A Coherent Model in Upholding General Deterrence Theory and Impact to Information Security Management

Myeonggil Choi* · Edwin R. Ramos** · Mansig Kim** · Jinsoo Kim* · Jaehoon Whang*** · Kijoo Kim****

Abstract

To establish an effective security strategy, business enterprises need a security benchmarking tool. The strategy helps to lessen an impact and a damage in any threat. This study analyses many aspects of information security management and suggests a way to deal with security investments by considering important factors that affect security manager's decision. To address the different threats resulting from a major cause of accidents inside an enterprise, we investigate an approach that followed ISO17799. We unfold a criminology theory that has designated many measures against the threat as suggested by General Deterrence Theory. The study proposes a coherent model of the theory to improve the security measures especially in handling and protecting company assets and human lives as well.

Keywords : Information Security Management, Security Threats, General Deterrence Theory

Received : 2009. 09. 02.　　　　Final Acceptance : 2009. 09. 16.

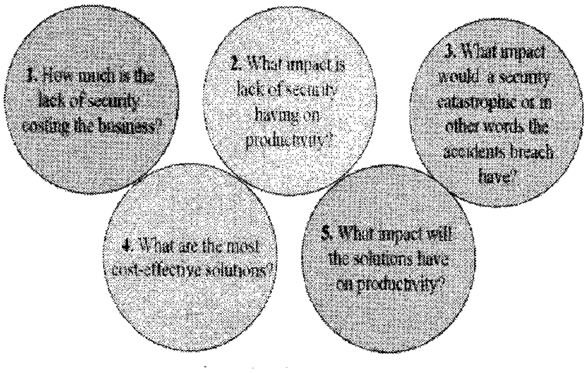
※ This paper was presented in the International Conference on ITAM and revised for JITAM.

* Department of Business Administration, Chung-Ang University, Korea, the 1st author, e-mail : mgchoi@cau.ac.kr
** Department of System Management Engineering, Inje University, Korea
*** Department of Management Information Systems, Yonsei University, Korea
**** Department of Management Information Systems, Konyang, University, Korea

1. Introduction

In these days, hackers, computer viruses and cyber-terrorists are constantly increased. Having these viruses, hackers and cyber-terrorists are making headlines daily and security has become a major priority in all of enterprises. To make a decision in investing appropriate resources for the measures of information security is one of the most important tasks to the manager of information security [Sonnenreich, 2000].

Security professionals armed with the necessary skills and knowledge try to create an added-value to their enterprises. In order to surely operate functions of the enterprises, security professionals can direct their security measures and security policy which could be implemented securely. Before security professionals push to implement security measures, they have to analyze the impact of the security measures. The strength of the security measures depends on the amount of the resource invested. In order for security manager to calculate the exact the cost of the security measures, they have to consider the cost related questions which is shown in <Figure 1>. Before they invest security measures, the security manager has to analyze whether the security measures could be financially justified. Security has to be considered in term of business natures. To consider security measure in terms of business natures, the security managers have to analyze security metrics that show how security expenditures could be appropriate. The costs of implementing security measure is greater than those of overall risks, and the security measure could not be introduced into an organization.


1. How much is the lack of security costing the business?
2. What impact is lack of security having on productivity?
3. What impact would a security catastrophic or in other words the accidents breach have?
4. What are the most cost-effective solutions?
5. What impact will the solutions have on productivity?

<Figure 1> Considerations which a Security Manager Has Before Implementing Security Systems

We simultaneously consider in calculating overall risks and threats, and compare the costs of them in implementing security. The objectives of this study are as following. The first is raising the awareness of the different threats and risks which are essential elements in deciding on the protection mechanism selected to protect the assets. The second is to understand the skills how we can combat and mitigate different threat agents. The third is to unfold criminology theory that has designated the measures against security accidents, The fourth is to address the threats based on ISO17799 and to improve the Security Action Cycle Model.

