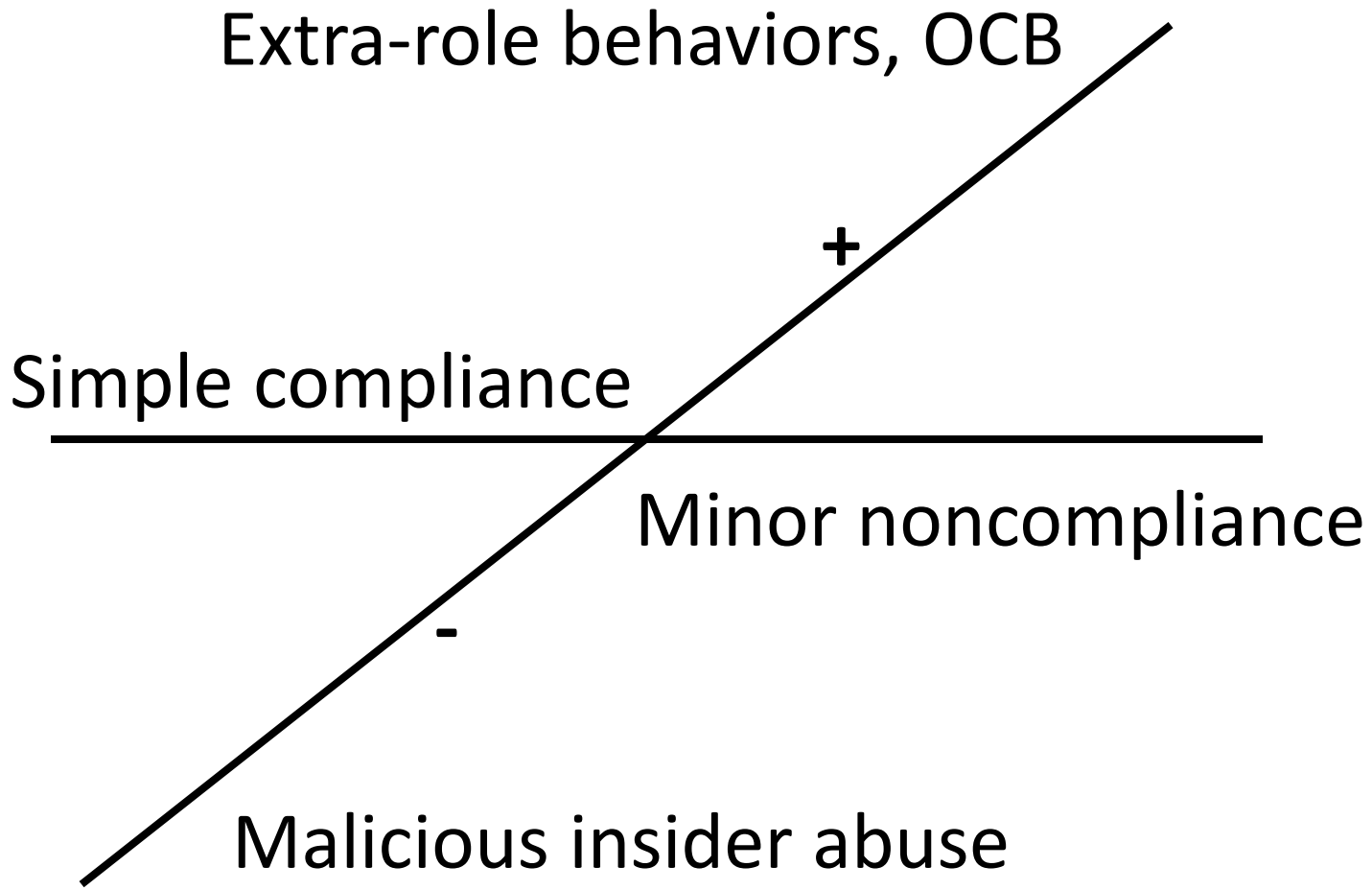
[a] Mississippi State University, Management and Information Systems, PO Box 9581, 302 McCool Hall, Mississippi State, MS 39762, USA
[b] University of Alabama at Birmingham, 1530 3rd Avenue South, School of Business, Birmingham, AL 35294, USA
[c] City University of Hong Kong, P7912 Academic Building I, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong, China
[d] Iowa State University, 2211 Gerdin Business Building, Ames, IA 50011, USA
[e] Georgia State University, PO Box 4015, Atlanta, GA 30302-4015, USA

ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE & SECURE KNOWLEDGE MANAGEMENT, JUNE 5-6, 2012, ALBANY, NY

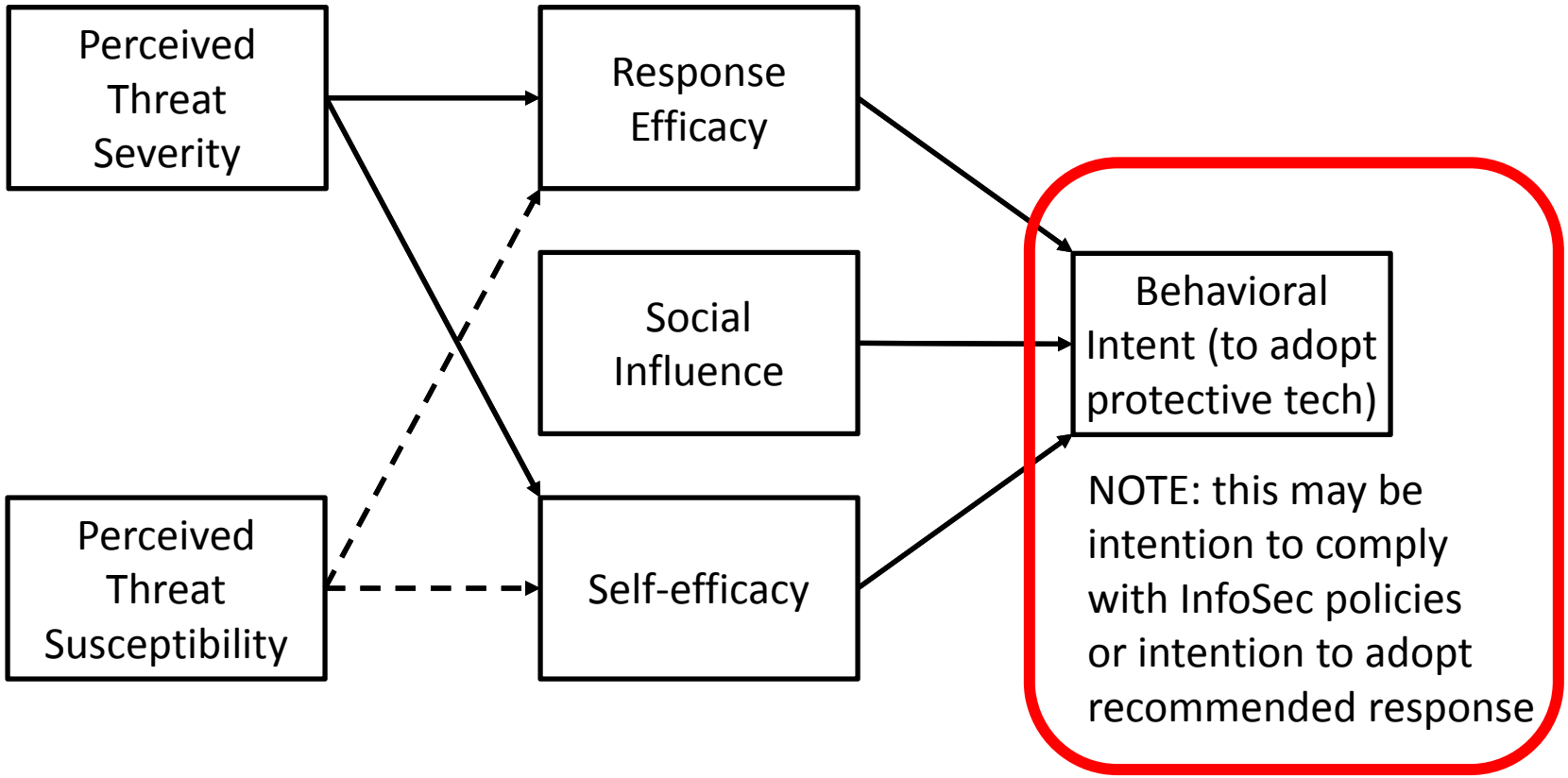
Featured Talk: Measuring Secure Behavior: A Research Commentary

Merrill Warkentin[a], Detmar Straub[b], and Kalana Malimage[a]
[a] *Mississippi State University* [b] *Georgia State University*

