MIS Quarterly

SPECIAL ISSUE

NEUTRALIZATION: NEW INSIGHTS INTO THE PROBLEM OF EMPLOYEE INFORMATION SYSTEMS SECURITY POLICY VIOLATIONS

By: **Mikko Siponen**
Information Systems Security Research Centre
Department of Information Processing Science
University of Oulu
Linnanmaa
Oulu 3000
FINLAND
mikko.siponen@oulu.fi

Anthony Vance
Information Systems Department
Marriott School of Management
Brigham Young University
Provo, UT 84602
U.S.A.
anthony@vance.name

Appendix A

Measurement Items and Hypothetical Scenarios

Table A1. Measurement Items

Constructs	Item	Source
Intention	What is the chance that you would do what [the scenario character] did in the described scenario?	Paternoster and Simpson (1996)
Neutralization: Denial of responsibility 1	It is OK to violate the company information security policy if you aren't sure what the policy is.	Adapted from Thurman (1984)
Neutralization: Denial of responsibility 2	It is OK to violate the company information security policy if the policy is not advertised.	New item
Neutralization: Denial of responsibility 3	It is OK to violate the company information security policy if you don't understand it.	New item
Neutralization: Denial of injury 1	It is OK to violate the company information security policy if no harm is done.	New item
Neutralization: Denial of injury 2	It is OK to violate the company information security policy if no damage is done to the company.	New item
Neutralization: Denial of injury 3	It is OK to violate the company information security policy if no one gets hurt.	Adapted from Thurman (1984)

Table A1. Measurement Items (Continued)

Constructs	Item	Source
Neutralization: Condemnation of the condemners 1	It is not as wrong to violate a company information security policy that is not reasonable.	Adapted from Thurman (1984)
Neutralization: Condemnation of the condemners 2	It is not as wrong to violate a company information security policy that requires too much time to comply with.	New item
Neutralization: Condemnation of the condemners 3	It is not as wrong to violate a company information security policy that is too restrictive.	New item
Neutralization: Appeal to higher loyalties 1	It is all right to violate a company information security policy to get a job done.	Adapted from Thurman (1984)
Neutralization: Appeal to higher loyalties 2	It is all right to violate a company information security policy if you get your work done.	New item
Neutralization: Appeal to higher loyalties 3*	It is all right to violate a company information security policy if you complete the task given by management.	New item
Neutralization: Defense of necessity 1	It is all right to violate the company information security policy under circumstances where it seems like you have little other choice.	Adapted from Thurman (1984)
Neutralization: Defense of necessity 2	It is all right to violate the company information security policy when you are under a tight deadline.	New item
Neutralization: Defense of necessity 3	It is all right to violate the company information security policy when you are in a hurry.	New item
Neutralization: Metaphor of the ledger 1	I feel my general adherence to company information security policy compensates for occasionally violating an information security policy.	New item based on Eliason and Dodder (1999)
Neutralization: Metaphor of the ledger 2	I feel my good job performance compensates for occasionally violating information security policy.	New item based on Eliason and Dodder (1999)
Neutralization: Metaphor of the ledger 3	I feel my hard work in the company compensates for occasionally violating an information security policy.	New item based on Eliason and Dodder (1999)
Formal sanctions—certainty 1*	What is the chance you would receive sanctions if you violated the company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Formal sanctions—certainty 2	What is the chance that you would be formally sanctioned if management learned that you had violated company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Formal sanctions—certainty 3	What is the chance that you would be formally reprimanded if management learned you had violated company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Formal sanctions—severity 1*	How much of a problem would it be if you received severe sanctions if you violated the company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Formal sanctions—severity 2	How much of a problem would it create in your life if you were formally sanctioned for doing what [the scenario character] did?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)

Table A1. Measurement Items (Continued)

