The Role of "Eyes of Others" in Security Violation Prevention: Measures and Constructs

Sahar Farshadkhah
Louisiana Tech University
sfa005@latech.edu

Tom Stafford
Louisiana Tech University
stafford@latech.edu

Abstract

Security research recognizes the effect of "being seen" in reducing the likelihood of security violations in the workplace. This has typically been construed in the context of formal monitoring processes by employers, but there is an emerging notion that workers care about what their workplace colleagues think of them and their activities. We leverage this idea of the "Eyes of Others" in motivating pro-security behaviors to apply to security contexts. We find that, for a set of worker self-perceptions including Morality and Self-Consciousness, the likelihood of engaging in mundane workplace security violations is impacted by the knowledge that coworkers are watching. This has important implications for novel expansions of deterrence research in IS Security, going forward.

1. Introduction

Organizations rely heavily on their information systems, and for this reason the need to protect confidential information and reduce information security risks has become vital [2]. As is widely agreed in the literature, company employees (corporate insiders, to use the rubric) are the weak link in the organizational security chain [7, 8, 31], and improving the employees' security awareness and compliance has always been a crucial task [2]. Most of the research has focused on formal security policies and the factors which have led to their breach or observance, with an eye towards building a better security cultures in firms. Hence, there is a lack of consideration for informal factors which may influence employee security compliance behavior. One of these factors is a potential violator's awareness of being overseen by onlookers in the workplace, when contemplating behavior that violates the security policies of the firm.

We characterize this onlooker dynamic on the part of coworkers watching each other as the "Eyes of Others" in terms of the potential motivational impact that the knowledge of being seen in performance of some sanctioned activity might have on perpetrators. The organizational behavior literature has a number of interesting examples of the onlooker effect and how it influences employee behavior, ranging from social desirability effects of being seen with the "right group" [6], to the influence of peers and their visibility during the performance workplace activities [22, 28] to actual technology use implications related to influences on workplace behavior arising from the knowledge of being seen by others using some inappropriate technological application in the workplace [26].

Individuals, whether at work or in their private lives, are vulnerable to the self-perceived perceptions of others in their groups of association [6], and our view is that this interpersonal approval dynamic can influence how workers adhere to security policy practices when their activity is discernable by their coworkers. As we consider the literature, however, we see several studies reinforcing the impact of onlooker awareness on individuals [11, 25], but nothing specific to the likely influence it might have on security practices; hence, this remains a fruitful area for inquiry.

The onlookers we consider as influencing these interesting peer-pressure effects in the workplace are actors for whom the coworker's action is visible, but who are not directly involved in the coworkers' activities [22, 26]. We call this peer visibility effect the "Eyes of Others," and suggest that it is probative for preventing security violations in the workplace in addition to likely influencing pro-security behaviors, as well.

To that end, the purpose of this paper is to develop and begin the validation process for measures that can be used to assess onlooker effects which may influence security behaviors in the workplace. We consider that, in addition to developing the emergent "Eyes of Others" construct, a second contribution of this study might be the development of a set of measures for mundane workplace security violations, as there are no formal measurement inventories for such violations in the literature.

The paper proceeds as follows: after a brief review of the onlooker effect, we describe our methodology for measure development and then report the results of a study of a model that examines the impact of the

URI: https://hdl.handle.net/10125/59927
ISBN: 978-0-9981331-2-6

"Eyes of Others" construct on an inventory of typical workplace security policy violations. We conclude with theoretical directions and applications for measures of the onlooker effect and security violations.

2. The onlooker effect: Eyes of others.

Individuals are not alone in the workplace; most of the time they have colleagues around who may play an informal, even inadvertent, monitoring role as regards the propriety of certain technology use behaviors on the job. Onlookers are those who are available in a situation and are aware of another individual's action by seeing or hearing it but are not personally involved in the action, themselves, other than as observers. The onlooker role in the specific context of unauthorized use of personal technology at work has been discussed [26], in the specific setting of handheld personal devices in medical workplaces. This work suggests that onlookers' inferences, judgments, and reactions can trigger users to reflect on consequences of their unauthorized technology use and to adjust their use as a result.