Continuum of InfoSec Behaviors



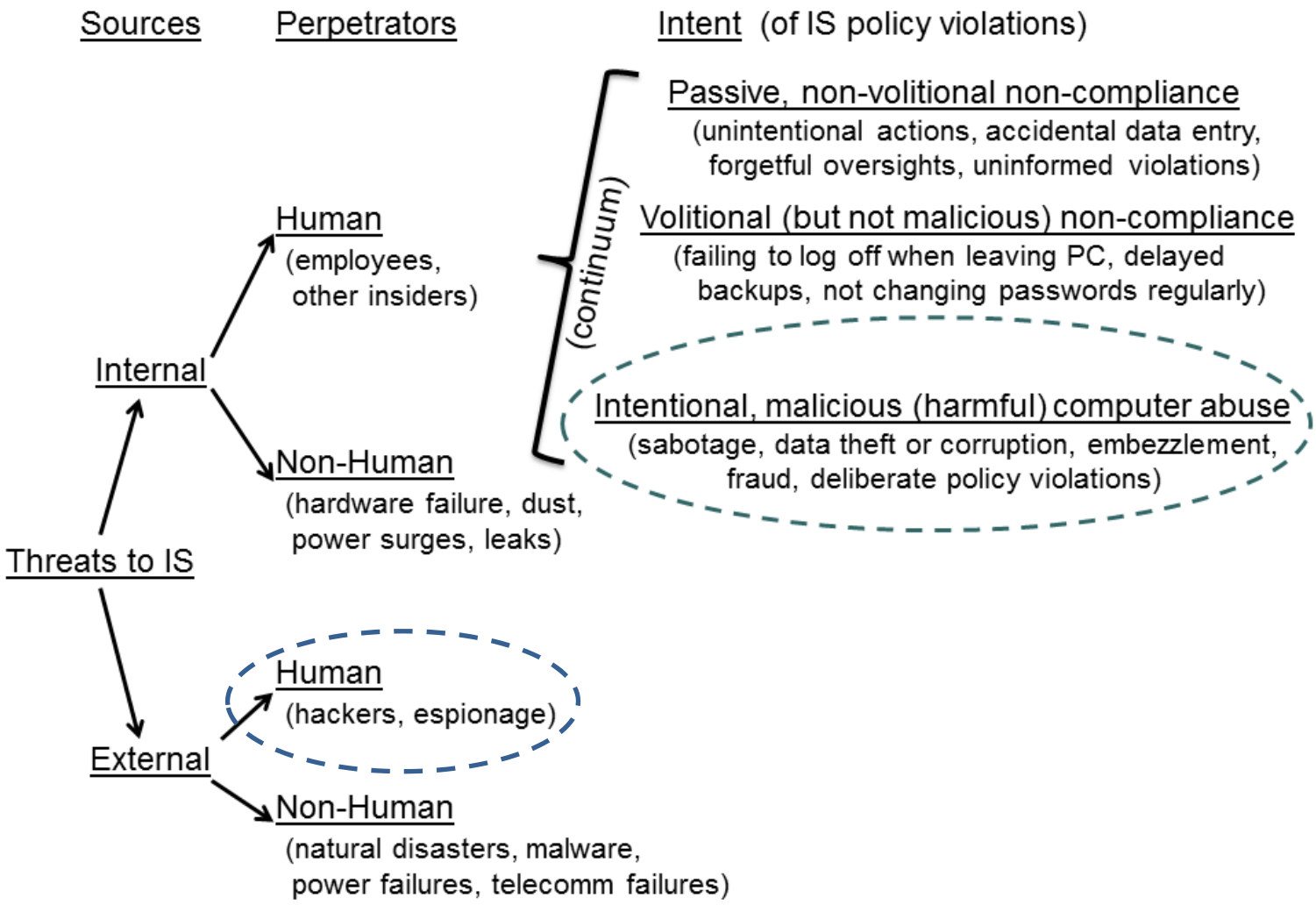
Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549–566.



“The road to hell …
is paved with good intentions.”

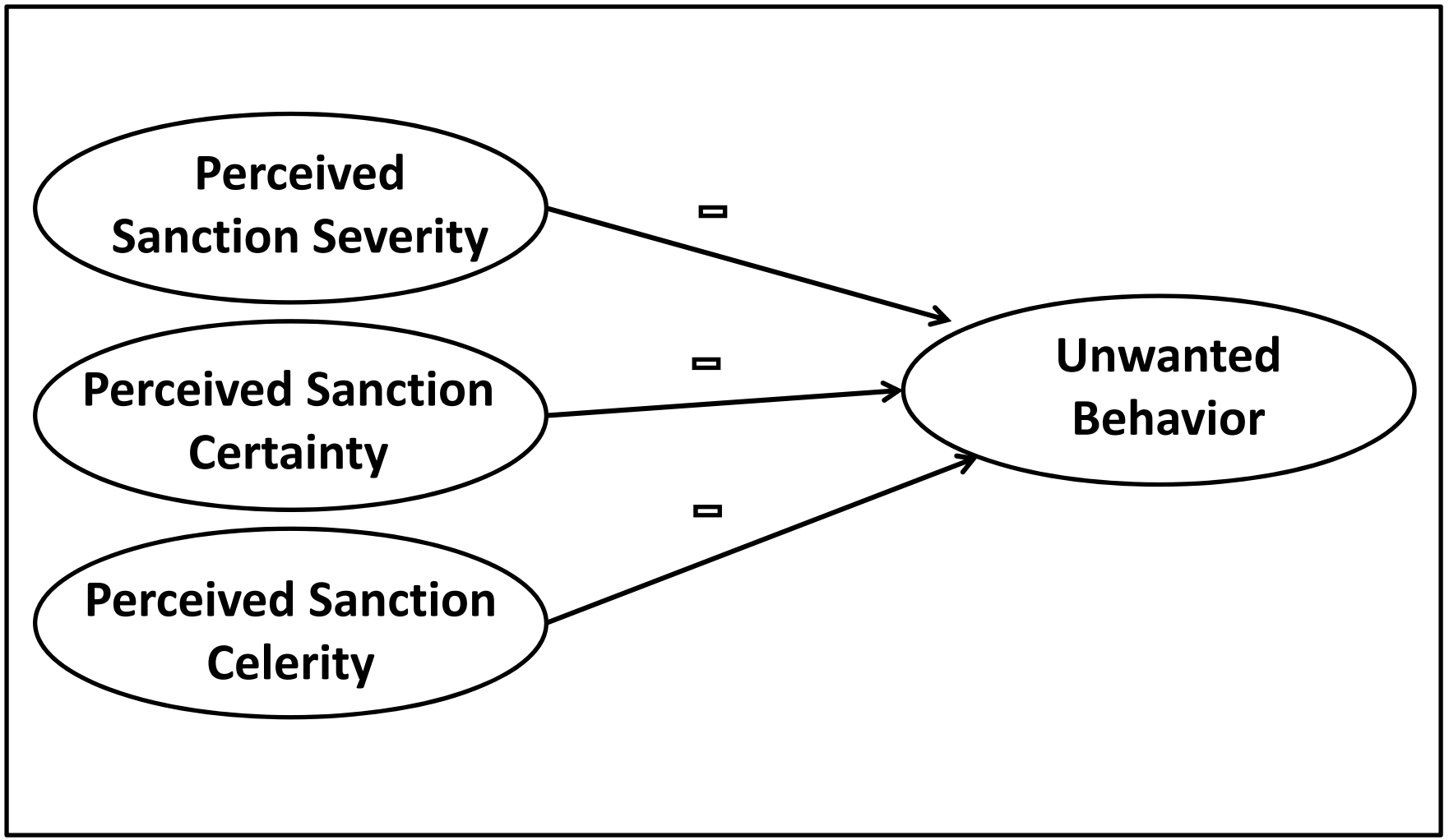
Saint Bernard of Clairvaux
(1091-1153), paraphrased

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly* 37(1), 1-20.

