International Journal of Applied Business and Economic Research

ISSN : 0972-7302

available at http: www.serialsjournals.com

Volume 15 • Number 23 (Part 2) • 2017

Are Information Systems Security Policies Effective in Organizations? An Empirical Study of Employees' Non-compliant Behavior

Swaminathan Rajendran[1] and Shenbagaraman V.M.[2]

[1]*Corresponding author, Department of Information Technology, SRM University, Kattankulathur. Email: rajendran.s@ktr.srmuniv.ac.in*
[2]*Faculty of Management, SRM University, Kattankulathur. Email: shenbagaraman.v@ktr.srmuniv.ac.in*

ABSTRACT

Security breaches and compromise of sensitive information by insiders is a real concern for organizations. According to studies and other available reports the financial losses through lost contracts and penalties run into billions of dollars. Security violations also lower the reputation of an organization as a secure service provider. Apart from implementing technical controls to mitigate insider threats, organizations design information systems security policies to provide guidelines and enforce compliant behavior. The basic concepts of these policies come from the deterrence theory of criminology field. According to deterrence theory punishment is the suggested form to discourage rule breaking behavior. Similar to the criminal law, organizational security policies spell out penalties for policy violations. In this work, we study the effectiveness of these policies and try to determine whether they really work and deter employees from non-compliant behavior.

Keywords: Information systems security policy, compliance, insider threat, deterrence theory, non-compliant behavior.

1. INTRODUCTION

Securing confidential information and ensuring employees follow the established guidelines in the work place have become a major concern for the management of any organization. Organizations face huge financial loss and loss of reputation because of insiders' intentional or unintentional rule-breaking activities[1-3]. CERT-US (Computer Emergency Response Team) defines an insider threat [4] as "*the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization*". Ernst & Young [5] global information security survey-2015 highlights the number of malicious behavior by insiders and the cost to companies due to the security

breaches. The report points that outdated information security controls, unaware and disgruntled employees were the major causes of insider threat. PwC and Data Security Council of India [6] survey reports that approximately 50% of the IT Services and BPO sectors are affected by malicious activities of employees. Dhillon & Moores[7] explored the threat due to insiders and determined possible reasons for employees' malicious activities. This paper also discusses about the importance of establishing formal and informal controls to mitigate insider threat. In traditional crime, law makers framed rules based on the deterrence theory of criminology [8]. Criminal law is designed with the belief that punishments would deter rule breaking activities. Effective punishment has three components- severity, certainty and celerity. All the three components are necessary for deterrence. If punishment is severe, certain and accorded quickly, people would think twice before committing a crime. Research studies on traditional crime have established that the severity and certainty of punishments have negative influence criminal behavior. The celerity of punishment does not have significant effect[8,9].

2. REVIEW OF RELEVANT LITERATURE

The basic concept of deterrence theory is to prevent criminal act using fear of sanctions or punishments. The criminal justice system exists both to detain wrongdoers and influence the would-be wrongdoers from committing crime[8,10,11]. The scholars say that before committing a crime, a criminal weighs his options and if the benefits are more than the costs, he commits the crime (Beccaria 1738-1794; Bentham 1748-1832). The deterrence theory has three components, namely, severity of punishments, certainty of punishments, and celerity of punishments. The theory posits that if the punishment to a crime is severe, then the person who intends to commit a crime would stay away from performing the crime. He/she weighs the benefits and costs of the crime and if the costs are higher, he/she may not involve in rule-breaking activities. Straub and Nance [12] in their study applied deterrence theory in IS field and advocated computer misuse detection and punishment act as a deterrent. Subsequent studies also strengthened the view that application of deterrent theory improved the effectiveness of IS security compliance. Empirical studies do not comprehensively support the theory that increase in the severity of the punishment reduces the crime [13,14].

The second component, certainty of punishments the deterrence theory suggests that individuals will not involve in criminal activities. However, severe may be the crime and punishment, if the probability of getting punished is low, then a person would definitely involve in deviant activities. Research findings state that certainty of sanctions has more deterrence effect compared to severity of sanctions [9,15,16]. According to the third component, celerity of punishments, if the criminal is punished quickly for the crime, then next time he/she would not involve in criminal activities. Since the judicial process consumes more time in general, it is difficult to determine the effectiveness of celerity. There is not much research done on celerity of punishments.

