Cerdika: Jurnal Ilmiah Indonesia, Juli 2025, 5 (7) 2025, 2096-2102
p-ISSN: 2774-6291 e-ISSN: 2774-6534

Available online at http://cerdika.publikasiindonesia.id/index.php/cerdika/index

Absolute Versus Restrictive Deterrence on Information Security Policy Compliance Behavior in Organizations: A Systematic Review of the Literature

Yulia Megasari[1], Sony Warsono[2], Noorfaiz Athallah Koeswandana[3]
Universitas Gadjah Mada, Indonesia[1,2,3]
Email: Yuliamega17.yms@mail.com, swarsono@ugm.ac.id, Noorfaiz.Koeswandana@uii.ac.id

Keywords
Deterrence Theory (DT); Rational Choice Theory (RCT); Absolute Deterrence; Restrictive Deterrence; Security, Behavioral Security; Organizational Security

Abstract
In the digital era, organizations are increasingly vulnerable to insider threats and non-compliance with information security policies. This study presents a systematic literature review aimed at conceptually distinguishing between absolute and restrictive deterrence within the context of employee compliance with organizational information security policies. The review draws upon academic databases such as MIS, Springer, JSTOR, ScienceDirect, AISeL, and EBSCO using keywords including deterrence theory, compliance, and information security behavior. The findings reveal that while absolute deterrence focuses on formal, law-enforced sanctions to prevent insider criminal acts, restrictive deterrence seeks to reduce the frequency of policy violations by imposing informal or less severe formal controls. This review highlights inconsistencies in how deterrence constructs are operationalized across studies—some blending severity, certainty, and swiftness into a single variable, others substituting deterrence indicators with proxies like awareness and education. Despite these differences, the review underscores that research on deterrence in information security remains in its developmental stage. It suggests a need for further empirical studies that compare the impact of deterrence mechanisms with positive motivational strategies to encourage compliance. Additionally, this review calls for future research to address different types of criminal decision-making processes and contextual organizational factors that influence behavior. These insights are valuable for designing more effective information security governance frameworks tailored to human behavior in the workplace.

**Correspondence Author: Yulia Megasari*
Email: Yuliamega17.yms@mail.com

INTRODUCTION

In the current digital era, safeguarding the security of *information systems* has become exceedingly crucial for organizations. Incidents involving *information security* have witnessed a rapid increase, resulting in significant losses. The widespread adoption of *information systems* (*IS*) has led to the misuse of technology, making it a critical asset within organizations (D'Arcy et al., 2014; Tarafdar et al., 2015). The presence of *Information Technology* (*IT*) has a dark side, with the potential to violate the well-being of individuals, organizations, and society (Tarafdar et al., 2015). For example, the Chinese ride-hailing firm *Didi Global* incurred a $1.19 billion fine for violating network security, data security, and personal information protection laws imposed by the *Cyberspace Administration of China* (Hill, 2022). Similarly, the American multinational technology company *Amazon* was fined $877 million for breaching *GDPR* cookie

regulations (Hill, 2022). Non-compliance with IT policies by employees—often considered passive policies—contributes to the misuse of *information systems* (Willison & Lowry, 2018). Data breaches impose a substantial financial impact on organizations, with an average cost of $4.35 million globally in 2022, marking a 2.6% increase from the previous year (Hill, 2022). Managers are increasingly driven to explore ways to make decisions or establish rules that ensure employee compliance with *information security policies* to mitigate such incidents, as organizations have developed such policies (Moody et al., 2018; Siponen & Vance, 2010).

Information system security encompasses policies and procedures implemented to protect sensitive information from both internal and external threats. However, despite stringent security policies that can be implemented, issues arise concerning user compliance with these policies. Some users within an organization may not adhere to *information system security policies*, increasing the risk of attacks or security breaches. The perceived formal and informal sanctions faced by employees—as perpetrators—that limit the frequency of their violations are referred to as *restrictive deterrence*, while *absolute deterrence* aims to reduce employee participation in criminal activities through legally enforced formal systems (Gibbs, 1968). Employee behavior within organizations is influenced by both informal actions and formal control systems (Beusch et al., 2022; Einhorn et al., 2024; García Osma et al., 2022; Pfister et al., 2023). Additionally, Willison, Lowry et al. (2018) emphasize the distinction between *absolute* and *restrictive* prevention in the context of *information security* incidents. The objective of this article is to conceptually explain the differences between *absolute* and *restrictive deterrence* as managerial considerations for ensuring employee compliance with *information security policies* within organizations.