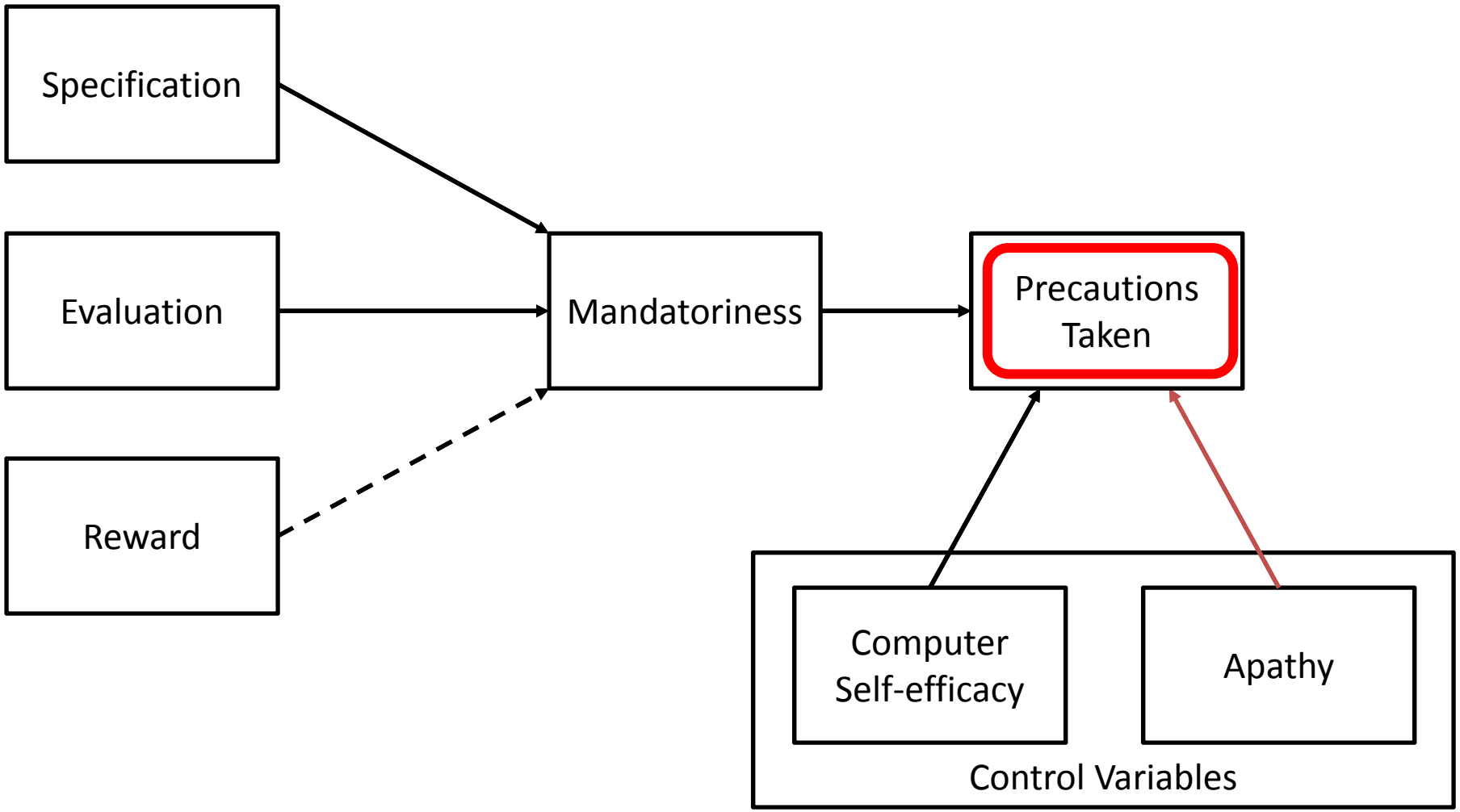


(adapted from Loch, et al., 1992)

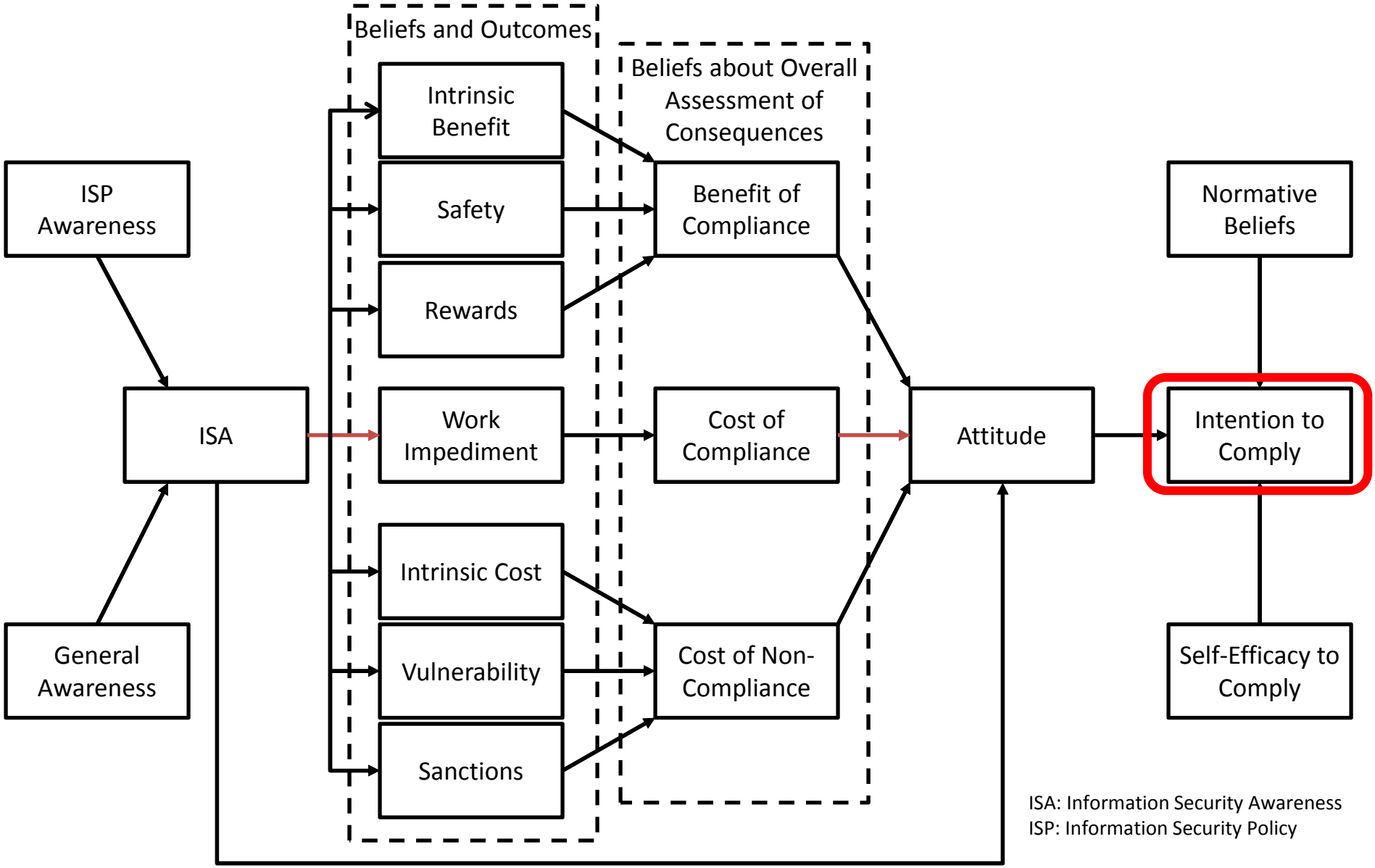
Deterrence Theory



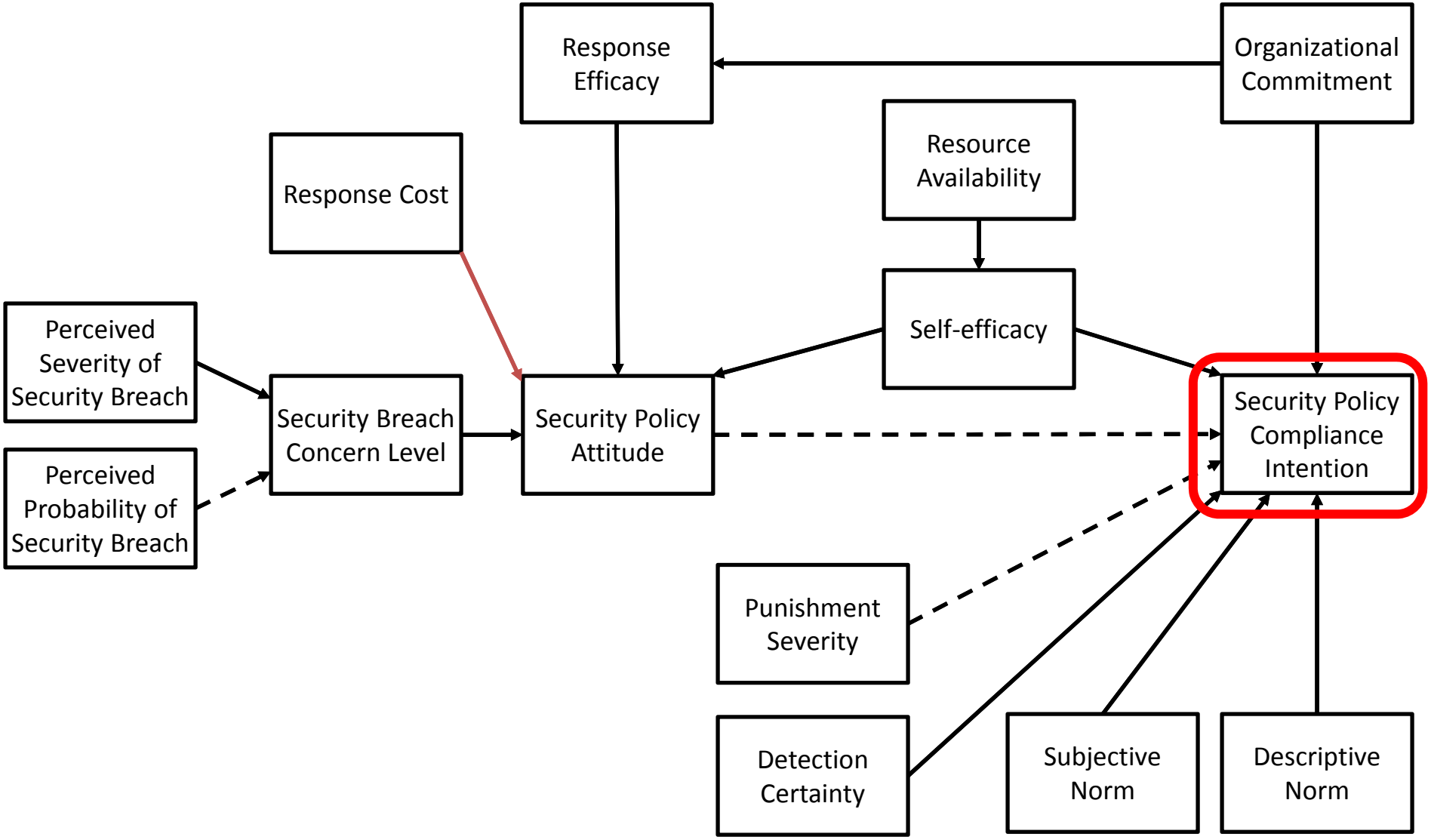
Boss, S. R. et al. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, *18*, 151-164.