Scholarly research in deterrence theory broadened the scope of deterrence and added number of extensions[17,18]. Two notable extensions are informal sanctions and shame on oneself [19-21]. Disapproval from family members, friends, and co-workers is an example of informal sanction [18]. Shame is defined as a painful emotion caused by consciousness of guilt, shortcoming, or impropriety (Merriam Webster Dictionary). When a person acts against social norms or standards, he/she goes through feeling of guilt or embarrassment. The informal sanctions and shame are generally known as "non-legal costs" [22] of committing a crime. Siponen [23] added informal sanctions and shame in their study of deterrence theory

applied to information security policy (ISP) violations. They used composite measures combining severity and certainty of sanctions with formal sanctions, informal sanctions, and shame to measure the effectiveness of the constructs. We decided to use them separately, since not combining them provides more granularity in determining the effectiveness of severity and certainty constructs independently.

3. RESEARCH MODEL

We developed the research model based on the literature review for deterrence theory[23-25]. The model consists of six components, the severity of formal sanctions, severity of informal sanctions, severity of shame on oneself, certainty of formal sanctions, certainty of informal sanctions, and certainty of shame on oneself.

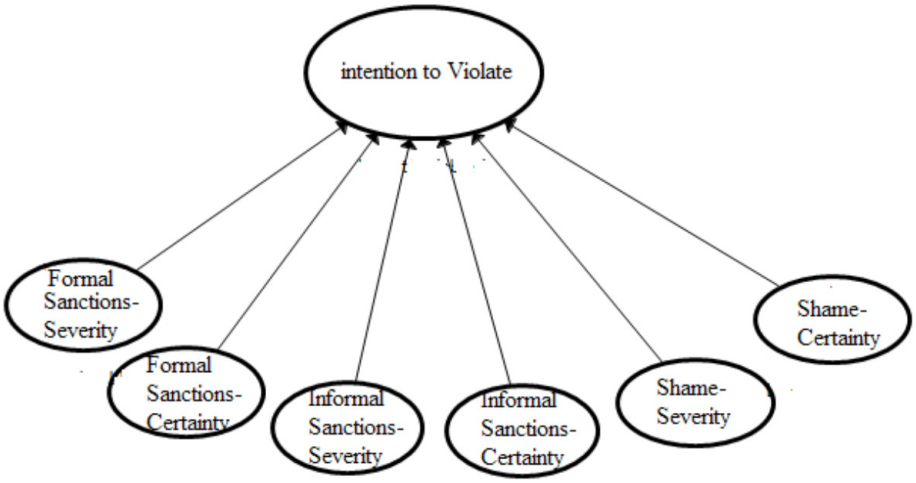

Figure 1: Research Model

Based on the available literature and arguments put forth above, we formulated the hypotheses as given below:

H_1: Severity of *formal sanctions negatively influences intention to violate ISPs*

H_2: Certainty of *formal sanctions negatively influences the intention to violate ISPs*

H_3: *Severity of informal sanctions negatively influences intention to violate ISPs*

H_4: *Certainty of informal sanctions negatively influences intention to violate ISPs*

H_5: *Severity of shame negatively influences intention to violate ISPs*

H_6: *Certainty of shame negatively influences intention to violate ISSPs*

4. RESEARCH DESIGN

As done in most of the behavior related research studies, we decided to use scenario based study. Scenario-based surveys have been used as a technique to assess the security readiness of organizational members in previous studies [26,27]. It is more effective to capture the participants' security readiness if they are not conscious that their awareness is being assessed [26], since they might act differently if they knew that their awareness was being assessed. We designed a scenario based on "sharing of password with colleagues"

which is one of the most common ISP violations. Scenario based studies are recommended for behavioral studies in literature [23,28]. The scenario used in our study is reproduced below:

Scenario: The Miles Stock Automation (MSA) Inc., management has been focusing on decreasing IT security policy violations by employees within their organization. They have a well-documented security policy with penalties for non-compliance. Sharing passwords among employees is a violation of information systems security policy. Ranjith, Senior Manager of MSA has gone out of station to attend to an important personal work. His coworker, John requests Ranjith for access to certain databases required for completion of a project. Since the work has to be completed to meet the deadline, Ranjith shares the password with John who is trustworthy. He is fully aware of the security policies and the penalty for not following them. Ranjith feels completion of the work is more important and the password may be changed later.