Constructs	Item	Source
Formal sanctions—severity 3	How much of a problem would it create in your life if you were formally reprimanded for doing what [the scenario character] did?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Informal sanctions—certainty 1	How likely is it that you would lose the respect and good opinion of your co-workers for violating the company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Informal sanctions—certainty 2	How likely is it that you would jeopardize your promotion prospects if management learned that you had violated company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Informal sanctions—certainty 3	How likely is it that you would lose the respect and good opinion of your manager, if management learned that you had violated company IT security policies?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Informal sanctions—severity 1	How much of a problem would it create in your life if you lost the respect and good opinion of your co-workers for violating the company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Informal sanctions—severity 2	How much of a problem would it create in your life if you jeopardized your future job promotion prospects for doing what [the scenario character] did?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Informal sanctions—severity 3	How much of a problem would it create in your life if you lost the respect of your manager for violating the company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Certainty of shame for oneself 1	How likely is it that you would be ashamed if co-workers knew that you had violated company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Certainty of shame for oneself 2	How likely is it that you would be ashamed if others knew that you had violated the company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Certainty of shame for oneself 3	How likely is it that you would be ashamed if managers knew that you had violated the company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Severity of shame for oneself 1	How much of a problem would it be if you felt ashamed that co-workers knew you had violated the company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Severity of shame for oneself 2	How much of a problem would it be if you felt ashamed that others knew you had violated the company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)
Severity of shame for oneself 3	How much of a problem would it be if you felt ashamed that managers knew you had violated the company information security policy?	New item based on Nagin and Paternoster (1993); Paternoster and Simpson (1996)

*Dropped to improve reliability or construct validity.

Table A2. Hypothetical scenarios

Violation	Scenario
USB drive	Pekka is a middle level manager in a medium-sized company where he has worked for several years. Pekka is currently working on a sales report that requires the analysis of the company's customer database. This database contains customer names, phone numbers, credit card numbers, and purchase histories. Because of the sensitive nature of corporate data, the company has a strict policy prohibiting the copy of corporate data to unencrypted portable media, such as USB drives. However, Pekka will travel for several days and would like to analyze the corporate database on the road. Pekka 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. The firm is experiencing growing sales and revenues in an industry that is economically deteriorating. He also knows that an employee was recently reprimanded for copying sensitive corporate data to a USB drive. Pekka copies the corporate database to his portable USB drive and takes it off company premises.
Workstation logout	Seija is a middle-level manager in a medium-sized company where she was recently hired. Her department uses an inventory procurement software application program to make inventory purchases. To ensure that only authorized individuals make inventory purchases, the company has a firm policy that employees must log out or lock their computer workstation when not in use. However, to make work more convenient, Seija's manager directs her to leave her user account logged-in for other employees to freely use. Seija expects that keeping her user account logged-in could save her company time. She also knows that keeping the workstation logged-in is a common practice in the industry and an employee recently was reprimanded for leaving the workstation logged-in. Seija leaves the workstation logged-in when she is finished.
Passwords	Hannu 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, Hannu is on a business trip and one of his co-workers needs a file on his computer. Hannu expects that sharing his password could save his company a lot of time. He also knows that the firm has mandatory information security training. Hannu shares his password with his co-worker.

Appendix B

Scenario Design

Two points highlighted in the literature must be kept in mind when designing hypothetical scenarios. First, Piquero and Hickman (1999) noted that vignettes must not describe scenarios that are uncommon to respondents. In order to address this concern, we used the belief elicitation process (Limayem and Hirt 2003), in which we sent an open-ended questionnaire via e-mail to 111 IS security experts and information security managers in Finnish organizations. We asked these professionals to assess the four most common and significant information security policy violations. A total of 54 information security experts responded. The response rate (49 percent) was reasonable, given the sensitive nature of the topic and typical problems encountered by previous studies to collect security-related data (Kotulic and Clark 2004). While we asked for four IS security policy concerns, some of the respondents reported more than four. Nineteen respondents answered that they could not rank their top IS security policy compliance problems. As a result, we did not count the ranking, but instead regarded all answers as equal. This process ensures that scenarios reflect real-world problems that are important and relevant to IS security practice (Benbasat and Zmud 1999). Content analysis (Krippendorff 2004) was used to categorize the responses, which are summarized in Table B1.

Second, previous studies utilizing criminological theories like neutralization suggest that specific details such as names of persons and companies should be mentioned in the cases (Piquero and Hickman 1999; Piquero et al. 2005). In keeping with these points, three scenarios were developed each describing a different setting and IS security policy violation. The use of three scenarios ensures that our findings are generalizable across different but important IS security violation policy violation contexts.