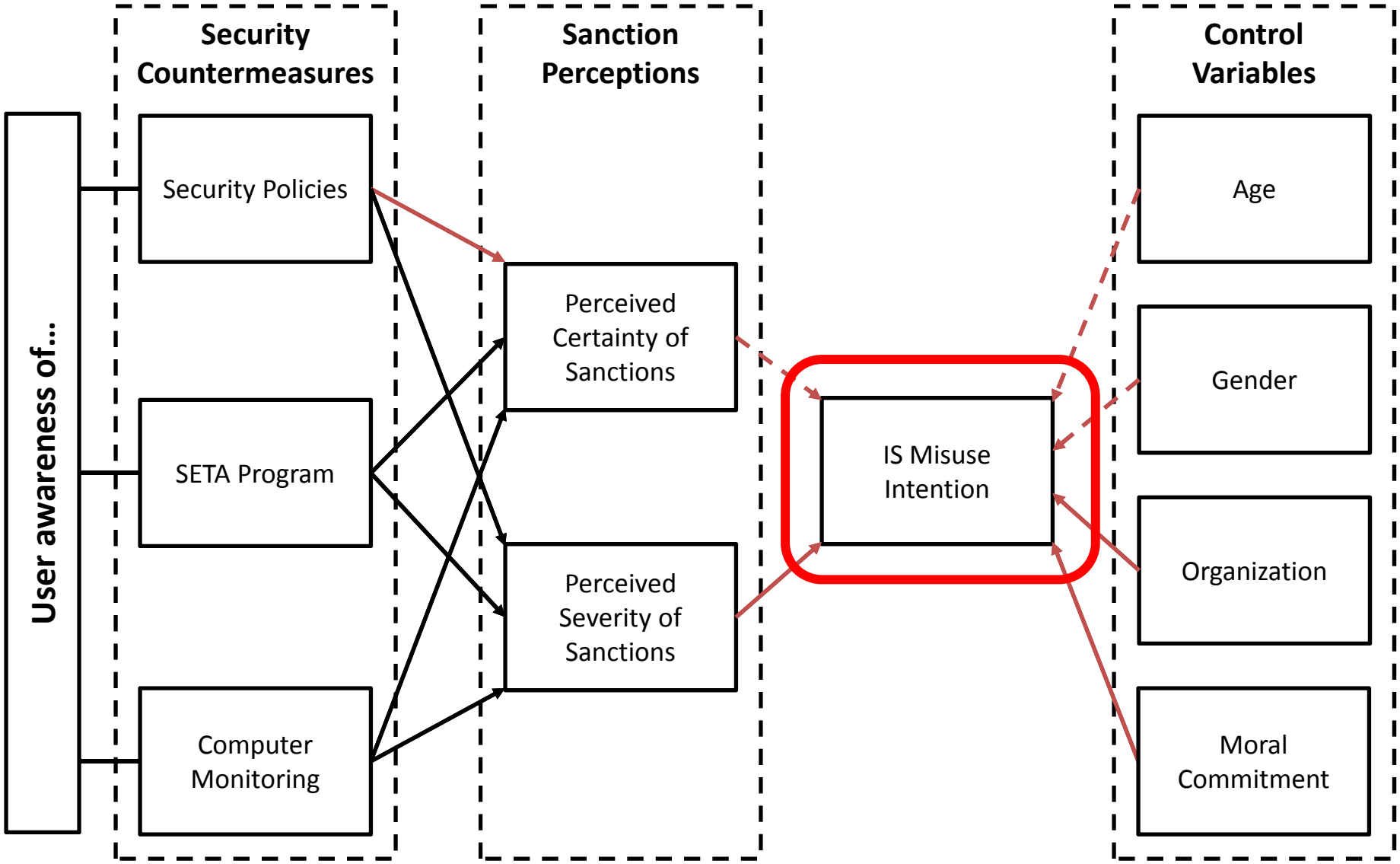
Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.



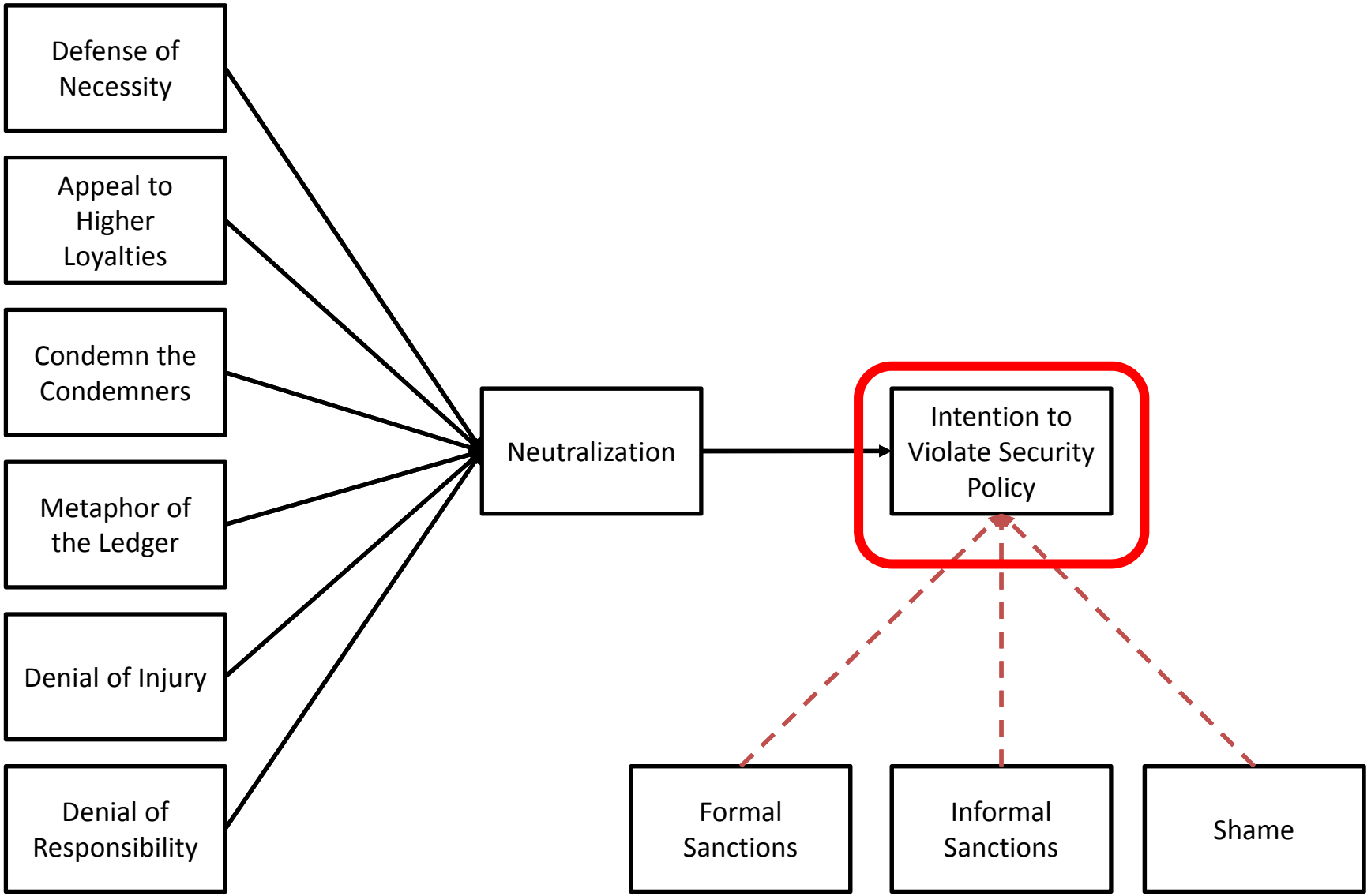
Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.



