Behavioral Security Research

Presented by Robert E. Crossler

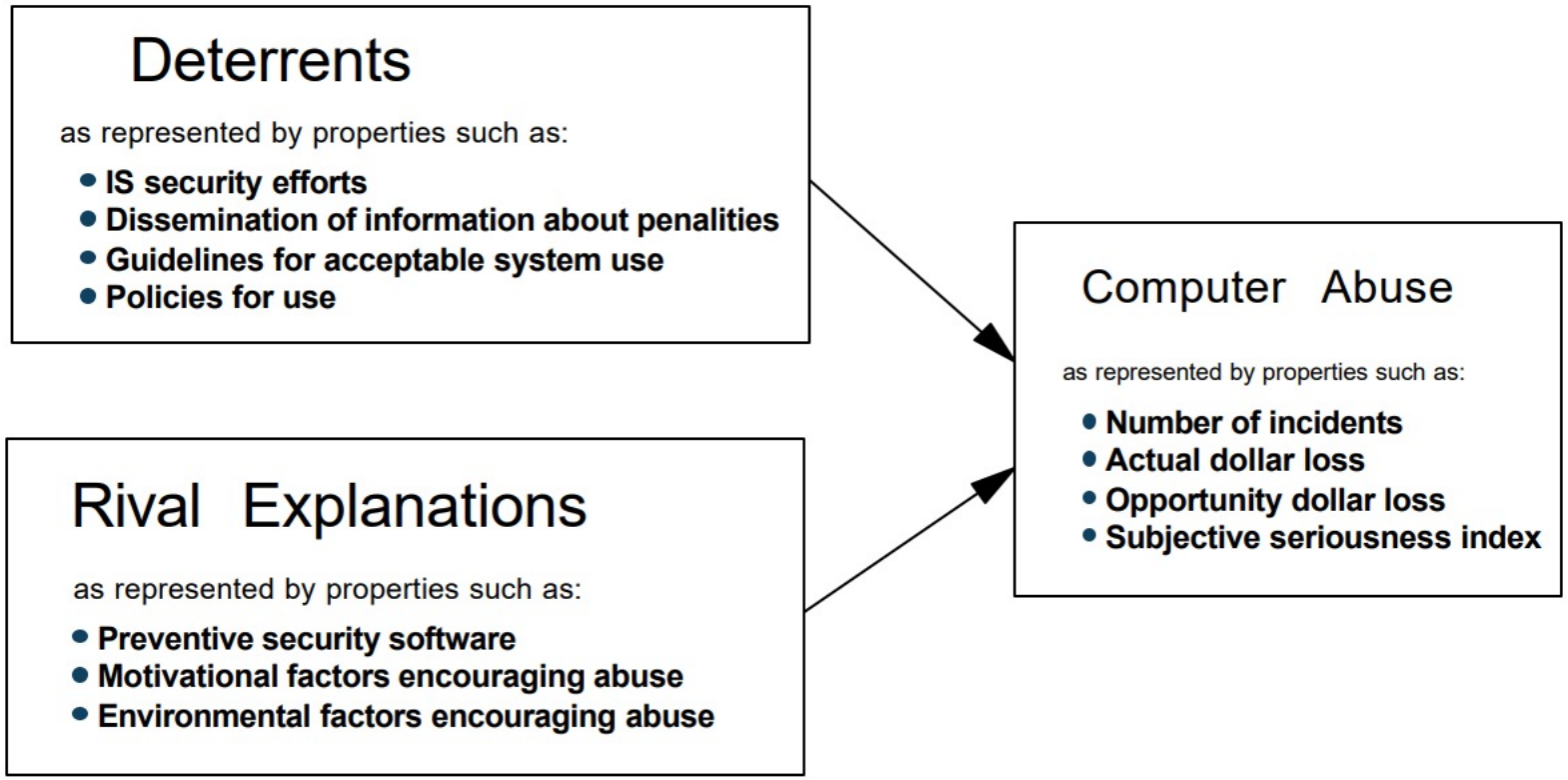
What is Behavioral Security Research?

"Behavioral InfoSec research is a subfield of the broader InfoSec field that focuses on the behaviors of individuals which relate to protecting information and information systems assets (Fagnot, 2008; Stanton et al., 2006), which includes computer hardware, networking infrastructure, and organizational information. Recently, a number of studies have been published about the behaviors of individuals in protecting these assets."

Crossler, R. E., Johnston, A.C., Lowry, P. B., Hu, Q., Warkentin, M., Baskerville, R., 2013, Future Directions for Behavioral Information Security Research, *Computers & Security*, (32:1), 90-101.

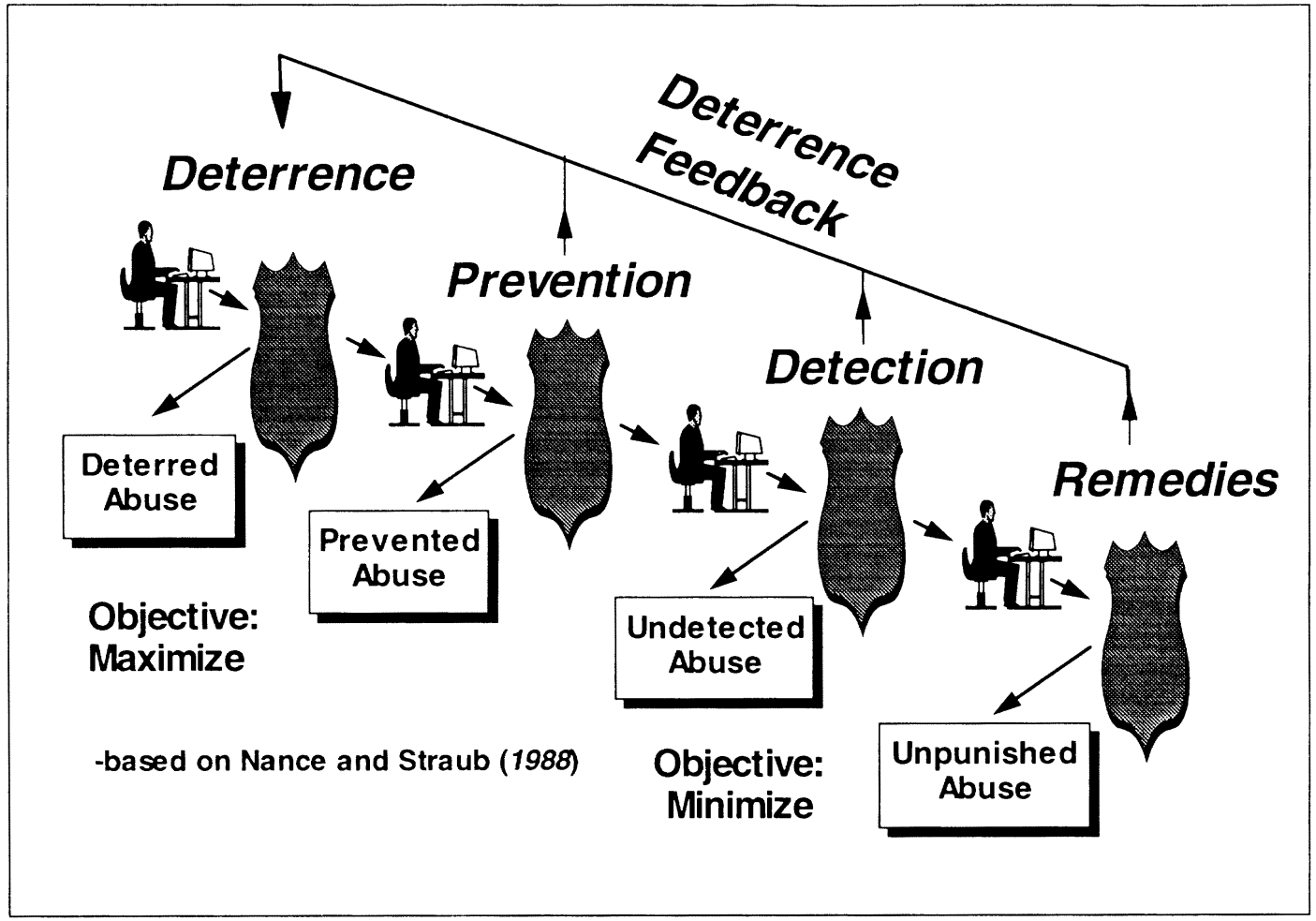
Criminological Theory of General Deterrence

Figure 1. The Security Impact Model



Straub, D. W. 1990. Effective IS Security: An Empirical Study. *Information Systems Research*, 1(3), p.255-276.