4.1. Instrumentation

We considered three deterrent constructs, namely, (i) formal sanctions, (ii) informal sanctions, and (iii) shame and divided this into two groups, severity and certainty. This method provides a chance to narrow down on the deterrent constructs that are significant which was not possible in Siponen et. al., [23] study where they used a composite measure. Three items were used for each construct. The items were adapted from previous research after suitably modifying to the environment. Each item was measured on a 7 point Likert scale ranging from "stronglydisagree" to "strongly agree". Along with these, demographic data like organization type, size, gender, age, education, and experience, were collected. A sample of the questionnaire with one item per construct is listed in Table 1.

Table 1
Instrumentation (Sample)

Theory	*Constructs*	*Item*	*Source*
	Intention to violate security policy	What is the chance that you would do what Ranjith (scenario character) did in the described scenario	Adapted from Paternoster & Simpson [29], Siponen et. al., [23]
Deterrence	Formal Sanction-Certainty	What is the chance you would be punished if you violated the company information security policy	Adapted from Nagin & Paternoster [30], Paternoster & Simpson [29] Siponen et. al., [23]
	Formal Sanctions-Severity	Will it be a severe problem if you received severe sanctions if you violated the company information security policy	
	Informal Sanctions-Certainty	How likely is it that you would lose the respect and good opinion of your co-workers for violating the company information security policy?	
	Informal Sanctions-Severity	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?	
	Certainty of shame for oneself	How likely is it that you would be ashamed if co-workers knew that you had violated company information security policy	
	Severity of shame for oneself	How much of a problem would it be if you felt ashamed that co-workers knew you had violated the company information security policy?	

4.2. Data Collection

Primary data for the research were collected from five different companies belonging to IT sectors. An online form containing the questionnaire was sent to approximately 3000 employees working in IT Services and BPOs for data collection. A total of 216 employees participated in the survey. All respondents had university degree and use computer as part of their day-to-day work. IS security policy had been implemented in their organization and everyone had knowledge about the policies. Table 2 provides basic descriptive statistics of the data.

Table 2
Descriptive Statistics

Sample Size	*Avg Age (years)*	*Avg work experience (years)*	*Male/Female %*	*Avg Realism score (10)*	*Average intention to violate score (10)*	*% of respondents with intention to violate*
216	29.5	5.8	52/48	6.73	3.72	25.5

The average realism score of 6.3 indicates that the scenario described is realistic and the respondents are aware of such events. The average intention to violate score of 3.72 demonstrates in the presence of punitive measures most of the participants do not intent to violate security policies.

5. MODEL ANALYSIS

The research model was conceptualized as a multidimensional reflective first order construct. We had chosen PLS path modeling because of its strength over other traditional statistical techniques such as multiple regression and analysis of variance. PLS does not impose multivariate homogeneity and normality requirements on the data [23,31,32]. We used "plspm" package in R developed by Gaston Sanchez [33].

As a part of the instrument, we included organization sector, size, experience, gender, age, and qualification. The one-way ANOVA test conducted for determining the effect of these control variables did not provide any significant support.

5.1. Assessment of Model Quality

Table 3 contains the reliability and convergent validity measures. The Cronbach's alpha and composite reliability are greater than 0.7 and satisfy the reliability criterion. Composite reliability measure is also used for convergent validity in PLS-based research [23,32]. Average Variance Extracted measure is used as a test for both convergent and discriminant validity. It reflects the average communality for each latent factor in a reflective model. All AVE values are greater than 0.5 and thereby satisfy the criteria for validity.