D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.



Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487–502.



Measuring the Dependent Variable
(problem of "low hanging fruit" (Straub 2009))

- Behavioral intention (common methods bias)
- Actual behavior – positive
  - electronic data gathering (logs, cameras, etc.) – IRB!
  - qualified observer (3rd party – avoid CMV)
- Actual behavior – negative
  - collect black-hat data from white-hats (not ideal)
  - measure behaviors from actual black-hat users
  - study of hackers (Hu et al. 2011)

How can we measure actual behaviors (for DV)? …

Measures	Description	Sample Data Source(s)	Examples	(Dis) Advantages
1. Serendipitous Electronic Data	Electronic Measures captured for alternate reasons	Electronic Monitoring of Employees & other users of networks/systems - Server logs, video cameras, system activity logs, cookies, IP addresses	Password changes, data backup history, surfing behaviors, spam-filtering behavior, patch management activities	Reduced biases (acquiescence, social desirability, Hawthorne Effect, etc.), archival data can be used (collected before research design)
2. Purposeful Electronic Data	Electronic Measures designed to capture specific behavior(s) in the security context	Honeypots, honeynets, cookies, IP addresses		
3. Evaluations by others	Assessment or judgments of subject's behavior by qualified third-party observer (supervisor, researcher, teacher, regulator, etc.)	Supervisory logs and other records, structured observation records,	Logging off workstations before walking away, closing doors before discussing sensitive info with customers/patients, locking door, shredding documents, etc.	Can measure behaviors that cannot be measured by electronic means. Sometimes available as historical archives, but is typically gathered as purposeful process
4. Scenario Evaluations	Factorial survey method which embed variables in the text of the scenario (vignette) versions.	Subject panels from traditional sources (companies, survey panels, etc.) appropriate to the research domain.	Intention to engage in the same behavior as the scenario character in the same circumstances or in the same situation.	Still measures behavioral intention, but subject is not reporting his own behavior, so is not as subject to social desirability and acquiescence biases

Source: Warkentin, Straub, and Malimage (2012)

Measures	Description	Sample Data Source(s)	Examples	(Dis) Advantages
5. Business process data – internal (private)	Structured, formal organizational data available through internal organizational sources	Transaction logs, invoices, internal accounting control data, internal audits, other business archival data collected for other reasons		Standardized collection methods and format makes comparisons reliable, organization-level data, regulated compliance leads to high-quality data,
6. Business process data – external (public)	Structured, formal organizational data available through public sources	Financial reporting data, 10K, 10Q, other SEC filings, public statements, financial reports, accounting data (varies between US, EU, etc.)		
7. Method-induced measures	Data resulting from any research methods that induce an effect (behavior, attitude, etc.)	Experimental manipulations. Measure user actions and behaviors in controlled environment under specific conditions, action research projects	Password selection, password recall, deception detection, IT selection decisions	Better controls, but reduced generalizability and realism.
8. Dialog/Discourse	Verbal and textual accounts and descriptions of dyads and group interactions, both verbal and written	Structured interviews, narratives, ethnographies, story-telling, forums, user groups, BBS, discussion databases, blogs, FB, committee reports, transcriptions of organizational meetings	Individual and organizational decisions and behaviors as described by observers, especially insiders	

Source: Warkentin, Straub, and Malimage (2012)

Measures	Description	Sample Data Source(s)	Examples	(Dis) Advantages
9. Individual Narratives	Verbal or written accounts by individuals (monologues)	narratives, ethnographies, story-telling	Individual and organizational decisions and behaviors as described by observers, especially insiders	
10. Neuro-Physiological Observations	Physiological indicators of individual brain activities associated with engagement with security (violations, interactions, compliance, decisions)	fMRI, EEG, EKG, heart rate, galvanic skin response		
11. Simulations	Computer-generated data meant to mimic security activities	Individual user and organizational behaviors and activities of all types, if they can be simulated properly	Individual user and organizational behaviors and activities of all types, if they can be simulated properly	Will generate results for studying problems that are intractable – when actual data cannot be collected.
12. InfoSec Repositories	Data repositories that collect information on security related constructs	CERT reports, data leakage reports, CSO and PwC annual survey, FBI reports, industry study white papers, state data breach notification law reports, www.privacyrights.org/data-breach	Data breaches, CERT data	Sometimes public availability, often fairly complete (required by law).

Source: Warkentin, Straub, and Malimage (2012)

Measures	Description	Sample Data Source(s)	Examples	(Dis) Advantages
13. Legal document	Data generated by legal actions	Libraries (e.g. Westlaw), court records and proceedings, transcripts of depositions, police investigations, forensic investigations, arbitrage hearings, proceedings of civil cases (lawsuits)	Individual and organizational level behaviors that involve criminal violations or actionable civil actions.	Publicly available, rich data sources, often the only window into illegal activities (such as hacking). Law compels data provision (testimony).
14. Study meta-data	Many kinds of data associated with a given piece of research, ultimately useful for meta-analysis and/or literature review	Correlations, study setting methodology (DET)		
15. Media Reports	Mass media (TV, radio, print) sources, websites	News accounts of computer crimes, investigative reports, magazine articles		Can be more complete and open than court records which are often clouded by plea bargains, negotiated settlements, or sealed court records

Source: Warkentin, Straub, and Malimage (2012)

DV Data Collection Methods

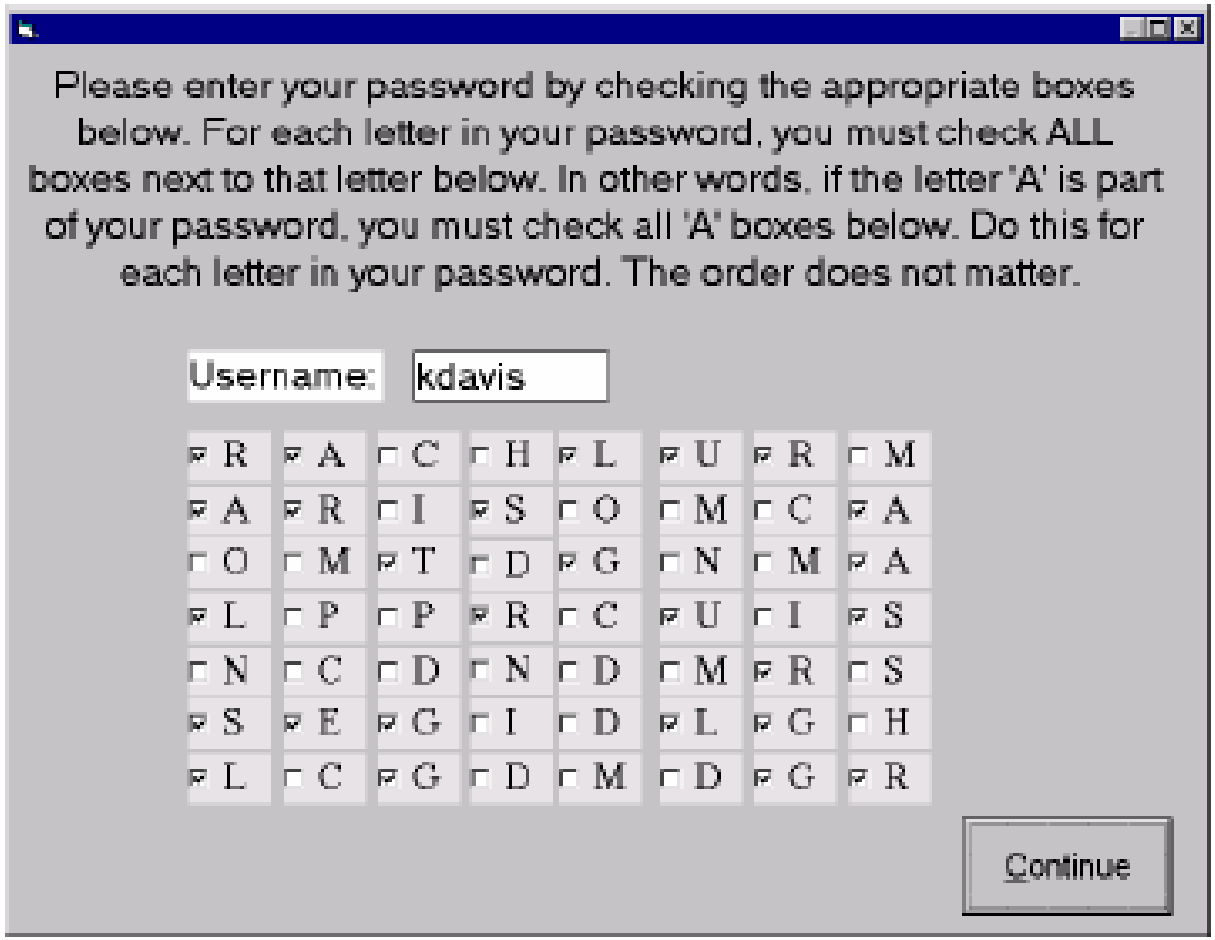
- deceptive Scenario to collect actual user behavior
- PhishMe (and other 3rd party companies) are hired to test security awareness by sending intentional phishing attacks on employees (penetration testing data) - PhishMe

