Understanding the Incentive Mechanism of Penalty for Information Security Policy Compliance Behavior

Xiaolong Wang[1,2,a*] and Wenli Li[1,b]

[1]Faculty of Management and Economics, Dalian University of Technology, Dalian, 116024, China

[2]Department of Management and Information, Shandong Transport Vocational College,
Weifang, 261206, China

[a]Michaelwangxl@mail.dlut.edu.cn, [b]Wlli@dlut.edu.cn

Keywords: Incentive mechanism, Information security policy, Compliance behavior, Principal-agent model with moral hazard, Penalty.

Abstract. A significant number of information security incidents have been attributed to the internal employees' failure to comply with the information security policy (ISP) in the organizational setting. There exists a principal-agent problem with moral hazard between the employer and the employee individual for the practical compliance effort of the employee is not observable without high costs. In this study, an ISP compliance game has been proposed to analyze the incentive mechanism of penalty on the compliance behavior of employee individual. It is shown that in a no-penalty contract, the employee will decline to comply with the ISP if the expected payoff obtained from her noncompliance is larger than that from the outside options; and in a penalty contract, an appropriate penalty will motivate her to exert the compliance effort level expected by her employer. A numerical example has been presented to show the validity of this game analysis.

Introduction

Internal employees' noncompliance behaviors violating the Information Security Policy (ISP) have resulted in a large number of information security incidents [1-7]. The ISP refers to a set of rules or regulations formulated by an organization and required to be followed by the internal employees [8-11]. The ISP noncompliance behaviors include the volitional but unmalicious noncompliance behaviors, and the intentional and malicious computer abuse behaviors [12]. The previous studies show that the anthropogenic incidents caused even by one employee can be potentially devastating [6,13,14]. Therefore, the influence factors of these noncompliance behaviors (or compliance behaviors) are worth to be studied for the information security management in the organization setting.

Empirical methods have been used to study the ISP noncompliance or compliance behaviors, and many of these studies are based on the deterrence theory [14-22]. Straub et al. suggested that sanction exerts deterrence on computer abuse, and the deterrence is believed to be the primary strategy preventing this noncompliance behavior from happening [23]. D'Arcy et al. pointed out that information system misuse could be reduced once the employees perceive the severity and certainty of sanction [24]. Similar results have been obtained in the studies of Bulgurcu et al. [13] and Chen et al., [25]. However, a different viewpoint regarding the influence of penalty on the ISP noncompliance behaviors has been raised in other studies [6, 26-29]. These studies show that penalty or sanction has insignificant effect on the ISP noncompliance behaviors of employees.

Alternatively, Beautement et al. suggested that the ISP compliance or noncompliance behavior of an employee individual can be understood from an economic perspective [30,31]. Their study indicates that the key factors affecting the compliance decision are the actual and anticipated cost and benefit of compliance behavior for the employee individual. It has also been found that understanding the economic essence of the compliance or noncompliance behavior of employee individual can provide a better basis for making countermeasure to influence her noncompliance. Therewith, the employer should accept that compliance with the ISP is a finite resource that needs to be carefully managed [30,31]. The study of Chen et al. also indicates that the employee individual will consider

DOI: 10.25236/ssehr.2018.005

the potential effect of penalty on her utility function when she decides not to comply with the ISP [25]. Paternoster proposed that the deterrence of penalty is essentially consistent with the economic hypothesis of rational actor [32]. Following the economic point of view, the employee individual is assumed to be a rational actor pursuing maximized payoffs in the organizational setting, and hence she would choose to comply with the ISP if the penalty for the noncompliance behavior exceeds the benefit obtained from this behavior. In the practical context of the ISP compliance management, however, the compliance effort of the employee individual (the agent) generally cannot be observed and accurately measured by the employer (the principal) without high costs. Therewith, in the present study the principal-agent model with moral hazard [33-40] is used to explore the incentive effect of penalty on motivating the employee individual to comply with the ISP.

The remainder of this study is organized as follows. Firstly, an extensive-form of the information security policy compliance game is proposed for exploring the incentive effect of penalty on the compliance behavior of the employee individual. Secondly, the incentive effect of penalty is shown by the compliance game analysis. Finally, a numerical example is given to show the validity of the suggestion of the compliance game.

The ISP Compliance Game

In order to study the incentive effect of penalty on the ISP compliance behavior of an employee individual in the organization setting, we first propose a principal-agent problem with moral hazard. It should also note that some random factors may influence the compliance outcome of the employee individual. The employer cannot design a contract specifying a transfer as a function of the compliance effort. Though the compliance effort of the employee individual cannot be observed and measured accurately, the ISP compliance outcome of the employee can be confirmed with certainty. A contract thus can be written by the employer based on this outcome.