2. General Deterrence Theory

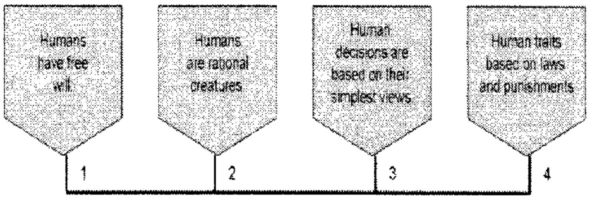
General Deterrence Theory (GDT) has been widely used in the study of criminal and anti-social behavior and is a well-established theory within the criminology field [Theoharidou, 2005]. It is based on the hypothesis that people makes logical decisions based on the maximization of their benefit and the minimization of cost [Beccaria, 1963]. It focuses on the 'disincentives' or 'sanctions' against committing a criminal act and their effectiveness as a deterrent.

The concept of deterrence shows that all human beings are familiar with each other. We can find many examples of deterrence in our daily lives. While we may be familiar with the concept due to the constant bombardment of this deterrence tactic, we have surely begun to be desensitized. Due to this constant exposure, we can easily forget the sources of deterrence, its purpose, the tactics and effects. As it relates to the criminal justice system, deterrence goes to great lengths in an attempt to keep the citizens of our communities-our families-safe and on many levels it succeeds.

Deterrence, as it has become known by the criminal justice system, has been used throughout the history of mankind. The earliest known example of deterrence as it relates to crime and punishment is the Code of Hammurabi. This ancient text was the first, a document set forth by a ruling party which categorized crimes and their corresponding punishments. This code was intended to educate members of society on what is expected of their conduct and what would happen if they violate those expectations [King, 1998]. The Code of Hammurabi also made it clear that "*ignorance of the law is no excuse for its breaking, another step along the path of crime deterrence.*" [Wikipedia, 2006]

Cesare Beccaria, an eighteenth-century philosopher, was the first to conduct information gathering on the correlation between the imposed punishment of crimes and complaint behavior of society [Keel and Robert, 2007]. Beccaria believed that criminal decisions were based on a few simple factors that humans have free will and a more logical sense they have a power to act upon their own accord. Humans are rational creatures and able to weigh prospective outcomes of their actions, and see which may benefit or detract from the quality of their lives. Human decisions are based on a simple view that it points out the pleasures preferable over pains. An organized system of laws and punishments which catered to these human traits is necessary to keep society compliant [Winfree, and Abadinsky, 2003]. To sum up everything, a simple diagram is shown in <Figure 2>.

As these traits heavily involve human choice and rationality, Beccaria's theories fall into the Rational Choice school of criminal theory and are closely related to rational choice that humans are notorious for considering their actions and weighing the pros and cons as it relates to themselves before acting. Beccaria's studies of deterrence theory waned and criminology theorists focused on the criminal mind instead of preventing the mind from acting for over a


Humans have free will.
Humans are rational creatures
Human decisions are based on their simplest views
Human traits based on laws and punishments
1
2
3
4

<Figure 2> Factors that Affect a Criminal Decision

century. In the early 1960's, United States refreshed the criminal justice community's view to deterrence. The government began to invest more time and effort to reflect these theories. Deterrence is a litte difficult concept to measure as it produces no solid, tangible primary results. All results from deterrent methods are dependent upon something else.

The concept of General Deterrence is the most proactive of all as it seeks to target potential crimes before they happen. This branch of theory is a starting point in the deterrence continuum and often targets the crime. One may ask how a rule deters a crime instead of a person. It is believed that General Deterrence does so by issuing blanket knowledge that if one commits a crime then there will be punishment. General Deterrence is related to issue law and make that it is not permitted and that there will be consequences if one commit such an act. For an example, a "No Trespassing" sign insides a private area in the manufacturing firm in which quotes a state law, such as the State of Washington's, is aimed to remind or educate general public that their entrance commits Criminal Trespass in the second degree [State of Washington, 2007]. Many examples of General Deterrence we see everyday do not even have to quote the law itself. Electronic article surveillance is a popular deterrence method in many groceries and department stores. Ominous tags attached cause pillars to sound when each time tags pass. Video surveillance cameras which watch our every move in retail establishments, convenient stores, banks and government buildings. All of these security measures deter the commission of crimes and are aimed at the general public. It is also important to note that General Deterrence is the most common, widespread form of this theory.