There are a variety of different onlooker influences to be found in workplaces: coworkers serve as onlookers [12, 30], as do managers [19] and even more informal collegial workplace relationships [26]. Co-workers provide a positive point of context for beneficial self-evaluation [6], but also serve as a social touchpoint for the value of working relationships [28], as a point of influence in organizational change [22], and as a preventive influence in mediating negative behaviors [11].

2.1. The onlooker effect and deterrence

The tie to behavioral security research for the importance of understanding the onlooker effect would come through various applications of deterrence theory [9, 10, 16]. Though the specific presence of social "others" viewing potential security breaches is not explicitly treated in the deterrence theory literature on information security, there are plentiful implications for a social role in prevention. One factor is embarrassment or shame that might arise from a perpetrator realizing that others in the workplace know of his/her inappropriate activities [9]. While classic deterrence approaches to IS security are comprised explicit influence factors such as likelihood of punishment, severity of punishment and speed of punishment for infractions, the notion of shame arising from the knowledge of the infraction on the part of others having a deterrent effect cannot be discounted. Deterrence theory approaches to behavioral IS security also consider the role that formal monitoring plays in preventing infractions [10], indicating that, to date, the monitoring effect in deterrence models has largely been construed as organizational surveillance of computer use. Even so, there is an undercurrent in the deterrence theory literature on IS security that implicitly acknowledges a potential role of "social others" in motivating against security infractions [16].

We seek to clarify the impact of the onlooker effect and to provide a validated measure of the phenomenon so that future research can operationally specify the effect with more precision as an aspect of models in which social dynamics are utilized in understanding user compliance with security policies.

3. Initial steps in measure development

This study documents the exploratory and confirmatory phases of measure development for the "eyes of others" construct, following orthodox methods of analysis [5, 20]. The first step, specifying the domain of construct, can take an inductive or deductive approach [19] and with no prior measures available for measuring the onlooker effect (what we call "Eyes of Others"), the inductive approach was chosen. We induced the domain of the construct through qualitative inquiry, engaging in a focus group encounter with a group of graduate students in information assurance.

3.1. Item generation: Focus research

A group of 20 MBA students with a concentration in security were recruited for focus research to explore the domain of the Eyes of Others construct. They were asked about the nature of their security perceptions and for purposes of developing definitions of processes and factors that might arise from the presence of informal onlookers in the workplace and their influence on security behaviors.

The group interview process provided us the ability to examine these perceptions in-depth with security-trained individuals, regarding their views of security processes, typical security breaches and hypothetical motivations for either following or not complying with security policies. These questions were couched as hypothetical in our interactions to avoid social desirability issues in response [4].

The result of our focus research was a distillation of key terms and definitions which could be used for questionnaire development in order to measure onlooker effects on motivations for security compliance.

3.1.1. Descriptive terms for development. Words used by respondents in the qualitative inquiry include "Observed," speaking to the knowledge of being overseen in the conduct of some activity. The terms "Guilt," "Self-Conscious," "Penalty," "Anxiety," and "Nervous" spoke to preventive motivational factors that might arise in response to knowledge of the presence of "the eyes of others" during a security violation.

Terms that implied motivations that would serve to support pro-security behaviors, when in the presence of others, included "Personal Integrity," "Personality Traits," "Security Code," "Morality," "Concern," "Safety," and "Trust." "Pressure" and "Enforcement" spoke to factors related to organizational mediation of security behaviors, in the eyes of others.

3.1.2. Descriptive terms for security violations. A search of the literature revealed a surprising lack of scales for measuring mundane workplace security violations. On the one hand, these behaviors come under the ready rubric of things that "everybody knows," but on the other hand, a more detailed analysis of such behaviors seemed warranted, if used for purposes of benchmarking performance of our Eyes of Others construct.