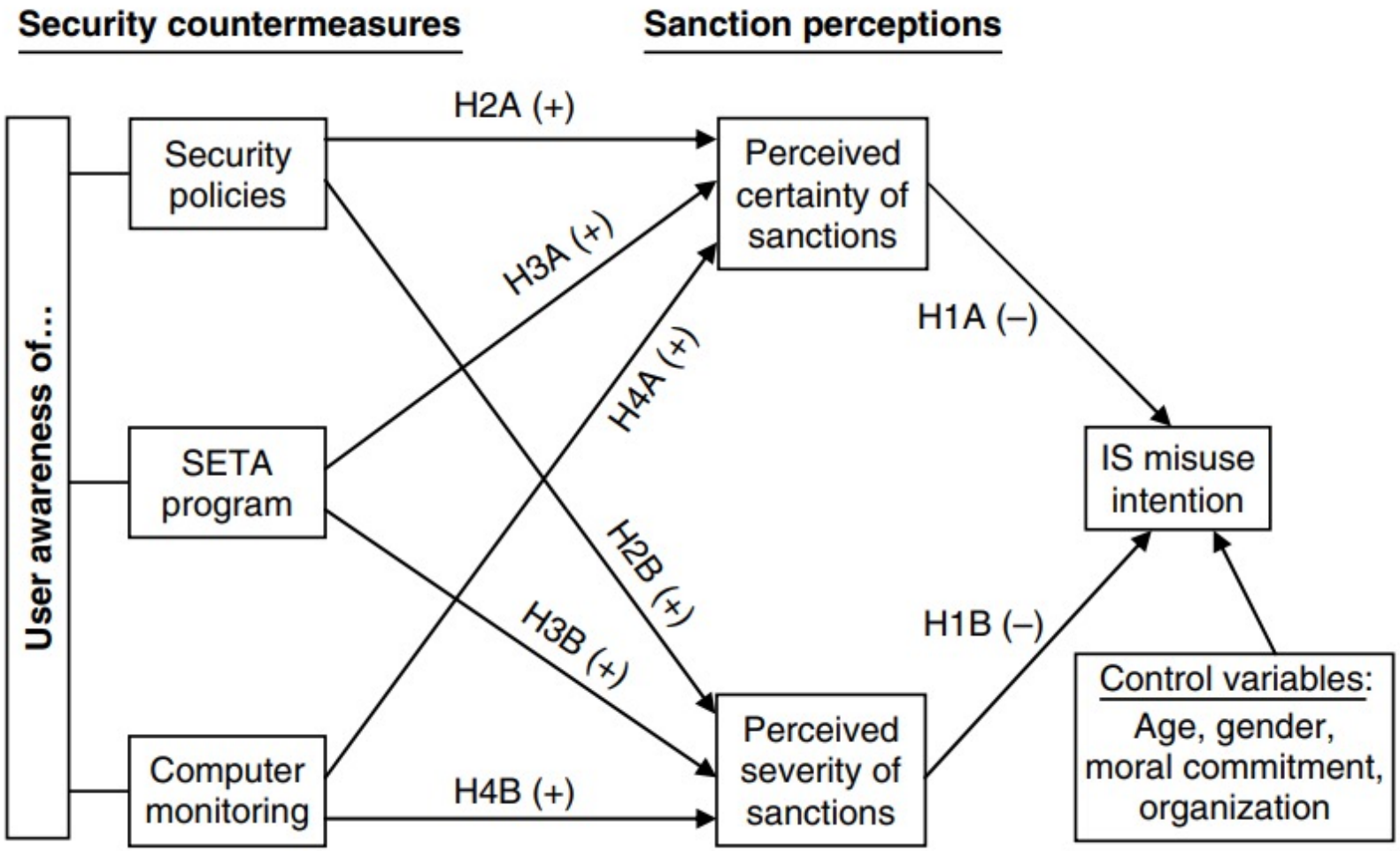
The Security Action Cycle



Straub, D. W., Welke, R. J., 1998. Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, 22(4), p.441-469.

General Deterrence Theory

Figure 1 The Extended GDT Model



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

Deterrence theory & Neutralization Theory

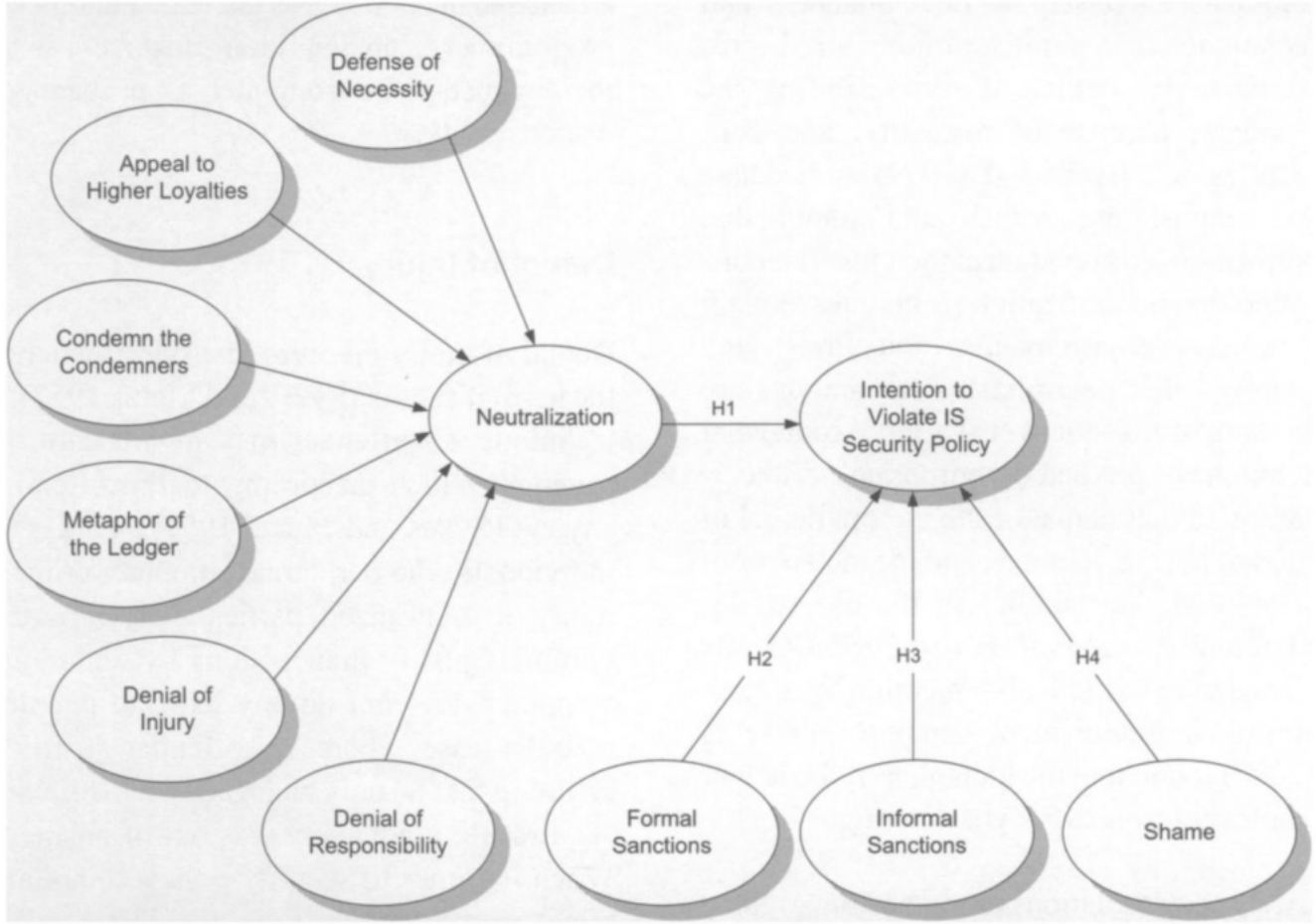


Figure 1. The Research Model

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

Protection Motivation Theory (PMT)

