International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.8, pp : 998- 1002 1 Aug 2014

Coping with Information Security Breaches from Inside: A Strategic Approach

Sangseo Park
The University of Melbourne
parks@pgrad.unimelb.edu.au

Abstract—*This study looks into the employment of deterrence to reduce security breaches within organisations. The result reveals that current deterrence is less influential. This study suggests that organisations should shift towards the detection of violations and the identification of perpetrators. The research also presents a conceptual architecture of multiple strategies.*

Keywords— Information Security, Information Security Strategy, Deterrence Strategy

I. Introduction

Realisation that the information systems and information assets have become one of the most important foundations for the increase of productivity and the strength of competitiveness has called organisations' attention to the control of information security breaches committed by employees. The traditional approach to deal with those breaches including policy non-compliance, policy violations, information leakage, information theft, and privilege abuse is from the deterrence perspective.

Deterrence is a strategy aimed at influencing people's behaviour using the fear of sanctions, which is characterised by the probability of capture and the degree of penalty. Straub [1] showed that deterrence is effective in lowering computer abuse. Straub and Nance [2] pointed out the need to take detective actions and to punish motivated abusers harshly. In a later paper, Straub and Welke [3] stressed the importance of education on security policies and guidelines. Kankanhalli et al. [4] found that deterrent efforts have positive effects on information security. Contrary to this study, D'Arcy et al. [5] found that the severity of penalty has a significant effect on the reduction of the abuse of information systems.

II. Research Method

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 [10]. Researchers can not only capture detailed information, perceptions, experience, and opinions from participants, but they can also examine how ideas are developed, and explore how the opinions are formed [11, 12]. In this respect, focus group research is suitable for providing a deep insight into how the issues of deterrence are dealt with within organisations

Data Collection

Even though it is normally recommended to compose a focus group with four to twelve people, small groups consisting of four to six people, rather than a bigger group, is appropriate in collecting specialised data in a particular discipline through the participants possessing a large volume of knowledge or experience in a specific area [12]. This study requires participants' vast knowledge about the employment of information security strategies in organisations as well as years of experience in information security. Therefore, the number of participants for this focus group needs not necessarily to be large; four to six expert participants are enough.

The initial focus group composed of five security managers was conducted in Korea. 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 [10]. This study also considered the homogeneity of the participants in terms of position, role, authority, years of experience, and the size of their company and business field [12]. All of them had 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 discussion was conducted for 106 minutes and digitally recorded after receiving consent from all participants at the beginning of the discussion. The author transcribed the discussion.

Data Analysis

It is appropriate to use a qualitative approach for analysing focus group data [13]. This study did not pay attention to the numerical data such as the number of participants who represented the same opinion since it may mislead the focus group result [12]. Instead, the analysis was primarily focused on interpretation of the context, what the participants wanted to mention and the meanings behind their conversations, based on themes. This study adapted an 'annotating-the-script' approach and a 'large-sheet-of-paper' approach at the same time [14].

III. Framework for Understanding Deterrence Strategy

As discussed in the introduction, deterrence departs from the perception that people tend to abandon their undesirable actions if they feel the probability of capture is high and the degree of penalty for the action is high, which is built on the theoretical constructs: the certainty of sanctions and the severity of sanctions [15]. Each construct can be subdivided into four sub-constructs as shown in Fig. 1 [16].

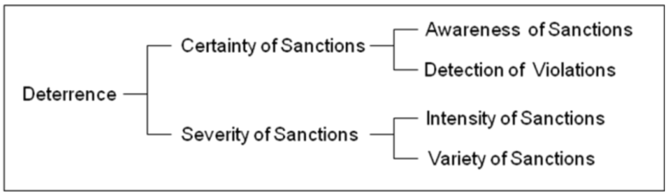

Fig. 1. Framework of Deterrence Strategy

Perception on the certainty of sanctions can be raised when employees realise that they are being watched, which means that the real possibility of capture is high, in addition to understanding the sanctions given as the consequence of breaches. Furthermore, when violations are detected and perpetrators are identified followed by a capture of perpetrators, the certainty will be achieved. Therefore, it is logical to subdivide certainty of sanctions into the awareness of sanctions and the detection of violations. This sub-categorisation can also be supported by the past studies that addressed informing [1], education [3-5], briefing [4], awareness [5, 6], and detective actions [2] as a means to deal with the certainty of sanctions.