To that end, we engaged in the identification of industry sources of information for security violations, and through the consideration of popular press information available from Chief Security Officer groups [15], Fortune 500 technology companies [23] and popular security sites online [27] we compiled a list of highly typical mundane workplace security violations: password sharing, laxity in maintaining anti-malware protection software, use of personal storage devices inside the company firewall, personal web surfing on company computers, and personal email use at work that involves downloading of attachments.

3.2. Initial testing

One hundred and four students majoring in computer information systems from a College of Business in a large university in the United States participated in a survey questionnaire for further model development. In developmental studies of new theory where broad generality is not the specific goal, students are generally considered useful subjects owing to advantageous homogeneity of variance considerations in theoretical development [3]. As we are entering the initial phases of defining and assessing the "Eyes of Others" construct, we consider this an appropriate tradeoff.

The questionnaire conveyed questions on two areas: the first part contained five items measuring the likelihood of engaging in mundane security violations, which we developed from sources in industry. The second part contained 14 descriptive Eyes of Oth3ers items developed in our qualitative pretest.

3.3. Exploratory refinements of the model

An initial exploration of factor structure was undertaken in order to determine the number of dimensions underlying the construct. Table 1 and Table 2 shows the factor loadings for the security violation and Eyes of Others construct, respectively. Three onlooker dimensions arose, along with two security violation. Onlooker factors were Tension, Morality and Self-Conscious; security violation factors were Violator and Loafer.

Table 1. Factor loadings on security violation items

	Component	
	Violator	Loafer
Sharing Password	-.039	**.844**
Antivirus	.286	**.678**
USB	**.674**	.237
Surfing	**.804**	.188
Personal Email	**.818**	-.079

Table 2. Factor loadings on eyes of others items

	Component		
	Tension	Morality	Self-Conscious
Penalties	.104	.125	**.715**
Observe	.077	.177	**.840**
Nervous	.414	.087	**.690**
Guilty	.372	.376	**.645**
Conscience	.109	**.810**	.249
Integrity	.098	**.820**	.305
Environment	.315	.174	.478
Personality	.497	.021	.115
Morality	.223	**.849**	.069
Stressful	**.733**	.302	.184
Trust	**.806**	.172	.166
Anxious	**.788**	.182	.215
Concern	.299	.523	.080
Unsafe	.527	.318	.243

As can be seen in the initial model of factor structure, where all paths between all constructs were explored (shown in Figure 1, with annotations), only two links between Eyes of Others constructs and Security Violations constructs arose for further consideration: Self-Consciousness and Morality, and in each case, only as regards their impact on the Violator dimension of security violations. A reduction in model structure was justified for further consideration based on the t-values for associated structural linkages, and this appears in Figure 2, showing just the Morality and Self-Consciousness constructs modeled against the Violator construct of mundane workplace security violations.