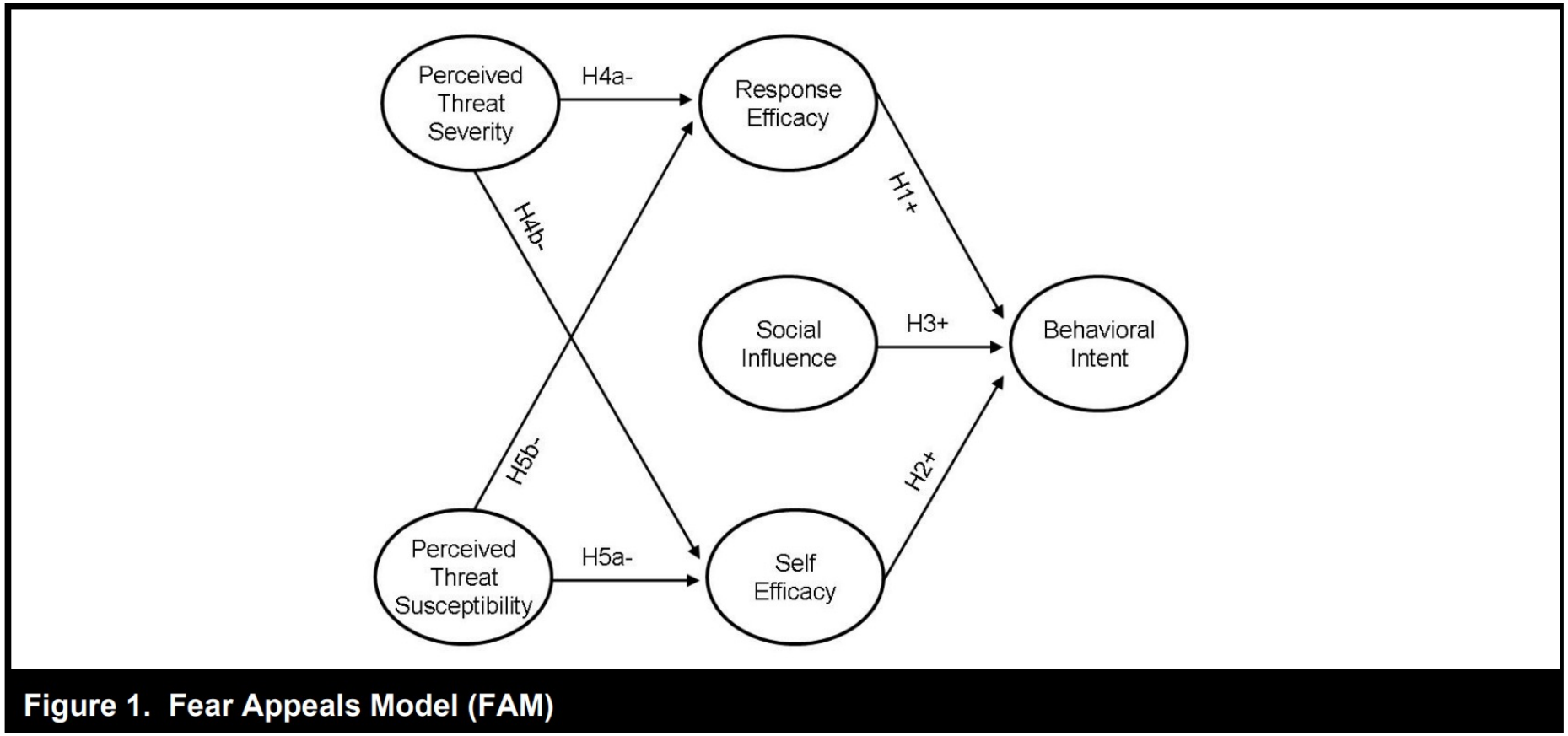
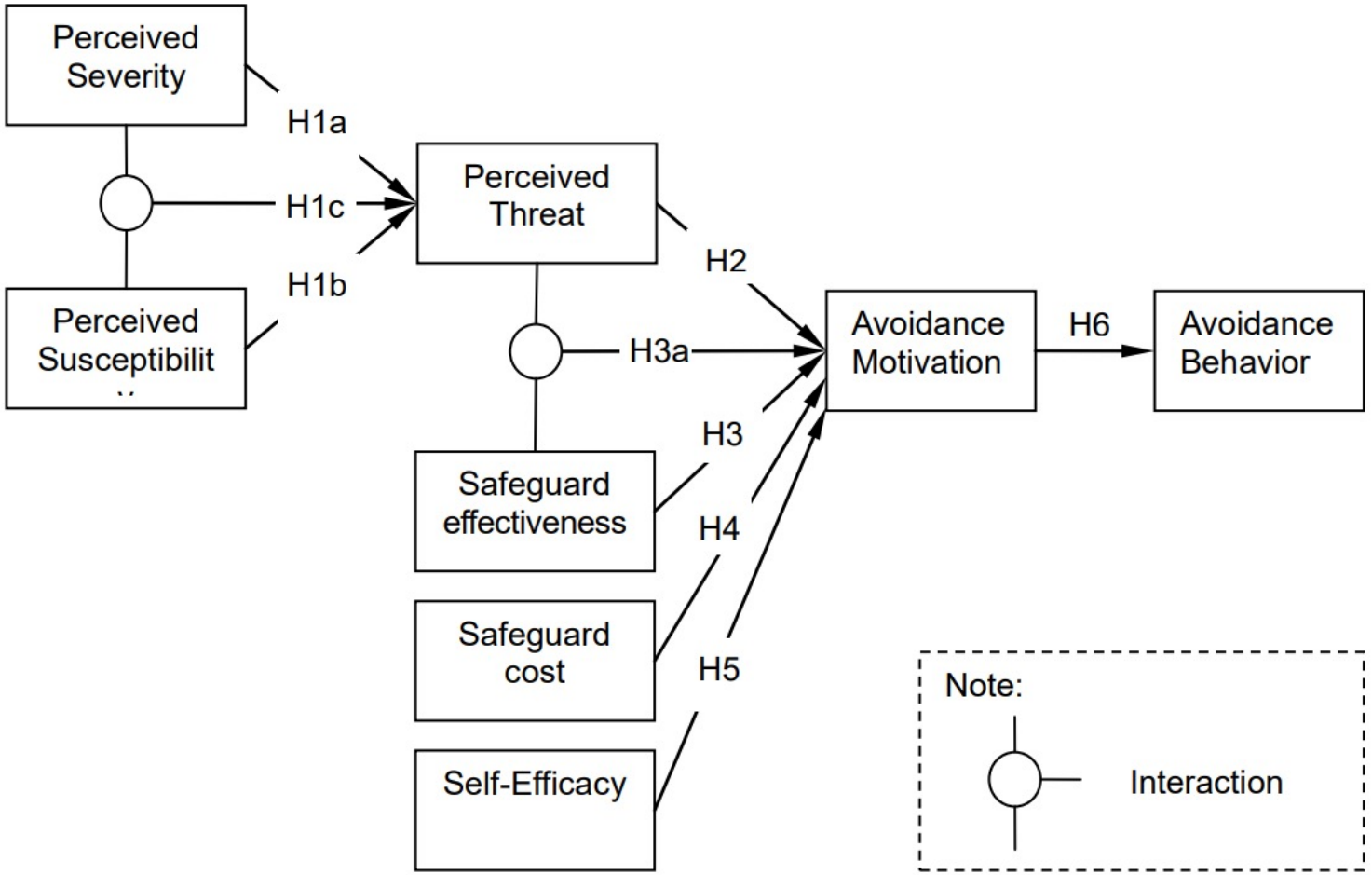


Figure 1. Fear Appeals Model (FAM)

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

Technology Threat Avoidance Theory



Liang, H & Xue Y. 2010. Understanding Security behaviors in personal computer usage: a threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), pp.394-413.

Protection Motivation Theory (PMT)