Table 3
Reliability and Convergent Validity Assessment Measures

S.No.	*Construct*	*Cronbach's alpha*	*Composite Reliability*	*AVE*
1	Formal Sanctions-Severity (FSS)	0.90	0.94	0.84
2	Formal Sanctions-Certainty (FSC)	0.92	0.95	0.86
3	Informal Sanctions-Severity (ISS)	0.93	0.96	0.88
4	Informal Sanctions-Certainty (ISC)	0.90	0.94	0.84
5	Shame-Severity (SSH)	0.94	0.96	0.89
6	Shame-Certainty (CSH)	0.92	0.95	0.86

Table 4 provides additional test of measure, known as Fornell-Larcker[34] criterion, for discriminant validity. According to this criterion, the square root of AVE should be higher than its with any other latent variable. We could observe this in Table 3, where the diagonal elements (AVEs) are the largest elements in the corresponding column. This criterion also is satisfied. Therefore, we conclude that the model has good reliability and validity [23, 35].

Table 4
Fornell-Larcker Criterion for Discriminant Validity

	CSH	*FSC*	*FSS*	*ISC*	*ISS*	*SSH*
CSH	0.93					
FSC	0.58	0.93				
FSS	0.65	0.75	0.92			
ISC	0.65	0.71	0.76	0.92		
ISS	0.77	0.74	0.78	0.78	0.94	
SSH	0.63	0.54	0.61	0.61	0.75	0.94

Recent researches using PLS models make use of additional measure known as hetero-trait mono-trait (HTMT) coefficients [36, 37]. All the HTMT coefficients in our study were less than the threshold value of 0.85 which indicates good discriminant validity. Goodness of fit of the model [36, 37] is assessed using standardized root mean square residual (SRMR). The SRMR value for our model is0.042which indicates an excellent model fit.

5.2. Results of PLS Analysis

After validating and verifying the quality of the model, we analyzed the relevant results of the analyses to check how many of our hypotheses were supported by the study. Table 5 provides the results for hypotheses testing in detail. Hypotheses H_2, H_3, and H_4 have Values > 1.96 and $p < 0.05$ and hence they are supported. Hypotheses H_1, H_5, and H_6 are not supported.

Table 5
Hypothesized Path coefficients

Hypothesis	*Path*	*Path-coeff*	*T Statistics*	*P value*	*Remark*
H_1	FSS -> intention to violate	–0.02	0.41	0.68	Not supported
H_2	FSC-> intention to violate	–0.40	9.39	0.00*	Supported
H_3	ISH -> intention to violate	–0.22	3.71	0.00*	Supported
H_4	ISC -> intention to violate	–0.43	7.63	0.00*	Supported
H_5	SSH-> intention to violate	0.05	0.76	0.45	Not supported
H_6	CSH-> intention to violate	0.05	0.78	0.44	Not supported

*$p < 0.001$

Figure 2 provides the path coefficients for the deterrent constructs. Formal sanctions (certainty) and informal sanctions (both severity and certainty) were significant. Though the formal sanctions (severity) has a negative path coefficient indicating it negatively influences "intention to violate", it is not significant (T value < 1.96 and $p > 0.05$).