Typically, the severity of sanctions has been understood to be heightened by controlling the level or intensity of disincentives according to the seriousness of the breach. For example, Kankanhalli et al. [4] identified four levels of punishment in terms of personnel practices: reprimand, suspension, dismissal, and prosecution. However, it has been argued that sole application of sanctions has no influence on deterring violations [7]. Equipped with various kinds of mechanisms to impose sanctions, organisations can achieve a higher severity of sanctions. Therefore, the method of sanctions was extended to include other methods such as shame and informal sanctions [6], and self-control, moral beliefs, and general deterrence based on rational choice [7]. Therefore, the severity of sanctions needs to consider both the variety of sanctions and the existing concept of the intensity of sanctions.

IV. Understanding Deterrence Strategy in Organisations

Awareness of Sanctions

According to the participants, organisations had developed various means for effective communication. Some companies delivered the information through e-training or bulletin boards on the company intranet on a regular basis. A corporate-wide assembly meeting was used as an opportunity to explain security policy and to warn about the consequences of its violations. A session at an orientation for new employees was found useful for informing them about the severity of disciplinary action resulting from violations as well as introducing them to corporate policy with the aim of improving compliance.

The contents delivered to the employees were information security policy that each employee had to comply with, legal authority the organisation had such as authority to monitor and delete employees' email, what the organisation could do to identify violations and perpetrators such as monitoring, and details of the disciplinary action when the policy was violated. As another form of increasing awareness, some companies received consent from each employee regarding the monitoring of his/her emails when he/she first joined the company. They sometimes requested employees to sign a document pledging their compliance with the company's security policy or they administered an oath of compliance.

One interesting finding was a participant's experience in successful deterrence through the conviction of being caught. According to him, two to three years of education aimed at new employees with the emphasis on the high possibility of being caught was effective. From this case, it can be surmised that the impact of awareness is more effective when education is focused on both new employees and the conviction of being caught.

Detection of Violations

Without applying appropriate, active, and working detection mechanisms, a deterrence strategy which is based on sanctions will not be effective because it would be hard to detect violations and subsequently difficult to specify a perpetrator. Therefore, the detection of violations should be systematic rather than opportunistic. However, organisations had used spot checks and internal audits by security manager(s) to detect security violations. Some audit tools turned out to have technical defects. Due to the use of passive and technically defective tools, with their application at transitory moments, the detection of violation and the identification of perpetrators were subject to chance.

The lack of detection mechanisms resulted in continuous attempts by employees to detour security hurdles as well as in the disregard of security regulations. Some security managers mentioned that employees attempted to take laptops out of the company without permission, to connect unregistered systems to enterprise intranet, to use unlicensed software, and to store confidential information on portable storage devices. Employees even failed to configure laptop security features to meet company regulations. However, these violations were difficult for security managers to detect.

Moreover, this study encountered a revealing experience that deterrence hardly worked when there is a resistance by employees. An organisation confronted the emotional resistance of employees against the company's security regulations on e-mail monitoring. The union demonstrated against the monitoring and perusal by the company. They worried that the company may infringe on an individual's privacy, or the managers or a person who has the privilege to read an email may abuse this prerogative. As a result, the company finally renounced real-time online monitoring and removed relevant privileges from the system, then changed its regulation on employees' email monitoring. Employees' emails were allowed to be traversed by an authorised administrator only for the purpose of evidence collection against serious violations or crimes.