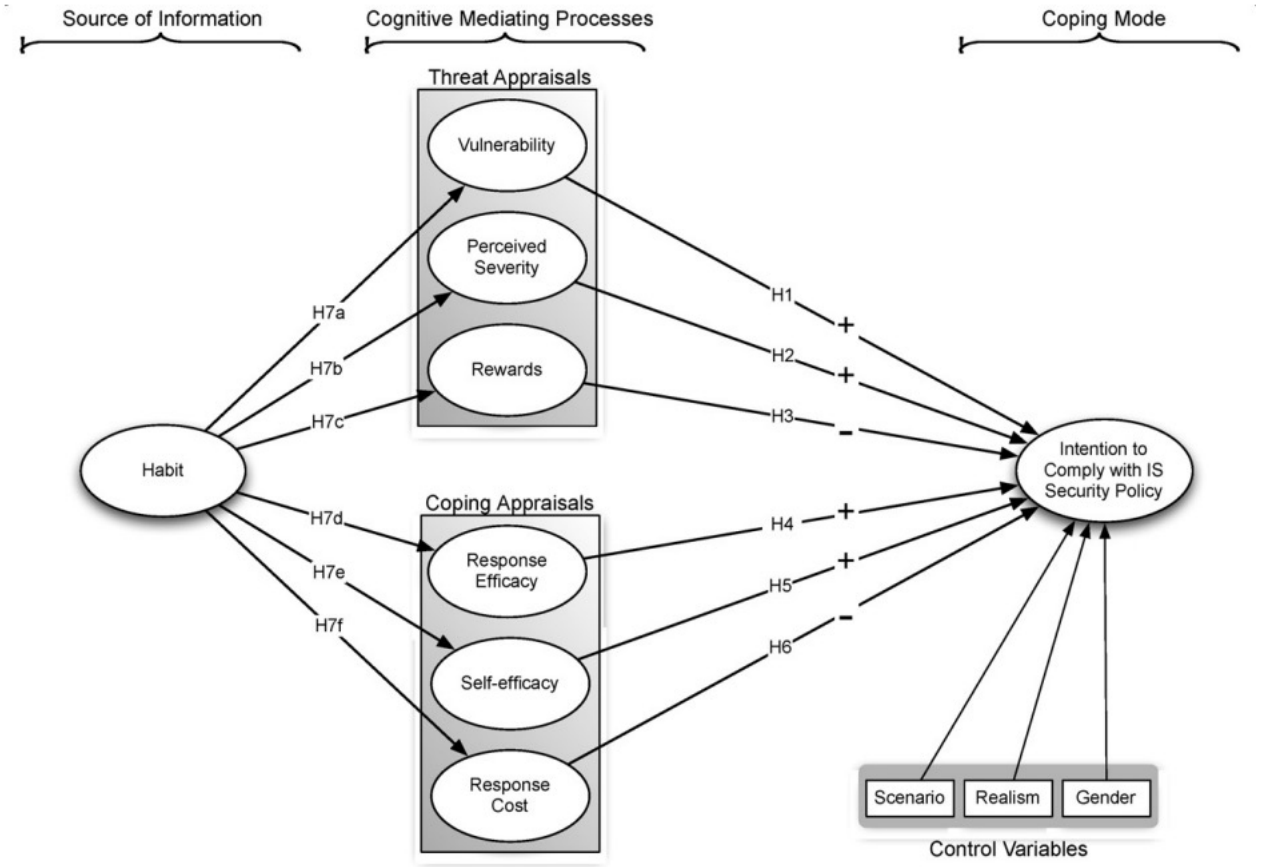


Fig. 1. Research model.

Vance, A, Siponen, M. & Pahnila, S. 2012. Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, 49, pp.190-198.

Protection Motivation Theory (PMT)

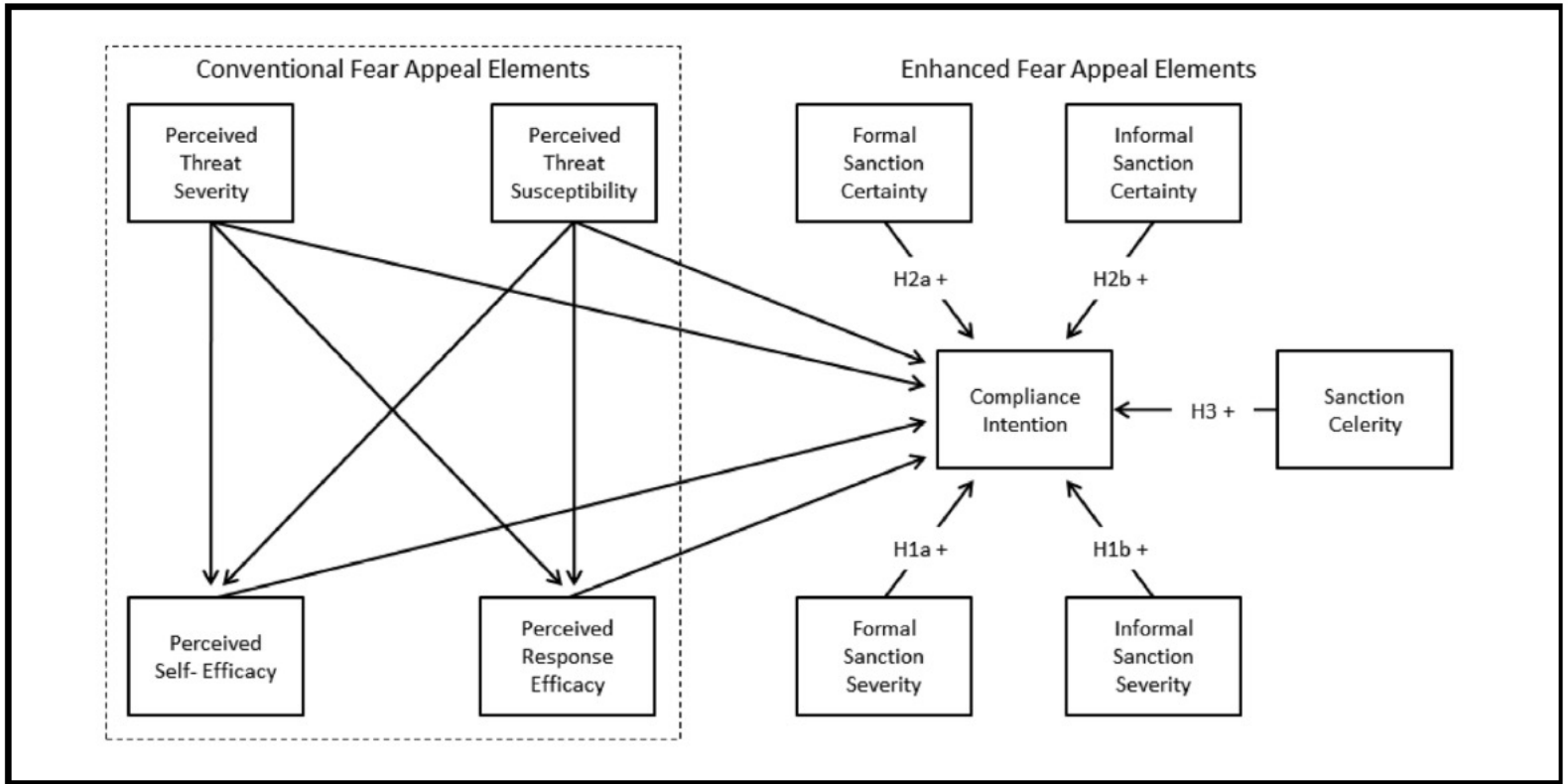


Figure 2. Research Model for Testing the Enhanced Fear Appeal Rhetorical Framework

Johnston, A.C., Warkentin, M., and Siponen, M. 2015. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1), PP.112-134.

