Chapter 3
Towards Understanding Deterrence: Information Security Managers' Perspective

Sangseo Park, Anthonie B. Ruighaver, Sean B. Maynard and Atif Ahmad

Abstract The enforcement of information security policy is an important issue in organisations. Previous studies approach policy enforcement using deterrence theory to deal with information security violations and focus on end-users' awareness. This study investigates deterrence strategy within organisations from the perspective of information security managers. The results primarily reveal that current deterrence strategy has little influence on reducing violations because it is only used as a prevention strategy due to the lack of means of detection. Our study suggests that organisations should shift to detection of violations and identification of violators, and expand the range of sanctions. The research also presents an architecture of information security strategies to be operated in a coordinated manner for use in deterring security violations.

Keywords Information security · Information security strategy · Deterrence strategy · Architecture of deterrence strategy

3.1 Introduction

As organisations realise the importance of information assets due to their contribution toward productivity and maximising competitive value in the marketplace, securing them from outside attacks and preventing abuse by employees becomes a

S. Park (✉) · S. B. Maynard · A. Ahmad
Department of Information Systems, The University of Melbourne,
111 Barry Street, Carlton, VIC 3010, Australia
e-mail: parks@pgrad.unimelb.edu.au

A. B. Ruighaver
School of Information Systems, Deakin University,
221 Burwood Highway, Burwood, VIC 3125, Australia

K. J. Kim and S. J. Ahn (eds.), *Proceedings of the International Conference on IT Convergence and Security 2011*, Lecture Notes in Electrical Engineering 120,
DOI: 10.1007/978-94-007-2911-7_3,

primary issue. In addition, as the current IT environment within organisations becomes more complex, with the introduction of wireless technologies, portable storage, and mobile computing devices, organisations face an increased probability of the misuse of information assets [1]. Subsequently many organisations have begun to establish information security policy to guide the legitimate use of information assets. As a result, 75% of the organisations have developed a compliance policy for their employees and an additional 17% of organisations have one under development [2].

However, a recent survey reports that 25% of respondents indicated that attacks by employees such as privilege abuse, information theft, and policy non-compliance are increasing [3]. Another recent survey reveals that 25% of organisations that responded experienced an internal abuse of information systems, whilst 13% of the organisations suffered from unauthorised access attempts by insiders [2].

The traditional approach for dealing with security attacks (including violations of security policy, information leakage and the illegitimate use and abuse of information assets) committed by employees is from the deterrence perspective [4–14]. The concept of deterrence is that people refrain from performing certain behaviour because of the fear of consequences if it is carried out [4]. Deterrence strategy has expanded its application from criminology to international relations in controlling another party or nation from initiating some course of action based on military measures [15]. The concept has been adapted to the information security field and is frequently used to attempt to control employee behaviour with respect to the violation of information security policies within organisations [5–7, 9–12]. It has also been adapted to military defence and national cyber space from the viewpoint of information warfare [16–19].

Our study, from the viewpoint of security managers, aims at understanding deterrence in information security policy in organisations and at devising better methods to increase the effect of deterrence. The interpretation of focus group discussion with security managers provides useful insights into the understanding of the use of deterrence strategy in organisations. Our research proposes an extended model of deterrence strategy and suggests that organisations should employ various measures to identify and deal with violations and violators. It then puts forward an architecture composed of various types of measures coordinated at a tactical level under the deterrence strategy.

The rest of this paper is composed of four parts. Section 3.2 summarises past research on deterrence strategy focused on information security. Section 3.3 focuses on the extended model of deterrence and Sect. 3.4 explains research method used. Sections 3.5 and 3.6 describes research results and discusses the findings.

3.2 Past Studies on Deterrence Strategy

A number of studies have been conducted focusing on deterrence and violative behaviours committed by employees in the information security discipline. Although some studies have argued that deterrence is not associated with the

reduction of abuse or security violations [20, 21], most research, based on empirical evidence, supports the contention that deterrence strategy is effective [5, 6, 9, 11].

Straub and Nance [6] approached issues of computer abuse from the discovery of abuse and the severity of penalties to the abusers. The study suggested the need to take detective actions and to punish motivated abusers harshly to lower computer abuse. This was based on 1,063 respondents with reports on 268 abuses.

Straub [5] showed that deterrence strategy is effective in lowering computer abuse based on the empirical evidence conducted with the collaboration of 1,211 organisations. The research found that the information security efforts, such as the number of security staff, the hours dedicated to security, severity of penalties, and the number of methods to inform employees of deterrence actions, deters potential abusers from committing violations. He indicated that employees have to be informed about the legitimate use of the systems and the penalties that follow when they do not comply with the guidelines. Straub and Welke [7] summarised the action research stressing the importance of security awareness that educates employees in security policies and guidelines.