Assume that (1) the ISP compliance is the only one task assigned to the employee individual in a given time duration, (2) the two players of the ISP compliance game are the employer and the employee individual in an organization, (3) the players are rational, (4) the players share the common knowledge, (5) each player is aware of the game rules, (6) the ISP compliance effort of the employee together with the random factors determine the compliance outcome, (7) the employer is risk neutral with utility function $u(x) = x$, where x stands for the amount of dollars of payment, (8) the employee is risk averse with utility function $v(x) = x^{\mu}, 0 < \mu < 1$, (9) a good compliance outcome will bring about a revenue m_1 to the employer, while a bad outcome results in a revenue of m_2, and (10) the two players interact as the extensive-form representation depicted in Fig. 1.

The game process proceeds as follows: (1) at the beginning of the game, the employer (*M*) offers the employee (*E*) a penalty and wage package. In particular, the employee is paid a wage w_1 regardless the compliance outcome, whereas the penalty f， $f > 0$, will be imposed only if the outcome is bad. Here, the penalty can be a formal sanction, e.g., financial penalty or incarceration, or an informal sanction, e.g., social disapproval, self-disapproval or shame [25, 41], (2) the employee decides whether or not to accept the contract. If she declines the contract, viz., she chooses *N*, the game ends. In this case, the expected payoffs of the employer and the employee are 0 and w_2^{μ}, respectively. Here, w_2^{μ} corresponds to the expected payoff of the employee obtained from outside options, and (3) if the employee chooses acceptance, viz., she chooses *Y*, then she has to decide whether to comply with the ISP (*C*) or not (*NC*). The choice of *NC* will result in a chance node (P_1) at which nature (the pseudo-player) selects randomly a good (*G*) or bad (*B*) compliance outcome. The probabilities of selecting *G* and *B* are set to $1 - q$ and q, respectively, and it is reasonable to assume $q > 1 - q$. Along the *C* extension, nature selects *G* and *B* with probabilities of p and $1 - p$ at the chance node P_2, respectively, and $p > 1 - p$ is assumed.

Assume that the employee chooses to comply with the ISP. If nature selects *G*, the perceived payoff of the employer is derived to be $m_1 - w_1$ from the utility function $u(x) = x$, and with the function $v(x) = x^{\mu}, 0 < \mu < 1$, the employee gets the utility $(w_1 - c)^{\mu}$, where c is the compliance effort cost of the employee. If nature selects *B*, the employer and the employee get the utilities

$m_2 - w_1 + f$ and $(w_1 - c - f)^\mu$, respectively. Assume that the employee does not comply with the ISP. The employer and the employee get respectively the expected utilities $m_1 - w_1$ and w_1^μ if nature selects *G*, and $m_2 - w_1 + f$ and $(w_1 - f)^\mu$ if nature selects *B*.

Consequently, the expected payoffs of the two chance nodes are obtained. When the employee selects *C*, the expected payoffs of the employer and the employee are calculated to be $p(m_1 - w_1) + (1-p)(m_2 - w_1 + f)$, and $p(w_1 - c)^\mu + (1-p)(w_1 - c - f)^\mu$, respectively. If the employee selects *NC*, the expected payoffs of the employer and the employee are $(1-q)\,(m_1 - w_1) + q(m_2 - w_1 + f)$ and $(1-q)w_1^\mu + q(w_1 - f)^\mu$, respectively. With these expected payoffs, the ISP compliance game is further illustrated in an extensive-form (Fig. 2).

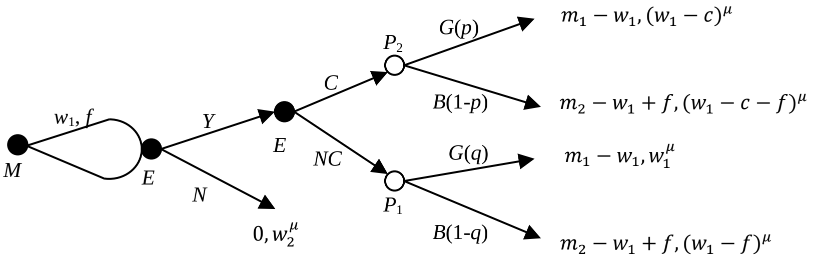

Fig. 1. The extensive-form of the ISP compliance game.

