

A Theoretical Review of Neutralization in Security Policy

Myeonggil Choi¹ and Jeongseok Song^{2*}

¹Department of Business Administration, Chung-Ang University, 84 Heukseak-Ro, Dongjak-Gu, Seoul, 156-756, Korea; mgchoi@cau.ac.kr.

²Department of Economics, Chung-Ang University, 84 Heukseak-Ro, Dongjak-Gu, Seoul, 156-756, Korea; jssong@cau.ac.kr

Abstract

Objectives: In these days, security violation could lead to vulnerabilities of organization. Many scholars tried to explain the violation and suggested ways to prevent user from violating information security policy. **Methods/Statistical Analysis:** While neutralization is used to explain the behavior of juvenile delinquency, neutralization is utilized to show the behavior of the violation in information security. Neutralization was used to explain the software piracy and the violation of information security. This study tries to investigate the extensive literature review explaining the violation behavior of information security policy and summarizes the important mainstreams giving the implications. This paper invests theoretical ground on neutralization. **Findings:** This study suggests the extensive adaptability of neutralization techniques applied in the information security policy. Individuals consider the violation of information security the minor rule breaking behavior. Neutralization has been utilized to explain the minor deviant behavior, so it also can be accepted to explain the various violation behaviors in the field of information security policy. **Improvements/Applications:** Neutralization can be useful in understanding the violation behavior of information security policy and used in designing security management systems in various organizations.

Keywords: Deterrence Theory, Information Security, Neutralization, Organization Theory, Rational Theory, Violation Behavior

1. Introduction

Most of information security incidents take place as a result of internal employee's negligence and carelessness of information systems for daily accomplishing tasks¹. Recent several studies have revealed that noncompliance of employees with information security policy have directly or indirectly related with incidents in organizations². The breach of employee is owed to the negligence and carelessness to IS security policy.

IS security researchers have explained the phenomena in noncompliance with IS security policies. Deterrence theory explains sanction could decrease the violation of IS policy³ but the violations of IS policy could not decreased in spite of many organization's use of sanctions. Recent IS research indicates that the reason of security incidents

occurring in a certain of formal sanctions is the use of neutralization techniques, which gives an justification for violations⁴. In⁵ applied neutralization techniques in order to account for a intention of employees' IS security policy compliance and reported that both neutralization techniques and deterrence theory influenced an intention to employees' IS police compliance. Neutralization techniques explain more sufficiently employees' compliance with IS security policies than deterrence theory. Many studies have applied empirical support for neutralization technique such as a study on the effects on the IT security breaches, a study of employees' intention on personal use of internet.

Since neutralization techniques are individual intrinsic factors, individual differences exist. As a result, individual neutralization techniques are inner nature, which is not easy to change in the short term. Much research offered

*Author for correspondence

explanations to applying neutralization techniques on organizational insider. In this study, we try to clarify what shuts up and gives influences on the neutralization in the violation of IS policy. Organization is able to establish appropriate measures, which of measures affect the employees' neutralization techniques.

2. Theoretical Review on Compliance with Information Security

The more individuals and organization are sharing their knowledge and making online transactions, the more problems arise from information security. Even though both IS security managers and industry are trying to figure out actively to improve security, non-technical factors, such as human resource.

One of the greatest threat of IS security is an organizational insider's intentional or unintentional violation of IS security not by external hackers. It has long been recognized by scholars that organizational insiders of IS security play an important roles to establish and practice an effective security procedures. IS researchers have given an explanation for investigating and revealing IS security with, organization theory, rational choice theory, deterrence theory and neutralization theory.

2.1 Organization Theory

On the perspective of organization theory, prior IS research have showed that organizational factors and individual factors influence on employees' IS security police compliancy. There are organizational factors such as the top management's participating for IS security², organizational culture⁶. It is indicated by individual factors such as self-efficacy, subjective norms belief and attitude¹, perceived control⁷.

2.2 Rational Choice Theory

IS research on the view of rational choice theory have proposed that rewards and punishments impact on employee' IS security compliance⁸. Consequently, the research drawing on rational choice theory have asserted the need of positive compensations for regulating employees' violation of IS security.