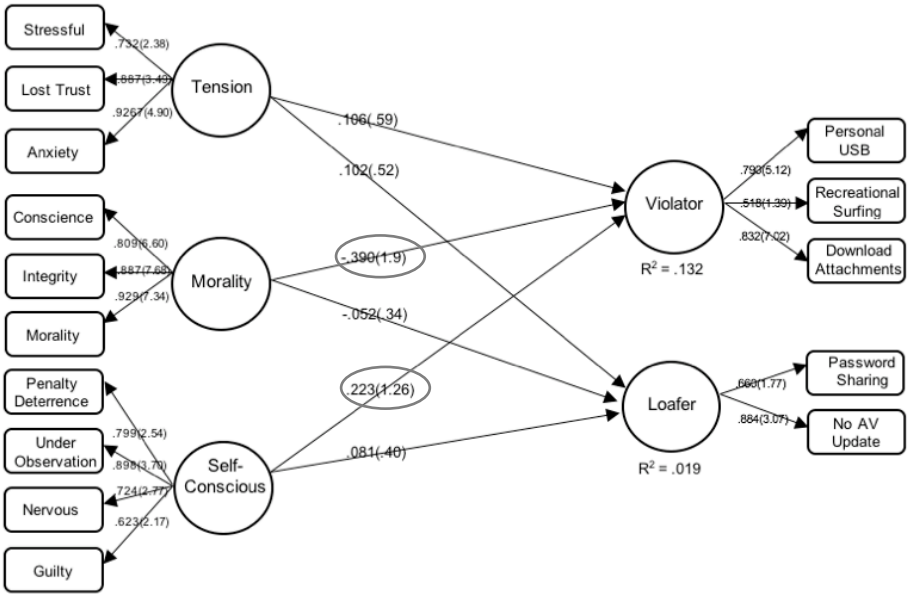

Figure 1. Initial PLS model

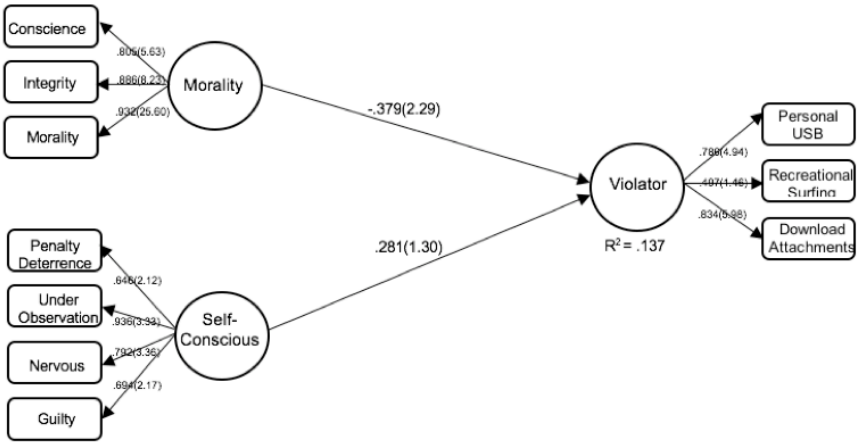

Figure 2. Reduced PLS model

3.4. Likely measurement properties of evolving indicators

A prudent step in exploratory measure development projects such as this is to consider the likely measurement properties of the proffered scale, related to trait validity; one way to check these factors is through the calculation of the Modified Multi-Trait Multi-Method matrix (MMTMM) [21].

In such an analysis, a calculation of weighted scores of each indicator in the model (weighted by its PLS path weight) is summed into a composite score for all indicators on the construct, which can then be compared in a correlation matrix for its fidelity with the actual indicators, themselves. The product of this analysis is shown in Table 3 for diagnostic use, and this information guided final revisions to the exploratory model.

Table 3. Modified MTMM on reduced model indicators

		Penalties	Observe	Nervous	Guilty	Conscience	Integrity	Morality	MoralComp	ConscComp
Penalties	Pearson Correlation	1	.522**	.402**	.363**	.270**	.343**	.200*	.308**	.717**
	Sig. (2-tailed)		.000	.000	.000	.005	.000	.039	.001	.000
	N	106	106	106	106	106	106	106	106	106
Observe	Pearson Correlation	.522**	1	.563**	.562**	.303**	.376**	.250**	.351**	.857**
	Sig. (2-tailed)	.000		.000	.000	.002	.000	.010	.000	.000
	N	106	106	106	106	106	106	106	106	106
Nervous	Pearson Correlation	.402**	.563**	1	.655**	.273**	.374**	.225*	.331**	.814**
	Sig. (2-tailed)	.000	.000		.000	.005	.000	.020	.001	.000
	N	106	106	106	106	106	106	106	106	106
Guilty	Pearson Correlation	.363**	.562**	.655**	1	.584**	.472**	.439**	.562**	.791**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000	.000	.000
	N	106	106	106	106	106	106	106	106	106
Conscience	Pearson Correlation	.270**	.303**	.273**	.584**	1	.652**	.617**	.848**	.436**
	Sig. (2-tailed)	.005	.002	.005	.000		.000	.000	.000	.000
	N	106	106	106	106	106	106	106	106	106
Integrity	Pearson Correlation	.343**	.376**	.374**	.472**	.652**	1	.719**	.902**	.486**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000	.000	.000
	N	106	106	106	106	106	106	106	106	106
Morality	Pearson Correlation	.200*	.250**	.225*	.439**	.617**	.719**	1	.890**	.342**
	Sig. (2-tailed)	.039	.010	.020	.000	.000	.000		.000	.000
	N	106	106	106	106	106	106	106	106	106
MoralComp	Pearson Correlation	.308**	.351**	.331**	.562**	.848**	.902**	.890**	1	.478**
	Sig. (2-tailed)	.001	.000	.001	.000	.000	.000	.000		.000
	N	106	106	106	106	106	106	106	106	106
ConscComp	Pearson Correlation	.717**	.857**	.814**	.791**	.436**	.486**	.342**	.478**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	
	N	106	106	106	106	106	106	106	106	106

