MIS Quarterly

RESEARCH ARTICLE

TOWARD A UNIFIED MODEL OF INFORMATION SECURITY POLICY COMPLIANCE

Gregory D. Moody
University of Nevada, Las Vegas, 4505 S. Maryland Parkway,
Las Vegas, NV 89154 U.S.A. {gregory.moody@unlv.edu}

Mikko Siponen
Faculty of Information Technology, University of Jyväskylä, P.O. Box 35,
FI-40014 Jyväskylä FINLAND {mikko.t.siponen@jyu.fi}

Seppo Pahnila
Faculty of Information Technology and Electrical Engineering, University of Oulu, P.O. Box 8000,
FI-90014 Oulu FINLAND {seppo.pahnila@oulu.fi}

Appendix A

Instruments

Scenarios (Siponen and Vance 2010)

Note that all scenarios were altered to use one common last name, Mattila. Further, this survey was distributed in Finnish, and Finnish does not have gendered pronouns (e.g., her/his or he/she); everything is referred to with a non-gendered pronoun.

USB Drive

Mattila is a mid-level manager in a medium-sized business where he has worked for several years. Mattila is currently working on a sales report that requires the analysis of the company's customer database, which contains sensitive financial and purchase history information. Because of the sensitive nature of the corporate data, the company has a strict policy prohibiting the copy of corporate data to unencrypted media, such as USB drives. However, Mattila will travel for several days and would like to analyze the corporate database on the road. Mattila expects that copying the data to the USB drive and taking it on the road could save the company a lot of time and money.

Workstation Logout

Mattila is a mid-level manager in a medium-sized company where he was recently hired. His department uses an inventory procurement software application program to allow only authorized employees to make inventory purchases. The company has a firm policy that employees must log out of or lock their computer workstation when not using it. Mattila expects that keeping his user account logged-in could save him and coworkers time in ordering inventory.

Passwords

Mattila is a low-level manager in a small company where he was recently hired. His company has a strong policy that each computer workstation must be password protected and that passwords are not to be shared. However, Mattila is on a business trip and one of his coworkers needs a file on his computer. Mattila expects that sharing his password could save his coworker a lot of time and effort.

Note: Unless noted, all items are measured on a typical seven-point Likert scale from strongly disagree to strongly agree.

Miscellaneous Questions

1. What is your current age?
2. What is your gender?
3. How many years of work experience do you have?
4. How realistic do you think the above scenario is?
5. Do you think this scenario is realistic? Why or why not?

Intention (Piquero and Piquero 2006)

1. What is the chance that you would do what Mattila did in the described scenario?
2. I would act in the same way as Mattila did if I were in the same situation.

Protection Motivation Theory (Milne et al. 2000; Woon et al. 2005)

Perceived Severity

1. An information security breach in my organization would be a serious problem for me.
2. An information security breach in my organization would be a serious problem for my organization.
3. If I were to do what Mattila did, there would be a serious information security problem for my organization.
4. If I were to do what Mattila did, a serious information security problem would result.

Perceived Vulnerability

1. I would be subjected to an information security threat if I were to do what Mattila did.
2. My organization would be subjected to an information security threat if I were to do what Mattila did.
3. An information security problem would occur if I were to do what Mattila did.

Response Efficacy

1. Complying with information security procedures in our organization keeps information security breaches down.
2. If I were to comply with information security procedures, IS security breaches would be scarce.
3. If I were to do the opposite to what Mattila did, it would keep IS security breaches down.
4. If I were to do the opposite to what Mattila did, IS security breaches would be minimal.

Self-Efficacy

1. I can comply with information security procedures by myself.
2. I can use information security measures if someone tells me what to do as I go along.
3. Doing the opposite of what Mattila did would be difficult for me to do.
4. Doing the opposite of what Mattila did would be easy for me to do.

Response Cost (Woon et al. 2005)

1. Complying with information security procedures would be time consuming.
2. Complying with information security procedures would take work time.
3. Doing the opposite of what Mattila did would be time consuming.
4. Complying with information security procedures makes my work more difficult.
5. Complying with information security procedures inconveniences my work.
6. There are too many overheads associated with complying with information security procedures.
7. Complying with information security procedures would require considerable investment of effort other than time.

Rewards (Abraham et al. 1994)

1. If I were to do what Mattila did, I would save time.
2. If I were to do what Mattila did, I would save work time.
3. Not complying with information security procedures saves work time.

Habit (Verplanken and Orbell 2003)

1. Complying with information security procedures is something I do frequently.
2. Complying with information security procedures is something I do automatically.
3. Complying with information security procedures is something I do without having to consciously remember.
4. Complying with information security procedures is something that makes me feel weird if I do not do it.
5. Complying with information security procedures is something I do without thinking.
6. Complying with information security procedures is something that would require effort not to do it.
7. Complying with information security procedures is something that belongs to my (daily, weekly, monthly) routine.
8. Complying with information security procedures is something I start doing before I realize I’m doing it.
9. Complying with information security procedures is something I would find hard not to do.
10. Complying with information security procedures is something I have no need to think about doing.
11. Complying with information security procedures is something that’s typically “me.”
12. Complying with information security procedures is something I have been doing for a long time.

Attitude (Triandis 1977)

The scales for these items are anchored with the words listed below.

If I were to do what Mattila did it would be a very:

(a) bad idea-good idea
(b) foolish idea-wise idea
(c) unpleasant idea-pleasant idea
(d) negative idea-positive idea

Subjective Norm (Johnston and Warkentin 2010)

1. I believe that top management in my organization thinks I should do what Mattila did.
2. I believe that my immediate supervisor in my organization thinks I should do what Mattila did.
3. I believe that coworkers in my organization think I should do what Mattila did.
4. I believe that the security staff in my organization thinks I should do what Mattila did.

Perceived Behavioral Control (Ajzen 2002)

1. If you were to do as Mattila did, how much would you feel like you were in charge of the situation?
2. If you were Mattila, how much would you feel able to not do as he did?
3. If you were Mattila, how much would you feel you were in control?

Desire (Kanfer and Ackerman 1989)

1. I want to comply with the organization's security procedures.
2. My desire to comply with the organization's security procedures can be defined as something that is very important to me.