Protection motivation theory & Self-Determination Theory

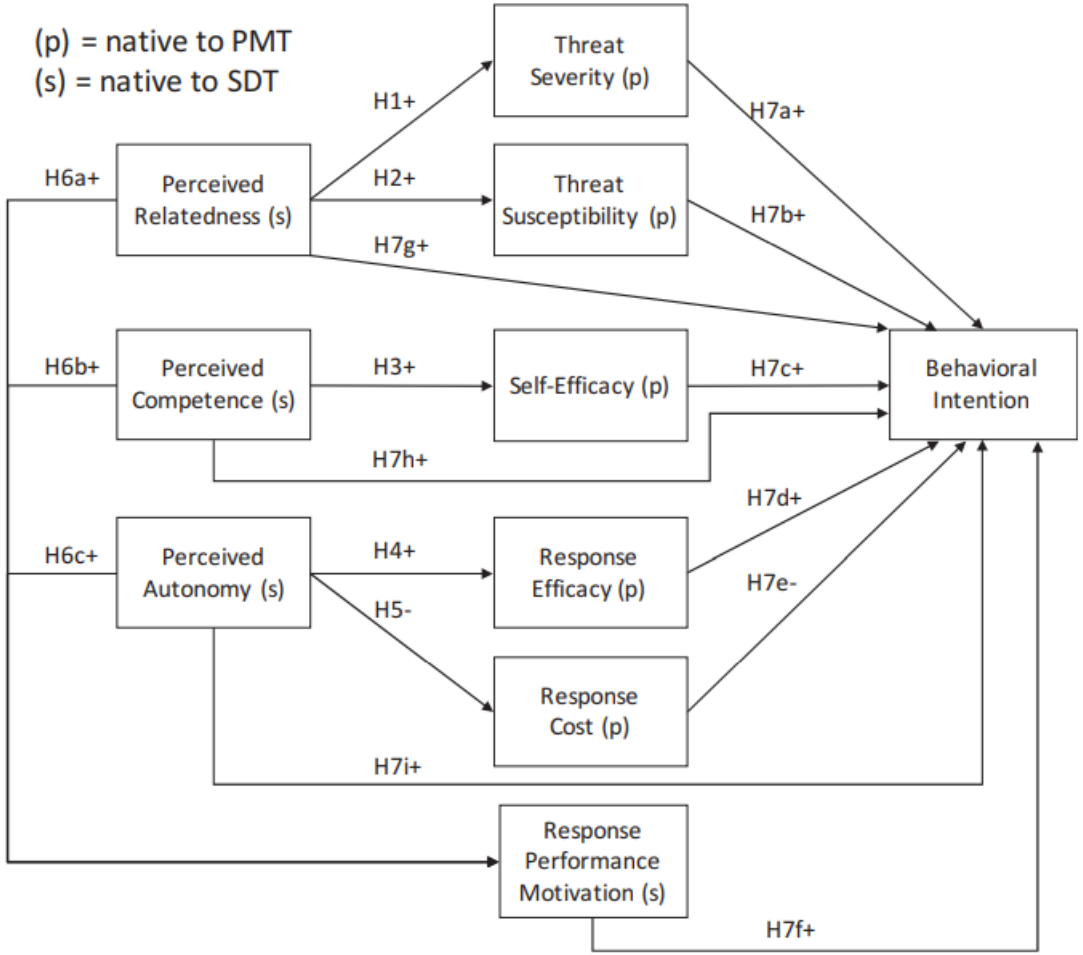
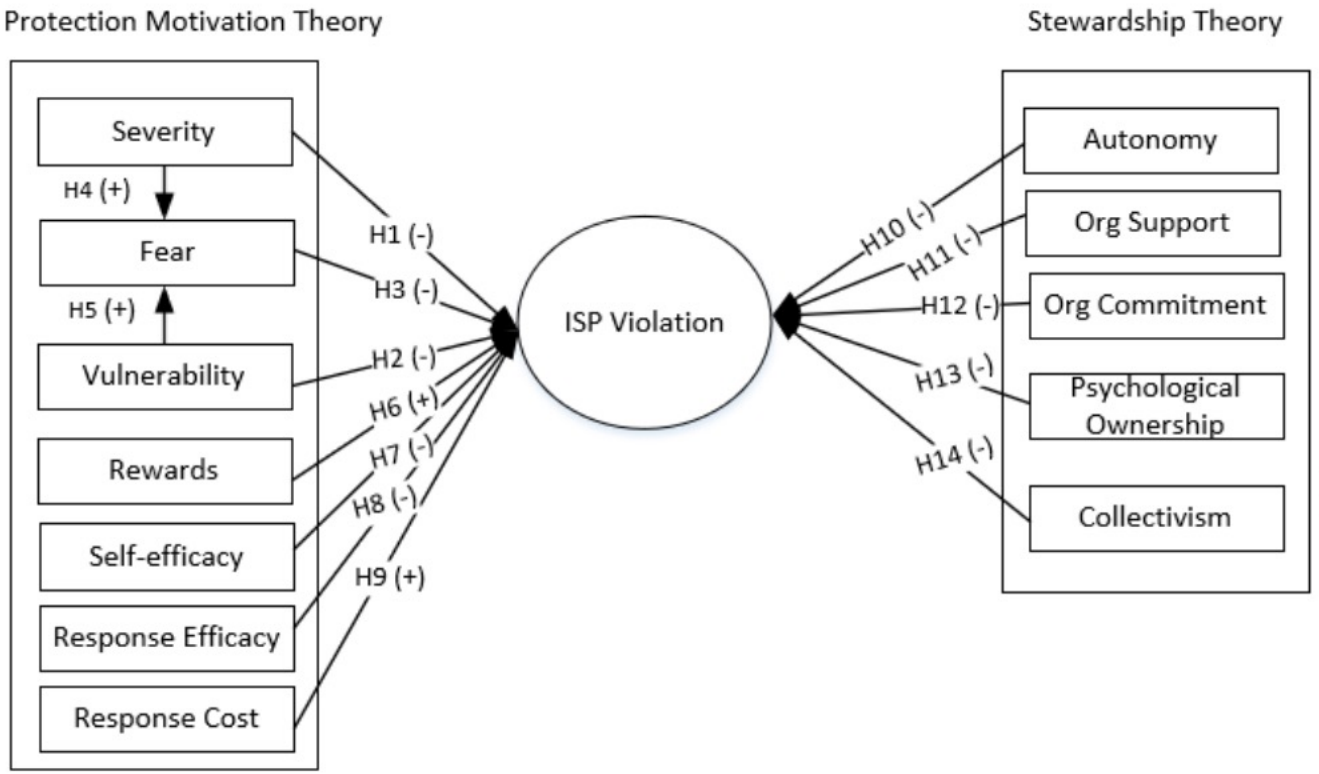


Figure 2. Integrated Model of SDT and PMT for Security Appeal Perceptions

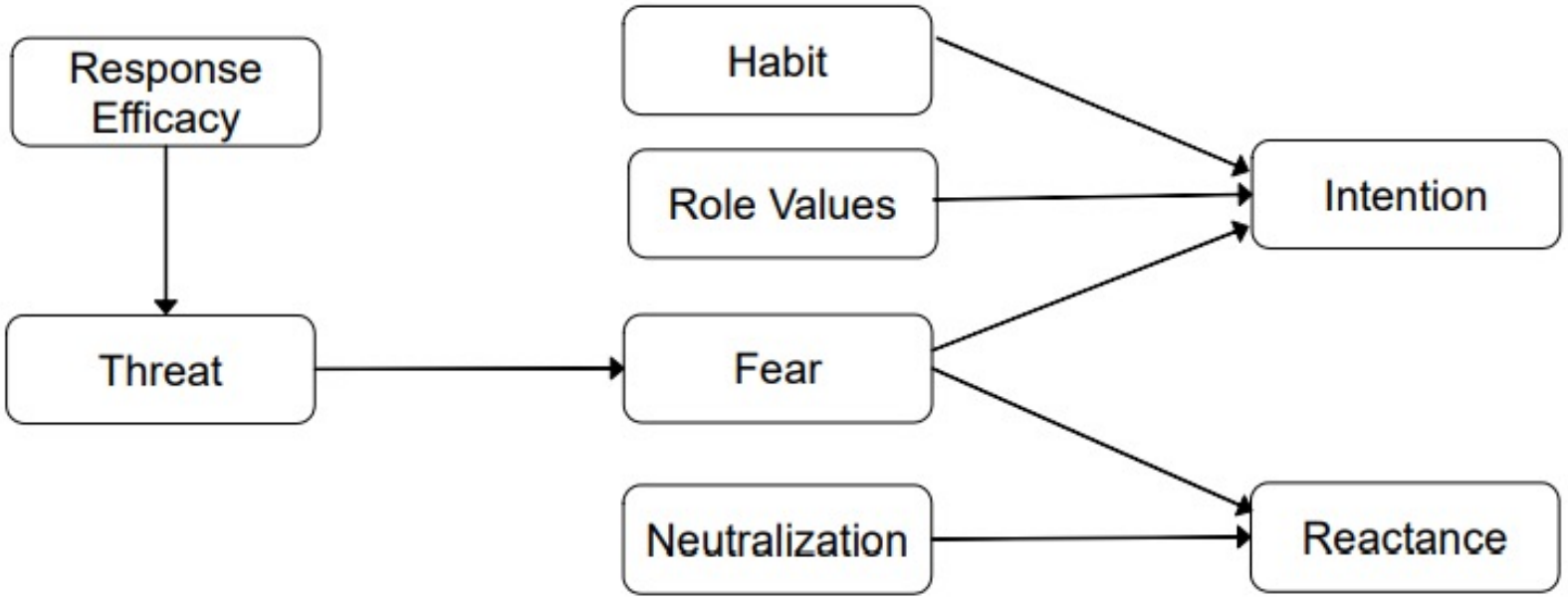
Menard, P., Bott, G.J., and Crossler, R.E., 2017. User motivations in protecting information security: protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, 34(4), pp.1203-1230.

Protection motivation and stewardship-based strategic theories



Ogbanufe, O., Crossler, R.E., and Biros, D. 2023. The valued coexistence of protection motivation and stewardship in information security behaviors. *Computer & Security*, 124.