2.3 Deterrence Theory

Deterrence theory posits that the severity and the certainty of sanctions produce an effect on employees' behavior

of IS security compliance. Deterrence theory, which severity and certainty of formal sanctions to violators can weaken a crime rate, is widely used in a study of criminology. Through the deterrence theory in IS, it is suggested that detection and punishment of violators minimizes computer abuse; the deterrence diminishes IS security abuse. It is effective on the simultaneous use of informal and formal sanction; security policy, SETA program and computer monitoring also weigh on the deterrence.

Since the deterrence influences on response effectiveness and self-efficacy, it has a positive effect on employees' IS security policy compliance³. Managing restraints and severity of sanction including individual security compliance affects the efficacy of IS security of organization. While the deterrence regulates the effectiveness of individual IS security compliance, the trust of employees to organization also can be reduced. Consequentially, employees take an opposite action against the deterrence of organization. Even when organization enforcing sanctions to employees, moral reasoning and neutralization technique of employees could justify their offence. Estimating that the deterrence is not enough to improve intention and action of employees' compliance on IS security, we suggest that neutralization technique is fairly persuasive to intention of employees to compliance with IS security policy.

3. Neutralization Theory

Not only the extent of relationship between rationalization and deviance on a study of crime have been directly affected by rationalization and deviance but also other regulating factors control the strength of relationships. Most studies of IS employing neutralization display the occurrence of neutralization, yet do not suggest how neutralization can be restrained.

In⁴ proposed neutralization theory with differential association and sub cultural theory⁴. According to the neutralization theory, while offenders rationalize their behaviors feeling that the law is not reasonable; offenders believe themselves to maintain social norm, conflicting with rational rules. Even offenders actually commit a crime; offenders have neutralizations to rationalize violations.

Neutralization techniques include five techniques, which are denial of injury, denial of the victim, denial of responsibility, condemnation of the condemners, and appeal to higher loyalties. Defense of necessity accounts

for white-collar crime and the metaphor of the ledger are added. Later theoretical category is expanded to twelve techniques.

Neutralization techniques are not based on the behavior of mistake; neutralization techniques are cunning and unconscious mechanism to protect one's ego from guilt; neutralization techniques also are well-honed ego-defense skills and strategies. Yet, several points relevant to neutralization techniques are limited to explain the behavior of violation; an individual who has fundamentally different concept regarding a crime (e.g. psycho-pass); an individual who change the perception of criminal act owing to ongoing crime (e.g. ongoing offender); an criminal who is caused by the difference of social and cultural concept (e.g. a hemp smoker). According to the previous studies, much studies showed the relationship between neutralization and deviance, whereas the relationship of both typically has been weak. Some of the studies have showed contra dictionary findings.

The acceptance of neutralizations and engagement in a crime shows a weak relationship, but a positive relationship. There is a strong correlation between neutralization and less serious deviant behaviors such as college cheating⁹, workplace deviance¹⁰, drinking behaviors¹¹, shoplifting⁷, and minor delinquency¹². Yet the negative relationship exists between neutralization and delinquent acts. According to the control theory, an individual with more strongly attached to society, has difficulty in using techniques of neutralizing the beliefs espoused by society¹².

Age is a potentially significant factor in using neutralization. Much evidences support that young and old people engage in their offence differently. Although older, more experienced criminals depend on neutralization less than younger offenders, gender is only accepted as control variables in reveal of privacy, employee's abuse of Internet. In addition, the impact of the age on differentiation association is needed to test further.

Most of studies regarding neutralizations on IS field have explained deviance regarding neutralization as a frame of explanation rather than have explored the reason restraining on occurrence of neutralization. Neutralization has been enough to explain on delinquents such as violation of IS security policy, invasion of privacy, computer abuse. When deviance is explained on IS field, neutralization is more persuasive than self-control theory, social learning theory, micro-anomie theory, planned behavior theory, protected motivation theory.