Costs/Benefits (McClenahan et al. 2007)

1. Mattila's behavior against the security procedures cause harm to the organization.
2. Mattila's behavior against the security procedures weakens the organization's security.
3. Mattila's behavior against the security procedures increases the vulnerability of the organization.

Facilitating Conditions (Bamberg and Schmidt 2003)

1. I am too busy to comply with information security procedures.
2. I have enough knowledge to follow information security procedures.
3. I need more guidance from my superiors with work-related information security policies.
4. I need more guidance from the IT/information security personnel regarding information security issues related to my work.
5. Support is available if I experience difficulties in complying with information security procedures.

Affect (Limayem and Hirt 2003)

1. What Mattila did is smart.
2. What Mattila did is enjoyable.
3. What Mattila did is boring.
4. What Mattila did is pleasant.

Roles (Bamberg and Schmidt 2003)

1. What Mattila did is compatible with his/her work.
2. What Mattila did fits with his/her work style.
3. What Mattila did can be justified due to the nature of Mattila's work.

Self-Concept (Gagnon et al. 2003)

1. I would feel guilty if I did what Mattila did.
2. What Mattila did is consistent with my principles.
3. It is acceptable to do what Mattila did.

Social Factors (Bergeron et al. 1995)

1. With respect to complying with information security procedures, I have to do as the top management of my organization thinks.
2. With respect to complying with information security procedures, I have to do as my colleagues think.
3. With respect to complying with information security procedures, I have to do as my superiors think.

Formal – Certainty (Siponen and Vance 2010)

1. What is the chance that you would be formally sanctioned (punished) if management learned that you had violated company information security policies?
2. I would receive corporate sanctions if I violated company information security procedures.
3. What is the chance that you would be warned if management learned you had violated company information security procedures?

Formal – Severity (Siponen and Vance 2010)

1. How much of a problem would it create in your life if you were warned for doing what Mattila did?
2. I would receive severe corporate sanctions if I violated company information security procedures.
3. How much of a problem would it create in your life if you were formally sanctioned for doing what Mattila did?

Informal – Certainty (Siponen and Vance 2010)

1. How likely is it that you would lose the respect and good opinion of your business associates for violating company information security procedures?
2. How likely is it that you would jeopardize your promotion prospects if management learned that you had violated company information security procedures?
3. How likely is it that you would lose the respect and good opinion of your manager for violating company information security policies?

Informal – Severity (Siponen and Vance 2010)

1. How much of a problem would it create in your life if you jeopardized your future job promotion prospects for doing what Mattila did?
2. How much of a problem would it create in your life if you lost the respect and good opinion of your business associates for violating company information security procedures?
3. How much of a problem would it create in your life if you lost the respect of your managers for violating company information security procedures?

Moral Definitions (Vance and Siponen 2012)

1. How morally wrong would it be to do what the person did in the scenario?
2. Is it morally right to violate company information security procedures?
3. I feel that violating company information security procedures is wrong.

Neutralization Techniques (Vance and Siponen 2010)

Condemnation of the Condemners

1. It is not as wrong to violate company information security procedures that are unreasonable.
2. It is not as wrong to violate company information security procedures that require too much time to comply with.
3. It is not as wrong to violate company information security procedures that are too restrictive.

Denial of Injury

1. It is OK to violate company information security procedures if no harm is done.
2. It is OK to violate company information security procedures if no damage is done to the company.
3. It is OK to violate company information security procedures if no one gets hurt.

Metaphor of the Ledger

1. I feel my general adherence to company information security procedures compensates for occasionally violating a policy.
2. I feel my good job performance compensates for occasionally violating information security procedures.
3. I feel my hard work in the company compensates for occasionally violating an information security procedure.

Appeal to Higher Loyalties

1. It is alright to violate company information security procedures to get a job done.
2. It is alright to violate company information security procedures if you get your work done.
3. It is alright to violate company information security policies if you complete the task given by management.

Defense of Necessity

1. It is alright to violate company information security procedures under circumstances where it seems like you have little other choice.
2. It is alright to violate company information security procedures when you are under a tight deadline.
3. It is alright to violate company information security procedures when you are in a hurry.

Denial of Responsibility

1. It is OK to violate company information security policies if you aren’t sure what the policy is.
2. It is OK to violate company information security procedures if the security procedures are not advertised.
3. It is OK to violate company an information security procedure if you don’t understand it.

Shame (Siponen and Vance 2010)

Certainty

1. I would be ashamed if business associates knew that I had violated company information security procedures.
2. How likely is it that you would be ashamed if others knew that you had violated company information security procedures?
3. How likely is it that you would be ashamed if managers knew that you had violated company information security procedures?

Severity

1. How much of a problem would it be if you felt ashamed that business associates knew you had violated company information security procedures?
2. How much of a problem would it be if you felt ashamed that others knew you had violated company information security procedures?
3. How much of a problem would it be if you felt ashamed that managers knew you had violated company information security procedures?

Reactance (Adapted from Witte et al. 1996)

To what degree do you

1. Think that the potential problems resulting from acting like Mattila did are realistic?
2. Feel that problems resulting from acting like Mattila did would not apply to you?
3. Feel that problems resulting from acting like Mattila did are overly exaggerated?
4. Think that problems resulting from acting like Mattila did are overstated?

Fear (Adapted from Osman et al. 1994)

1. Any problems that result from acting like Mattila did will never go away.
2. Something terrible will happen if I do what Mattila did.
3. Though doing what Mattila did is potentially harmful, I am going to be OK.
4. I am afraid of what may happen if I do what Mattila did.
5. Any problems that result from acting like Mattila did will go away with time.
6. Doing as Mattila did could cause a serious problem.
7. My computer might be compromised if I did what Mattila did.

8. Doing what Mattila did is terrifying.
9. I am afraid of doing what Mattila did.
10. My computer might become unusable if I did what Mattila did.
11. My computer might become slower if I did what Mattila did.