With the survey of 164 information security managers, Kankanhalli et al. [11] found that deterrent efforts contribute to the effectiveness of information security. They measured the influence of deterrence efforts and deterrence severity to the effectiveness of information security effectiveness. Deterrence efforts were measured using weekly hours expended on information security. On the other hand, deterrence severity was gauged through four types of punishments: reprimand, suspension, dismissal, and prosecution. They found that the severity of sanctions have little relation to the effectiveness of deterrence. Based on the result, they argued that organisations need to underline the certainty of deterrence rather than severity. They also suggested the use of policy statements and guidelines on the proper use of information systems, as well as security briefings on the punishment, and internal audits as methods for increasing certainty of sanctions.

In recent research, D'Arcy et al. [9] focused on the perception of both security measures and sanctions. They studied 269 professionals in terms of the influence of the awareness of security measures to the perception of sanctions. They found that security efforts composed of security policy, security education and training, as well as awareness of being monitored could reduce the abuse of information systems. They also concluded that the certainty of sanctions has little influence on security violations whereas the severity of sanctions has a significant direct effect. This was contradictory to the findings by Kankanhalli et al. [11] who suggested that the organisations need to strengthen awareness of information security through security education, training and awareness programs in order to control the abuse of information systems.

Siponen and Vance [12] introduced neutralization theory to explain the reason that deterrence efforts fail and security policies are violated. Their model expanded the realm of sanctions to include shame and informal sanctions. From the 395 respondents, they acquired the data proving that neutralization has a strong influence on the intention to violate security policies. On the other hand, they

found that punishment has little influence on deterrence. This is not consistent with the previous research results of Straub [5] and Kankanhalli et al. [11]. However, they suggest that organisations should increase awareness, and not neglect punishment because it is an efficient and important driver of deterrence.

Hu et al. [10] tested the intention of employees to violate policies based on the rational choice theory with 227 respondents to the survey. They found that security policy tends to be violated when the perceived benefit is substantial. In addition, the result showed that punishment alone is ineffective in lowering the intention to violate the policy. This result is consistent with the result of the study conducted by Siponen and Vance [12]. They suggest the organisations need to lower the perceived value of information assets as well as recruit employees having high moral standards and high self-control.

3.3 Deterrence Model

Deterrence is a strategy to influence the behaviour of people to follow a certain policy using the fear of sanctions. Therefore, it is composed of two main constructs: certainty of sanctions and severity of sanctions [22]. In other words, people abandon undesirable actions if they feel the probability of capture is high (certainty of sanctions) and/or the degree of penalty for the action is high (severity of sanctions) [23].

In the past, from the viewpoint of the certainty of sanctions, employees' being aware that the presence of sanctions resulted from violation and the existence of detective measures was regarded effective in deterring the abuse of information systems and the violation of security policies. Recently, it is reported that security policies are violated when the benefit of violation is substantial, or a neutralisation technique is involved [12]. This implies that organisations should not rely solely on awareness of sanctions because violation will occur regardless of the emphasis on it. As a result, organisations are required to consider the use of detection as a practical method to increase the probability of the identification of violation. The most certain way of increasing the certainty of sanctions is finding out every violation and identifying its violator. Therefore, the certainty of sanctions should be viewed from the perspectives of detection as well as awareness.

As to the severity of sanctions, the sort of sanctions considered was solely punishment with various degrees. However, it is argued that sole application of punishment has no influence on deterring violations [10]. The method of sanctions began to extended from that of sole punishment and to include other methods such as shame and informal sanctions [12], and self-control, moral beliefs, and general deterrence based on rational choice [10]. Therefore, the severity of sanctions needs to be approached also from the variety of sanctions in addition to the existing concept of the intensity of sanctions.

Thereby, this paper proposes that the construct of deterrence, the certainty of sanctions and the severity of sanctions can be divided into four sub constructs, as

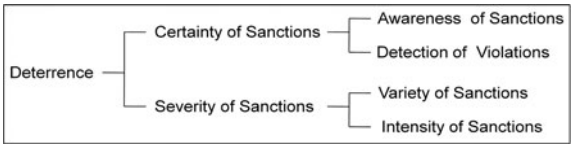

Fig. 3.1 Constructs and sub construct of deterrence strategy

shown in Fig. 3.1: the awareness of sanctions and the detection of violations, and the variety of sanctions and intensity of sanctions. Sanction awareness enhances the consciousness of employees thereby encouraging employees not to violate information security policies. On the other hand, detection is to find out violators when a violation has occurred. The variety of sanctions represents the kinds of sanctions including punishment, whereas the intensity of sanctions stands for the degree of sanctions.