In an organization context, deterrence is less affected but neutralization has influence on their relationship; Neutralization techniques have impact on the relationship than severity of deterrence. The shame, which is subcomponent of neutralizations and deterrence theory, has restrained the intention of piracy¹³. Internal factors such as neutralization, shame, moral belief than formal sanctions from external world impact on inhibitions.

Higher level of self-esteem has protected individuals from delinquency, whereas there are some studies that higher level of self-esteem has allowed individuals to engage in deviance.

According to a study on juvenile delinquents, neutralization techniques relying on the levels of self-efficacy have effect on using the strength of deviant behavior and neutralization [L4]. The relevance of self-esteem, neutralization and delinquent have come into contradiction.

The most commonly estimated relation between delinquency and self-esteem is that delinquency and self-esteem are inversely related. Self-esteem weakens deviant behavior. While an inverse relationship between self-esteem and initial delinquency is predicted, low self-esteem is related to delinquency as a means to enhance self-regard. Adults with high self-esteem have a strong tendency to participate in legitimate works and family. Consequently, Adults' self-esteem have predicted the duration of deviant behavior.

Social delinquency theory and neutralization theory have displayed negative relationship between criminal attitude on society and self-esteem. Tested several containments hypotheses, self-esteem and crime have been negative association. Self-esteem and delinquency have been positively related. Aggressive and violent individuals have a tendency to more high self-esteem than the average.

The relationship between neutralization theory and the commitment of traditional norms is curve linear. The commitment to traditional values has a relation to reduce delinquency. Given that individuals concentrate on moral commitment, the relation between deviant behavior and neutralization techniques is weakened. It is empirically tested that since individuals with commitment to ethics are rather difficult to overcome guilt, those individuals do not apply neutralizations regarding commit the crime.

Individuals with less commitment to conventional morality being absorbed in a sub cultural life-style, are no need for neutralizations. The commitment which has an effect on deviant behaviors is divided into the

commitments to unofficial social device and social norms and the commitment to criminal behaviors.

4. Discussion and Conclusion

To improve the intention to IS security compliance policy, direct means such as education of IS security and training have been stressed. Organizational values and commitment to norms have not yet be stressed. IS security policy can be recognized as a kind of organizational norm? Basically, information security is regarded as compliance of organizational norms. Not-stressing organizational values and commitment to norms makes it difficult to stop neutralizations, which weaken compliance of IS security policy.

5. References

1. Herath T, Rao HR. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems*. 2009; 47:154-65.
2. Puhakainen P. Oulu, Finland: University of Oulu: A design theory for information security awareness. 2006.
3. Kankanhalli A, Teo HH, Tan BCY, Wei KK. An integrative study of information systems security effectiveness. *International Journal of Information Management*. 2003; 23:139-54.
4. Sykes G, Matza D. Techniques of neutralization: a theory of delinquency. *American Sociological Review*. 1957; 22(6):664-70.
5. Siponen M, Vance A. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*. 2010; 34(3):487-502.
6. Knapp KJ, Marshall TE, Rainer RK, Ford FN. Information security: management's effect on culture and policy. *Information Management & Computer Security*. 2006; 14(1):24-36.
7. Agnew R, Ardith AR. The techniques of neutralization an analysis of predisposing and situational factors. *Criminal Justice and Behavior*. 1986; 13(1):81-97.
8. Kohn A. Why incentive plans cannot work. *Harvard Business Review*. 1993; 71(5):54-62.
9. Haines VJ, Diekhoff GM, LaBeff EE, Clark RE. College cheating: immaturity, lack of commitment, and the neutralizing attitude. *Research in Higher Education*. 1986; 25(4):342-54.
10. Hollingera RC. Neutralizing in the workplace: an empirical analysis of property theft and production deviance. *Deviant Behavior*. 1991; 12(2):169-202.
11. Doddera RA, Hughesb SP. Neutralization of drinking behavior. *Deviant Behavior*. 1993; 14(1):65-79.
12. Maruna S, Copes H. What have we learned from five decades of neutralization research? *Crime and Justice*. 2005; 32:221-320.
13. Straub DW. Effective IS security: an empirical study. *Information Systems Research*. 1990; 1(3):255-71.