Defense Avoidance (Adapted from Witte et al. 1996)

When I first read the scenario about Mattila, my first instinct was to

1. "Want to"/"not want to" think about the problems that may result from acting like Mattila did.
2. "Want to"/"not want to" do something to prevent my computer from suffering any problems that would result if I were to act like Mattila did.

Self-Control (Curry 2005)

1. I often act on the spur of the moment without stopping to think.
2. I often do whatever brings me pleasure here and now, even at the cost of some distant goal.
3. I am more concerned with what happens to me in the short run than in the long run.
4. I will try to get things I want even when I know it's causing problems for other people.

Control Balance (Curry 2005; Tittle 1995, 2005)

Please indicate how much control (given the definition of control above) you assert and experience in the following:

1. Friendships in general
2. People you tend to hang out with
3. Relationships with significant others
4. Other people (such as neighbors, or solicitors)
5. Relationships with family members
6. Recreational activities
7. Physical body (such as avoiding or regulating illness or fatigue, or maintaining your appearance)
8. Physical environment (such as the ability to control heat, cold, regularity of food, or cleanliness)
9. Society as a whole
10. Job/place of employment
11. Salary/pay-scale
12. Workload
13. Time at work

Appendix B

Validation and Analysis Details for Analysis of Eleven Theories Used in Previous IS Behavioral Security Research

Table B1 describes the results of our measurement model and validity tests. To perform these tests, we first assess the measurement model for each theory; this is reported in the respective column. Second, as part of the test for validity and as a check for common method variance, we load all of the items on to one latent construct. Next, we create the pathways between the latent constructs, as prescribed by the theory. Finally, we report the X^2 for the saturated model, which represents all potential relationships between the latent constructs in the model.

To demonstrate that the theory has sound validity, we would expect to see that the theoretical model (Column 3) would be associated with the lowest X^2. Likewise, to demonstrate that common method variance is not a likely problem for the dataset, we would want to see that the data are better fitted, as demonstrated by a lower X^2, for the theoretical model than for the model with one latent construct (Column 2).

Column 1 is used to assess the fit of the items to the measurement model itself and is an indication of convergent and divergent validity. Ideally, it would be expected that the data would fit better to the theoretical model in Column 3. Further, the inclusion of the X^2 in Column 4 is a test to verify whether the theory is the best fit model or whether additional relationships that are not predicted in the theory better fit the data, indicating some missing relationships beyond the theory.

Table B1. Results of Tests of Data Fitness for Each Theory, Using X^2

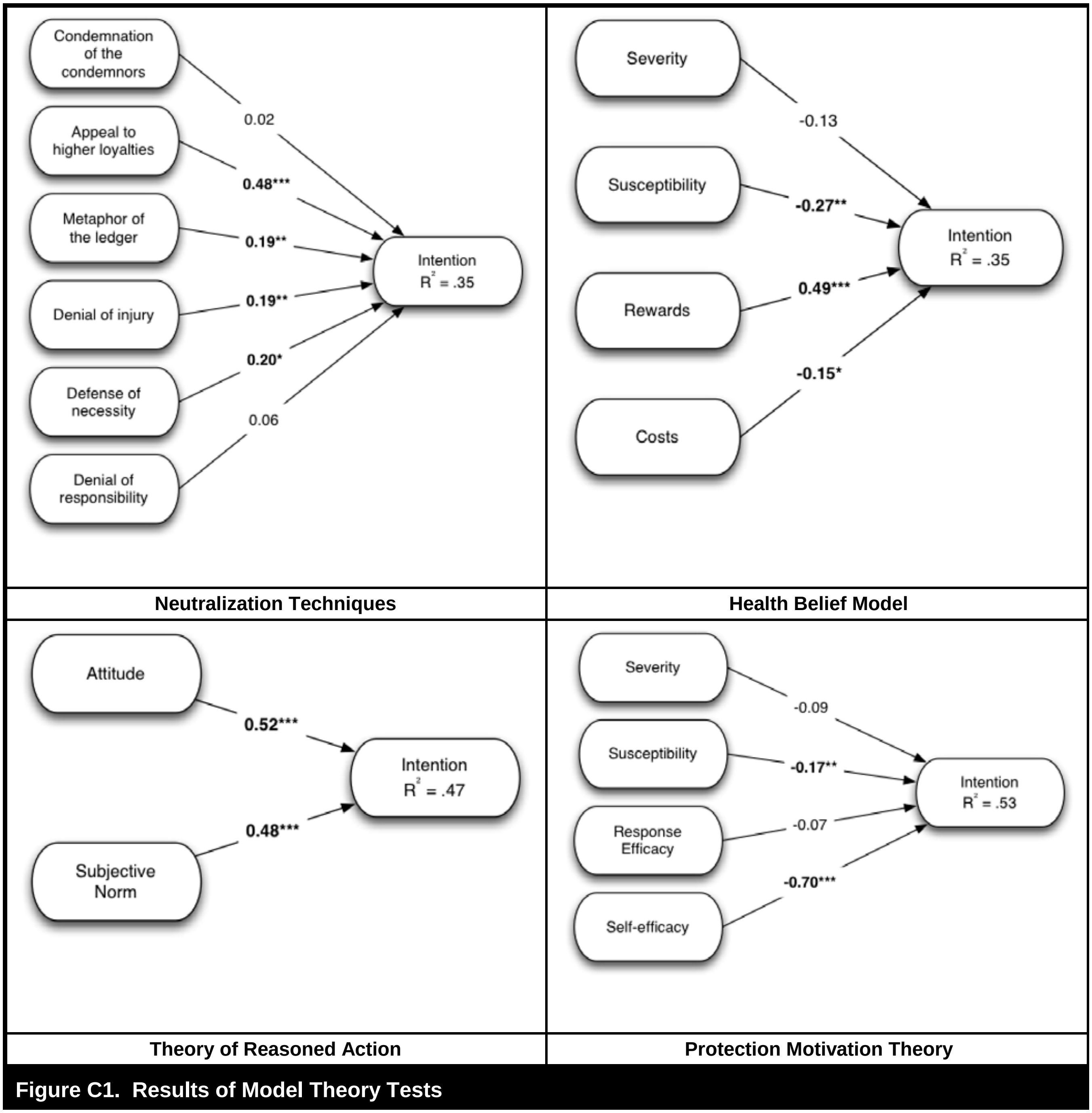
Theory	—1—	—2—	—3—	—4—
Neutralization techniques	495.89	266.34	235.09	394.07
Theory of self-regulation	452.98	238.36	112.20	94.92
Health belief model	844.12	2184.66	756.61	428.28
Theory of reasoned action	314.31	429.82	120.84	134.86
Protection motivation theory	1600.53	1255.67	720.77	545.36
Theory of interpersonal behavior	3442.23	6492.93	1773.46	1842.36
Deterrence theory	769.60	661.01	700.21	203.52
Extended protection motivation theory (PMT2)	1501.09	2334.81	1345.29	934.31
Theory of planned behavior	578.23	1036.81	393.93	269.09
Extended parallel processing model	1245.32	1741.10	816.54	622.78
Control balance theory	396.19	1217.96	364.84	191.69