3.4 Method

3.4.1 Focus Group

A focus group is a qualitative research method for eliciting deeper and richer information focused on a given topic from participants chosen purposively among a specific population in an interactive setting [24–26].

Researchers can capture detailed information about the subject from participants' expression of perceptions, viewpoints, and opinions [27–29]. Researchers can also study attitude and experience, examine how ideas and knowledge are developed, and explore how the opinions are formed [30]. Therefore, focus group research is suitable for having deep insight into how the issues of deterrence for the information security violations are dealt with within organisations, through the participants' perception, attitude, experiences, and opinions [24, 26].

3.4.2 Data Collection

It is normal to compose a focus group with four to twelve people although the group size can vary according to the purpose of study and the data being collected [29–33]. However, in the case that participants are required to have a large volume of knowledge or experience in a specific area, small groups consisting of four to six people, rather than a bigger group, is appropriate in order to collect specialised data in a particular discipline [29]. Because our study is aiming at collecting data on the use of deterrence in organisations, it requires participants' vast knowledge about current use of deterrence strategies as well as years of experience about the implementation and operation of them. Therefore, the number of participants in a group is not necessarily large; four to six expert participants are enough for this study.

The focus group was conducted in Korea. Security managers from five companies attended the discussion. The group was composed of participants who had no acquaintance with each other, in order to encourage honest expression of opinion and voluntary involvement, and to prohibit set behaviours [25, 26, 34]. We also considered the homogeneity of the participants such as their position, role, authority, years of experience, and the size of their company and business field [29]. All of them have been working for more than five years in information security and were in charge of IT and/or the information security department at management level.

The duration of the discussion was 106 min. It was digitally recorded after receiving consent from all participants at the beginning of the discussion. The first author transcribed the discussion.

3.4.3 Data Analysis

It is proper to use a qualitative approach for analysing focus group data [25, 29, 30, 35]. We did not pay attention to the numerical data such as how many participants represented the same opinion because this can mislead the focus group result [29, 36]. Our analysis was primarily focused on interpretation of the context, what the participants wanted to mention and the meanings behind their conversations, based on themes.

When analysing the data, we adapted an annotating-the-script approach and a large-sheet-of-paper approach at the same time [37]. As the first step of the analysis, we listened to the digitally recorded discussion and read through the transcript several times. The purpose of this step was to comprehend the discussion as a whole and to identify major themes (annotating-the-script approach). Then we coded the transcript in accordance with the themes because participants tended to mention what occurs to their minds even while they are discussing another topic. The unit of coding was the section of conversation discussing the same topic instead of a line-by-line coding. This enabled the section to be a unit of analysis and interpretation. The coded transcript was reallocated through a cut-order-paste approach (large-sheet-of-paper approach). When interpreting the theme, both coded transcript and whole transcript were referenced at the same time to interpret the discussion as a whole (annotating-the-script and large-sheet-of-paper approach).

3.5 Results

3.5.1 Certainty of Sanctions

Discussion on the certainty of sanctions was composed of the methods used to inform employees of company policies and penalties, and measures to detect violations. Organisations exerted various efforts to increase perception on the

compliance of information security policy. However, they were negligent in operating detective measures to find out violations and violators.

3.5.1.1 Awareness of Sanctions

Organisations usually informed their employees of information security policy, of what legal authority the organisation had, of what the organisation could do to identify violations and violators, and of the punishment when the policy was violated. They had developed various means to increase this awareness. Method of awareness was composed of informing and receiving consent. Some companies continuously delivered the information through e-training, bulletin boards on the company intranet, an assembly meeting, or orientation for new employees:

> My company informs (employees), through e-training, that the company has the authority to monitor and delete employees' e-mails.

> I warned that if anyone was identified (using unlicensed software), the organisation will accept (his/her) resignation.

> My company announces what you are talking about (the information security policy and organisational regulations) every month, informs employees that the company has security regulations, and asks them to comply with them. The company keeps making announcements in this way continuously.

Some companies had an IT policy that must be signed. The companies received an employee's consent to the company's right regarding the monitoring and opening of an employee's e-mail when the employee first joined the company. They sometimes requested employees to sign on the document pledging their compliance with the company's security policy or they administered an oath of compliance:

> We educate employees in security every year, receive signed document of pledge, and administer an oath.