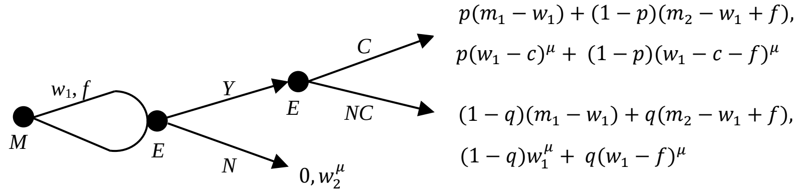
w_1, f
M
E
Y
N
$0, w_2^\mu$
E
C
NC
$p(m_1 - w_1) + (1-p)(m_2 - w_1 + f),$
$p(w_1 - c)^\mu + (1-p)(w_1 - c - f)^\mu$
$(1-q)(m_1 - w_1) + q(m_2 - w_1 + f),$
$(1-q)w_1^\mu + q(w_1 - f)^\mu$

Fig. 2. The ISP compliance game with expected payoffs.

The Incentive Effect of Penalty

Based on this ISP compliance game, the incentive effect of penalty on the compliance behavior of the employee individual can be reached. The no-penalty contract is first considered. When the employee chooses to comply with the ISP and if $f = 0$, her expected payoff satisfies obviously the equality: $p(w_1 - c)^\mu + (1-p)(w_1 - c - f)^\mu = (w_1 - c)^\mu$. When she picks a noncompliance action and if $f = 0$, the equality turns to be: $(1-q)w_1^\mu + q(w_1 - f)^\mu = w_1^\mu$. Note that $(w_1 - c)^\mu < w_1^\mu$, the employee will decide not to comply with the ISP when $w_2^\mu < w_1^\mu$.

In the case of $f \neq 0$, in order for the employee individual to be motivated to comply with the ISP, the penalty contract that she would like to accept must satisfy such a participation constraint: the expected payoff from C must be not less than that she can get from the outside options, viz., $p(w_1 - c)^\mu + (1-p)(w_1 - c - f)^\mu \geq w_2^\mu$. Meanwhile, the employer designs the penalty contract to pursue her maximized payoff as well. From this inequality relationship, the employer can increase the amount of penalty (f) such that the participation constraint is still satisfied. Thus it is obtained that the optimal penalty contract for the employer should satisfy the following equation:

$$p(w_1 - c)^\mu + (1-p)(w_1 - c - f)^\mu = w_2^\mu. \tag{1}$$

If such a contract is designed that the employee's expected payoff from *C* is not less than that from *NC*, the employee will be motivated to comply with the ISP. Therewith, the incentive compatibility condition can be reached: $p(w_1 - c)^\mu + (1-p)(w_1 - c - f)^\mu \geq (1-q)w_1^\mu + q(w_1 - f)^\mu$. Assume that the expected payoff of the employee is a constant r. Let $g(w_1)$ be the function that gives a penalty f corresponding to wage w_1 that yields r, and $g(w_1) > 0$, viz., $p(w_1 - c)^{\mu} + (1-p)(w_1 - c - g(w_1))^{\mu} = r$. Calculate the first-order derivative of $g(w_1)$. We get

$$g'(w_1) = 1 + \frac{p}{1-p}\left(1 - \frac{g(w_1)}{w_1 - c}\right)^{1-\mu}. \qquad (2)$$

When $w_1 - c \geq g(w_1)$,

$$g'(w_1) \geq 1. \qquad (3)$$

This result means that, when the penalty f is not less than the difference between the wage w_1 and the compliance cost c, f increases by one or more than one time the increasing amount of w_1. So, the expected payoff of the employee remains constant and the equation (1) is satisfied as well. This increases the employer's expected payoff while keeping that of the employee unchanged. Hence, the following equation holds:

$$p(w_1 - c)^{\mu} + (1-p)(w_1 - c - f)^{\mu} = (1-q)w_1^{\mu} + q(w_1 - f)^{\mu}. \qquad (4)$$

From the equations (1) and (4), we obtain

$$(1-q)w_1^{\mu} + q(w_1 - f)^{\mu} = w_2^{\mu}. \qquad (5)$$

The employee individual will accept the contract in which f and w_1 satisfy the equation (5), and she will choose to exert high effort to comply with the ISP.