1 – Measurement model
2 – Single latent construct model
3 – Theoretical model
4 – Saturated model
Note: This table does not report on every single latent construct combination that could be provided for each theory, for the sake of brevity.

Appendix C

Results of Theory Model Tests

The results of each theory are presented in chronological order of publication. These results are based on CB-SEM analyses, using STATA/SE 14.1.



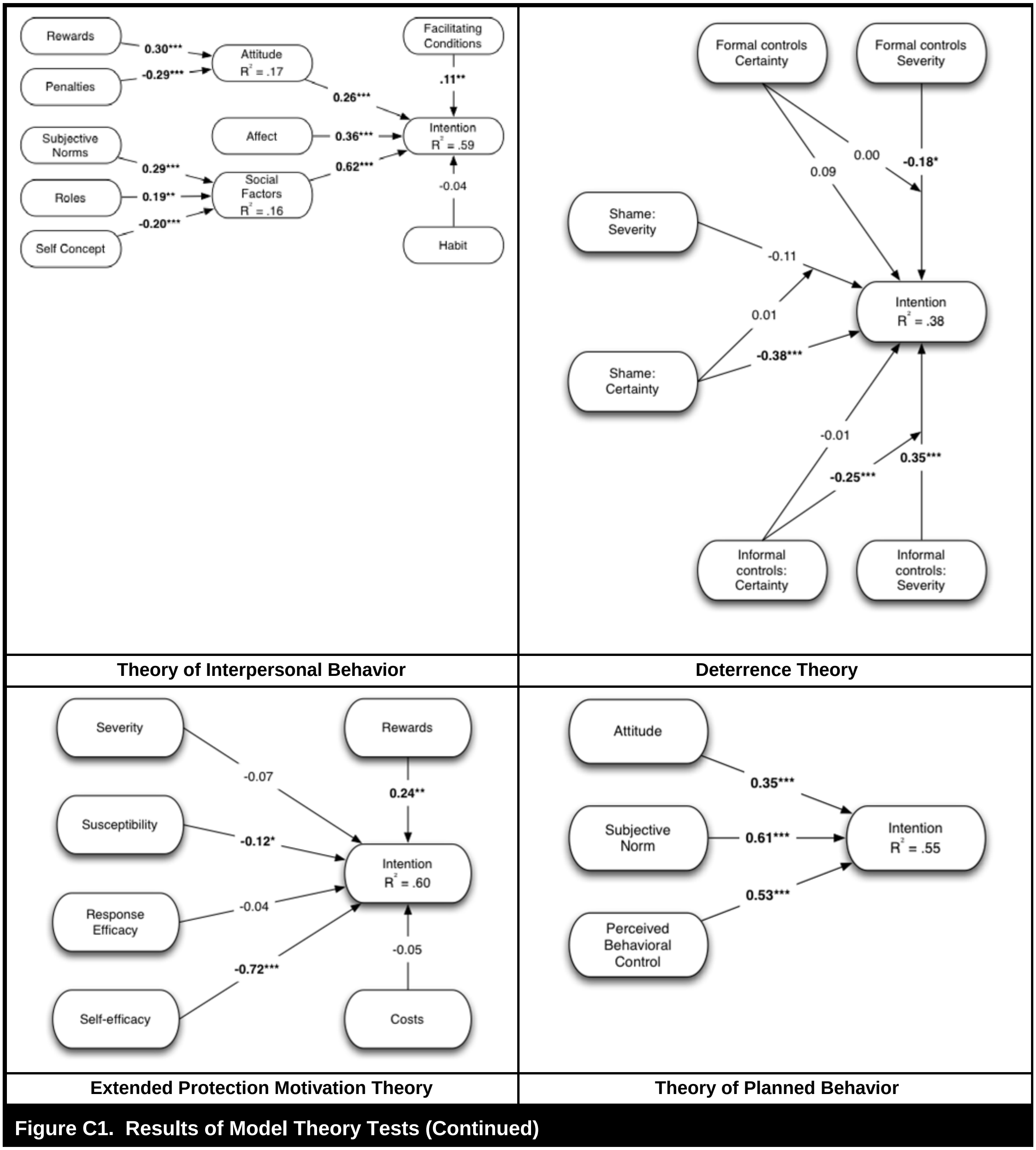
Neutralization Techniques

Health Belief Model

Theory of Reasoned Action

Protection Motivation Theory

Figure C1. Results of Model Theory Tests



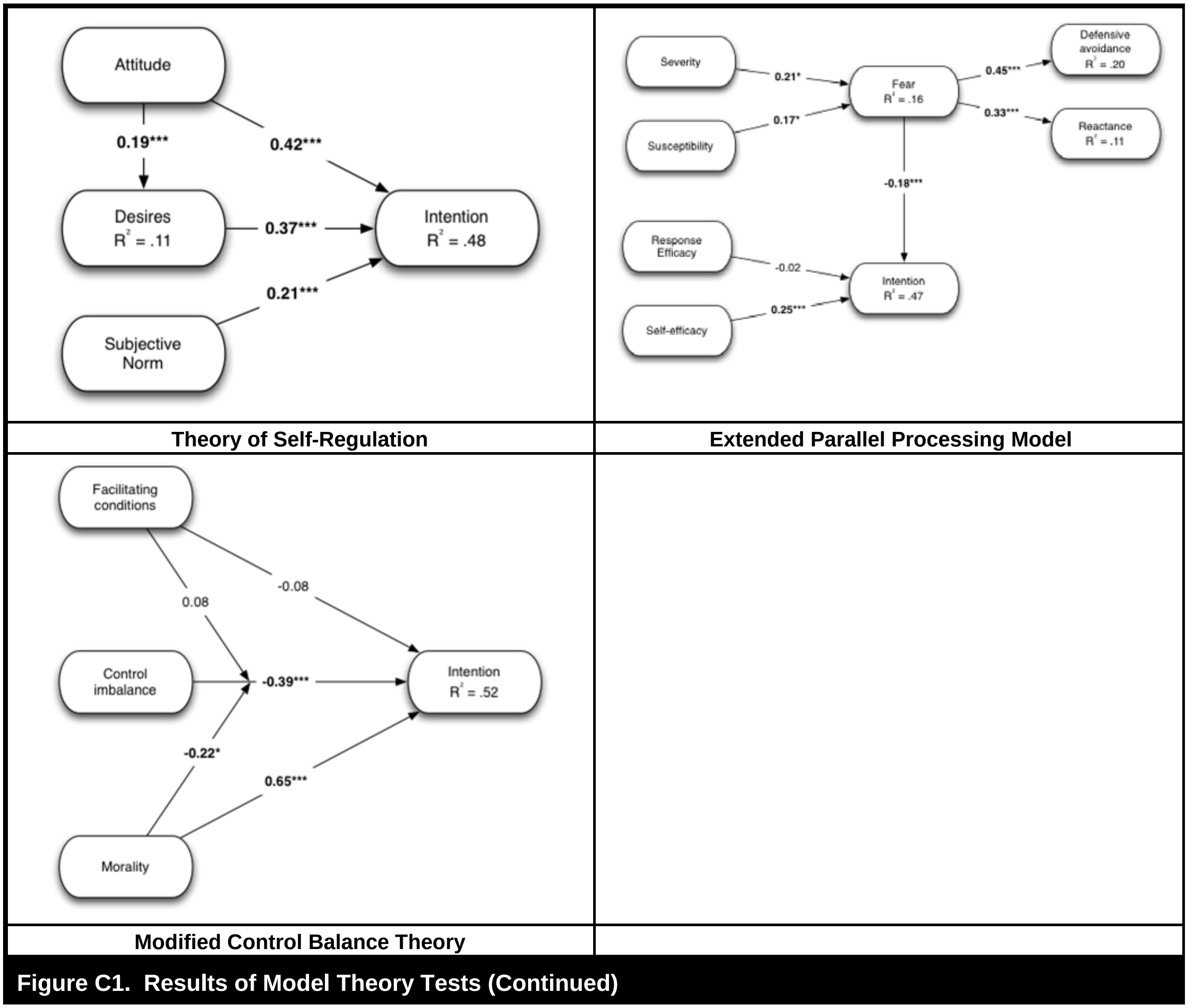
Theory of Interpersonal Behavior

Deterrence Theory

Extended Protection Motivation Theory

Theory of Planned Behavior

Figure C1. Results of Model Theory Tests (Continued)



Theory of Self-Regulation

Extended Parallel Processing Model

Modified Control Balance Theory

Figure C1. Results of Model Theory Tests (Continued)

Appendix D

Analysis Details for Data Reduction Analysis for UMISPC

Item Mapping for UMISPC

Table D1 show the results of the exploratory factor analysis we conducted to determine the factors needed to develop the UMISPC. Only loadings with absolute values above 0.40 were displayed to make it easier to see moderate to high loading items.

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1

Item	Factor1		Factor3	Factor4	Factor5	Factor6	Factor7	Factor8
Q1Intent1	0.5322	0.4535						
Q2Intent2	0.5514	0.4809						
Q3Sever1						0.5084		
Q4Sever2						0.5687		
Q5Sever3						0.6831		
Q6Vulner1						0.6550		
Q7Vulner2						0.8079		
Q8Vulner3						0.8019		
Q9RespEffi1								
Q10RespEffi2								