3. Interrelations among Security Standards, Compliance, Risks Analysis, Threats and Controls

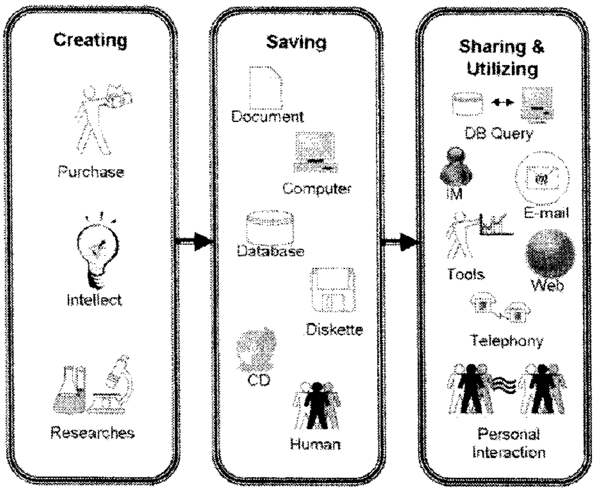
3.1 Security Standards

Standards play an essential role for drawing the roadmap of information security [Karabacak, 2006]. One of the leading standards in information security is ISO17799 as it provides a set of recommendation for security management. It mainly focuses on the protection of information as an asset, nevertheless it adopts a broad perspective that covers most aspects of IS security such as physical security and personnel security etc. Meanwhile, we need to simplify the meaning of the two terms. Information security refers to the preservation of confidentiality, integrity and availability of information. On the other hand, IS security refers to the protection of all elements constituting an IS which are the hardware, software, information, people and processes. Therefore, IS security is a broader term that can be used for accommodating information security as well [Theoharidou, 2005].

(1) ISO17799

ISO17799 provides a set of recommendations for information security management. Its focus is on the protection of information as an asset, nevertheless it adopts a broad perspective that covers most aspects of IS security like for instance physical security, personal security etc. At this point we should clarify the meaning of the two terms. Information security refers to the preservation of confidentiality, integrity and availability of information [ISO/IEC, 2002]. Respectively, IS security refers to the protection of all elements constituting an IS that is a hardware, software, information, people and processes. Therefore, IS security is a broader term that can be used for accommodating information security as well. Information security management in ISO17799 is based on risk management. The latter is defined in the standard as the "process of identifying, controlling and minimizing or eliminating somehow security risks that may affect information systems, for an acceptable cost" [ISO/IEC, 2002]. Risk mitigation is achieved, mainly, through the implementation of appropriate controls, which address a wide range of threats.

Information security management in ISO17799 is based on risk management. The latter is defined in the standard as the "process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost" [ISO/IEC, 2002].



〈Figure 3〉 A Lifecycle of Business Firm Records

Modern information systems are confronted to a variety of threats. Although attacks originating from hacking attempts or viruses, have gained a lot of publicity, insider threats pose a significantly greater level of risk [Schultz, 2002]. There are controls and tools that are used for the protection of the IS from externally initiated attacks.

3.2 Compliance

Compliance to what the security standards require is not an easy task to do. It is necessay to define what compliance is. From the definition of the standard dictionaries, compliance has meaning as the cooperation with or obedience to the law. In Information Technology IT compliance means an accordance of corporate IT systems with predefined policies, procedures, standards, guidelines, specifications or legislation [Kim, 2007].

Within an industrial information systems, an e-mail, instant messenger (IM) message, DB query and contents interacted via the world wide web (WWW) are recognized as critical business records which should be secured, monitored, maintained, retrieved and controlled. A lifecycle of an industrial manufacturing firm records consists of three phases which primarily are : (a) creation, (b) saving and (c) sharing and utilizing available methods. To have a clear picture of these three phases, <Figure 3> has been illustrated.