Despite these awareness efforts to inform employees of policy, the importance of compliance, and punishment against non-compliance, participants noted that employees usually tend not to comply with the policy. Instead, we found that awareness was effective when employees began to convince that they would be caught when they violated the policy. A participant explained his experience of achieving deterrence by convincing employees of capture:

> I experienced that education of the new employees about these (information security policy and punishment against the violation) is effective. Sometimes, employees who use unlicensed software were found in former days. However, for two or three years I have kept talking to new employees telling them that they would be in trouble if they have been detected using unlicensed software. As a result, employees rarely use unlicensed software.

3.5.1.2 Detection of Violations

The detection of violations should be conducted systematically, rather than opportunistically. However, because the organisations used passive and technically defective tools, the identification of violation and violators was subject to chance. Mechanisms used to detect violations in the organisations were spot checks and audits by security managers and resulted in penalties to the identified violators:

> We internally audit all systems every three months to check whether or not employees obey company policies. Any violator has to pay the penalty.

These mechanisms are insufficient for use as deterrent measures. Without applying appropriate, active, and working detection mechanisms, a deterrence strategy which is based on sanctions, will not be effective because it is hard to identify violations and subsequently difficult to specify a violator.

The lack of detection mechanisms is also related with the continuous attempt to bypass security hurdles as well as the ignoring of security regulations. Some security managers mentioned that employees attempt to carry out laptops without permission, to connect unregistered systems to company intranets, to use unlicensed software, to store confidential information on portable storage devices, and fail to configure laptop security features. However, these violations were difficult to detect, even though the companies maintained a security policy:

> It is prohibited from storing confidential data in USB memories or portable hard disks. … Violation of non-compliance has to be punished. … However, due to several issues, detection is in a somewhat loose status. … Only laptops and desktops registered to the company can connect to the company network. … If any unregistered system is connected in that way, a penalty is imposed because it is a violation of internal regulation. However, it is hard to detect the violation.

It is not hard to surmise that deterrence will hardly work when there is resistance by employees. A typical example is the conflict between the privacy of employees and the security of the organisation. For the company, safeguarding the information that the organisation owns may be more important than maintaining employees' privacy. On the other hand, employees will feel that their privacy is more valuable than the secrecy; thereby they tend to stand on the side of privacy. A case of the abandonment of monitoring was reported by one of the focus group participants. An organisation confronted the emotional resistance of their employees against the company's security regulations on e-mail monitoring. The union showed strong refusal to support the monitoring and perusal by the company with the worries that the company may infringe an individual's privacy, or the managers or person who has the privilege may abuse this prerogative:

> Finally we withdrew. Therefore, we removed all the privilege (to peruse employees' e-mail) from the systems. We did not make public to the employees that an administrator can monitor and peruse an employee's e-mail. However, it happened to be talked about and spread. As a result, the union made a strong protest against it. Despite the fact that

e-mail monitoring could be performed according to company regulation, it was hard to enforce the regulation due to the emotional resistance.

3.5.2 Severity of Sanctions

Severity of sanctions can be viewed in terms of variety and intensity. We found that intensity of sanctions was well-developed. However, organisations solely used punishment for sanctions and it seemed more similar to retribution rather deterrence.

3.5.2.1 Intensity of Sanctions

Punishment was well-developed and well-known. There were five types of punishments:

- Reduction of payment (Reduction of welfare benefits)
- Reflection on performance assessment
- Financial compensation
- Dismissal
- Accusation or lawsuit

The primary punishment was financial disadvantage being the reduction of salary (during the specified months). However, welfare benefits were diminished instead in consideration of emotional morale. Practically, financial support for purchase of books, recreational expenses, or physical exercise would be affected. The breach was sometimes reflected in annual performance assessment. Then, the record would be considered when deciding on the person's promotion, increase of the person's annual salary, or receiving an award for the specified duration of years. Direct financial disadvantage was monetary compensation in proportion to the damage that the breach might bring to the company. We found that serious violations such as a leak or the selling of important internal information would be punished to the extent of dismissal from the company or an accusation for a possible legal punishment. In the worst case, a violator might have to compensate for the damage, be discharged from the company, and then be accused for judicial punishment, all at the same time.