Q11RespEffi3								
Q12RespEffi4								
Q13SelfEffi1								
Q14SelfEffi5								
Q15SelfEffi2								
Q16SelfEffi3								
Q17SelfEffi4								
Q18Responsecost1			0.8074					
Q19Responsecost2			0.7311					
Q20Responsecost4			0.7403					
Q21Responsecost5			0.6846					
Q22Rewards/Costs1			0.6540					
Q23Rewards/Costs2			0.6285					
Q24Rewards/Costs3			0.5630					
Q25Rewards1			0.8169					
Q26Rewards2			0.8349					
Q27Rewards3			0.7513					
Q29Rewards4			0.6941					
Q31Habit1				0.7587				
Q32Habit10				0.7635				
Q33Habit11				0.7759				
Q34Habit12				0.5634				
Q35Habit2				0.6172				

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor1		Factor3	Factor4	Factor5	Factor6	Factor7	Factor8
Q36Habit3				0.4613				
Q37Habit4				0.7488				
Q38Habit5				0.6078				
Q39Habit6				0.5768				
Q40Habit7								
Q41Habit8				0.7505				
Q42Habit9				0.7372				
Q43Atti1						-0.4250		
Q43Atti2								
Q43Atti3								
Q43Atti4								
Q44Subnorm1	-0.4233							
Q45Subnorm2								
Q46Subnorm3	-0.5712							
Q47Subnorm4								
Q49PercBehCont1								
Q50PercBehCont2	-0.6449							
Q51PercBehCont3								
Q52Desire1	-0.5234							
Q53Desire2	-0.5292							
Q54CostBenefits1	-0.6151							
Q55CostBenefits2	-0.4990							
Q56CostBenefits3	-0.5454							
Q57FacCon1								
Q58FacCon2								
Q59FacCon3								
Q60FacCon4								
Q61FacCon5								
Q62Affect1	0.7398							
Q63Affect2	0.6698							
Q64Affect3	-0.7604							
Q65Affect4	0.7658							
Q66Roles1	0.7551							
Q67Roles2	0.7529							
Q68Roles3	0.7294							
Q69SelfCon1	-0.7164							
Q70SelfCon2	0.7460							
Q71SelfCon3	0.8250							
Q72NeutCondB	0.5133							
Q73SocialFact1								
Q75SocialFact2								
Q76SocialFact3								