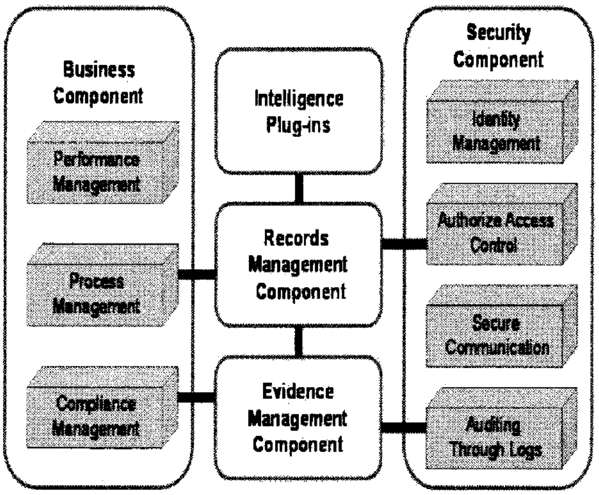
The first phase is creating information wheerin information can be created through purchasing, researching and even through intellectual activities. Second phase is known as the saving of information. Saving information can be dealt in many ways. Saving information is storing documents, computer, database, floppy diskettes, compact discs and flash or handy drives. In addition to that, information can also be remembered and retrieved by humans using their brains. Final phase would be the sharing and utilizing. Humans will tend to use different means on how they can pass the information to others. Such means are via data base query (DB Query), instant messengers (IM), E-mail, business tools, Web/Internet, Telecommunication and of course even person interaction. The sharing and utilizing of information by the employees to other people who does not involve into any business transactions of the company commits the regulation of the company.

However, it is not easy for a business firm to handle and manage records where these are linked in a centralized system. Instant messengers and e-mail records are the representative technology make the business has difficulty in recoding information contained. These records are typically stored, accessed and managed by many distributed users. Instant messengers provide a live communication and file transferring functions to many unknown persons outside. These messengers can easily downloaded files using its browser [Kim and Leem, 2005a].

In order to follow the compliance of an industrial information, a framework has been suggested which is based on the general background of technology management, industrial engineering and information and security engineering. The complete compliance framework is shown in <Figure 4>.

Each component is as following;

1. Business Component which consists of performance management, process management and compliance management. Any operational records are reported and economic value of compliance systems are estimated by the performance management functions. The process management module administers all the components of the system in the compliance framework. The compliance management verifies whether the entire systems comply the framework and maintain proofs.
2. Intelligence Plug-ins: Most of the data in industrial information systems are stored in database, personal computers and other storage devices, which are practically communicated and retrieved via E-mail, World



<Figure 4> a Suggested Compliance Framework

Wide Web and E-Business System Tools. These plug-ins connect or link all lines that flow the information of the business [Kim and Leem, 2005a; Kim, and Leem, 2005c].

3. Records Management Component obtains and gathers all of the business records that are passed through the intelligence plug-ins. The obtained and gathered data records are stored, maintained and accessed [Young and Fairlamb, 2004].
4. Evidence Management Component attains a successful presentation of evidence. Business records prior to its formats and specifications must meet the requirements of legal specification. Furthermore, the presentation of these evidences must be approved and profiled, correctly.
5. Security Component covers four major things which include identity management, access control for authorization, secure communication and auditing logs. The identity management and access control authenticate and authorize user to access a system while user has to be proven as the authorized one by user's name and password or user's certificate. The secure communication encrypts the message and guarantees confidentiality, integrity and privacy of business records. Access to business records can be monitored and analyzed through the logs [Krutz, and Vines, 2001].