Integration of 11 theories

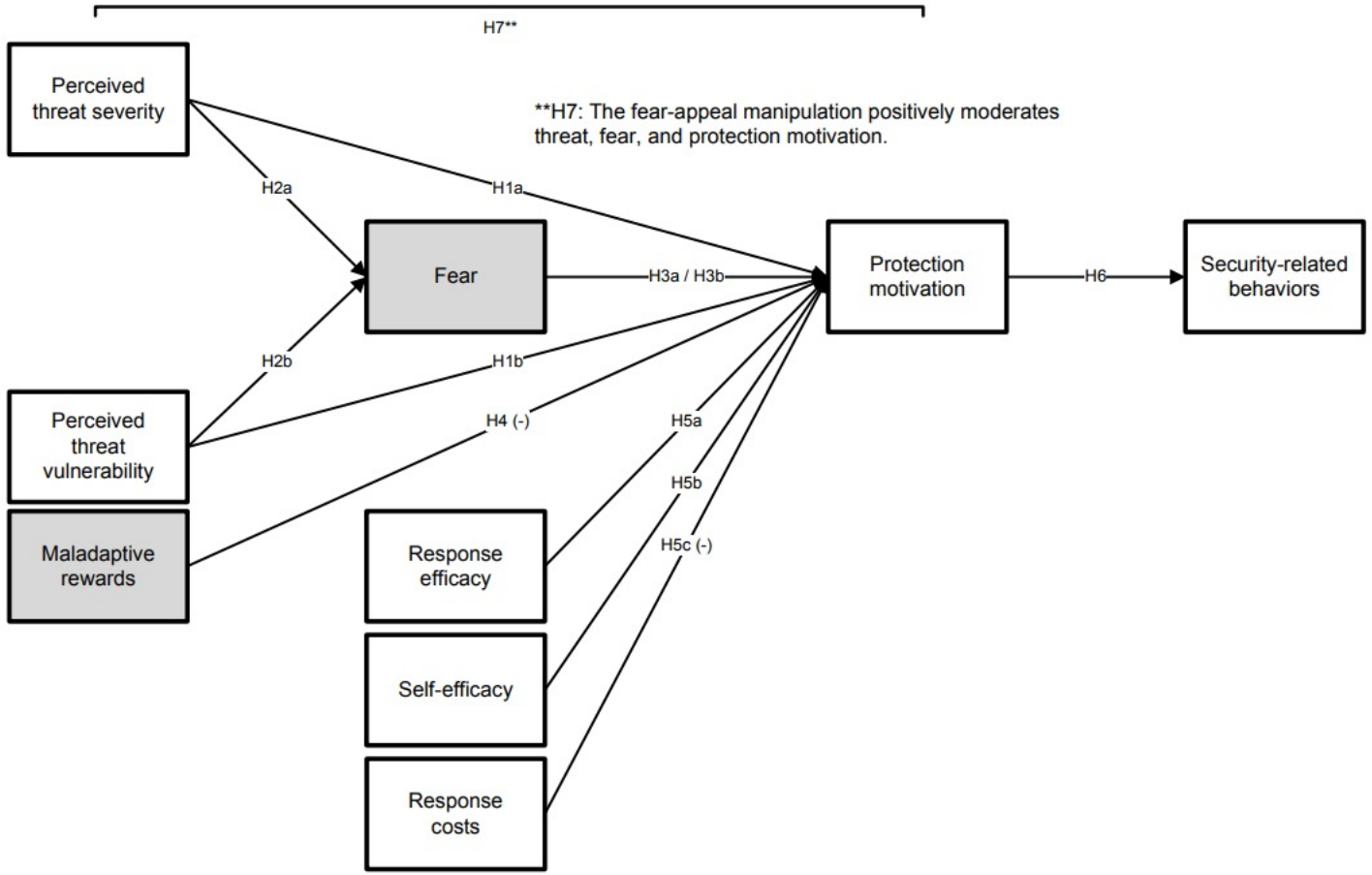


Moody, G.D., Siponen, M., and Pahnila, S. 2018. Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), pp.285-311.

11 theories:

1. The theory of reasoned action
2. Neutralization techniques
3. The health belief model
4. The theory of planned behavior
5. The theory of interpersonal behavior
6. The protection motivation theory
7. The extended protection motivation theory
8. Deterrence theory and rational choice theory
9. The theory of self-regulation
10. The extended parallel processing model
11. The control balance theory

Protection Motivation Theory (PMT)



Boss, S.R., Galletta, D.F., Lowry P.B., Moody, G.D., & Polak, P., 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), pp.837-864.

Meta-analysis

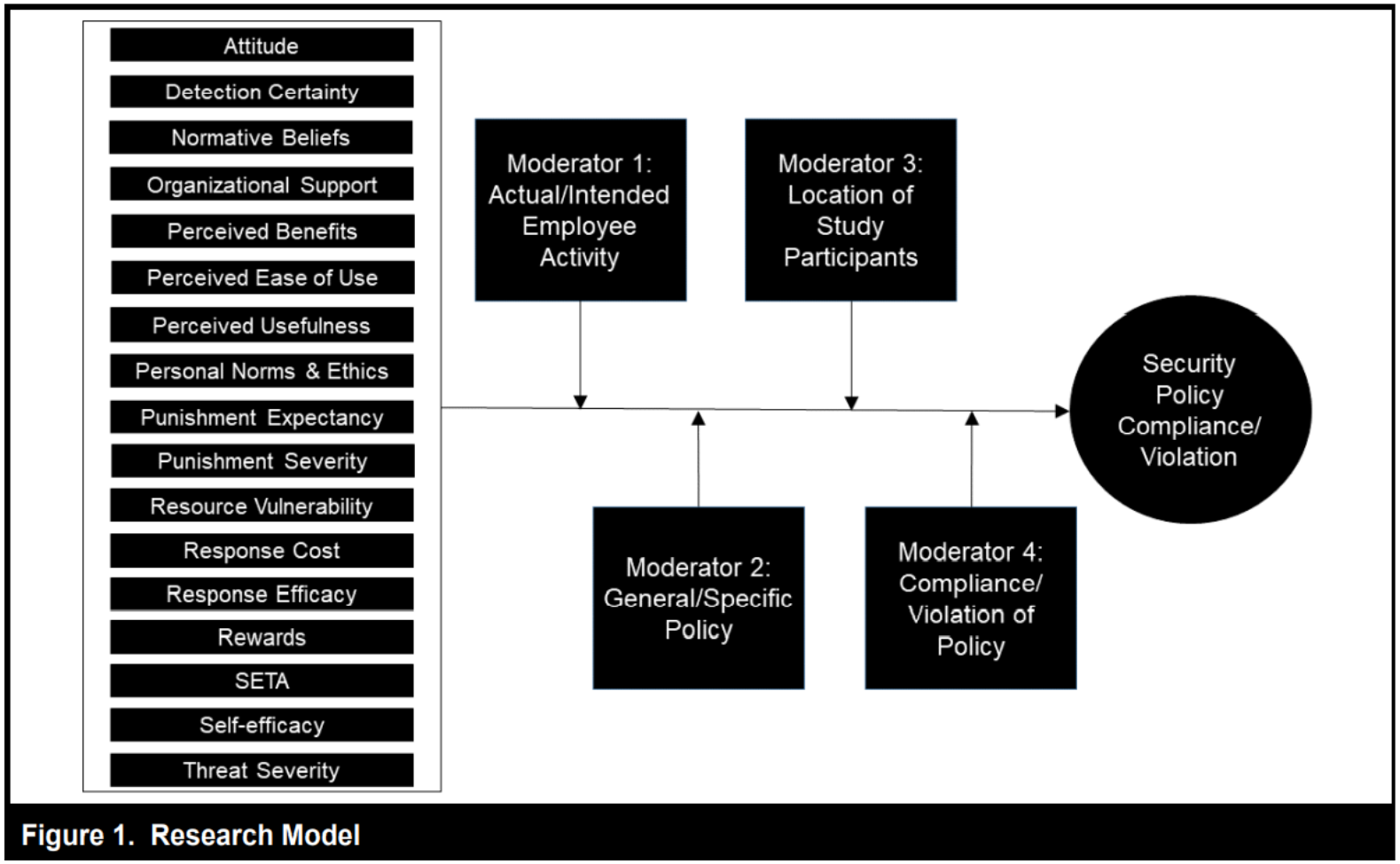
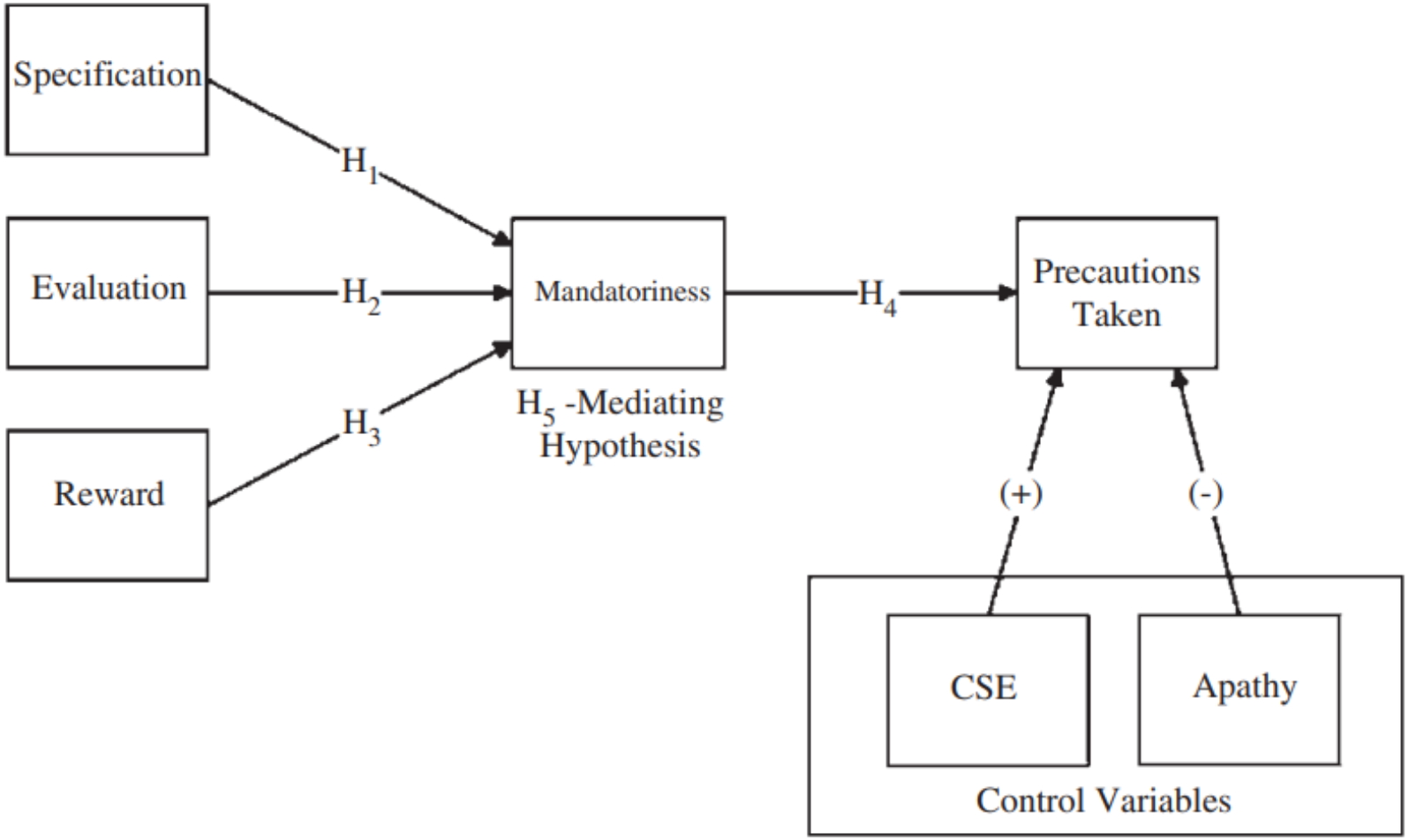