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor1		Factor3	Factor4	Factor5	Factor6	Factor7	Factor8
Q77NeutLoyB	0.6585							
Q78NeutLedgC	0.6479							
Q79NeutInjA	0.6106							
Q80NeutInjB	0.6340							
Q81ShameSevC	-0.4544							
Q82ShameCertA	-0.5447							
Q83MoralA	-0.7466							
Q84FormSevA								
Q85FormCertC					0.6566			
Q86NeutNecB		0.6143						
Q87InformCertB					0.6754			
Q88InformSevA							0.4720	
Q89NeutRespB		0.5273						
Q90NeutLedgA		0.6037						
Q91NeutRespA								
Q92FormCertA					0.7821			
Q93ShameSevA					0.4172		0.6880	
Q94InformSevC							0.7212	
Q95MoralB		0.4760						
Q96ShameCertB							0.6560	
Q97FormSevC							0.6207	
Q98NeutCondC		0.6988						
Q99InformCertC					0.6925			
Q100NeutLoyC		0.6546						
Q101InformSevB							0.7309	
Q102NeutCondA		0.6734						
Q103InformCertA					0.6375		0.4147	
Q104NeutLedgB		0.6670						
Q105MoralC		-0.4122						
Q106NeutNecC		0.6433						
Q107ShameSevB							0.7717	
Q108NeutInjC		0.8300						
Q109FormCertB					0.8468			
Q110NeutLoyA		0.8097						
Q111FormSevB					0.7893			
Q112NeutNecA		0.7179						
Q113ShameCertC					0.4027		0.6931	
Q114Fear2					0.4844			
Q115Fear3		0.5360						
Q116Fear4								
Q117Fear5		0.4509						
Q118Fear6								

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor1		Factor3	Factor4	Factor5	Factor6	Factor7	Factor8
Q119Fear7								0.7379
Q120Fear8								
Q121Fear9		0.5360						
Q122Fear10								0.9334
Q123Fear11								0.8710
Q124aDefenceAvoid1								
Q124bDefenceAvoid2								
Q125aReactance1								
Q125bReactance2								
Q125cReactance3		0.4631						
Q125dReactance4		0.4689						
Q126NeutRespC		0.4237						

Note: All factor loadings < |.40| have been suppressed from the output.

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor9	Factor10	Factor11	Factor12	Factor13	Factor14	Factor15	Factor16
Q1Intent								
Q2Intent								
Q3Sever1								
Q4Sever2								
Q5Sever3								
Q6Vulner1								
Q7Vulner2								
Q8Vulner3								
Q9RespEffi1								0.7268
Q10RespEffi2								0.7657
Q11RespEffi3				0.9469				
Q12RespEffi4				0.7751				
Q13SelfEffi1								
Q14SelfEffi5							0.9860	
Q15SelfEffi2							0.6517	
Q16SelfEffi3								
Q17SelfEffi4								
Q18Responsecost1								
Q19Responsecost2								
Q20Responsecost4								
Q21Responsecost5								
Q22Rewards/Costs1								
Q23Rewards/Costs2								

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor 9	Factor10	Factor1 1	Factor1 2	Factor1 3	Factor1 4	Factor1 5	Factor1 6
Q24Rewards/Costs3								
Q25Rewards1								
Q26Rewards2								
Q27Rewards3								
Q29Rewards4								
Q31Habit1								
Q32Habit10								
Q33Habit11								
Q34Habit12								
Q35Habit2								
Q36Habit3								
Q37Habit4								
Q38Habit5								
Q39Habit6								
Q40Habit7								
Q41Habit8								
Q42Habit9								
Q43Atti1		0.4259						
Q43Atti2		0.4982						
Q43Atti3		0.6877						
Q43Atti4		0.7946						
Q44Subnorm1			0.4826					
Q45Subnorm2			0.4202					
Q46Subnorm3								
Q47Subnorm4			0.4830					
Q49PerchBehCont1								
Q50PerchBehCont2								
Q51PerchBehCont3								
Q52Desire1								
Q53Desire2								
Q54CostBenefits1			0.4058					
Q55CostBenefits2			0.4840					
Q56CostBenefits3			0.4611					
Q57FacCon1								
Q58FacCon2	-0.6061							
Q59FacCon3	0.8458							
Q60FacCon4	0.8822							
Q61FacCon5	-0.4555							
Q62Affect1								
Q63Affect2								
Q64Affect3								
Q65Affect4								

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)								
Item	Factor 9	Factor10	Factor1 1	Factor1 2	Factor1 3	Factor1 4	Factor1 5	Factor1 6
Q66Roles1								
Q67Roles2								
Q68Roles3								
Q69SelfCon1								
Q70SelfCon2								
Q71SelfCon3								
Q72NeutCondB								
Q73SocialFact1								
Q75SocialFact2								
Q76SocialFact3								
Q77NeutLoyB								
Q78NeutLedgC								
Q79NeutInjA								
Q80NeutInjB								
Q81ShameSevC					0.6755			
Q82ShameCertA					0.6273			
Q83MoralA								
Q84FormSevA								
Q85FormCertC								
Q86NeutNecB								
Q87InformCertB								
Q88InformSevA								
Q89NeutRespB								
Q90NeutLedgA								
Q91NeutRespA								
Q92FormCertA								
Q93ShameSevA								
Q94InformSevC								
Q95MoralB								
Q96ShameCeertB								
Q97FormSevC								
Q98NeutCondC								
Q99InformCertC								
Q100NeutLoyC								
Q101InformSevB								
Q102NeutCondA								
Q103InformCertA								
Q104NeutLedgB								
Q105MoralC								
Q106NeutNecC								
Q107ShameSevB								
Q108NeutInjC								