The Numerical Example

Let $w_2 = 1$ and $q = 1$. From the equation (5) we obtain $w_1 = f + 1$. Let $c = 1$ and $p = {}^{2}/_{3}$. From the equation (1), the optimal contract delivers a penalty $f = ({}^{2}/_{3})^{1/\mu}$ and a wage $w_1 = ({}^{3}/_{2})^{1/\mu} + 1$. In this case, the employee individual will accept this contract and exert high ISP compliance effort. Further, let $m_1 = 10$ and $m_2 = 1$, the expected utilities of the employer and the employee are calculated to be $6 - ({}^{3}/_{2})^{{}^{1-\mu}/_{\mu}}$ and 1, respectively. The payoff of the employer is $6 - ({}^{3}/_{2})^{{}^{1-\mu}/_{\mu}} = 5$ when $\mu = 1$, thus the risk premium that the employee requires to exert ISP compliance high effort is $5 - \left(6 - ({}^{3}/_{2})^{{}^{1-\mu}/_{\mu}}\right) = ({}^{3}/_{2})^{{}^{1-\mu}/_{\mu}} - 1$, $0 < \mu < 1$.

Based on the above no-penalty contract and the penalty contract, the employer's expected payoffs are worked out to be 1 and $6 - ({}^{3}/_{2})^{{}^{1-\mu}/_{\mu}}$, respectively. Hence, she will choose the penalty contract if and only if $6 - ({}^{3}/_{2})^{{}^{1-\mu}/_{\mu}} \geq 1$, we thus obtain $\mu \cong 0.2$ from this inequality. Further, we can obtain $1 - \mu = 0.8$. This situation means that the employer can write a penalty contract to motivate the employee individual to select high compliance effort if the risk aversion measure of the employee individual is not more than 0.8.

Summary

The information security policy compliance behavior of employee individual in the organizational setting has been considered within the framework of the principal-agent theory. The employer and the employee assume a principal-agent relationship with moral hazard for the employee's compliance effort cannot be observed and accurately measured by the employer without high costs. The extensive-form of the ISP compliance game has been proposed for analyzing the incentive effect of penalty. In a no-penalty contract, if the expected payoff of the employee individual obtained from the noncompliance behavior is larger than that from the outside options, the employee will decide not to comply with the ISP. A penalty contract can be designed by the employer to motivate the employee individual to exert high ISP compliance effort. The validity of this game analysis has been tested with a numerical example. The incentive effect of bonus is not considered in this study. More insight on the incentive mechanism of the ISP compliance maybe obtained in a comparative study of the roles of bonus and penalty.

Acknowledgements

This work was funded in part by the National Natural Science Foundation of China (Nos. 70972058, 71272092, and 71431002).

References

[1] G. D. Moody, M. Siponen, and S. Pahnila, *Toward a unified model of information security policy compliance*, MIS Quart., vol. 42 (2018), p. 285-311.

[2] R. Willison, P. B. Lowry, and R. Paternoster, *A tale of two deterents: considering the role of absolute and restrictive deterrence in inspiring new directions in behavioral and organizational security*, J. Assoc. Inf. Syst., in press.

[3] D. D. Pham, S. Pittayachawan, and V. Bruno, *Application of social network analysis in behavioural information security research: concepts and empirical analysis*, Comput. Secur., vol. 68 (2017), p. 1-15.

[4] The Verizon Risk Team, *2017 Data breach investigation report*, http://www.verizon-bussiness.com.

[5] The Verizon Risk Team, *2016 Data breach investigation report*, http://www.verizon-bussiness.com.

[6] M. A. Mahmood, M. Siponen, D. Straub, H. R. Rao, and R. Santanam, *Moving toward black hat research in information systems security: an editorial introduction to the special issue*, MIS Quert., vol. 34 (2010), p. 431-433.

[7] S. R. Boss, D. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, *What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors*, MIS Quart., vol. 39 (2015), p. 837-864.

[8] M. Warkentin, D. Straub, and K. Malimage, *Featured talk: measuring secure behavior: a research commentary*, in: Proceedings of the Annual Symposium on Information Assurance & Secure Knowledge Management, Albany NY (2012), p. 1-8.

[9] W. Robert, and W. Merrill, *Beyond deterrence: an expanded view of employee computer abuse*, MIS Quart., vol. 37 (2013), p. 1-20.

[10] C. Vroom, and R. von Solms, *Towards information security behavioural compliance*, Comput. & Secur., Vol. 23 (2004), p. 191-198.

[11] M. Siponen, M. A. Mahmood, and S. Pahnila, *Employees' adherence to information security policies: an exploratory field study*, Inform. Management, vol. 51 (2014), p. 217-224.

[12] M. Warkentin, and A. C. Johnston, *IT governance and organizational development for security management*, *Information Security Policy, Processes and Practices*, edited by D. W. Straub, S. Goodman, and R. L. Baskerville, Armonk, NY (2008), paper 4, p. 46-68.

[13] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, *Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness*, MIS Quart.,vol. 34 (2010), p. 523-548.