Dear Employee,
We are migrating to a new 401k provider.
Please login with your corp credentials to complete enrollment.
http://401k.hr-communication.com/enroll

Measuring Actual Behavior …

- COPS Study (Warkentin, Davis, & Bekkering)

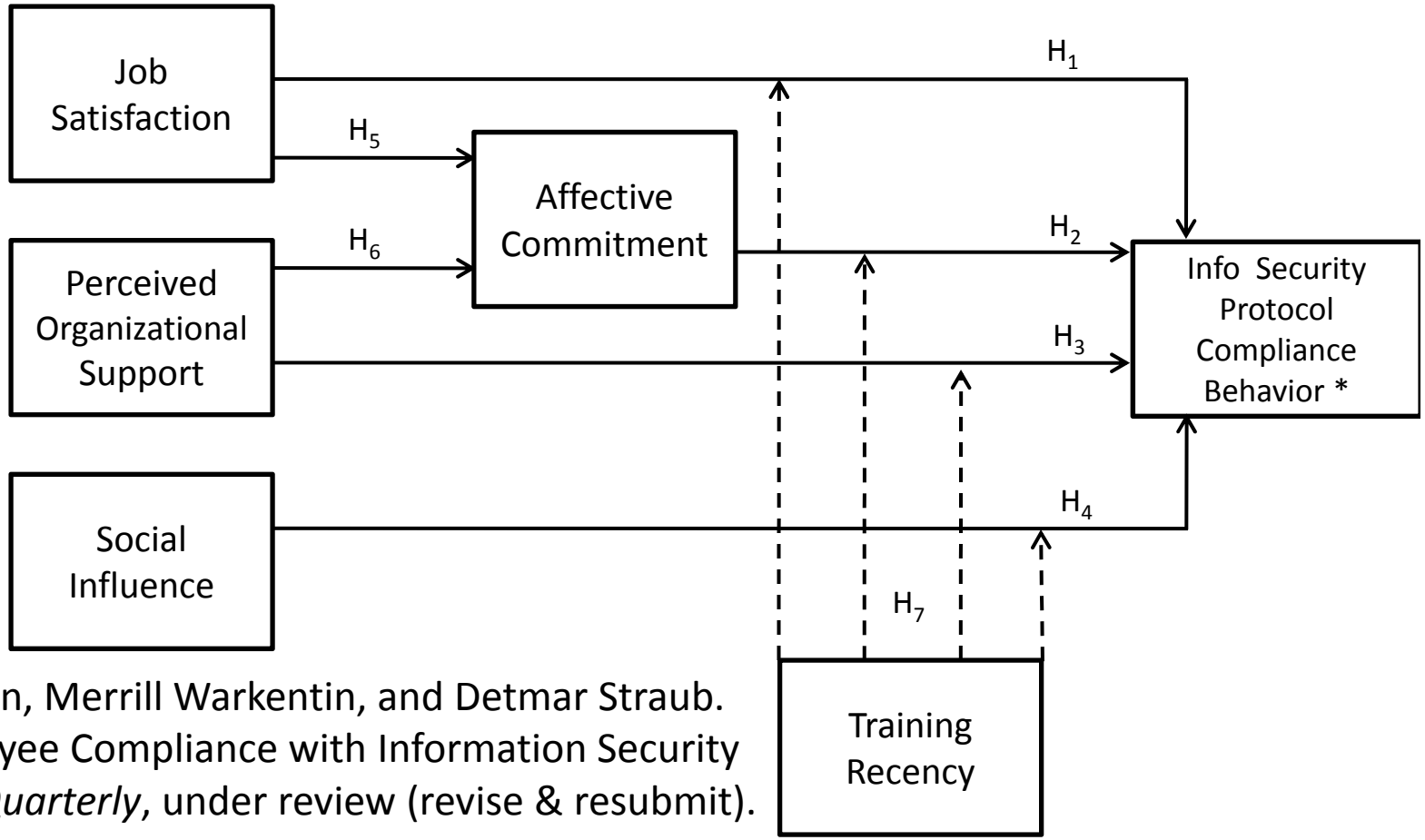
Check-off Password System (Warkentin, Davis, & Bekkering, 2004)



Measuring Actual Behavior …

- COPS Study (Warkentin, Davis, & Bekkering)
- OCB Study (Shropshire, Warkentin, & Straub)

OCB Study
(Shropshire, Warkentin, & Straub)



Shropshire, Jordan, Merrill Warkentin, and Detmar Straub. "Fostering Employee Compliance with Information Security Protocols," *MIS Quarterly*, under review (revise & resubmit).

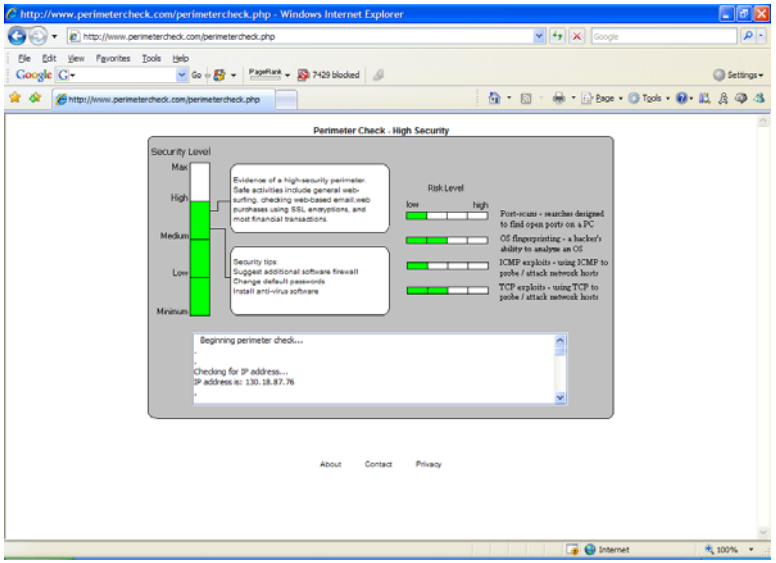
* DV measured independently by supervisor ratings (Observations)

Measuring Actual Behavior …

- COPS Study (Warkentin, Davis, & Bekkering)
- OCB Study (Shropshire, Warkentin, & Straub)
- Personality Study (Warkentin, Shropshire, & Sharma)

Personality Study
(Warkentin, Shropshire, Sharma)

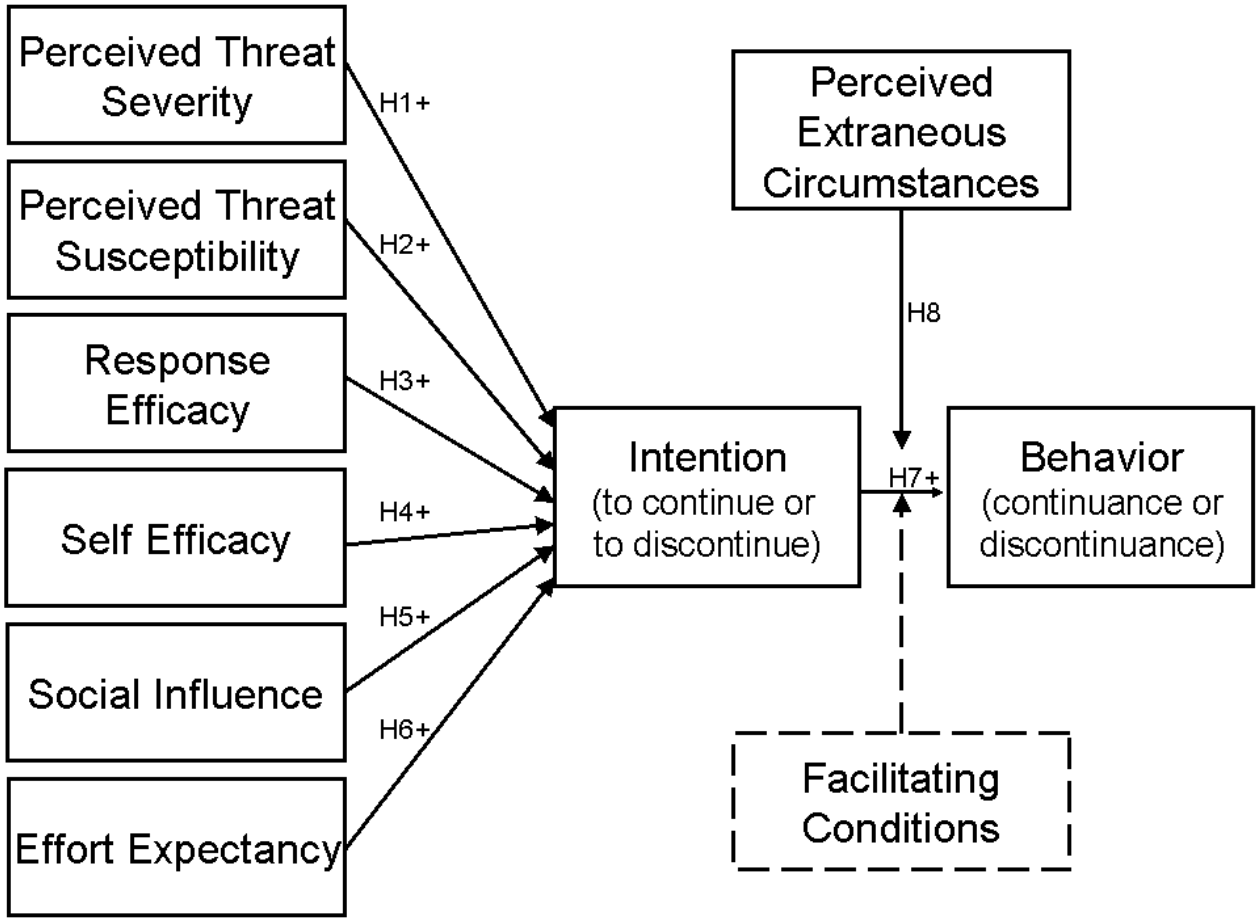
- What personality types are more likely to exhibit actual secure behaviors?
- Expose potential subjects to “PerimeterCheck” and see who uses it