3.3 Risk Analysis

Understanding risk analysis is important in deciding to select the protection mechanism for secure information. The experts of information security have been challenged by problem that how much resource could be invested to corrective countermeasures for effectively protecting the information It is true that there is no risk that can be completely removed. While controls could mitigate the loss of information, risks could be only reduced. Risk analysis can be categorized into quantitative risk analysis and qualitative risk analysis. Quantitative risk analysis simply quantifies risk by giving a value and the results which extract from the data concerning information assets. Qualitative risk analysis is based on the subjective information, which directs the results into how vulnerable or how high the risk [Magalhaes]. In the calculation of risk, it is very useful to understand what the cost of asset protected. Assets have different risks. It is essential to correlate each risks with each of the assets.

3.4 Threats

After certain risks are identified, a company finally determined how much loss can be expected from a security accident. The company could make a decision on how to protect the company. The threat could harm one's assets such as data kept in a part of records. Computer network system might be also jeopardized. The firewall system was considered as a secure tool in that it could protect the intellectual resources inside the network. As the resources of the threats has came from either an external source or internal source, the system could not com-

〈Table 1〉 an Example of Threat Agents

List of Threat Agents
Natural Disasters
Fire
Floods
Freezing
Heat
Manmade Threats
Virus
Malware
Spyware
Trojan
Worms

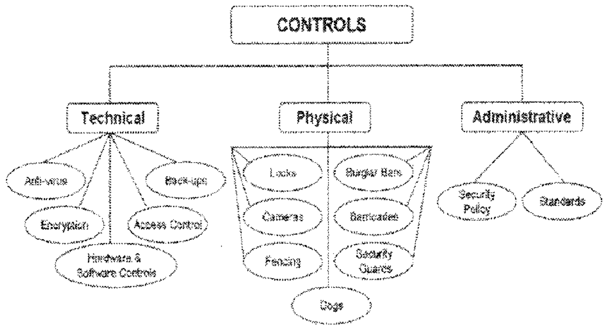
pletely protect the information assets inside network. When threats influence the information resources, they could originate from inside or outside of the network.

Threats could orignate from threat agents, which are varisous [Magalhaes]. <Table 1> shows examples of threat agents.

3.5 Controls

When it comes to risks, there are plenty of solutions to manage them. Most of the risks are mitigated by the security measures. To limit risks, it is important to isolate the asset which is worth protecting.

Before applying the control to the assets, isolating the asset turn out to be cost-effective. It is effective to remove the vulnerable asset from the environment in that the vulnerable asset cause attracts many threats. To mitigate risks, we have to anaylze which countermeasure is appropriate for the risk. There are three types of controls which could be considered countermeasure. They are technical control, administrative control and physical control. <Figure 5> shows a control tree. <Table 2> describes each measure of the three kind controls.



〈Figure 5〉 The Structre of Control Tree

4. Modeling General Deterrence Theory

4.1 The Impact of General Deterrence Theory on Information Security Management

The analysis of the literature on threats has

〈Table 2〉 The Major Type of Controls

Controls	Description
1. Technical Controls	These can be installed and applied to mitigate risks. E.g. anti-virus, back-ups, access control, encryption, etc.
2. Physical Controls	These can be implemented physically to control the access of the assets. E.g. locks, cameras, burglars, fencing, etc.
3. Administrative Controls	These are written like policy and standards which are implemented or regulated to reduce the risk. E.g. security policy and standards.

showed that the tools and methods have their roots in criminology, since concepts such as 'computer crime', 'computer abuse/misuse', 'deterrence', 'motives' and so on are widely used. General Deterrence Theory which are employed in criminology are used. presented. The theoretical origin of the tools and methods lead to useful conclusions that it is possible to draw a rationale for improving behavior.

General Deterrence Theory (GDT) has been widely used in the study of criminal and anti-social behavior. It is a well-established theory within the criminology field. It is based on the hypothesis that people make logical decisions based on the maximization of their benefit and the minimization of cost. It focuses on the 'disincentives' or 'sanctions' against committing a criminal act and their effectiveness as deterrent.