Intensity of Sanctions

Judging from the participants' discussion, sanctions imposed on perpetrators were well-developed. There were five kinds of disciplinary actions depending on the seriousness of the violation: reduction of payment, reflection on performance assessment, financial compensation, dismissal, and accusation or lawsuit.

Although the reduction of salary (for a specified duration) was an effective means to control employees' violative behaviour, the company, in fact, reduced welfare benefits, such as financial support for the purchase of books, recreational expenses, or physical exercise, in the consideration of emotional morale. A security breach record reflected in an annual performance assessment would affect the employee's promotion or salary increase for the specified duration of years. In one organisation, an employee was punished to compensate financially for his/her loss of a laptop. If the lost laptop had contained important information such as financial data or personnel records, the involvement in a crime was preferentially investigated. In the case of a serious violation such as the intentional leakage or the sale of important internal information, the disciplinary action would be dismissal from the company. In addition to the dismissal, the company might also press charges against the perpetrator if the violation is believed to be associated with any criminal activity.

Not all single violations earned immediate disciplinary action. For comparatively light and simple violations, which are normally the most common, disciplinary action was not considered until the number of violations had accumulated to several. For example, an employee would be punished with a salary decrease for three months after he/she had committed violations three times. For serious cases, on the other hand, a single violation would result in immediate disciplinary action.

The concept of an additional disciplinary action was also devised. If an employee was believed not to have taken appropriate security action as recommended by the organisational guidelines, he/she had to pay an additional penalty for this non-compliance. According to one participant's experience, an employee had to compensate 120 per cent of the purchased price of a laptop when he/she lost it; the employee had to compensate additional 20 per cent of the purchase price for the loss.

Variety of Sanctions

Instead of diversifying the method of sanctions by including other mechanisms such as shame or informal sanctions, the only sanction employed was an internal disciplinary action following the company's own policies and procedures. Moreover, the disciplinary action was usually used as a means of retribution rather than a method to impede employees from committing further violation, in that the difference between disciplinary action and retribution is whether or not a perpetrator or a violation becomes an example. To be a successful deterrent, disciplinary action has to be seen to be delivered in order to discourage potential perpetrators. There was no comment at all on the public exposure of the disciplinary action, which can be interpreted that a violation will be met with a corresponding personal retribution.

IV. Towards Effective Deterrence

Although organisations exert themselves to deter security breaches by insiders, the focus group revealed that there is room to make current deterrence strategy more effective.

Convincing the Certainty of Detection

This study suggests that organisations should expand the topics of awareness to include the increased possibility of capture followed by disciplinary action, and then to highlight it using existing examples. When employees perceive that the probability of capture is high due to the operation of detective measures, a deterrence strategy works more effectively [1]. This study also has a supporting finding from the experience of one participant who successfully implemented deterrence through convincing new employees of the probability of being caught if they committed a violation.

Topics of education aimed at raising awareness have continued to expand. In the past, according to Straub [1], perception of the existence of policy and guidelines explaining legitimate use of information assets was sufficient to deter security violations. Later, topics began to include a definition of the illegitimate use of information assets, and the scale of disciplinary actions that perpetrators could expect to pay for their non-compliance [1, 4]. Employees' awareness of the existence of detective measures was reported to have a positive effect on the reduction of violations [1, 5].

However, most organisational awareness programs were focused on the delivery of information on policy and disciplinary action itself. Now, this study has evidence that convincing employees of capture had a positive influence on the raising of awareness, which, in turn, contributed to the reduction of security violations by increasing the fear of sanctions. Therefore, the context of the awareness of sanctions needs to instill the probability of capture in the employees.

Employment of Detective Measures

This study suggests that organisations should employ various types of detection measures as well as fundamentally change their attitude towards the operation of those measures from 'passive' to 'active'. However harsh the disciplinary action is and however high the awareness is, it is impossible to sanction perpetrators unless organisations detect any violation and identify the perpetrator. A Security breach is known easily attempted_especially when the neutralisation technique is involved [6], or the benefit of violation is substantial [7]. Therefore, in order to make sanctions real thereby making them an example, organisations should be equipped with appropriate detection measures, which were believed to have effect on deterring security violations [1-4].