[14] B. Muhire, *Employee compliance with information systems security policy in retail industry. Case: store level employees*, in: Honors Thesis Program in the College of Mnangement, paper 12 (2012).

[15] K. D. Loch, H. H. Carr, and M. Warkentin, *Threats to information systems: today's reality, yesterday's understanding*, MIS Quart., vol. 16 (1992), p. 173-186.

[16] R. Willison, and M. Siponen, *Overcoming the insider: reducing employee computer crime through situational crime prevention*, Commun. ACM, vol. 52 (2009), p. 133-137.

[17] M. Warkentin, and R. Willison, *Behavioral and policy issues in information systems security: the insider threat*, Eur. J. Inform. Syst., vol. 18 (2009), p. 101-105.

[18] T. Herath, and H. R. Rao, *Protection motivation and deterrence: a framework for security policy compliance in organizations*, Eur. J. Inform. Syst., vol. 18 (2009), p. 106-125.

[19] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, and A. Vance, *What levels of moral reasoning and values explain adherence to information security rules? An empirical study*, Eur. J. Inform. Syst., vol. 18 (2009), p. 126-139.

[20] M. Siponen, and A. Vance, *Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations*, MIS Quart., vol. 34 (2010), p. 487-502.

[21] Q. Hu, T. Dinev, P. Hart, and D. Cooke, *Managing employee compliance with information policies: the role of top management and organizational culture*, Decision Sci., vol. 43 (2012), p. 615-660.

[22] A. Hovav, and J. D'Arcy, *Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea*, Inform. Management, vol. 49 (2012), p. 99-110.

[23] D. Straub, *Effective IS security: an empirical study*, Inf. Systems Res., vol. 1 (1990), p. 255-276.

[24] J. D'Arcy, A. Hovav, and D. Galletta, *User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach*, Inf. Systems Res., vol. 20 (2009), p. 79-98.

[25] Y. Chen, K. Ramamurthy, and K. Wen, *Organizations' information security policy compliance: stick or carrot approach*, J. Manage. Inform. Syst., vol. 29 (2013), p. 157-188.

[26] D. Weirich, *Persuasive password security*, PhD Thesis, Department of Computer Science, University College London, UK (2006).

[27] S. Pahnila, M. Siponen, and A. Mahmood, *Employees' behavior towards IS security policy compliance*, in: Proceedings of the 40th Annual Hawaii International Conference on System Science (2007).

[28] J. D'Arcy, and T. Herath, *A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings*, Eur. J. Infor. Syst., vol. 20 (2011), p. 643-658.

[29] Q. Hu, Z. Xu, T. Dinev, and H. Ling, *Does deterrence work in reducing information security policy abuse by employees*, Commun. ACM, vol. 54 (2011), p. 54-60.

[30] A. Beautement, A. Sasse, and M. Wonham, *The compliance budget: managing security behavior in organizations*, in: Proceedings of the 2008 Workshop on New Security Paradigms, Lake Tahoe, California (2008).

[31] A. Beautement, and A. Sasse, *The economics of user effort in information security*, Comput. Fraud Secur., vol. 10 (2009), p. 8-12.

[32] R. Paternoster, *How much do we really know about criminal deterrenc*, J. Crim. Law Criminol., vol. 100 (2010), p. 765-824.

[33] J. A. Mirrlees, *Notes on welfare economics, information and uncertainty*, in: Essays on Economic Behavior under Uncertainty, edited by M. Balch, D. McFadden, and S. Wu, Amsterdam: North-Holland Pub. Co., (1974).

[34] J. A. Mirrlees, *The theory of moral hazard and unobservable behaviour: part I*, Mimeo, Nuffield College, Oxford University (1975).

[35] J. A. Mirrlees, *The optimal structure of authority and incentive within an organization*, Bell J. Econ., vol. 7 (1976), p. 105-131.

[36] B. Holmström, *Moral hazard and observability*, Bell J. Econ., vol. 10 (1979), p. 74-91.

[37] B. Holmström, *Moral hazard in team*, Bell J. Econ., vol. 13 (1982), p. 324-340.

[38] S. Grossman, and O. Hart, *An analysis of the principal-agent problem*, Econometrica, vol. 51 (1983), p. 7-45.

[39] E. Rasmusen, *Games and information: an introduction to game theory*, Fourth Edition, Wiley-Blackwell (2006).

[40] J. Watson, *Strategy: an introduction to game theory*, Third Edition, W. W. Norton & Company (2013).

[41] J. D’Arcy, and S. Devaraj, *Employee misuse of information technology resources: testing a contemporary deterrence model*, Decision Sci., vol. 43 (2012), p.1091-1124.