Table B1. Most Cited IS Security Policy Violations	
Security Policy Noncompliance Problems	Responses
Failing to lock or log out of workstations	24
Writing down personal passwords in visible places	17
Sharing passwords with colleagues or friends	14
Copying sensitive data to insecure USB practices	14
Revealing confidential information to outsiders	13
Disabling security configurations	13
Using laptops carelessly outside of the company	11
Sending confidential information unencrypted	11
Creating easy-to-guess passwords	10

Appendix C

Model Validation

To establish factorial validity and reliability for the measurement model, we followed the PLS validation procedures outlined by Gefen and Straub (2005). To test convergent validity, we performed a bootstrap with 600 resamples and then examined the t-values of the outer model loadings. Convergent validity is demonstrated when all indicators load significantly on their respective latent construct. In our case, all indicators exhibited loadings that were significant at the .001 level (see Table C1), denoting strong convergent validity. An additional test of convergent validity put forward by Fornell and Larcker (1981) is that the average variance extracted (AVE), a measure of variance explained by a latent construct for the variance observed in its measurement items, should be at least .50 or higher. The AVE values are shown in Table C2. Both tests indicate a high degree of convergent validity.[2]

[2] N.B.: These convergent validity tests were not performed for the dependent variable, *intention to violate IS security policy*, because these tests are not applicable for single-item measures.

Table C1. T-statistics for Convergent Validity

Construct	Subconstruct	Indicator	T-Statistic
Formal Sanctions	N/A	FormA ← Formal	11.13***
		FormB ← Formal	48.89***
		FormC ← Formal	10.47***
Shame	N/A	ShameA ← Shame	38.12***
		ShameB ← Shame	99.52***
		ShameC ← Shame	53.95***
Informal Sanctions	N/A	InformA ← Informal	49.84***
		InformB ← Informal	38.55***
		InformC ←Informal	57.64***
Neutralization	Denial of Injury	NeutInjA ← NeutInj	33.83***
		NeutInjB ← NeutInj	48.3***
		NeutInjC ← NeutInj	34.6***
	Appeal to Higher Loyalties	NeutLoyA ← NeutLoy	71.58***
		NeutLoyB ← NeutLoy	30.37***
		NeutLoyC ← NeutLoy	36.9***
	Defense of Necessity	NeutNecA ← NeutNec	46.13***
		NeutNecB ← NeutNec	29.43***
		NeutNecC ← NeutNec	33.32***
	Condemnation of Condemners	NeutCondA ← NeutCond	54.06***
		NeutCondB ← NeutCond	22.68***
		NeutCondC ← NeutCond	28.61***
	Denial of Responsibility	NeutRespA ← NeutResp	51.1***
		NeutRespB ← NeutResp	31.49***
		NeutRespc ← NeutResp	36.43***
	Metaphor of the Ledger	NeutLedgA ← NeutLedger	40.53***
		NeutLedgB ← NeutLedger	62.36***
		NeutLedgC ← NeutLedger	42.79***

***p < .001

Table C2. AVE Scores

Construct	AVE
Formal	.77
Informal	.78
NeutCond	.66
NeutInj	.71
NeutLedger	.75
NeutLoy	.80
NeutNec	.67
NeutResp	.70
Shame	.83

To evaluate discriminant validity, two tests were performed. First, the cross-loadings of measurement items on latent constructs were examined. In this test, discriminant validity is demonstrated when an item more highly loads on its intended construct than on any other construct. Following Gefen and Straub, this difference in loadings should be at least .10. In this test, all items showed excellent discriminant validity (see Table C3). Therefore, the model demonstrates high discriminant validity.