Figure 1. Research Model

Cram, W.A., D'Arcy, J., and Proudfoot, J. G., 2019. Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, 43(2), pp.525 – 554.

Organizational Control



Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, 18, pp.151 – 164.

Self-Determination Theory & Interest Theory

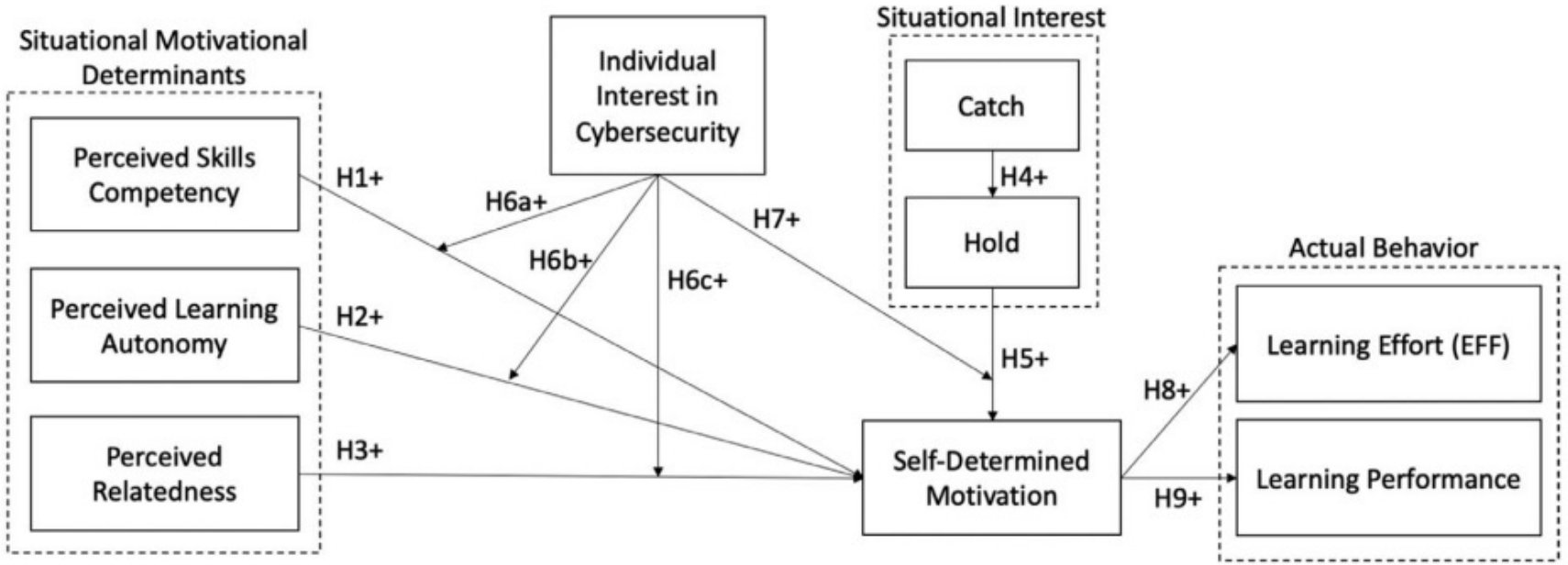
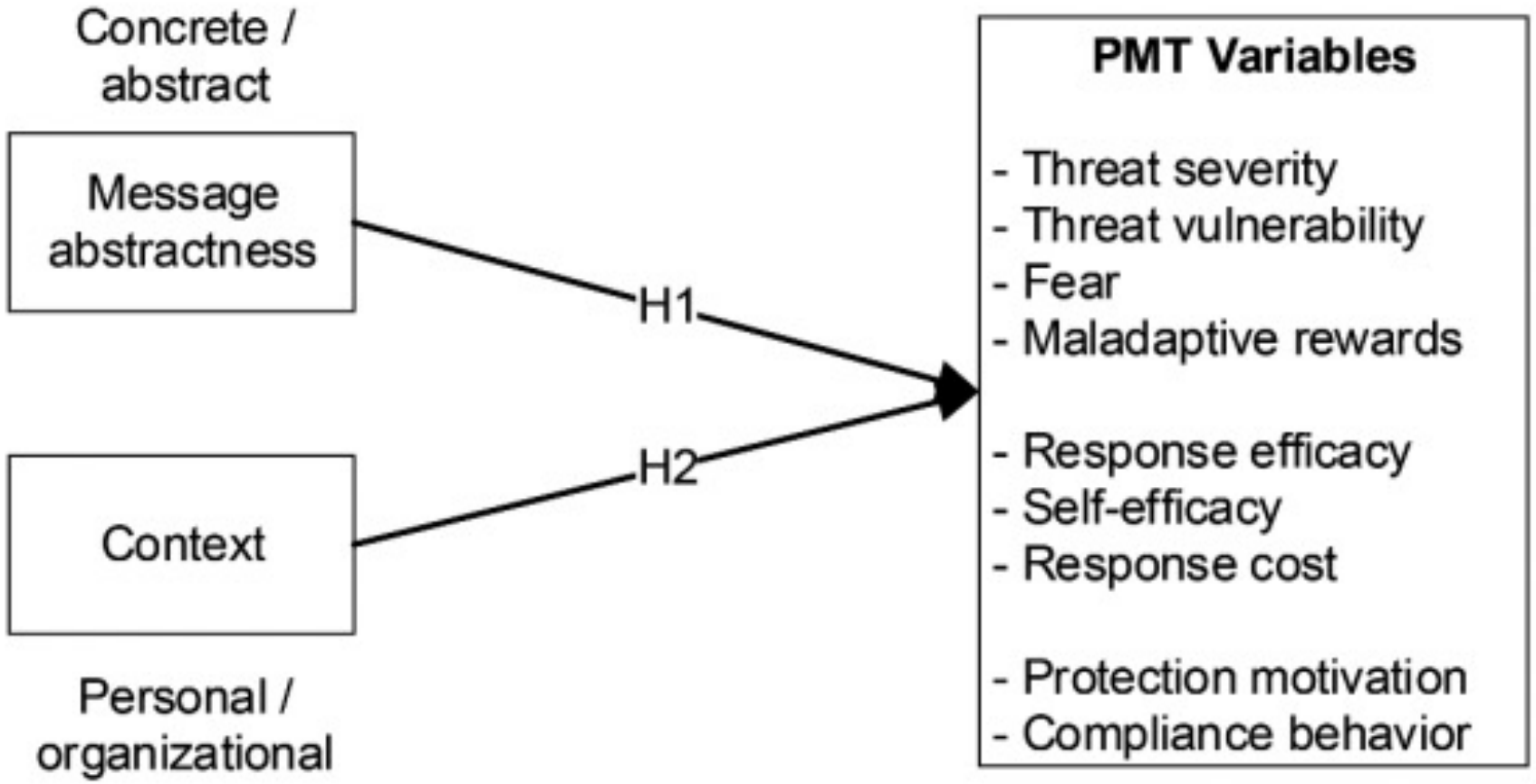