The MMTMM analysis is intended to provide support for convergence and discrimination on the part of a proffered set of measures when the indicators on a given construct correlate highly with the composite scores for the respective construct, and at the same time do not correlate highly with composite scores for different constructs. In our case, Morality and Self-Consciousness are the Eyes of Others constructs we are examining in the matrix, and their performance is indicated by the strong correlations seen for MoralComp (the composite for the Morality construct) with the actual Morality construct indicators (Conscience, Integrity and Morality) as well as in ConscComp (the composite score for Self-Consciousness construct) with its actual indicators (which are Penalties, Observed, Nervous and Guilty).

As can be seen by the annotations on the matrix in Table 3, excellent on-construct correlations are obtained for almost every indicator, the sole exception being the Guilty indicator which loads strongly across both constructs.

Since the Guilty indicator loads with its regular group of items on the Self-Consciousness construct, it cannot necessarily be said that it does not converge with the related scale items. It can, however be said that it does not discriminate against related but distinct constructs (Morality, in this case) owing to its cross loading at better than .5. For this reason the conclusion was to remove the indicator from the inventory and re-fit the model without it.

One last version of the PLS model was specified with the Guilty indicator removed, and this is shown in Figure 3, below. A second MMTMM was then calculated for good measure without the Guilty indicator (see Table 4), and shows, as annotated, the expected strong on-construct and weak off-construct loadings supportive of trait validity for the remaining set of indicators for the two constructs.