Table C3. Cross Loadings of Measurement Items to Latent Constructs

Construct	Item	1	2	3	4	5	6	7	8	9
Formal sanctions (1)	FormA	**.76**	.62	-.19	-.11	-.07	-.18	-.20	-.14	.50
	FormB	**.94**	.73	-.30	-.25	-.26	-.34	-.35	-.26	.60
	FormC	**.71**	.61	-.26	-.23	-.16	-.24	-.25	-.23	.57
Informal sanctions (2)	InformA	.65	**.88**	-.32	-.27	-.24	-.31	-.35	-.21	.66
	InformB	.75	**.87**	-.32	-.24	-.23	-.30	-.32	-.22	.66
	InformC	.74	**.90**	-.36	-.31	-.32	-.37	-.36	-.31	.73
Neutralization—Condemn (3)	NeutCondA	-.32	-.34	**.85**	.54	.49	.58	.65	.49	-.35
	NeutCondB	-.19	-.30	**.76**	.52	.47	.50	.52	.41	-.23
	NeutCondC	-.25	-.28	**.83**	.49	.44	.54	.57	.45	-.26
Neutralization—Injury (4)	NeutInjA	-.17	-.25	.47	**.84**	.46	.56	.49	.39	-.25
	NeutInjB	-.22	-.28	.52	**.87**	.49	.60	.58	.42	-.30
	NeutInjC	-.25	-.26	.59	**.81**	.55	.61	.70	.52	-.28
Neutralization—Ledger (5)	NeutLedgA	-.23	-.28	.45	.47	**.85**	.58	.55	.50	-.31
	NeutLedgB	-.20	-.27	.53	.56	**.89**	.67	.64	.48	-.31
	NeutLedgC	-.17	-.23	.52	.53	**.85**	.62	.58	.49	-.28
Neutralization—Loyalty (6)	NeutLoyA	-.33	-.36	.64	.65	.69	**.90**	.80	.50	-.34
	NeutLoyB	-.31	-.39	.55	.60	.54	**.80**	.57	.39	-.32
	NeutLoyC	-.22	-.21	.51	.54	.62	**.84**	.62	.46	-.22
Neutralization—Necessity (7)	NeutNecA	-.40	-.37	.61	.60	.54	.68	**.83**	.53	-.34
	NeutNecB	-.20	-.31	.54	.58	.58	.67	**.81**	.43	-.27
	NeutNecC	-.25	-.28	.61	.57	.56	.58	**.81**	.48	-.27
Neutralization—Responsibility (8)	NeutRespA	-.25	-.27	.46	.43	.47	.43	.50	**.87**	-.28
	NeutRespB	-.19	-.20	.43	.51	.48	.43	.50	**.79**	-.23
	NeutRespc	-.24	-.24	.51	.40	.46	.46	.48	**.84**	-.25
Shame (9)	ShameA	.52	.63	-.25	-.25	-.29	-.29	-.25	-.23	**.88**
	ShameB	.69	.76	-.37	-.33	-.34	-.36	-.38	-.32	**.94**
	ShameC	.66	.74	-.34	-.32	-.32	-.29	-.34	-.28	**.91**

A second test of discriminant validity is to compare the AVE score for each construct. In the AVE test of discriminant validity, the square root of a given construct's AVE should be larger than any correlation of the given construct with any other construct in the model (Chin 1998). All of the results of this test were generally acceptable, but two items (Formal A and NeutLoyaltyC) were dropped from the model to improve discriminant validity. Our results, depicted in Table C4, again demonstrate strong discriminant validity.

Finally, to test the reliability of measurement items, SmartPLS was used to compute the Cronbach's α as well as a composite reliability score (Fornell and Larcker 1981) which is evaluated in the same way as Cronbach's α. Both scores are reported in Table C5. All constructs exhibited a reliability score well over the .60 threshold accorded to exploratory research (Nunnally 1967).

Table C4. Correlation of the Latent Variable Scores with the Square Root of AVE										
Index	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Formal (1)	**.88**									
Informal (2)	.76	**.89**								
Intention (3)	-.28	-.30	**1.00**							
NeutCond (4)	-.29	-.38	.45	**.81**						
NeutInj (5)	-.23	-.31	.53	.64	**.84**					
NeutLedger (6)	-.23	-.30	.55	.58	.60	**.86**				
NeutLoy (7)	-.34	-.41	.66	.67	.70	.69	**.89**			
NeutNec (8)	-.34	-.39	.57	.72	.71	.68	.77	**.82**		
NeutResp (9)	-.25	-.28	.34	.56	.53	.56	.50	.59	**.84**	
Shame (10)	.62	.78	-.26	-.35	-.33	-.35	-.37	-.36	-.30	**.91**