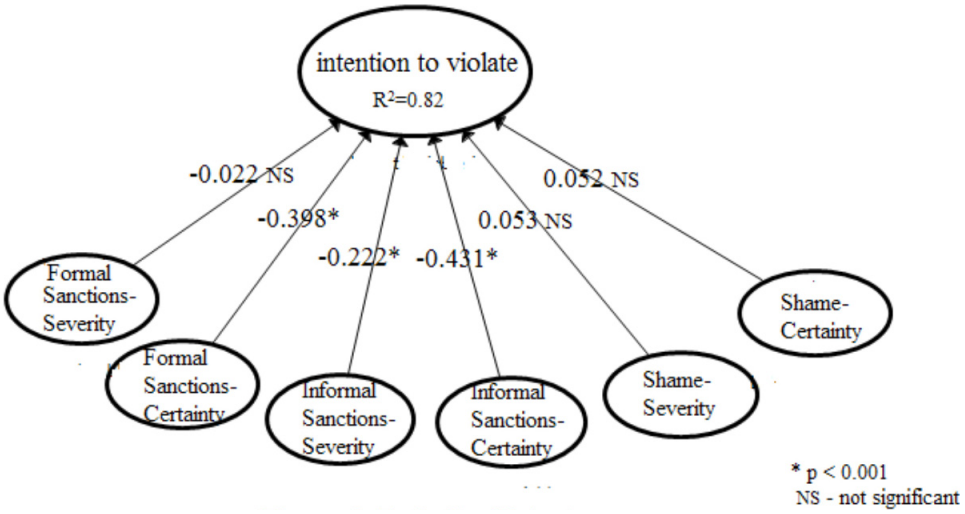

Figure 2: Path Coefficients

6. LIMITATIONS

The study mostly focused only on millennial employees those born between 1980 and 1995. Since we did not collect data from the Gen X employees, it is difficult to compare with other generation employees. This work was based on a hypothetical scenario and a question on respondent's intention to violate ISS policies, the actual behavior is not directly captured. But according to past research [11, 23, 38] the intention acts as a precursor to actual behavior. It is difficult to generalize the employees' behavior based on the responses from one or two industries. Nonetheless, our findings are similar to studies conducted in other countries and available literature [23].

7. PRACTICAL IMPLICATIONS

Non-compliant behavior is present in most of the organizations where ISS policies are implemented and organizations fail to study the causes for such rule-breaking behaviors. Using IS security policy as a means of deterrence is not sufficient. Our study finds that the severity of formal sanctions is not effective. The results of our study suggest the severity of punishment did not matter to employees with an intention to break rules, as long as the policies remain only on paper The management should ensure that the policies work and initiate steps to ensure strict enforcement. Whenever someone is punished, it should be made known other employees as a deterrent measure. Also the policies, grounded on the severity and the certainty of shame on oneself, are not effective based on our analysis. It also demonstrates human relationship within an organization is important.

8. CONCLUSIONS

Our study reinforces the findings in traditional criminology field and some of the studies conducted in the IS field that people violate rules irrespective of the severity of the punishments. This is a fact which a common man could observe in day-to-day life. Unless rules are enforced strictly and punishment is made certain, one or another employee would involve in unacceptable behavior and put organizations under risk. Creating awareness about IS security policies through information security education, rigorous monitoring,

and stringent punishments are the measures through which organizations could mitigate IS security policy violations.

References

Tsiakis, T. and Stephanides, G. (2005). "The economic approach of information security", Computers & Security, vol. 24(2), pp. 105-108.

Carl Colwill. (2009). "Human Factors in Information Security: The Insider Threat- Who can you Trust These Days, Information Security Technical Report", pp. 186-19.

Cook, R. (2013). "Next Generation Insider Threat", https://www.csiac.org/sites/default/files/Talk 6_Richard Cook.pptx

(accessed on Aug 27, 2016)

CERT (2014). "2014 US State of Cybercrime Survey" http://resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_298322.pdf

(accessed on October 6,2016)

Ernst & Young. (2015). Ernest & Young 2015 Global Information Security Survey http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf (accessed on Mar 4,2016)

DSCI-PwC Survey. (2011). " The Threat Within".

http://www.pwc.in/en_IN/in/assets/pdfs/publications-2011/The_Threat_Within.pdf(accessed on Sep 18,2016)

Dhillon,G. and Moores, S. (2001). "Computer Crimes: Theorizing about the Enemy Within", Computer and Security,20(8): 715-723.

Chris Mark, (2012). "A Failed State of Security: A Rational Analysis of Deterrence Theory and The Effect on CyberCrime ".https://maritimerisk.files.wordpress.com/2012/03/deterrence-theory-in-cybercrime_final.pdf

(accessed on Sep 10,2016)

Kevin C Kennedy. (1983). "A Critical Appraisal of Criminal Deterrence Theory", 88 Dick.L.Rev.1(1983-1984).

http://digitalcommons.law.msu,edu/facpubs

(accessed on Sep 10,2016)

Nagin, D.S. (1998). "Criminal Deterrence Research at the Outset of in the 21st Century", Crime and Justice,University of Chicago Press, Vol 23: 1-42.

Paternoster, R. (2010). "How Much We Really Know About Criminal Deterrence", Journal of Criminal Law and Criminology, 100(3):765-823.

Straub, D.W., and Nance, W.D. (1990). "Discovering and Disciplining Computer Abuse in Organizations: A Field Study", MIS Quarterly, 14(1): 45-62.