However, the results showed that organisations, in terms of the certainty of sanctions, were relying too much on awareness while depending less on detection of violations. Besides, the use of limited types of detection measures, such as spot checks and internal audits, and even defective tools in concert with their passive and opportunistic operation seemed to be insufficient and to affect the deterrence in a negative way resulting in continual security breaches in organisations. The surest way of increasing the certainty of sanctions is to unearth every violation and to identify every perpetrator.

Employment of the Diverse Methods of Sanctions

This study suggests that organisations should expand the method of sanctions. The focus group revealed that the sole method of sanctions was disciplinary action, which proposes the idea that organisations should accept alternative methods to widen the effect of sanctions. As an alternative, the concept of 'futility', based on rational choice theory, can be considered aiming at the consuming of a perpetrator's time and resources. The best way of implementing the notion would be through deception strategy that is included as a component in Fig. 2.

Another alternative would be 'making the disciplinary action public', which is regarded as effective in deterring future violation by making an example of the perpetrator. Publicising can be performed through education, or through the official notice board. What organisations need to consider when pursuing the alternative would be an influence it had on the morale of employees and in turn on the enterprise-wide atmosphere. Therefore, the application of this method should be both firm and considerate. Organisations may put other methods such as 'informal sanctions', 'shame', 'self-control', and 'moral beliefs' on the table, as some research contemplated [6, 7].

Multi-strategy Approach

This study proposes that organisations, in addition to detection strategy, should employ various types of additional strategies and coordinate them to work together in order to maximise the effect of deterrence. For example, organisations will need to warn employees of suspicious behaviour and to collect evidence of violation before taking legal action. Therefore, this study suggests a compound strategy, composed of Detective Strategy, Evidencing Strategy, Feedback Strategy, Deceptive Strategy, and Situation Awareness Strategy, working in an architectural framework (Fig. 2). The arrow between strategies represents information flow. Preventive Strategy is never a part of it but is presented to show the relationship among its components.

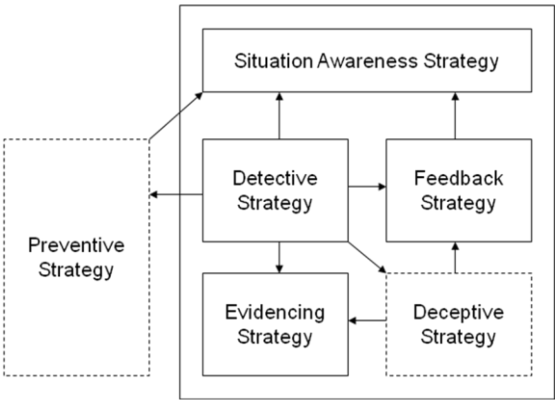

Fig. 2 Concept of Multi-Strategy Approach

Detective Strategy, which is a beginning point of the architectural concept and plays a central role in the concept, surveils users' behaviour and identifies violations including potential ones to observe. This strategy not only includes prior security measures, internal audits and spot checks but also consists of the monitoring of internet use, system access, security event, and network traffic, the detection of malicious or unusual behaviour, the specification of the perpetrator, and the trace of perpetrator's track. Information about any events requiring special attention needs to be passed to Preventive Strategy so that preventive actions, aimed at preventing future recurrence of the same violations, take place. Situation Awareness Strategy, with the support of visualisation techniques, aims at understanding the whole deterrence situation based on temporal data acquisition by Detective Strategy. Evidencing Strategy includes collection and preservation of information and events, and mining of information for evidence purposes. Feedback Strategy begins its operation when Detective Strategy detects suspicious behaviour. It aims at alerting security managers about possible violation, at the same time, warning a potential perpetrator who is under observation. Feedback to the employee will have an immediate deterring effect since the person will stop suspicious behaviour instantly if warned. Deceptive Strategy misleads a perpetrator by creating an illusion with the intention of wasting the perpetrator's time and resources.