Table C5. Reliability Scores		
Construct	Composite Reliability	Cronbach's α
Formal	.87	.76
Informal	.92	.86
NeutCond	.85	.74
NeutInj	.88	.79
NeutLedger	.90	.83
NeutLoy	.89	.75
NeutNec	.86	.75
NeutResp	.87	.78
Shame	.94	.90

Appendix D

Tests for Common Methods Bias

Common methods bias is "variance that is attributable to the measurement method rather than to the constructs the measures represent" (Podsakoff et al. 2003, p. 879) and is a major contributor to systematic measurement error (Bagozzi and Yi 1991). Like all forms of measurement error, if common methods bias is sufficiently high, then incorrect conclusions may be drawn about relationships between constructs. To reduce the likelihood of common methods bias, items were randomized within the instrument to limit the ability of participants to detect underlying construct patterns that could influence their answers (Cook and Campbell 1979; Straub et al. 2004). However, because both the dependent variable (the reported intention of behaving as the scenario character did) and independent variables were measured using the same instrument, the occurrence of common methods bias was still possible. Therefore, several tests were performed to rule out common methods bias as a factor in this study.

First, we performed Harman's one-factor test (Podsakoff et al. 2003). In this test, all items are entered into an unrotated exploratory factor analysis to determine whether a single factor emerges or a single factor accounts for the majority of the variance. In our test, 27 factors emerged, the largest of which accounted for 37 percent of the variance. Both results indicate that common methods bias is not an issue in this study.

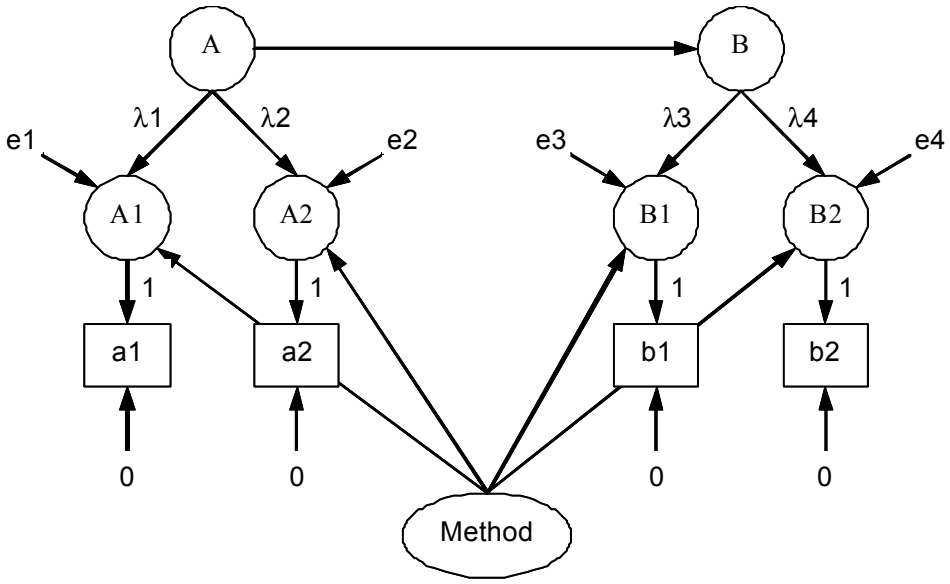

Figure D1. Liang et al.'s Example of Modeling Indicators as Single-Indicator Constructs (Figure E2 from "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management," H. Liang, N. Saraf, Q. Hu, and Y. Xue, *MIS Quarterly* (31:1), 2007, p. 86)

However, because Harman's one-factor test is increasingly contested for its ability to detect common methods bias (Podsakoff et al. 2003), we also performed a test performed by Pavlou et al. (2007). In their test, the construct correlation matrix as calculated by PLS (reported in Table C4) is examined to determine whether any constructs correlate extremely highly (more than .90). In our case, none of the constructs were so highly correlated. This finding likewise indicates that common methods bias is not a problem.

Finally, a more rigorous test of common methods bias test suggested by Podsakoff et al. (2003) and adapted to PLS analysis by Liang et al. (2007) was performed. The purpose of this technique is to measure the influence of common methods bias on indicators *vis-à-vis* the influence of the theorized constructs in the model.