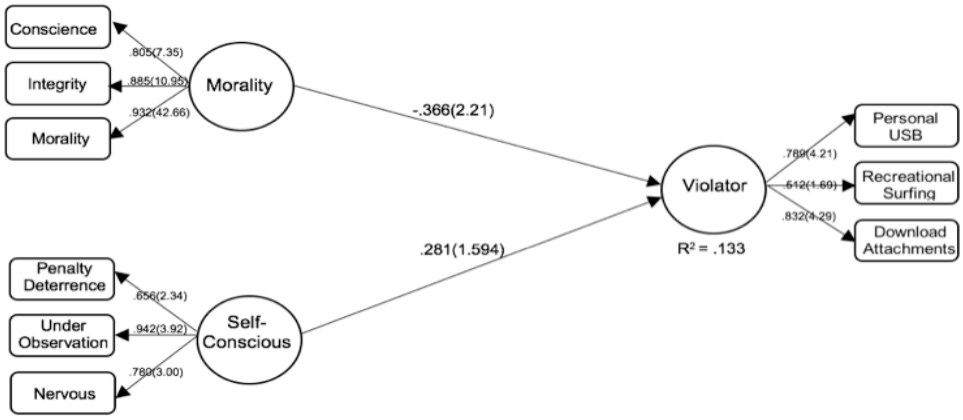

Figure 3. Final reduced model

Table 4. Final modified MTMM

		Penalties	Observe	Nervous	Conscience	Integrity	Morality	ConscComp2	MoralCOmp2
Penalties	Pearson Correlation	1	.522**	.402**	.270**	.343**	.200*	.773**	.307**
	Sig. (2-tailed)		.000	.000	.005	.000	.039	.000	.001
	N	106	106	106	106	106	106	106	106
Observe	Pearson Correlation	.522**	1	.563**	.303**	.376**	.250**	.878**	.351**
	Sig. (2-tailed)	.000		.000	.002	.000	.010	.000	.000
	N	106	106	106	106	106	106	106	106
Nervous	Pearson Correlation	.402**	.563**	1	.273**	.374**	.225*	.789**	.331**
	Sig. (2-tailed)	.000	.000		.005	.000	.020	.000	.001
	N	106	106	106	106	106	106	106	106
Conscience	Pearson Correlation	.270**	.303**	.273**	1	.652**	.617**	.346**	.848**
	Sig. (2-tailed)	.005	.002	.005		.000	.000	.000	.000
	N	106	106	106	106	106	106	106	106
Integrity	Pearson Correlation	.343**	.376**	.374**	.652**	1	.719**	.446**	.902**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000	.000
	N	106	106	106	106	106	106	106	106
Morality	Pearson Correlation	.200*	.250**	.225*	.617**	.719**	1	.277**	.890**
	Sig. (2-tailed)	.039	.010	.020	.000	.000		.004	.000
	N	106	106	106	106	106	106	106	106
ConscComp2	Pearson Correlation	.773**	.878**	.789**	.346**	.446**	.277**	1	.405**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.004		.000
	N	106	106	106	106	106	106	106	106
MoralCOmp2	Pearson Correlation	.307**	.351**	.331**	.848**	.902**	.890**	.405**	1
	Sig. (2-tailed)	.001	.000	.001	.000	.000	.000	.000	
	N	106	106	106	106	106	106	106	106

4. Implications for evolving measure development of "Eyes of Others"

The most parsimonious form of the model that we specify indicates interesting relationships between the Morality and Self-Consciousness "Eyes of Others" constructs and the Violator factor for typical workplace security violations. This is an initial foray into the exploration of the domain of the emergent Eyes of Others construct. To that end, we choose to interpret our findings tentatively; the results provide significant insight into the further development of an Eyes of Others measurement inventory. Our review of the security literature suggests the likely usefulness of modeling an onlooker effect in workplace security behavior, which can perhaps be linked to evolutions of the deterrence theory models in found in prior studies [9, 10, 16] since they correspond well with what we see in our exploration of the Eyes of Others construct, here.

The typical deterrence theory framework, which is where we see the onlooker effect potentially fitting in future research, typically specifies the influence of motivating factors such as punishments, including their likelihood and severity [9, 10], but also the likely role that knowledge of being monitored by sanctioning authorities for compliance might play in motivating pro-security behaviors (or, preventing violations) [10]. There is very little in the security literature leveraging deterrence theory that provides an avenue for applying peer oversight, but there are some implications well worth investigating as further refinements are made to the Eyes of Others construct and its measures.

For instance, the implication for self-perceived "shame" in the knowledge of workplace others of one's inappropriate security activities [9] might correspond with what we are learning here about onlooker effects. Certainly, the role of formal monitoring is well acknowledged, but at the same time certain authors have speculated on the role of "social others" in serving as a factor to potentially prevent violations [16].

To that end, what we learn in the final version of our reduced model (Figure 3), has implications worth considering for future Eyes of Others measure use and final validation steps in the context of a nomological network arising from existing theory. We can easily see that a sense of morality augurs against committing violations, particularly in the view of others. This seems to imply a notion that workers of strong moral fiber would not want to be seen violating their moral codes by others. That is a useful implication, to the extent that employees with that sort of orientation can be identified for recruitment, or if the characteristics of morality can be "trained up" in keeping with the robust role of SETA programs in the deterrence theory perspective on IS security [10].