FIGURE 2 Proposed research model

Kam, H.J., Ormond, D.K., Menard, P., and Crossler, R. E., 2021. That's interesting: an examination of interest theory and self-determination in organizational cybersecurity training. *Information Systems Journal*, pp.888-926.

Construal Level Theory



Schuetz, S.W., Lowry, P.B., Pienta, D.A., and Thatcher, J.B. 2020. Effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, 3, pp.723-757.

The Perceptual Cycle Model

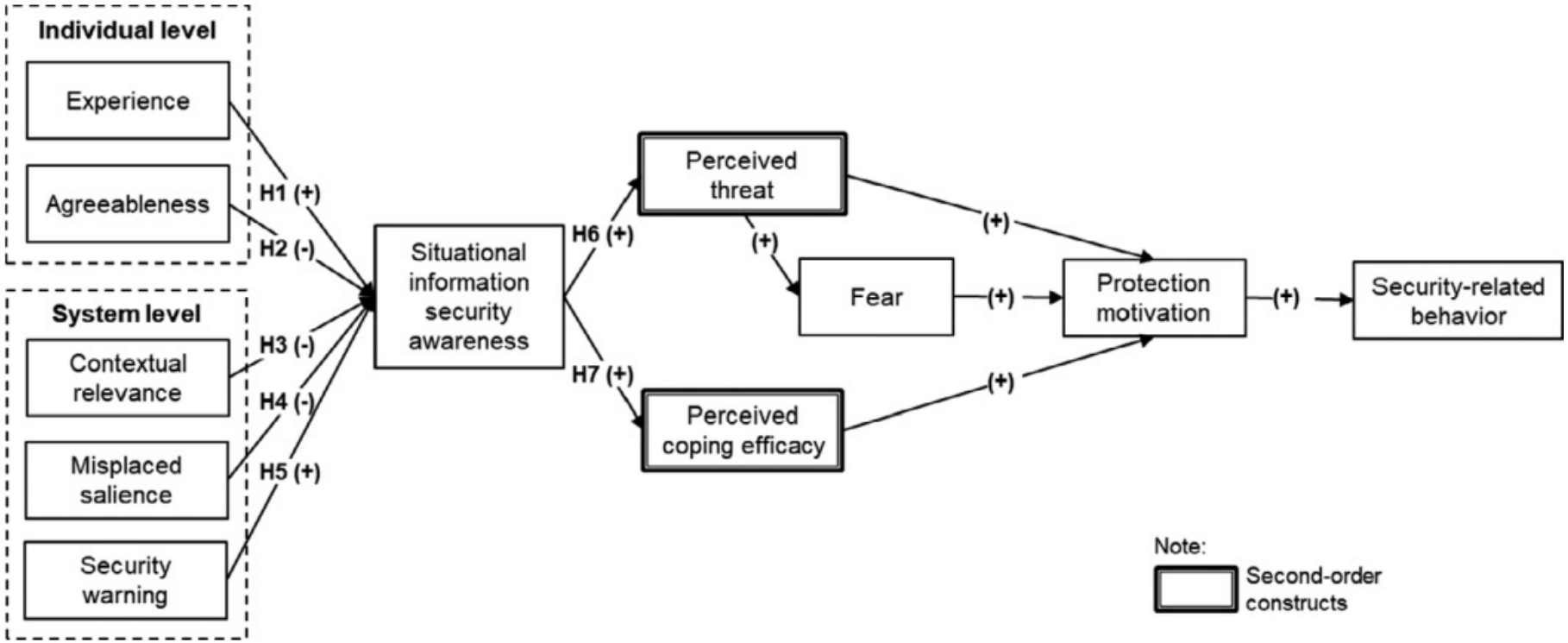


FIGURE 1 Research model

Jaeger, L. & Eckhardt, A. 2020. Eyes wide open: the role of situational information security awareness for security-related behaviour. *Information Systems Journal*, pp.429-472.

Affective Flow

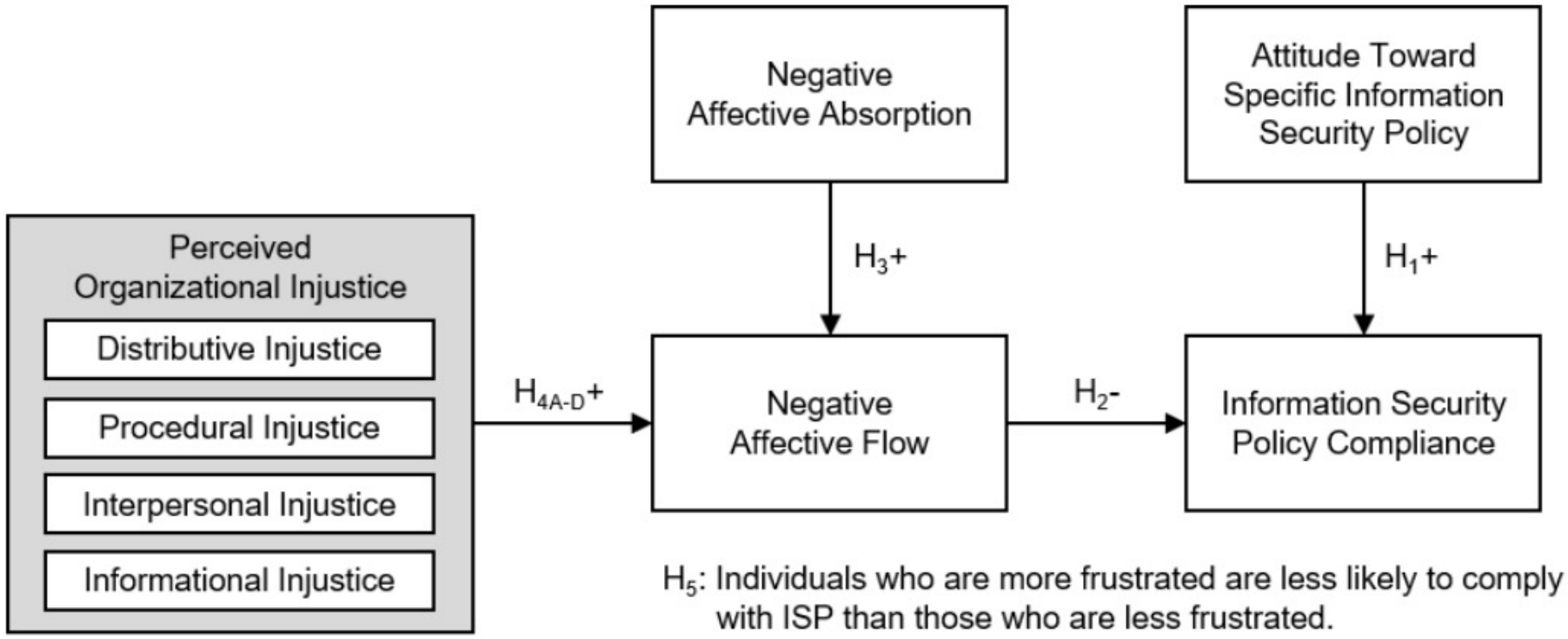


Figure 1. Conceptual Model with Hypotheses

Ormond, D., Warkentin, M. and Crossler, R.E. 2019. Integrating cognition with an affective lens to better understand information security policy compliance. *Journal of the Association for Information Systems*, 20 (12), pp.1974-1843.

Theory of panned behavior
Prekinetic events – work-related events
Affective events theory