To perform this technique in PLS, the constructs of the theoretical model and their relationships are created as for a typical analysis. Additionally, a single-indicator construct is created for each indicator in the measurement model. Each substantive construct is linked to the single-indicator constructs for the indicators that it comprises. This effectively makes each substantive construct in the model a second-order reflective construct. Next, a construct representing the method is created, reflectively composed of all indicators of the instrument. Finally, paths are created between the method construct and each single-item construct. Figure D1 depicts this approach.

To interpret these results, the coefficients of paths (from substantive constructs to single-indicator constructs, as well as coefficients of paths from the method construct to single-indicator constructs,) are considered loadings, represented by λ in the table (Marcoulides and Moustaki 2002). Following Williams et al. (2003), common method bias can be assessed by examining the statistical significance of the loadings of the method construct and by comparing the variance of each indicator as explained by the substantive and method factors. For both substantive and method constructs, the square of the loading is interpreted as the percentage of indicator-explained variance. If the method construct loadings are generally insignificant, and the percentages of indicator variance explained by substantive constructs are substantially greater than those explained by the method construct, then common methods bias is demonstrated to have minimal effect and thus be of little concern.

Applying these guidelines, we can see that variance of indicators due to substantive constructs is substantially greater than that due to the method construct (see Table D1). The average variance due to substantive constructs is 71 percent versus 1 percent for the method constructs. This indicates that the influence due to the method factor was considerably smaller than that due to substantial factors. Examining the loadings of the method factor, we find that the majority are insignificant. In light of our previous tests, and the results of this procedure, we concluded that our results reflect a negligible influence due to common methods bias, and it is, therefore, not a concern.

Table D1. Common Method Bias Analysis

Construct	Indicator	Substantive Factor Loading (λ_s)	Variance Explained (λ_s^2)	Method Factor Loading (λ_m)	Variance Explained (λ_m^2)
Formal sanctions	FormalA	.95***	.91	.15***	.02
	FormalB	.82***	.67	-.11***	.01
Informal Sanctions	InformA	.89***	.79	.02	.00
	InformB	.92***	.85	.05	.00
	InformC	.85***	.72	-.07*	.01
Neutralization—Condemn	NeutCondA	.79***	.62	.08	.01
	NeutCondB	.74***	.55	.01	.00
	NeutCondC	.90***	.81	-.09	.01
Neutralization—Injury	NeutInjA	.98***	.97	-.16***	.03
	NeutInjB	.94***	.87	-.06	.00
	NeutInjC	.58***	.34	.25***	.06
Neutralization—Ledger	NeutLedgerA	.89***	.78	-.04	.00
	NeutLedgerB	.85***	.73	.04	.00
	NeutLedgerC	.85***	.73	.00	.00
Neutralization—Loyalty	NeutLoyA	.78***	.60	.15***	.02
	NeutLoyB	.85***	.71	-.02	.00
Neutralization—Necessity	NeutNecA	.73***	.53	.12*	.01
	NeutNecB	.85***	.72	-.04	.00
	NeutNecC	.88***	.77	-.08	.01
Neutralization—Responsibility	NeutRespA	.91***	.82	-.04	.00
	NeutRespB	.73***	.53	.07	.00
	NeutRespC	.87***	.75	-.02	.00
Shame	ShameA	.65***	.42	-.10**	.01
	ShameB	.94***	.89	-.03	.00
	ShameC	.99***	.97	.03	.00
Average		**.84**	**.72**	**.00**	**.01**

*p < .025, * p < .01, ***p < .005

N.B.: Intention is not included in the above analysis because it is itself a single item construct and is not amenable to this technique. Please refer to the construct correlation matrix to assess CMV for this construct.