Doob, A.N. and Webster, C.M. (2003). "Sentence Severity and Crime: Accepting the Null Hypothesis", Crime and Justice, 30:143-195.

Kleck,G.B.,Sever,S.,Li and M.Gertz. (2005)."The missing Link in General Deterrence Research," Criminology,43(3):623-660.

Valerie Wright.(2010). "Deterrence in Criminal Justice- evaluating certainty Vs severity of punishment", The Sentencing Project.

Donald Ritchie. (2011)."Does Imprisonment Deter? A Review of the Evidence", Sentencing Advisory Council, Victoria, Australia.

https://www.sentencingcouncil.vic.gov.au/publications/does-imprisonment-deter

Grasmick, H.G., and Bryjak,G.J. (1980). "The Deterrent Effect of Perceived Severity Punishment," Social Forces (59:2), pp 471-491.

Piquero, A.R., and Tibbetts, S.G.(1996). "Specifying the Direct and Indirect Effects on Low Self-Control and Situational Factors in Offenders Decision Making: Toward a More Comparative Model of Rational Offending," Justice Quarterly (13:3), pp 481-510.

Piquero, A.R., and Tibbetts, S.G. (2002).Ed. "Rational Choice and Criminal Behavior: Recent Research and Future Trends", Routledge Publishers, 2002.

Braithwaite, J. (1989). "Crime, Shame and Reintegration", New York: Cambridge University Press.

Paternoster, Raymond, and Sally Simpson. (1997). "Sanction Threats and Appeals to Morality: Testing a Rational Choice Theory of Corporate Crime", Law and Society Review 30:549-84.

Pratt,T.c, and Cullen, F.T. (2000). "The Empirical Status of Gottfredson and Hirschi's General Theory of Crime: A Meta-Analysis," Criminology (38:3), pp 931-964.

Siponen, M. and Vance, A. (2010). "NEUTRALIZATION: New Insights into the Problem of Employee Information System Security Policy Violations", MIS Quarterly 34(3): 485-502.

Siponen, M. and Iivari, J. (2006). "Six Design Theories for IS Security Policies and Guidelines", Journal of the Association for Information Systems 7 (7):445-472.

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

Nohlberg, M. (2005). "Social Engineering Audits Using Anonymous Surveys- Conning the Users in Order to Know if Thaey Can Be Conned," In Proceedings of the 4th Security Conference, Las Vegas, USA.

Flores, W.R., Holm,H., Svensson, G., and Ericsson, G. (2013). " Using Phishing Experiments and Scenario-Based Surveys to Understand Security Behaviors in Practice," Proceedings of the European Information Security Multi-Conference.

Hanisch,K.A., Hulin,C.L.,&Roznowski, M. (1998). "The importance of individuals' repertoires of behaviors: The Scientific appropriateness of studying multiple behaviors and general attitudes". Journal of Organizational Behaviour,Vol 19:463-480.

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.

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

Kankanhalli A.,Teo,H.H., Tan, B.C.Y. and Wei, K.K. (2003). "An Integrative Study of Information Systems Security Effectiveness", International Journal of Information Management,23(2): pp.139-154.

Wynne W. Chin. (1998). "The Partial Least Squares Approach for Structural Equation Modeling", Modern Methods for Business Research, vol. 295(2), pp. 295-336.

Sanchez, G. (2013). "PLS Path Modeling with R", Trowchez Editions, Berkeley.

http://www.gastonsanchez.com/PLS_Path_Modeling_with_R.pdf.

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

Wynne W. Chin. (2010). "How to Write Up and Report PLS Analyses: Handbook of Partial Least Squares: edited by V. Esposito Vinziet al", Springer Handbooks.

JorgHenseler, Geoffrey Hubona, Pauline Ray. (2016). "Using PLS path modeling in new technology research: updated guidelines", Industrial management and Data Systems, Vol 116, No:1,2016 pp 2-20.

Jr Hair, J.F., Hult, G.T.M.,Ringle, G. and Sarstedt,M. (2014). "A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)", Sage Publications.

Bachman, Ronet, Raymond Paternoster, and Sally Ward. (1992). "The Rationality of Sexual Offending: Testing a Deterrence/ Rational Choice Conception of Sexual Assault", Law and Society Review 26: pp. 343-372.