1. **RQ1.** What is the difference between the *absolute deterrence* and *restrictive deterrence* approaches in driving compliance with *information system security policies* in an organizational context?
2. **RQ2.** How does the *absolute deterrence* approach influence user behavior and compliance with *information system security policies*?
3. **RQ3.** How does the *restrictive deterrence* approach affect user behavior and compliance with *information system security policies*?

The focus of this research is to conduct a *systematic literature review* to analyze the differences and impacts of the *absolute deterrence* and *restrictive deterrence* approaches on compliance with *information system security policies* in the context of organizational behavior. Thus, this study aims to provide a better understanding of the factors that influence compliance and to identify effective strategies for enhancing adherence at the organizational level.

The subsequent study is structured as follows: Section 2 presents the methodology; Section 3 explores deterrence in the context of *information security policy compliance behavior* in organizations; Section 4 discusses *absolute* versus *restrictive deterrence*; Section 5 concludes the study.

The research gap lies in the fragmented operationalization of deterrence constructs across empirical studies. Many researchers conflate severity, certainty, and swiftness of punishment into a single measure, while others substitute these with proxies such as *security awareness* or *ethical codes*. As a result, a coherent framework distinguishing *absolute* and *restrictive deterrence* and their respective effects on compliance remains underdeveloped.

Furthermore, few studies have examined how these deterrent approaches function in dynamic organizational environments or in conjunction with positive incentives.

This gap signals an urgent need for systematic research that compares the efficacy of *absolute* versus *restrictive deterrence* in shaping employee behavior. In the face of escalating cyber threats and increased regulatory scrutiny, organizations must ensure their deterrence strategies are not only theoretically sound but also practically effective. Understanding how different deterrent mechanisms influence behavior can help organizations prevent security breaches before they occur.

The novelty of this research lies in its comprehensive literature review that systematically distinguishes between *absolute* and *restrictive deterrence* in the context of *information system policy compliance*. By focusing on behavioral mechanisms rather than solely on technical controls, this study offers new insights into how *deterrence theory* can be adapted and applied to organizational security policies. It also integrates insights from *criminology*, *organizational behavior*, and *information systems* into a unified conceptual framework.

The primary objective of this research is to conceptually explain the differences between *absolute* and *restrictive deterrence* and how each influences employee compliance with *information security policies*. It also aims to identify gaps in current empirical approaches and propose future research directions that incorporate contextual variables and behavioral theory integration for improved compliance outcomes.

This study contributes to the field of *information systems* by clarifying theoretical ambiguities in *deterrence theory* applications. It enhances our understanding of how different deterrent strategies affect internal security behavior and supports the development of more targeted compliance programs. By comparing the deterrent effects with competing motivational frameworks (such as *positive reinforcement*), the study also broadens the theoretical landscape of compliance research.

The research implications are twofold. Theoretically, it encourages the refinement of *deterrence theory* in the context of *IS security* by distinguishing between types of deterrence and their psychological impacts. Practically, it guides organizations in designing more effective security policies by balancing punitive measures with proactive behavioral strategies. As cyber threats evolve, understanding how to prevent insider misconduct through appropriate *deterrence frameworks* becomes essential for sustainable organizational resilience.

METHOD

The method used in this study is a *Systematic Literature Review* (*SLR*). To find publications related to *deterrence theory* and employee security behavior in the workplace, the author conducted a systematic literature review using various keyword combinations such as *"deterrence," "deterrence theory," "absolutely deterrent"* or *"absolute deterrence,"* and *"restrictive deterrence"* or *"restrictive deterrent."* In addition, several other keywords were used to explore literature on compliance with *information security* rules, including *"information security," "compliance with information security," "compliance with information security policies," "computer misuse," "information misuse," "computer crime," "protection motivation," "security awareness," "security policies,"* and *"information security breaches."*

The selected databases for the review included *MIS*, *Springer*, *Wiley*, *AISeL*, *JSTOR*, *ScienceDirect*, *JAIS*, *EBSCO*, *Emerald*, *ABI INFORM*, *USENIX*, *JAIS*, and *Google Scholar*. The studies were chosen based on systematic review criteria, including: (1) exploring the effectiveness of *deterrence* on compliance with *information security policies*; (2) examining the managerial impact on various organizational aspects such as *organizational behavior*, *organizational strategy*, *performance measurement*, *information systems governance*, and *corporate social responsibility*; and (3) including only studies published in the English language.