The Self-Consciousness construct speaks to more basic and better-understood security dynamics; this construct is indicated by measures that are thematically related to deterrence precepts. Being nervous about being observed, in conjunction with concern about penalties for security violations and the overarching role of being observed in causing such outcomes, is a far closer match with deterrence theory precepts. The issue here, in this exploratory analysis, is the causal influence of Self-Consciousness on violations. With a positive link arising in our modeling, as compared the more easily interpreted negative link for the Morality-Violator relationship, more investigation is required to understand its true nature as to the influence Self-Consciousness plays on security violation propensity or prevention. One interpretation, purely speculative, of course, might be that where Morality clearly serves to prevent mundane security violations such as personal USB use or personal email attachment downloads, the Self-Conscious worker might be more concerned about things that bear specific, severe and highly undesired penalties (per deterrence precepts), and might not be as concerned about things that "everybody does" and which likely bear minimal organizational sanction.

4. Conclusion and implications for future research

This is an exploratory study, aimed at putting operational substance into the concept of onlooker effects in the form of the "Eyes of Others," which connotes the informal surveillance of workplace activities by coworkers. Our goal was to initiate the operationalization of the construct, and, secondarily, to benchmark a group of measures for mundane workplace security violations. Given the lack of objectively benchmarked measures for mundane security violations in the literature, that outcome, alone, has probative value for future research. Measures of security violations, however, were not the primary goal of our study; rather, they are a mere convenience for purposes of exploratory modeling of our key construct of interest, "Eyes of Others," which we have explicated and initially explored, here.

To that end, we have achieved our objective by exploring the domain of the informal onlooker effect construct, examining dimensionality and investigating preliminary cause and effect relationships with the security violation factors that we specified. The next step in the evolution of the process is to examine the emergent constructs and their prospective measures in

a broad sample of useful generality for confirmatory analysis.

It is clear that there is a time and a place for exploratory investigations that leverage conveniently accessed students for a starting point. The precision of execution and statistical benefits of homogeneity of variance found in such samples are strong benefits from these samples [3]. The generality of student samples is the typical weakness [1]. Our sample was thematically useful, being comprised of students trained in an IS security program; many of them had employment positions in technological workplaces, particularly at the graduate level, but the fact remains that this work is based on student samples and is explicitly limited by that. For that reason, we clearly delimit our findings and their implications to the typical benefit of any exploratory study: this is a starting point for something truly interesting, and the real work lies ahead in conducting a rigorous confirmatory analysis with a broad sample of generality, such as technology industry workers in full time employment.

Until that time, what we have learned here suggests to us that deterrence theory perspectives, particularly those which speculate on the potential influence of social others [16], are excellent departure points for further exploration of the Eyes of Others construct in broader and more general contexts. It is well understood that people in every walk of life, but particularly in their place of work, prize the positive approval of their peers [6], and this peer group normative influence can easily be leveraged for useful pro-security outcomes when artfully managed by the firm, is our general sense from what we have learned in this study.

10. References

[1] Anderson, J.C., and D.W. Gerbing, "Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities", Journal of Applied Psychology 76(5), 1991, pp. 732-740.

[2] Bulgurcu, B., H. Cavusoglu and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," MIS Quarterly, 34(3), 2010, pp. 523-548.

[3] Calder, B. J., L.W. Phillips and A.M. Tybout, A. M. (1981). Designing research for application. Journal of Consumer Research, 8(2), 1981, pp. 197-207.

[4] Chung, J., and Monroe, G.S., "Exploring Social Desirability Bias," Journal of Business Ethics, 44, 2003, pp. 291-302.

[5] Churchill, G.A., "A Paradigm for Developing Better Measures of Marketing Constructs", Journal of Marketing Research 16(1), 1979, pp. 64–73.

[6] Ciladini, R.B., R.J. Borden, A. Thorne, M.R. Walker, S. Freeman and L. R. Sloan, "Basking in Reflected Glory: Three (Football) Field Studies," Journal of Personality and Social Psychology 34(3), 1976, 366-375.

[7] Crossler, R.E., A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research", Computers & Security 32, 2013, pp. 90–101.

[8] Dang-Pham, D., S. Pittayachawan, and V. Bruno, "Towards a complete understanding of information security misbehaviours: a proposal for future research with social network approach", Proceedings of the 25th Australasian Conference on Information Systems, 2014, p. 10.