According to Blumstein [Blumstein, 1978], the effectiveness of such disincentives is based on : (a) certainty of sanction and (b) severity of sanction [Straub and Welke, 1998]. According to the theory, while the possibility of punishment is high and the sanction is severe, potential criminals will be deterred from committing illegal acts especially when their motives are weak. In this context, sanctions are considered to be effective in that deterrence mechanisms prevent employees, having a weak desire to break the social norms for the benefit from committing break the social norms. GDT is also well established within the IS security field and could be applied in order to deter computer abuse [Straub, 1990]. The Security Action Cycle is an application of the GDT.

4.2 The Improved Security Action Cycle Model

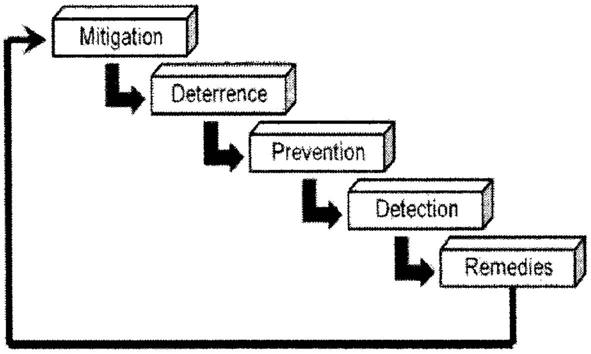
The improved coherent model identifies the aim of IS security management as the maximization of the number of deterred and prevented abusive acts, and the minimization of the number of detected and punished ones. In addition, this cyclical model has a feedback mechanism which includes a new step that starts from mitigation followed by the four other stages and continues back and forth. This model reveals and realizes its fundamental doctrines. The complete model is shown in <Figure 6>.

(1) Mitigation

To mitigate the risk, it is necessary to audit the entire system and establish an incident response plan before incident happen. Mitigation leads to a proactive management which eliminates a possibility of a problem in advance. Mitigation lessens the impact, the damage and the stress of any incident affecting the assets and human lives.

(2) Deterrence

Most of the potential offenders are deterred



<Figure 6> The Cyclical Model of General Deterrence Theory

through mechanisms such as policies, guidelines and awareness programs.

(3) Prevention

If deterrence proves to be ineffective, prevention mechanisms are used, such as physical or procedural controls.

(4) Detection

The mechanisms at this stage address the realization of computer abuse, aiming to make abuses.

(5) Remedies

When an abuse of a computer is detected, its consequences should be treated against the offender according to the organization's policy

4.3 Mitigations of Risks

All of the things happened inside a plant could be hazardous or non-hazardous. It is important to adopt a way to lessen the number risk and severity of risk inside an enterprise. When security infrastructure is so solid, there may be a problem. Most of the time, security is not something that gave a lot room to be thought. In this study, we tried to enlist some possible process on how we can mitigate risks. The procedures are as follows :

a : Creating information security policies, which have to be documented, supported and approved by the management. This includes a security policy or guidelines, disaster recovery policy, a continuity plan and so forth.

b : Testing every detail of policies. Policies documented needs to be tested. Policies have to incorporate a time span. Prepare specific scenarios and establish a way of these policies to be operated and to observed.

c : Have a constant audit and assessment of network, system and staff. Possible questions that can be taken for consideration are : "Who is assessing the network?, When they are assessing it?, Who exactly has the administrative rights and who has been delegated rights and etc."

d : Verify your back up and restore solution. Awareness of where back ups are maintained, who can access them and inclusion of procedures of data restoration and system recovery.

e : Implement defensive measures. This includes security measures and tools such as firewall, intrusion detection, secure communication and etc.

f : Implement changes in management solutions. Total control is needed over your network and systems. Make sure that every change on the network either set-up or installation is properly documented and back up with a back out plan.

g : Train security IT staffs and end users. It is essential to establish this kind of program to keep networks safe.

h : If there is a complete locker, do an independent audit. Invite a team to come over and test the security.

I : Build an Incident Response Plan. Create a single plan when everything falls apart.