Measuring Actual Behavior …

- COPS Study (Warkentin, Davis, & Bekkering)
- OCB Study (Shropshire, Warkentin, & Straub)
- Personality Study (Warkentin, Shropshire, & Sharma)
- Continuance Study (Warkentin, Shropshire, Johnston, & Barnett)

Continuance – Research Model (Warkentin, Shropshire, Johnston)

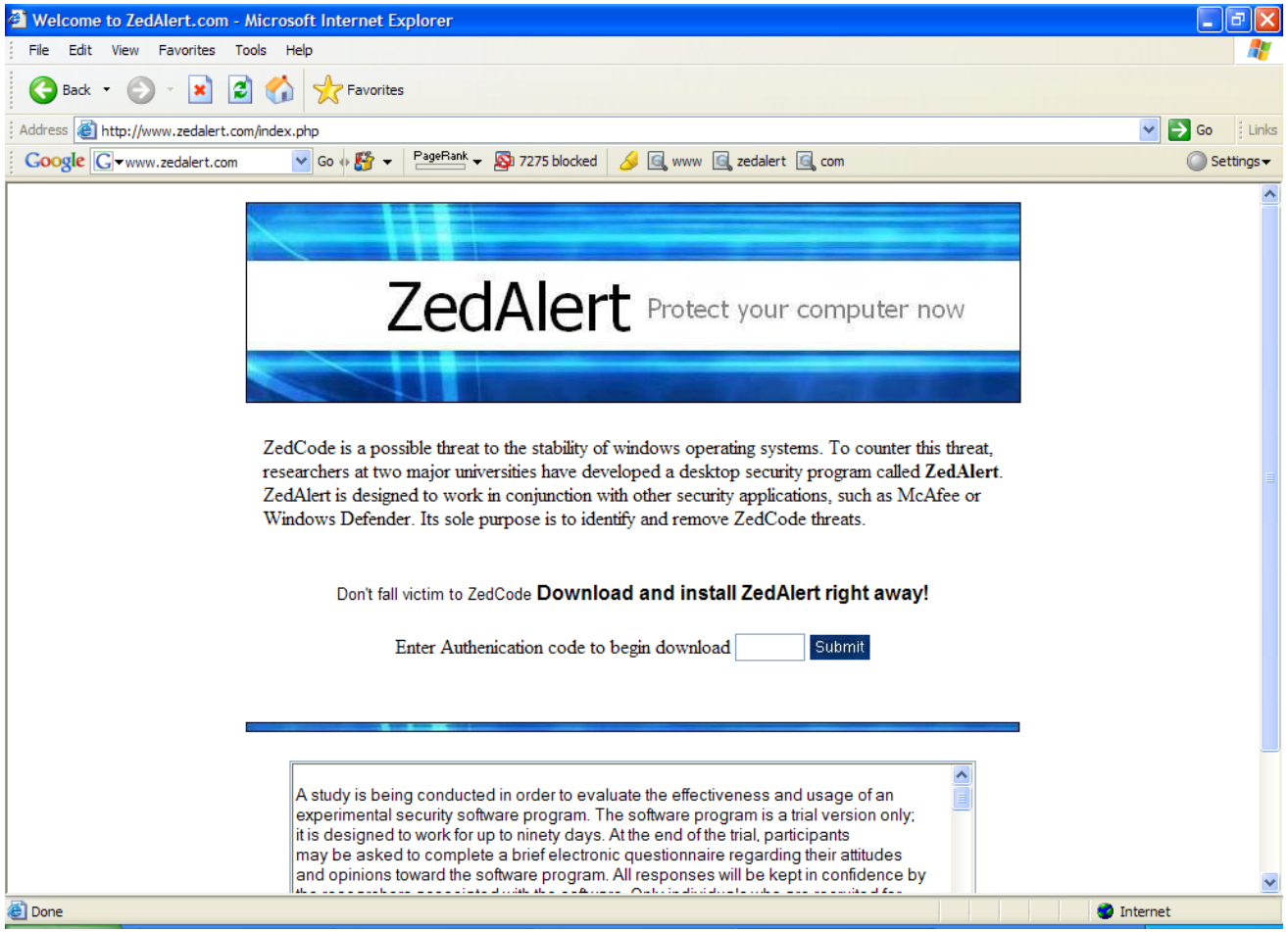


Experiment

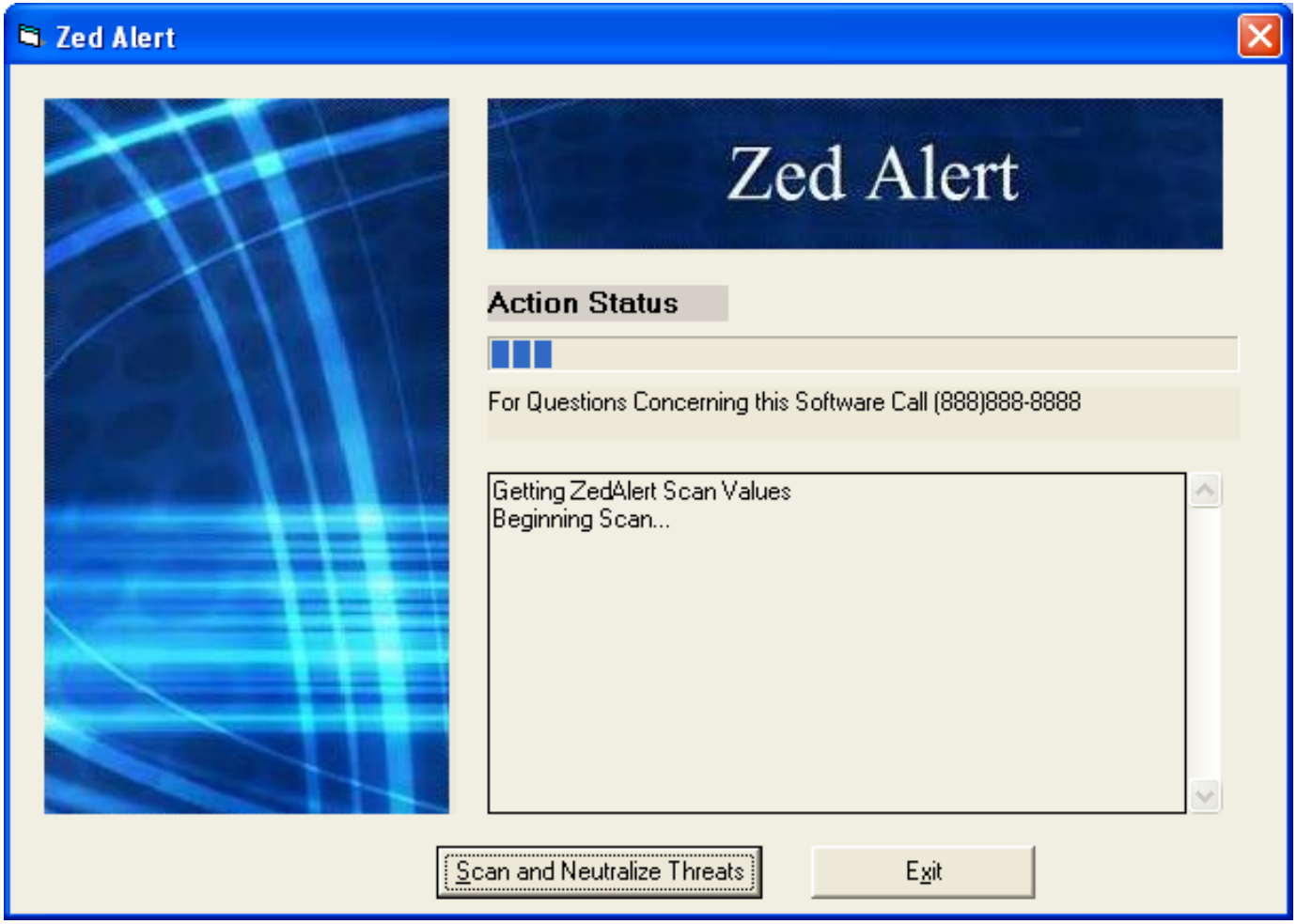
- required actual usage data (not just BI)
  - properly motivated voluntary behavior
  - Avoid problems with Common Method Variance (CMV)
- created & distributed desktop security program
  - deceit scenario* – be careful for “ZedCode” !!
  - must adopt “ZedAlert” and use it <u>every</u> week
  - each subject received unique software download key
- upon “discontinuance” (10 days without scanning)
  - users electronically completed a survey
  - full disclosure, then upload data