[9] D'Arcy, J., and T. Herath, "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," European Journal of Information Systems, 20, 2011, pp. 643-658.

[10] D'Arcy, J, A. Hovav, and D. Galetta, "User Awareness of Security Countermeasures and its Impact on Information Security Misuse: A Deterrence Approach," Information Systems Research, 20(1), 2009, pp. 79-98.

[11] DiFranzo, D., S.H. Taylor, F. Kazerooni, O.D. Wherry, and N.N. Bazarova, "Upstanding by Design: Bystander Intervention in Cyberbullying", Proceedings of the 2018 CHI Conference on Human Factors in Computing, 2018, pp. 1–12.

[12] Eriksson, D., and G. Svensson, "Managers' psychological challenges in implementing corporate responsibility in supply chains", Corporate Governance: The International Journal of Business in Society, 18(3), 2018, pp. 564-578.

[13] Fulk, J., C.W. Steinfield, J. Schmitz, and J.G. Power, "A Social Information Processing Model of Media Use in Organizations", Communication Research 14(5), 1987, pp. 529–552.

[14] Gefen, D., and D. Straub, "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example", Communications of the AIS, 16, 2005, pp. 91–109.

[15] Grimes, R.A. "The 5 Cyber Attacks you're Most Likely to Face," CSO Online, https://www.csoonline.com/article/2616316/data-protection/security-the-5-cyber-attacks-you-re-most-likely-to-face.html. Current June 2018.

[16] Herath, T., and H.R. Rao, "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations," European Journal of Information Systems, 18, 2009, pp. 106-125.

[17] Hinkin, T.R., "A Brief Tutorial on the Development of Measures for Use in Survey Questionnaires", Organizational Research Methods 1(1), 1998, pp. 104–121.

[18] Baron, R.M., and D.A. Kenny, "The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations," Journal of Personality and Social Psychology, 51(6), 1986, pp. 1173-1182.

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

[20] MacKenzie, S.B., P.M. Podsakoff, and N.P. Podsakoff, "Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques", MIS Quarterly 35(2), 2011, pp. 293–334.

[21] Marakas, G., R. Johnson, and P. Clay, "The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time.", Journal of the Association for Information Systems 8(1), 2007, pp. 16–46.

[22] Nicolini, D., J. Hartley, and J. Hurcombe, "Through the Eyes of Others: Using Developmental Peer Reviews to Promote Reflection and Change in Organizations," Journal of Organizational Change Management 24(2), 211-228.

[23] Oracle Corporation. Common Security Violations.https://docs.oracle.com/cd/E23823_01/html/820-3508/appol-5.html, current June 2018.

[24] Petter, S., Straub, D., and Rai, A., "Specifying Formative Constructs in IS Research," MIS Quarterly, 31(4), 2007, pp. 657-679

[25] Safa, N.S., and R. Von Solms, "An information security knowledge sharing model in organizations", Computers in Human Behavior 57, 2016, pp. 442–451.

[26] Sergeeva, A., M. Huysman, M. Soekijad, and B. van den Hoof, "Through the Eyes of Others: How Onlookers Shape the Use of Technology at Work", MIS Quarterly 41(4), 2017, pp. 1153–1178.

[27] Stewart, J.M. Top 5 Common Activities that Break Company Security Policy. https://www.globalknowledge.com/blog/author/jstewart/, current June 2018.

[28] Tyler, J.M., "In the Eyes of Others: Monitoring for Relational Value Cues," Human Communication Research 34(4), 521-549.

[29] Vieira da Cunha, J., "A Dramaturgical Model of the Production of Performance Data", MIS Quarterly 37(3), 2013, pp. 723–748.

[30] Wang, Y., D.B. Meister, and P.H. Gray, "Social Influence and Knowledge Management Systems Use: Evidence from Panel Data", MIS Quarterly 37(1), 2013, pp. 299–313.

[31] M. Warkentin, and R. Willison, "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," European Journal of Information Systems 18(2), 2009, pp. 101-105.