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor9	Factor10	Factor11	Factor12	Factor13	Factor14	Factor15	Factor16
Q110NeutLoyA								
Q111FormSevB								
Q112NeutNecA								
Q113ShameCertC								
Q114Fear2								
Q115Fear3								
Q116Fear4								
Q117Fear5								
Q118Fear6								
Q119Fear7								
Q120Fear8								
Q121Fear9								
Q122Fear10								
Q123Fear11								
Q124_aDefenceAvoid1								
Q124_bDefenceAvoid2								
Q125aReactance1								
Q125bReactance2								
Q125cReactance3						0.7595		
Q125dReactance4						0.7908		
Q126NeutReespC								

Appendix E

Validation and Analysis Details for UMISPC

Table E1 summarizes the model validation of the measurement model for UMISPC. All item loadings were significant at the p < .0001 level. Table E2 summarizes further validation procedures for this model. Namely, it verifies that the data fit, based on X^2, of the measurement model is improved by moving to the theoretical model. We also verify that the fitted model is more fit to the data than the saturated model of UMISPC, which provides assurance of no misspecification errors and indicates that our model is not lacking any relationships or constructs. Finally, comparing the model fit with a model that has all items loaded on to one latent construct in order to test for the common method bias shows a strong lack of support for that bias, indicating that method bias is not likely present in our sample.

Table E1. Item Loadings for UMISPC Validation

Identified Factor	Item	Loading
Social factors	roles2	.857
	roles3	.784
	moral1	.812
	affect1	.911
	affect4	.786
	selfcon1	.889
	selfcon2	.752
	selfcon3	.833
	percbehcont2	.866
Punishment	formalcert1	.755
	formalcert2	.959
	formalcert3	.796
	formalsev2	.904
	informalcert1	.781
	informalcert2	.753
	informalcert3	.743
Rewards/Costs	respcost1	.858
	respcost2	.818
	respcost4	.780
	respcost5	.892
	reward1	.881
	reward3	.700
	reward4	.701
Habit	habit1	.785
	habit2	.800
	habit3	.762
	habit5	.849
	habit7	.799
	habit8	.783
	habit11	.862
	habit12	.847
Neutralization	neutcond3	.791
	neutloyal1	.916
	neutinjury3	.811

Table E1. Item Loadings for UMISPC Validation

Identified Factor	Item	Loading
Threat	vulner1	.884
	vulner2	.894
	vulner3	.908
	sever3	.854
Fear	fear7	.858
	fear10	.969
	fear11	.943
Response efficacy	respeff2	.836
	respeff3	.861
	respeff4	.861
Facilitating conditions	facicond3	.798
	facicond4	.859
Reactance	react3	.842
	react4	.994
Intention	intent1	.958
	intent2	.982

Table E2. Item Loadings for UMISPC Validation

Measurement Model	Single Latent Factor Model (CM Bias Model)	Theoretical Model	Fully Saturated Model
2524.99	6594.95	1665.91	1985.50

Appendix F

Strengths and Weaknesses of Different Measurement Approaches

These approaches have different strengths and potential weaknesses regarding *specifying violation type*, *allowing capturing context*, *intimidation concern*, *capturing current behavior*, and *capturing future intention* (Table 3). Besides the fact that both can be used to specify the type of violation (or insecure act), the scenario approach allows presentation of the context. The scenario approach presents a scenario that describes a case and context where the scenario character typically violates a law, norm, or policy (Pogarsky 2004; Siponen and Vance 2010). Describing the context is difficult, if not impossible, with typical survey statements capturing actual behavior like "I select an easy-to-break password" or "I lock my computer." Including context can have two benefits. First, it puts respondents in a specific situation where the insecure act is committed (Pogarsky 2004). Besides specifying and clarifying the situation, this is believed to have the potential to increase realism (D'Arcy et al. 2009; Hu et al. 2011; Pogarsky 2004). Second, one can vary the contextual information in the scenario (Siponen and Vance 2014). Importantly, context can explain the results, too (Dudwick et al. 2006). Scenarios allow examination of the extent to which the model (or its independent variables) holds for different IS security violation types when the contexts of the violations are different. If the model can explain the different violation types (or insecure acts), but the relationships are also significant with different context descriptions, then this provides further evidence that the model is applicable in explaining various insecure acts and that the contexts do not explain the results.

The behavior statement approach is a good choice if there is a theoretical reason to avoid any contextual information. For example, let us assume that scholars used the scenario approach and the same model and received different results for different scenarios, and it is believed that the context could explain the results. Then, one could try avoiding the entire context and including behavior questions such as "I lock my computer" and so on. This could help to determine if the context characteristics, rather than the different insecure types, influence the different results. We did not have this concern and we preferred to have a context to increase realism and to see if the results hold with the different scenarios (with different contexts) (Siponen and Vance 2014).

Intimidation concern is another reason to use scenarios in our case. When it comes to self-report studies, the scenario approach has been reported as the most commonly used technique for examining ethically sensitive acts in business ethics (O'Fallon and Butterfield 2005) and illegal acts in criminology (Pogarsky 2004). In these fields, it is believed that in the scenario setting, respondents are in a less threatened position to admit such an act, because scenarios describe third-person behavior (Trevino 1992; Pogarsky 2004). Fisher (1993) reports that indirect questioning reduces social desirability bias, compared with questions that ask the persons to report their own current behavior. A number of IS security scholars note the decreased intimation concern as a key reason for using the scenario approach (Barlow et al. 2013; D'Arcy et al. 2009; Guo et al. 2011; Hu et al. 2011; Siponen and Vance 2010).

The last issue is *capturing current behavior* versus *capturing prospective behavior intention*. The behavior approach captures current or retrospective self-reported behavior, while the scenario approach captures prospective self-reporting behavior (Pogarsky 2004) (Table 3). The self-report behavior captures current behavior or retrospective behavior without giving context (Pogarsky 2004). The scenario approach poses subjects with a hypothetical situation, followed by a question asking the likelihood that they would behave in the same way under similar circumstances (Paternoster and Simpson 1996; Pogarsky 2004). Therefore, scenario-based self-report captures "the prospective behavior" intention (Pogarsky 2004). The weakness of self-reported current or retrospective behavior is the link between current and future behavior, because it provides no evidence of future behavior (Pogarsky 2004). Similarly, the concern in prospective scenario-based measures is whether "how individuals intend to behave" in future translates to actual future behavior (Pogarsky 2004 p. 114). Available evidence suggests that self-reported scenario responses to projected rule violations correspond to actual rule violations in the future (Pogarsky 2004). Rogers (1983) notes that "protection motivation is best measured by behavioral intention" (p. 172). This makes sense if the focus is on prospective behavior.