There are three principals to consider in designing the conceptual architecture. Firstly, some strategies have to be implemented in a selective or limited manner in accordance with the importance of the information assets. Deceptive Strategy falls into this category; if information assets requiring protection are vital, for example, R&D information for future business opportunities, the organisation may need to implement the strategy. Secondly, each strategy has to share sufficient information and to work together in a coordinated way. Finally, 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. This feedback loop will contribute to the increase of overall security of organisations.

IV. Conclusion

Most previous studies on deterrence have proposed to alter users' attitudes through the increase of awareness or the introduction of alternative methods of sanctions. However severe the sanctions, inspired the awareness, or various the methods of sanctions, users tend to violate security policy by using diverse techniques. Perpetrators will not stop violating unless they feel threatened by the probability of both the detection of their offense and the identification of them, which is the most effective and practical driver of deterrence.

Therefore, deterrence efforts in organisational information security need to shift to detective perspective. Organisations should adapt various strategies designed to operate in a coordinated way in an architectural framework to make detection more workable. Organisations should also increase employee's clear perception on the detection, apply alternate sanctions, and consider employee's resistance in terms of privacy.

From a theoretical point of view, this research deepened the general deterrence model composed of the certainty of sanctions and the severity of sanctions by distinguishing each construct into two, respectively: the awareness of sanctions and the detection of violations, and the variety of sanctions and the intensity of sanctions. The extended model will offer a frame for the comprehensive understanding of deterrence.

References

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

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

iii. *Straub, D. W. and Welke, R. J., Coping with Systems Risk: Security Planning Models for Management Decision Making, MIS Quarterly, 22 (1998), 441-469.*

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

v. *D'Arcy, J., Hovav, A. and Galletta, D. F., User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research, 20 (2009), 79-98.*

vi. *Siponen, M. and Vance, A., Neutralization: New Insights into the Problem of Employee Information Systems security Policy Vilations, MIS Quarterly, 34 (2010), 487-502.*

vii. *Hu, Q., Xu, Z., Dinev, T. and Ling, H., Does Deterrence Work in Reducing Information Securiuty Policy Abuse by Employees?, Communications of the ACM, 54 (2011), 54-60.*

viii. *Richardson, R., 2010/2011 CSI Computer Security Crime & Security Survey, Cmputer Security Institute, (2011).*

ix. *Kessel, P. v., Outpacing Change: Ernst & Young's 12th Annual Global Information Security Survey, Ernst & Young, (2009).*

x. *Morgan, D. L. and Spanish, M. T., Focus Groups: A New Tool for Qualitative Research, Qualitative Sociology, 7 (1984), 253-270.*

xi. *Kitzinger, J., Qualitative Research: Introducing Focus Groups British Medical Journal, 311 (1995), 299-302.*

xii. *Kreuger, R. A. and Casey, M. A., Focus Groups: A Practical Guide for Applied Research, 4th Edition ed. Sage Publications, Inc., (2009).*

xiii. *Liamputtong, P., Focus Group Methodology: Principles and Practice. Sage, (2011).*

xiv. *Catterall, M. and Maclaran, P., Focus Group Data and Qualititive Analysis Programs: Coding the Moving Picture as Well as the Snapshots, Socilogical Research Online, 2 (1997).*

xv. *Williams, K. R. and Hawkins, R., Perceptual Research on General Deterrence: A Critical Review, Law & Society Review, 20 (1986), 545-572.*

xvi. *Park, S., Ruighaver, A. B., Maynard, S. B., and Ahmad, A., Towards Understanding Deterrence: Information Security Managers' Perspective, Proceedings of the International Conference on IT Convergence and Security 2011, Lecture Notes in Electrical Engineering 120, (2011), 21-37.*