My company reduces the salary of an employee if he/she has committed a violation three times. The company reduces welfare benefits in practice because reduction of salary is not easy to do emotionally. The penalty is reflected in the performance assessment. … If the person who lost the lap top computer belongs to a financial department or a human resource department that deals with confidential data, the employee is, in the worst case, discharged from the company. The employee may be accused of a crime when he/she is

believed to have sold the information arbitrarily. Therefore an investigation may be started. In the worst case, an employee has to compensate and be dismissed.

In addition to the categorisation above, there was the concept of additional punishment. If an employee is believed not to have taken appropriate security action as recommended by the organisational guidelines, he/she has to pay an additional penalty for this non-compliance. We found that, in case of financial compensation, an employee has to compensate up to a maximum of two-hundred per cent of the purchased price in accordance with the employee's security efforts. There was a real example that additional punishment was imposed due to the loss of a lap top computer:

There was a real example. An employee left a lap top computer and lost it. The amount of compensation was not the exact purchased price. … The employee did not comply with any security requirements. The person did not lock the computer in the cabinet, did not lock the screen, and did not set the system password. The employee compensated one hundred and seventy per cent of the purchased price.

3.5.2.2 Variety of Sanctions

As described above, a violation of policy was punished according to its seriousness. Organisations did not use other deterrent mechanisms such as shame or informal sanctions. Further, punishment was solely used as a tool for retribution against non-compliance rather than a method to restrain employees from committing a violation in the future. The difference between punishment and retribution is whether a violator or a violation becomes an example or not. To be a deterrent, punishment has to be associated with the discouragement of potential violators by setting the current violation as an example in public. In the focus group discussion, there was no comment on the public release of the punishment imposed on employees for violations. When interpreting this discussion, we found that a violation was ended with a corresponding retribution. Participating security managers seemed to have rarely considered deterrence as one of the active information security strategies effective in controlling attempts and incidents by affecting the (potential) violator's psychology through the punishment.

3.6 Discussions

3.6.1 Effectiveness of Current Deterrence

Although organisations exert themselves to deter security violations, the overall results explain the reason why current deterrence on information security violations by employees in an organisation is ineffective. The most important finding from the focus group is that organisations should emphasise the detection of

violations. This finding is consistent with the result of Kankanhalli et al. [11]. If organisations discover a violation, they can punish violators. On the other hand, if organisations cannot find any violation, it is impossible to punish violators, however, harsh the punishment organisations have. Furthermore, results show that organisations that focus on the certainty of sanctions rely too much on awareness, without operating appropriate measures.

Previous studies suggested that organisations should employ detective measures to identify information security violations [5–7]. However, we found that organisations are still employing passive measures, and thus detection of violations is opportunistic. In addition, one organisation cut its detection measures by reducing its e-mail monitoring functionality to simple logging in. Our results suggest that organisations should employ various types of measures to increase detection. Solely increasing user perceptions that organisations may operate detective measures as D'Arcy et al. [9] argued, is no longer effective. Employees tend to ignore security guidelines and to breach security policies when a violation is seen as more beneficial [38]. Moreover, if they are strongly-motivated people, the probability of violation then escalates [39]. For example, connecting an unregistered laptop to the intranet using a wireless hub is more beneficial than acquiring official permission because of convenience: the latter takes time, requires paper work (that many employees may think useless), and requires technical inspection including a vulnerability test, virus scan, etc., whereas the former is easy and simple. This can be supported by the claim of the participants that security breaches occur continually, however, their detection is hard. The study also addresses employee attitudes in that that they believe that privacy is important and behave accordingly when privacy conflicts with security.

Secondly, awareness has little influence on deterrence. In the past, the existence of policy and guidelines, and the introduction of them were effective in deterring security violations [5, 11]. Nowadays, employees usually ignore security policies and this incurs security violations [13]. Therefore, awareness has to be changed for deterrence to generate effectiveness. Previous studies point out that awareness includes the policies and guidelines to increase employees' understanding about legitimate and illegitimate use of information assets, security education and training programs, and punishments that violators will pay for their non-compliance with the policy/guidelines [5, 9, 11, 40]. The organisations in this study were no exception. They attempted to increase awareness of employees through the same themes. In this respect, we need to address, based on the example described in previous section, that highlighting the certainty of identification of violation is more effective in achieving deterrence.

Finally, from a severity perspective, we could not find any positive relationship between the intensity of punishment and the occurrence of violations. We found that the method of sanction is punishment only and therefore there are no alternatives, and this is insufficient. This result suggests that organisations need to accept other sanctioning methods to enrich the effect of sanctions. Also, even though punishment is developed well, it is worthwhile to note that severe

punishment has no influence in reducing violations if it is not associated with detection.