References

Abraham, C. S., Sheeran, P., Abrams, D., and Spears, R. 1994. "Exploring Teenagers' Adaptive and Maladaptive Thinking in Relation to the Threat of HIV Infection," *Psychology & Health*, (9:4), pp. 253-272.

Ajzen, I. 2002. "Residual Effects of Past on Later Behavior: Habituation and Reasoned Action Perspectives," *Personality and Social Psychology Review* (6:2), pp. 107-122.

Bamberg, S., and Schmidt, P. 2003. "Incentives, Morality, or Habit? Predicting Students' Car Use for University Routes with the Models of Ajzen, Schwartz, and Triandis," *Environment and Behavior* (35:2), pp. 264-285.

Barlow, J., Warkentin, M., Ormond, D., and Dennis, A. 2013. "Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation," *Computers & Security* (39:Part B), pp. 145-159.

Bergeron, F., Raymond, L., Rivard, S., Gara, M.-F. 1995. "Determinants of EIS Use: Testing a Behavioral Model," *Decision Support Systems* (14:2), pp. 131-146.

Curry, T. R. 2005. "Integrating Motivating and Constraining Forces in Deviance Causation: A Test of Causal Chain Hypotheses in Control Balance Theory," *Deviant Behavior* (26:6), pp. 571-599.

D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (23:1), pp. 79-98.

Dudwick, N., Kuehnast, K., Jones, V. N., and Woolcock, M. 2006. "Analyzing Social Capital in Context: A Guide to Using Qualitative Methods and Data," Stock No. 37260, The International Bank for Reconstruction and Development, The World Bank, Washington, DC.

Fisher, R. J. 1993. "Social Desirability Bias and the Validity of Indirect Questioning. Journal of Consumer Research, 20(2): 303-315.

Guo, K.H., Yuan, Y., Archer, N.P., Connelly, C.E. 2011. Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of management information systems* 28(2): 203-236.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM* 54(6) 54-60.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Kanfer, R., and Ackerman, P. L. 1989. "Motivation and Cognitive Abilities: An Integrative/Aptitude-Treatment Interaction Approach to Skill Acquisition," *Journal of Applied Psychology* (74:4), pp. 657-690.

Limayem, M., and Hirt, S. G. 2003. "Force of Habit and Information Systems Usage: Theory and Initial Validation," *Journal of the Association for Information Systems* (4:1), pp. 65-97.

Gagnon, M.-P., Godin, G., Gane, C., Fortin, J.-P., Lamothe, L., Reinharz, D., and Cloutier, A. 2003. "An Adaptation of the Theory of Interpersonal Behavior to the Study of Telemedicine Adoption by Physicians," *International Journal of Medical Informatics* (71:2-3), pp. 103-115.

McClenahan, C., Shevlin, M., Adamson, G., Bennett, C., and O'Neill, B. 2007. "Testicular Self-Examination: A Test of the Health Belief Model and the Theory of Planned Behavior," *Health Education Research* (22:2), pp. 272-284.

Milne, S., Sheeran, P., and Orbell, S. 2000. "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory," *Journal of Applied Social Psychology* (30:1), pp. 106-143.

O'Fallon, M., and Butterfield, K. 2005. "A Review of the Empirical Ethical Decision-Making Literature: 1996–2003," *Journal of Business Ethics* (59:4), pp. 375-413.

Osman, A., Barrios, F. X., Osman, J. R., Schneekloth, R., and Troutman, J. A. 1994. "The Pain Anxiety Symptoms Scale: Psychometric Properties in a Community Sample," *Journal of Behavioral Medicine* (17:5), pp. 511-522.

Paternoster, R., and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law & Society Review* (30:3), pp. 549-584.

Piquero, N. L., and Piquero, A. R. 2006. "Control Balance and Exploitative Corporate Crime," *Criminology* (44:2), pp. 397-430.

Pogarsky, G. 2004. "Projected Offending and Implications for Heterotypic Continuity," *Criminology* (42:1), pp. 111-135.

Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in *Social Psychophysiology*, J. Cacioppo and R. E. Petty (eds.), New York: Guilford, pp. 153-176.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Siponen, M., and Vance, A. 2014. "Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations," *European Journal of Information Systems* (23:3), pp. 289-305.

Tittle, C. R. 1995. *Control Balance: Toward a General Theory of Deviance*, Boulder, CO: Westview Press.

Tittle, C. R. 1997. "Thoughts Stimulated by Braithwaite's Analysis of Control Balance Theory," *Theoretical Criminology* (1:1), pp. 99-110.

Trevino, L. K. 1992. "Experimental Approaches to Studying Ethical–Unethical Behavior in Organizations," *Business Ethics Quarterly* (2:2), pp. 121-136.

Triandis, H. 1977. *Interpersonal Behavior*, Pacific Grove, CA: Brooks/Cole Publishing Company.

Vance, T., and Siponen, M. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Vance, T., and Siponen, M. 2012. "IS Security Policy Violations: A Rational Choice Perspective," *Journal of Organizational and End User Computing* (24:1), pp. 21-41.

Verplanken, B., and Orbell, S. 2003. "Reflections on Past Behavior: A Self-Report Index of Habit Strength," *Journal of Applied Social Psychology* (33:6), pp. 1313-1330.

Witte, K., Cameron, K. A., McKeon, J. K., and Berkowitz, J. M. 1996. "Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale," *Journal of Health Communications* (1:4), pp. 317-341.

Woon, I. M. Y., Tan, G.-W., and Low, R. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," in *Proceedings of the 26th International Conference on Information Systems*, D. Avison, D. Galletta, and J. I. DeGross (eds.), Las Vegas, NV, December 11-14, pp. 367-380.