(*IRB Challenges”)

Security Application



ZedAlert Scan Interface



Measuring Actual Behavior …

- COPS Study (Warkentin, Davis, & Bekkering)
- OCB Study (Shropshire, Warkentin, & Straub)
- Personality Study (Warkentin, Shropshire, & Sharma)
- Continuance Study (Warkentin, et al.)
- Training Study (Barlow, Warkentin, Ormond, & Dennis)
- Password Threat/Change Study
  (Johnston, Warkentin, & Siponen)
- fMRI Study (Warkentin, Walden, Straub, & Johnston)

Measuring Actual Behavior …

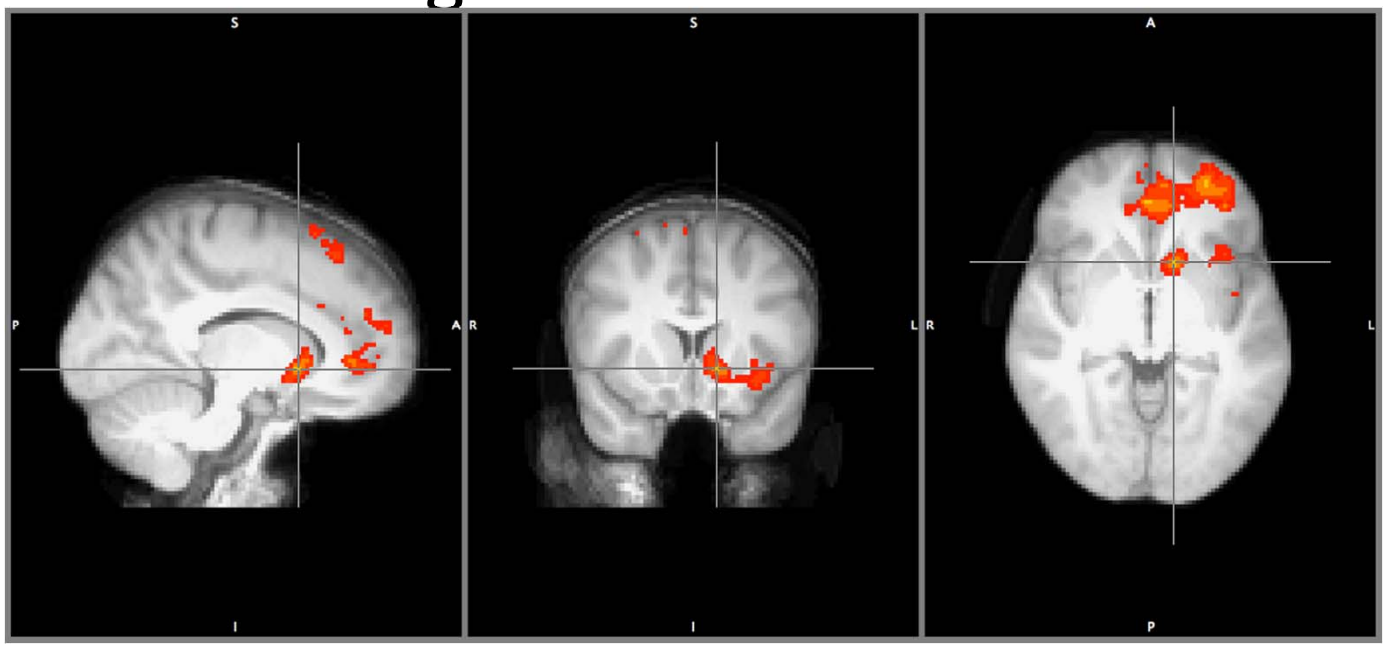
- COPS Study (Warkentin, Davis, & Bekkering)
- OCB Study (Shropshire, Warkentin, & Straub)
- Personality Study (Warkentin, Shropshire, & Sharma)
- Continuance Study (Warkentin, et al.)
- Training Study (Barlow, Warkentin, Ormond, & Dennis)
- Password Threat/Change Study
  (Johnston, Warkentin, & Siponen)
- fMRI Study (Warkentin, Walden, Straub, & Johnston)

Measuring Actual Behavior …

- COPS Study (Warkentin, Davis, & Bekkering)
- OCB Study (Shropshire, Warkentin, & Straub)
- Personality Study (Warkentin, Shropshire, & Sharma)
- Continuance Study (Warkentin, et al.)
- Training Study (Barlow, Warkentin, Ormond, & Dennis)
- Password Threat/Change Study
  (Johnston, Warkentin, & Siponen)
- fMRI Study (Warkentin, Walden, Straub, & Johnston)

Results when response generated more activity than the threat

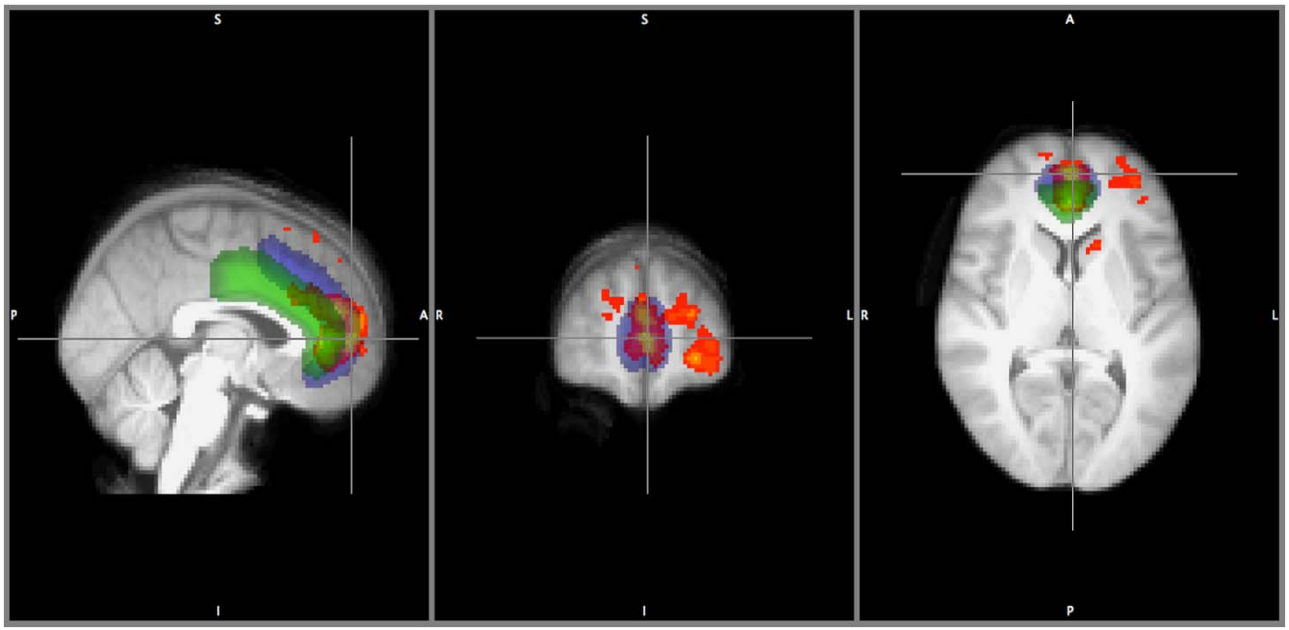
- left caudate nucleus
- rewards, utility, trust
- stress relieving



Source: Warkentin, Walden, Johnston, and Straub

Results when response generated more activity than the threat

- paracingulate cortex /anterior cingulate cortex
- fear, social cognition (group rhetoric?)



Source: Warkentin, Walden, Johnston, and Straub

Concluding Remarks

- InfoSec research experiencing increasing rigor
- Seeking better measures of DV (and IVs!)
- Also seeking improved theoretical foundations (see Baskerville, 2009)
  - Goal: native theories that fit context
- Encourage participation in our WG …
  http://ifip.byu.edu
- Contact: m.warkentin@msstate.edu