Appendix E

Variance of Deterrence Measures

Table E1 presents descriptive statistics for deterrence items used in the model analysis. Because we adapted our deterrence items from those of Paternoster and his associates, we also modeled their technique of creating calculated measures for each deterrence construct to "create a sanction measure that reflected both the risk and cost of perceived punishment (Nagin and Paternoster 1993, p. 481; Paternoster and Simpson 1996). This was done by multiplying a severity measure by its corresponding certainty measure. For example, FormA was calculated by multiplying "Formal Sanctions—certainty 1" by "Formal Sanctions—severity 1". Because each original item was measured on a scale from 0 to 10, the possible range for the calculated measure was 0 to 100 (this was also the observed range for each variable). The descriptive statistics in Table E1 show ample variance in each calculated measure.

Table E1. Descriptive Statistics for Deterrence Measures						
Measure	**Range**	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**	**Variance**
FormA	100	0	100	30.74	30.19	911.18
FormB	100	0	100	30.27	31.17	971.27
FormC	100	0	100	47.81	31.10	967.43
InformA	100	0	100	40.76	30.33	919.93
InformB	100	0	100	39.18	30.07	904.19
InformC	100	0	100	55.96	30.75	945.57
ShameA	100	0	100	45.12	34.51	1191.09
ShameB	100	0	100	52.66	32.81	1076.41
ShameC	100	0	100	57.69	33.07	1093.92

References for the Appendices

Bagozzi, R. P., and Yi, Y. 1991. "Multitrait-Multimethod Matrices in Consumer Research," *Journal of Consumer Research* (17:4), pp. 426-439.

Benbasat, I., and Zmud, R. W. 1999. "Empirical Research in Information Systems: The Practice of Relevance," *MIS Quarterly* (23:1), pp. 3-16.

Chin, W. 1998. "Issues and Opinions on Structural Equation Modeling," *MIS Quarterly* (22:1), pp. vii-xvi.

Cook, T. D., and Campbell, D. T. 1979. *Quasi Experimentation: Design and Analytical Issues for Field Settings*, Chicago: Rand McNally.

Eliason, S. L., and Dodder, R. A. 1999. "Techniques of Neutralization Used by Deer Poachers in the Western United States: A Research Note," *Deviant Behavior* (20:3), pp. 233-252.

Elis, L. A., and Simpson, S. 1995. "Informal Sanction Threats and Corporate Crime: Additive Versus Multiplicative Models," *Journal of Research in Crime and Delinquency* (20:3), pp. 233-252.

Fornell, C., and Larcker, D. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39-50.

Gefen, D., and Straub, D. W. 2005. "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example," *Communications of the AIS* (16:5), pp. 91-109.

Kotulic, A. G., and Clark, J. G. 2004. "Why There Aren't More Information Security Research Studies," *Information & Management* (41:5), pp. 597-607.

Krippendorff, K. 2004. *Content Analysis: An Introduction to Its Methodology*, Thousand Oaks, CA: Sage Publications.

Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management," *MIS Quarterly* (31:1), pp. 59-87.

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

Marcoulides, G., and Moustaki, I. 2002. *Latent Variable and Latent Structure Models*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Nagin, D. S., and Paternoster, R. 1993. "Enduring Individual Differences and Rational Choice Theories of Crime," *Law & Society Review* (27:3), pp. 467-496.

Nunnally, J. C. 1967. *Psychometric Theory*, New York: McGraw-Hill.

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.

Pavlou, P., Liang, H., and Xue, Y. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31:1), pp. 105-136.

Piquero, A. R., and Hickman, M. 1999. "An Empirical Test of Tittle's Control Balance Theory," *Criminology* (37:2), pp. 319-342.

Piquero, N. L., Tibbetts, S. G., and Blankenship, M. B. 2005. "Examining the Role of Differential Association and Techniques of Neutralization in Explaining Corporate Crime," *Deviant Behavior* (26:2), pp. 159-188.

Podsakoff, P. M., MacKenzie, S. B., Lee, J., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.

Straub, D. W., Boudreau, M., and Gefen, D. 2004. "Validation Guidelines for IS Positivist Research," *Communications of the Association for Information Systems* (13:24), pp. 380-427.

Thurman, Q. C. 1984. "Deviance and the Neutralization of Moral Commitment: An Empirical Analysis," *Deviant Behavior* (5), pp. 291-304.

Williams, L., Edwards, J., and Vandenberg, R. 2003. "Recent Advances in Causal Modeling Methods for Organizational and Management Research," *Journal of Management* (29:6), pp. 903-936.