3.6.2 Strategic Approach to Improve Current Deterrence

Current deterrence in organisations has room for improvement even though they endeavour to have good awareness.

3.6.2.1 Emphasise the Certainty of Detection

Employees should have a clear perception on the certainty of being caught for their violation. Our study suggests that awareness efforts including making announcements, education and training have to emphasise that violations are definitely detected and violators are certainly identified. Compared to previous studies that emphasise the need to inform employees, to operate education and training, and to convince employees that they may be monitored, this study suggests specific and practical propositions.

3.6.2.2 Employ the Architecture of Deterrence Strategy

We suggest that organisations should employ several information strategies for the purpose of deterrence because deterrence is hard to achieve without employing various means working together. It is crucial for the organisations to employ detection strategy to find out violations and violators as Kankanhalli et al. [11] pointed out. Current measures composed of only internal audits and spot checks are insufficient. In addition, organisations need to provide feedback to employees in the form of detection results to reinforce that employees are being observed and thus can be identified if they violate security. Organisations will need evidence to act on violations and to punish their employees. For a severe sanction such as dismissal, they may have to present strong evidence of a critical violation. Therefore, our study suggests the necessity of a compound strategy working in an architectural framework. The Architecture of Deterrence Strategy (Fig. 3.2) is composed of five constructs of strategies: Detective Strategy, Evidencing Strategy, Feedback Strategy, Deceptive Strategy, and Situation Awareness Strategy. Preventive Strategy is not part of this architecture. However, it is presented to show the relationship between Preventive Strategy and the other strategies in the architecture.

This Situation Awareness Strategy aims at understanding the whole deterrence situation with an emphasis on temporal data acquisition and the support of visualisation [41]. Detective Strategy is used to observe users' behaviour and to identify violations including potential ones to watch. This strategy includes a prior

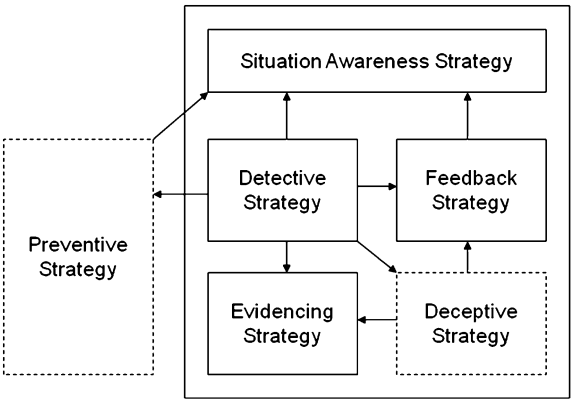

Fig. 3.2 Architecture of deterrence strategy

security internal audit and spot checks as primary measures. These measures also include monitoring that continuously watches the behaviour of users in terms of internet use, system access, security event, and network traffic [42, 43], detection that detects malicious or unusual behaviour [44, 45], and tracing that tracks the violator back to specify the user [46]. Evidencing Strategy includes logging and forensics [47]. The purpose of Feedback Strategy is to warn the user about his/her behaviour that is believed to be suspicious and is being watched and, at the same time, alerting the security manager about the possible violation when Detective Strategy detects suspicious behaviour. This measure includes warning [48, 49] and alarm software [5]. Deceptive Strategy misleads a violator by the creation of illusions in order to waste time and resources of the violator [50, 51]. Operation of this architecture starts from Detective Strategy when suspicious behaviour has been detected. Information then flows following the arrows. After all, the result of important to note or serious violations are fed back to preventive measures.

When designing this architecture, the following three principals were considered. First, some strategies have to be implemented strategically in a selective and limited manner in accordance with the importance of the information assets. Because all the information 'assets may not necessarily be treated with the same significance, the importance of the information assets has to be considered in order to focus the surveillance. Deceptive Strategy falls into this category. Second, each strategy has to be combined to share necessary information and to work together and be coordinated in order to work in tandem. Their relationship in terms of information flow has been presented as an arrow. Third, the experience learnt from deterrence efforts has to be reflected in prevention. The weak points causing frequent violations have to be screened using preventive mechanisms on a tactical level. This feedback loop will contribute to the increase of overall security of organisations.

To implement the architecture successfully, organisations need to consider two main factors: deployment location and employees' resistance. Organisations are required to deploy measures around the site that is believed to be important and is

estimated to be easy to compromise. Also, it is best that measures are free from the debate on privacy. However, when this is impossible to achieve, the relationship between security and privacy has to be considered at the same time.