Let's say you've been attacked and an issue comes up like losing a file server and deletion of the contents of the hard disks.

j : Create a team responsible for computer security. This composes of group of people that is built with responsibilities for dealing with any security risks or incidents. A part of their tasks is to ensure that no area is left uncovered.

5. Conclusion

Security threat is an issue with enhancing importance for Information security management. The issues covered in General Deterrence Theory considering its origin is under the scientific field of criminology. Analyzing ISO17799 as a dominant standard in IS security management, we discovered that it follows the General Deterrence Theory, the most classical and oldest criminology theory. Apparently, this theory emphasizes on measures such as posing sanctions, reinforcing access control, auditing the system, creating an incident response plan and implementing training and awareness programs.

Utilizing ISO17799 as a Code of Practice for Information Security Management could be a framework to guide an approach to manage security. Based on the analysis and results from the case study, there are around 9 different clauses under ISO17799 that the company has controlled.

The cyclical model of General Deterrence Theory shows an improved cycle from four to five stages which consider a proactive mode of Security Management. This mode tells us that elimination of a possibility of a problem in an advance can minimize the impact, the damage and the stress of any incident.

Reference

[1] Beccaria C. On crime and punishments. Indianapolis, IN : Bobbs Merril; 1963.

[2] Blumstein A. Introduction. In : Blumstein A, Cohen J., Nagin D, editors. Deterrence and incapacitation : estimating the effects of criminal sanctions on crime rates. Washington, DC : National Academy of Sciences; 1978.

[3] ISO/IEC. Information technology-code of practice information security management. ISO/IEC 17799 : 2000(E), Geneva, Switzerland; 2002.

[4] Karabacak, B. A Quantitative Method for ISO17799 Gap Analysis. Computer and Security, Vol. 25, 2006, pp. 413-419.

[5] Keel, Robert, Rational Choice and Deterrence Theory Lecture Notes. Retrieved June 20, 2007, from University of Missouri, St. Louis website, 2005, http://www.umsl.edu/~rleel/200/ratchoc.html.

[6] Kim, S., IT compliance of industrial information systems : Technology management and industrial engineering perspective. The Journal of Systems and Software, Vol. 80, 2007, pp. 1590-1593.

[7] Kim, S. and Leem C. S., Security of the internet-based instant messager : risks and safeguards. Internet Research : Electronic net-working Applications and policy, Vol. 15, No. 1, 2005a, pp. 88-89.

[8] Kim, S. and Leem, C. S., A case study on real-time click stream analysis system. Lecture Notes in computer Science Vol. 3314, 2005c, pp. 788-793.

[9] King, L. W. , Ancient History Sourcebook : Code of Hammurabi, c. 1780 BCE. Retrieved June 20, 2007, from Fordham University website, 1998, http://www.fordham.edu/halsall/ancient/hamcode.html.

[10] Krutz, R. L. and Vines, R. D., The CISSP Prep Guide : Mastering the Ten Domains of Computer Security, John Wiley and Sons, New York, 2001.

[11] Magalhaes, R. Risk Analysis : Things to consider when working out how much risk we carry, WindowsSecurity.com. pp. 1-4.

[12] Schultz EE. A frame work for understanding and predicting insider attacks. Computers and Security, Vol. 21, No. 6, 2002, pp. 526-31.

[13] Shimonski, R. Threats and your Assets-What is really at Risk?. GFI LANguard N.S.S. pp. 1-10.

[14] Sonnenreich, W. Return on Security Investment(ROSI) : A Practical Quantitative Model, SageSecure, LLC. 2000, pp. 1-7.

[15] State of Washington, Chapter 9A.52 RC W : Burglary and trespass. Retrieved June 18, 2007, from website : http://apps.leg.wa.gov/RCW/default.aspx?cite = 9A.52.

[16] Straub, D. W., Welke R. J. Coping with systems risk : security planning models for management decision making. MIS Quarterly, Vol. 22, No. 4, 1998, pp. 441-65.