This article aims to provide a balanced understanding, so the systematic review also includes literature considered to be of lower quality but still relevant (Borenstein et al., 2011; Rosenthal, 1979; Wu & Lu, 2013; Wu & Lederer, 2009). Therefore, the author did not restrict the journals used or the publication years of the articles, in order to gather a comprehensive population and include relevant supporting sources, including theses and dissertations (*APPENDIX A*).

RESULTS AND DISCUSSION

The main problem with deterrence theory (DT) in information security (ISec) is the inconsistency of research results, primarily due to empirical reasons. However, it is important to acknowledge that certain issues also have conceptual roots, which is the main focus of this paper. D'Arcy & Herath (2011) conducted a critical analysis of the shortcomings in previous research and provided several recommendations for future studies in their literature review on ISec DT. They also emphasize the importance of comparing the effectiveness of sanctions with competing positive incentives to gain a more thorough understanding of the deterrence process. Therefore, addressing these conceptual problems is crucial for the development of ISec DT research.

The majority of studies, except for one, primarily focused on the traditional costs associated with formal sanctions, which aligns with findings in the field of criminology since the 1980s. Piliavin et al., (1986) argued that DT researchers had placed excessive emphasis on examining the isolated effects of punishment severity and certainty on criminal behavior. They proposed that studying DT within a clear theoretical framework would be more beneficial. This allowed them to assess how offenders evaluate the expected utility and disutility of illegal behavior compared to legal alternatives. Their conclusion was that the likelihood of engaging in illegal actions increases when the perceived expected utility of those actions exceeds that of the legal alternatives.

Similarly, Paternoster (1989a, 1989b, 2010) expressed dissatisfaction with the lack of theoretical and conceptual advancements since the seminal work of Gibbs (1968) and highlighted the disconnect between criminological research on Deterrence Theory (DT) and general theories of control. Paternoster argued that DT criminologists had not clearly specified which criminal decisions would be influenced by formal sanctions. As a result, both classical and contemporary deterrence theorists had overlooked the fact that individuals make various types of criminal decisions that can be differentially affected by specific explanatory factors (Paternoster, 1989b)

(Paternoster, 1989a, 1989b) highlighted several criminological research studies that recognized the multiple choices made by criminals in the process of making criminal decisions.

As an example, he referred to the research conducted by Blumstein (1986), who examined criminal careers and focused on the sequence of offenses committed by individuals over a specific period of time. It is important to clarify that the term "career" in this context refers only to the pattern of offenses and does not imply that the offender derives their livelihood from illegal earnings. Researchers in this field emphasized that a criminal career consists of three stages: involvement, continuation (duration of the criminal career), and cessation (end of the criminal career). Additionally, these decisions are associated with the frequency of offending, which refers to the number of offenses committed.

According to (Paternoster, 1989a), the offender's decision-making process involves two forms of deterrence. The first form is traditional deterrence, where an offender is dissuaded from committing additional criminal acts, leading to a reduction in the frequency of offending. The second form addresses the deterrence of initial involvement in crime, also referred to as the presence or absence of a "beginning" to a criminal career, as defined by Blumstein (1986). To support his argument, Paternoster (1989a) referenced Gibbs (1968), who made a distinction between absolute and restrictive deterrence. Absolute deterrence occurs when an individual refrains from a specific type of illegal act throughout their lifetime.

The term "absolute deterrence" is used in the context of information security (ISec) to describe the prevention of insider criminal activity (ICA) among company insiders. For example, if insiders refrain from engaging in any form of criminal behavior using their work computers for fear of detection, they have been effectively deterred. On the other hand, “restrictive deterrence” refers to restricting certain criminal acts by a person for a certain period of time. This limitation stems from an individual's belief that limiting such activities reduces the risk of punishment in response to their actions (Gibbs, 1968). In the context of ISec, restrictive safeguards are particularly applicable to insiders who have previously conducted an ICA and are now facing a decision whether to engage in further illegal acts.

CONCLUSION

Compliance of employees with *information security policies* within an organization can be influenced by the *deterrent* approach applied. There are two main approaches discussed in the literature, namely *absolute deterrence* and *restrictive deterrence*. *Absolute deterrence* focuses on the implementation of formal sanctions enforced by law to reduce employee participation in criminal activities. This approach aims to prevent violations of *information security policies* by emphasizing serious legal consequences for offenders. An example of *absolute deterrence* is the imposition of high fines or legal actions against companies that violate *information security* regulations.

On the other hand, *restrictive deterrence* involves formal and informal sanctions faced by employees as offenders, which limit the frequency of violations committed by them. This approach emphasizes reducing employee participation in criminal activities through formal control systems implemented by the organization. Informal sanctions, such as social norms and peer pressure, can also play a role in *restrictive deterrence*.