3.6.2.3 Diversify the Methods of Sanctions

This study suggests that organisations should expand the method of sanctions. In addition to punishment, this study suggests that the concept of deterrence in organisational information security needs to include the concept of 'futility' based on rational choice theory. The purpose of this concept is to lead a violator to consume his/her time and resources. Deception technique will be the most prominent way of implementing futility in organisations. However, the application has to be decided discreetly based on the seriousness that the violation will cause because the demand for this technique must be limited to only some situations. For example, in order to deter security violations to the information system containing R&D results, an organisation may need to use the deception technique to consume the violator's time and resources while obtaining no important information.

The next possible method will be the 'publication' of punishment, which is the fundamental spirit of deterrence. Organisations may have to start a discussion on the method used to publicise punishments. Publicising examples of violation and punishment can be conducted through education, or through the official notice-board. At the same time, organisations need to be considerate because publicity may have an influence on the emotional atmosphere of the company and the morale of employees. Therefore, the method has to be firm and considerate. Other sanction methods such as 'informal sanctions', 'shame', 'self-control', and 'moral beliefs' can also be considered [10, 12].

3.7 Conclusion

It is typical that users tend not to comply with security policy. Previous research focusing on the control of policy violations has been conducted from the deterrence perspective. Mainstream studies have focused on the alteration of users' attitudes through an awareness program composed of informing, educating and training; as well as the perception of the existence of monitoring. However, users will usually violate security policy when the benefit is substantial or neutralisation techniques are employed.

This study analysed the effectiveness of deterrence strategy from the viewpoint of information security managers of organisations. The results suggested that organisations are endeavouring to work on the severity of sanctions that are known to have less influence on deterrence, whereas these same organizations hardly work on any certainty of sanctions that are known to have a positive influence on deterrence. Our study found that organisations should strengthen the detection of violations. In

addition, since the purpose of deterrence is hard to be accomplished by operating a single detection strategy, other strategies to support it have to be combined together.

With this understanding, this study proposed an architecture of deterrence strategy that can improve the effectiveness of current deterrence by adapting several security strategies and coordinating them to work in tandem. From a theoretical point of view, our research deepened the general deterrence model composed of certainty of sanctions and severity of sanctions by distinguishing each construct into two, respectively: awareness of sanctions and detection of violations, and variety of sanctions and intensity of sanctions.

This study focused on the deterrence of internal users. Therefore, future research may need to involve external users. Also, lessens learned from the implementation of the architecture need to be communicated to improve the model. We hope that this study may stimulate others to extend our results.

References

1. Hayward C, Glendinning D (2010) Delivering enterprise-wide data protection controls for mobile computing devices. RSA conference 2010, San Francisco
2. Richardson R (2011) 2010/2011 CSI computer security crime and security survey. Computer Security Institute
3. Kessel PV (2009) Outpacing change: Ernst and Young's 12th annual global information security survey. Ernst and Young
4. Forcht KA (1994) Computer security management. Boyd and Fraser, Danvers
5. Straub DW (1990) Effective is security: an empirical study. Inf Syst Res 1(3):255–276
6. Straub DW, Nance WD (1990) Discovering and disciplining computer abuse in organizations: a field study. MIS Q 14(1):45–62
7. Straub DW, Welke RJ (1998) Coping with systems risk: security planning models for management decision making. MIS Q 22(4):441–469
8. Dhillon G (1999) Managing and controlling computer misuse. Inf Manag Comput Secur 7(4):171–175
9. D'arcy J et al (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf Syst Res 20(1):79–98
10. Hu Q et al (2011) Does deterrence work in reducing information security policy abuse by employees? Commun ACM 54(6):54–60
11. Kankanhalli A et al (2003) An integrative study of information systems security effectiveness. Int J Inf Manag 23:139–154
12. Siponen M, Vance A (2010) Neutralization: new insights into the problem of employee information systems security policy vilations. MIS Q 34(3):487–502
13. Vroom C, Solms RV (2004) Towards information security behavioural compliance. Comput Secur 23(3):191–198
14. Wood C (1982) Policies for deterring computer abuse. Comput Secur 1(2):139–145
15. Huth PK (1999) Deterrence and international conflict: empirical findings and theoretical debate. Ann Rev Political Sci 2:25–48
16. Alberts DS (1996) Defensive information warfare. NDU Press Book, Washington
17. Agrell W (1987) Offensive versus defensive: military strategy and alternative defence. J Peace Res 24(1):75–85
18. Tirenin W, Faatz D (1999) A concept for strategic cyber defense. MILCOM '99, pp 458–463
19. Waterman S (2009) U.S takes aim at cyberwarfare. The Washington Times, Washington