[17] Straub, D. W., Effective IS security : an empirical study. Information System Research, Vol. 1, No. 3, 1990, pp. 255-76.

[18] Theoharidou, M. The Insider Threat to Information Systems and the Effectiveness of ISO1779. Computers and Security, Vol. 24, 2005, pp. 472-484.

[19] Wikipedia, Code of Hammurabi. Retrieved June 19, 2007, from website, 2006, http://en.wikipedia.org/wiki/Code_of_hammurabi.

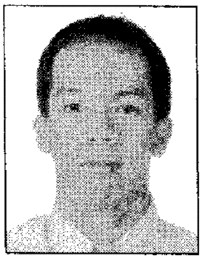
[20] Winfree, L. T. and Abadinsky, H., Understanding crime : Theory and practice. Belmont : Thomson Wadsworth, 2003.

[21] Young, N., Fairlamb, R., Business Continuity Planning Guidelines, Texas Department of Information Resources, Austin, Texas, 2004.

Author Profile

Myeonggil Choi

Myeonggil Choi is a professor of MIS at Chung-Ang University, Korea. He received the M.S. degree from Pusan National University and Ph.D. from Korea Advanced Institute of Science and Technology (KAIST). He worked for Electronics and Telecommunications Research Institute (ETRI) and Agency for Defense Department (ADD) as a senior researcher. He also served a professor in Inje University. His recent research issues include Information System Security Evaluation, Information Security Management and Innovation and Entrepreneurship.



Edwin R. Ramos

Edwin Ramos received his B.S. degree in Electronics and Communications Engineering from Saint Louis University, Philippines in 2006. He just finished his M.S. degree in Systems Management Engineering from INJE University, Gimhae, South Korea last August 2009. His research interests are Network and Industrial Security, E-Manufacturing, Concurrent Engineering and Information Security Management.

Mansig Kim

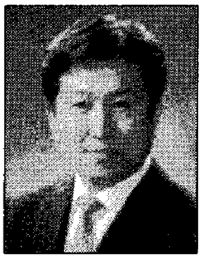
Mansig Kim is a professor of Systems Management Engineering at Inje University in Korea. He received B.S. in Computer Science from the University of Denver, U.S.A., M.S. in Computer Science and Manufacturing Engineering from Worcester Polytechnic Institute, U.S.A., and Ph.D. in Manufacturing Engineering from Worcester Polytechnic Institute. His research interests include Artificial Intelligence in Design, Information Systems Integration, Tool Design in Powder Metallurgy, and Factory Automation. He is a recipient of the Vice Prime Minister Award of the Small and Medium Enterprise Tech-Innovation Expo.

Jinsoo Kim

Jinsoo Kim is professor of MIS at Chung-Ang University, Korea. He holds a BA from Yonsei University, an MBA from University of Texas (Arlington), and a Ph.D. in MIS from Louisiana State University. He is also working as the Chairman of Korea Database Society and the director of graduate school of entrepreneurship at Chung-Ang University. His research interests focus on database modeling, u-biz strategy, and entrepreneurship. Current research interests include privacy issues on RFID applications, green factory, and global IT strategies.

Jaehoon Whang

He got B.A. in Business Administration at Yonsei University, Korea, and Ph.D. in MIS at University of Nebraska-Lincoln. He has a variety of experiences on IS strategic planning and ERP implementation including BRP and ERP consulting at Samsung, and is currently a professor in the College of Government and Business, Yonsei University. His research interests are ERP and extended solutions, and strategic management of IT.



Kijoo Kim

Kijoo Kim is an associate professor at the Department of MIS in Konyang University. He studied his PH.D. course at the University of Nebraska-Lincoln and received the MBA degree from Bowling Green State University at Ohio and the Bachelor's degree from Hankuk University of Foreign Studies. His research interests include ERP system, Business Process Management, SCM, Information Systems Strategy, and IT service Management.

◆ 이 논문은 2009년 09월 02일 접수하여 1차 수정을 거쳐 2009년 09월 16일 게재확정되었습니다.