This literature review shows that there are differences in the operationalization of the *deterrence* construct in research on compliance with *information security policies*. Some studies combine constructs such as severity, certainty, and swiftness of sanctions into one construct called *sanctions/deterrence*, while others use substitute constructs such as *security awareness*,

security programs, *education*, and *security consciousness* as proxies for sanctions.

Although there are various approaches and varying results in this research, this literature review concludes that research on *deterrence* in the context of *information security* is still in its early stages. There are many opportunities to further develop *deterrence theory* by considering contextual factors and theoretical limitations.

Furthermore, this literature review highlights the need for deeper and more contextual research in applying *deterrence* to *information security*. In order to develop a better understanding of *deterrence* in compliance with *information security policies*, this review recommends comparing the effectiveness of sanctions with competing positive incentives to gain a more comprehensive understanding of the *deterrence* process. Additionally, the *deterrence* approach needs to be expanded to cover various types of criminal decisions made by individuals, as well as to consider relevant contextual factors in the context of *information security*.

REFERENCES

Beusch, P., Frisk, J. E., Rosén, M., & Dilla, W. (2022). Management control for sustainability: Towards integrated systems. *Management Accounting Research, 54*, 100777. https://doi.org/10.1016/j.mar.2021.100777

Blumstein, A. (1986). *Criminal careers and career criminals*. Washington, DC: National Research Council.

Borenstein, M., Hedges, L. V., Higgins, J. P., & Rothstein, H. R. (2011). *Introduction to meta-analysis*. Wiley.

D'Arcy, J., Gupta, A., Tarafdar, M., & Turel, O. (2014). Reflecting on the "dark side" of information technology use. *Communications of the Association for Information Systems, 35*. https://doi.org/10.17705/1CAIS.03505

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643–658. https://doi.org/10.1057/ejis.2011.23

Einhorn, S., Fietz, B., Guenther, T. W., & Guenther, E. (2024). The relationship of organizational culture with management control systems and environmental management control systems. *Review of Managerial Science, 18*(8). https://doi.org/10.1007/s11846-023-00687-0

García Osma, B., Gomez-Conde, J., & Lopez-Valeiras, E. (2022). Management control systems and real earnings management: Effects on firm performance. *Management Accounting Research, 55*, 100781. https://doi.org/10.1016/j.mar.2021.100781

Gibbs, J. P. (1968). Crime, punishment, and deterrence. *The Southwestern Social Science Quarterly, 48*(4), 515–530.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hill, M. (2022). How much does a data breach cost? *CSO ASEAN*. https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

Paternoster, R. (1989a). Absolute and restrictive deterrence in a panel of youth: Explaining the onset, persistence/desistance, and frequency of delinquent offending. *Social Problems, 36*(3), 289–309. https://doi.org/10.2307/800696

Paternoster, R. (1989b). Decisions to participate in and desist from four types of common delinquency: Deterrence and the rational choice perspective. *Law & Society Review, 23*(1), 7. https://doi.org/10.2307/3053879

Paternoster, R. (2010). How much do we really know about criminal deterrence? *Journal of Criminal Law & Criminology, 100*(3), 765–824.

Pfister, J. A., Peda, P., & Otley, D. (2023). A methodological framework for theoretical explanation in performance management and management control systems research. *Qualitative Research in Accounting and Management, 20*(2). https://doi.org/10.1108/QRAM-10-2021-0193

Piliavin, I., Gartner, R., Thornton, C., & Matsueda, R. L. (1986). Crime, deterrence, and rational choice. *American Sociological Review, 51*(1), 101. https://doi.org/10.2307/2095480

Rosenthal, R. (1979). The file drawer problem and tolerance for null results. *Psychological Bulletin, 86*(3), 638–641. https://doi.org/10.1037/0033-2909.86.3.638

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64–71.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487. https://doi.org/10.2307/25750688

Tarafdar, M., Gupta, A., & Turel, O. (2015). Editorial. *Information Systems Journal, 25*(3), 161–170. https://doi.org/10.1111/isj.12070

Willison, R., & Lowry, P. B. (2018). Disentangling the motivations for organizational insider computer abuse through the rational choice and life course perspectives. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 49*(SI), 81–102. https://doi.org/10.1145/3210530.3210537

Wu, J.-H., & Lederer, A. L. (2009). A meta-analysis of the role of environment-based voluntariness in information technology acceptance. *MIS Quarterly, 33*(2), 419. https://doi.org/10.2307/20650298