20. Wiant TL (2003) Policy and its impact on medical record security. University of Kentucky, Lexington
21. Foltz CB (2000) The impact of deterrent countermeasures upon individual intent to commit misuse: a behavioral approach. University of Arkansas, Fayetteville
22. Blumstein A et al (eds) (1978) Introduction, deterrence and incapacitation: estimating the effects of criminal sanctions on crime rates. National Academy of Science, Washington
23. Williams KR, Hawkins R (1986) Perceptual research on general deterrence: a critical review. Law Soc Rev 20(4):545–572
24. Hess JM (1968) Group interviewing. In: King RL (ed) New science of planning. American Marketing Association, Chicago
25. Morgan DL, Spanish MT (1984) Focus groups: a new tool for qualitative research. Qual Sociol 7(3):253–270
26. Thomas L et al (1995) Comparison of focus group and individual interview methodology in examining patient satisfaction with mursing care. Soc Sci Health 1:206–219
27. Avison D et al (1999) Action research. Commun ACM 42(1):94–97
28. Kraemer S, Carayon P (2006) Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. Appl Ergon 38:143–154
29. Kreuger RA, Casey MA (2009) Focus groups: a practical guide for applied research, 4th edn. Sage Publications Inc., Thounsand Oaks
30. Kitzinger J (1995) Qualitative research: introducing focus groups. Br Med J 311(7000):299–302
31. Stewart DW, Shamdasani PN (1990) Focus groups: theory and practice. Sage, London
32. Lewis M (1995) Focus group interviews in qualitative research: a review of the literature. Action Research Eletronic Reader
33. Neuman WL (2003) Social research methods: qualitative and quantitative approaches, 5th edn. Allyn and Bacon, New York
34. Fern EF (1982) The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality. J Mark Res 19:1–13
35. Rabiee F (2004) Focus-group interview and data analysis. Nutr Soc 63:655–660
36. Dudley T, Phillips N (2006) Focus group analysis: a guide for hiv community planning group members. University of Texas Southwestern Medical Center Web site
37. Catterall M, Maclaran P (1997) Focus group data and qualitative analysis programs: coding the moving picture as well as the snapshots. Sociological Research Online 2(1)
38. Tunnell K (1990) Choosing crime: close your eyes and take your choices. Justice Q 7(4):673–690
39. Chambliss R (1967) Types of deviance and the effectiveness of legal sanctions. Wisconsin Law Review p 708
40. Lee J, Lee Y (2002) A holistic model of computer abuse within organizations. Inf Manag Comput Secur 10(2):57–63
41. Bearavolu R et al (2003) A visualization tool for situational awareness of tactical and strategic security events on large and complex computer networks. Military communications conference (MILCOM) 2003, pp 850–855
42. Doyle J et al (2001) Agile monitoring for cyber defense. 2001 DARPA information survivability conference and exposition II (DISCEX '01), pp 318–328
43. Dourish P, Redmiles D (2002) An approach to usable security based on event monitoring and visualization. 2002 Workshop on new security paradigms, Virginia Beach, Virginia, USA, pp 75–81
44. Bauer DS et al (1989) Intrusion detection: an application of expert systems to computer security. IEEE international carnahan conference on security technology (ICCST), Zurich, Switzerland, pp 97–100
45. Debar H et al (2005) An infrastructure for distributed event acquisition. European institute for computer antivirus research (EICAR) 2005 conference best paper, Saint Julians, Malta, pp 86–98

46. Kang HW et al (2003) A new intruder traceback mechanism based on system process structure. ISCA 16th international conference on computer applications in industry and engineering (CAINE), pp 117–121
47. Kim K et al (2009) Lessons learned from the construction of a korean software reference data set for digital forensics. Digit Investig 6:S108–S113
48. Henauer M (2003) Early warning and information sharing. Workshop on cyber security and contingency planning: threats and infrastructure protection, Zurich, Switzerland, pp 55–62
49. Stolfo SJ (2004) Worm and attack early warning: piercing stealthy reconnaissance. IEEE Secur Priv 2(3):73–75
50. Cohen F (1998) A note on the role of deception in information protection. Comput Secur 17(6):483–506
51. Michael JB (2002) On the response policy of software decoys: conducting software-based deception in the cyber battlespace. 26th annual international computer software and applications conference (COMPSAC'02), pp 957–962