International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:5, No:6, 2011

Determinants of Information Security Affecting Adoption of Web-based Integrated Information Systems

Jaehun Joo, Mie-jung Kim, Ismatilla Normatov, and Lyunhwa Kim

***Abstract*—**The purpose of this paper is to analyze determinants of information security affecting adoption of the Web-based integrated information systems (IIS). We introduced Web-based information systems which are designed to formulate strategic plans for Peruvian government. Theoretical model is proposed to test impact of organizational factors (deterrent efforts and severity; preventive efforts) and individual factors (information security threat; security awareness) on intentions to proactively use the Web-based IIS .Our empirical study results highlight that deterrent efforts and deterrent severity have no significant influence on the proactive use intentions of IIS, whereas, preventive efforts play an important role in proactive use intentions of IIS. Thus, we suggest that organizations need to do preventive efforts by introducing various information security solutions, and try to improve information security awareness while reducing the perceived information security threats.

***Keywords*—**Information security, *Deterrent efforts, deterrent* severity, preventive efforts, information security awareness, information security threats, integrated information systems

I. Introduction

NOWADAYS, many information systems are integrated through World Wide Web. The Web-based integrated information systems (IIS) allow organizations to share information and collaborate with partners. However, the Web-based IIS can be vulnerable to information security threats such as hacking, cracking, and computer viruses. Thus, it is necessary to identify what kinds of factors have influence on use intentions of the Web-based IIS.

The purpose of this study is to analyze determinants of information security affecting adoption of the Web-based IIS. We introduce a case of Web-based information systems which are designed to formulate strategic plans for Peruvian government. A research model and hypotheses will be tested by using data collected from users working in national and regional government in Peru. This study can contribute to offering guidelines and formulating policies related to information security.

II. Literature Review and a Case of Web-based Integrated Information Systems

A. Literature Review

Previous literature review mainly focuses on several factors influence information security effectiveness.

J. Joo is with Department of Information Management, Dongguk University, Gyeongju, South Korea (phone: 82-54-770-2346; e-mail: givej@ dongguk.ac.kr).

M. Kim is with Department of International Commerce, Dongguk University, Gyeongju, South Korea (e-mail: meajung@ dongguk.edu).

I. Normatov and L. Kim are with Master course of Dongguk University.

In particular, deterrent efforts and severity, preventive efforts, information security awareness (ISA) and information security threats.

Deterrent Efforts. In general context, deterrent measures are efforts to discourage people from criminal or anti-social behavior through fear of sanctions or by the administration of strong sanctions related to these acts [1], [8], [20]. Certainty and harshness of punishments for such illegal or unethical acts of behavior increase the effectiveness of sanctions [32]. Hence, many scholars distinguish sanctions as deterrent measures into certainty and severity of sanctions [1].

Deterrence theory is extensively advocated by IS scholars [18], [11], [25], [29], [33], [37]. In the Information System (IS) security context, deterrent efforts correspond to certainty of sanctions affecting the probability that IS abusers will be caught [11]. Extended meanings of deterrent efforts imply attempts to discourage deliberate attacks against a system through dissemination of information and threat of sanction in the form of penalties for violations of security policies and security awareness training [26]. The following examples from previous studies were found to be effective:

- *Administrative policies, employee training, and visible security functions* [18],
- *Policy statements and guidelines on legitimate use of IS assets, security briefings on the consequences of illegitimate use of IS assets, total man-hours expended on IS security purposes per week* [29],
- *Multiple methods to disseminate information about penalties and acceptable systems usage, statements of penalties for violations* [33].

[29] while studying 1,211 organizations found out that fewer IS abuses were achieved through deterrent efforts. [30] research study highlights the importance of communicating certainty and severity of sanctions as a part of employee education and training programs in order to minimize security violations. Following this research, [11] and [33] studied whether the use of sanctions led to enhanced IS security effectiveness and found that deterrents, as measured in man-hours spent in security efforts, led to better IS security effectiveness and reduce levels of abuse. [25] applied both formal and informal sanctions in order to explain employees' IS security policy compliance and found that deterrent efforts predicted employees' compliance with IS security policies.

Deterrent Severity. Scholars agree upon the fact that deterrent efforts are particularly effective if the punishment for IS abuses is also severe [29]. Deterrent severity corresponds to severity of sanctions which can dissuade people from IS security abuses because they will be severely punished when they are caught, such as reprimand by management,

suspension of duties, dismissal from appointment, and prosecution in court [11].

Enforcing more severe penalty for IS abusers, who are caught in their act, does not seem to dissuade IS abuses. Indeed, [23] found that deterrent severity does help to discourage crimes involving human victims but not crimes involving property or other non-human artifacts (which supposed to include IS abuses). Hence, in the context of IS security, [11] suggests that organizations should focus their attention on deterrent and preventive efforts rather than deterrent severity. Moreover, greater deterrent efforts and preventive measures were found to lead to enhanced IS security effectiveness.

Preventive Measures; When potential abusers choose to ignore deterrent measures, one of the main option is the hardening of systems against these threats, via countermeasures known as preventive measures, constitute the next line of defense [30], [33]. In general, preventive measures are attempts and safeguards to ward off criminal behavior through controls [8] as well as enforce policy statements and guidelines [9]. In other words, these safeguards impede security violations by actively enforcing aspects of the organization's security policy [26].

The main objective of preventive measures is to wear abusers down through implementing security software to impede unauthorized access to and use of IS assets [29]. Preventive efforts include the following:

- *Measures needed to detect, document, and counter potential threats* [37].
- *Deploying advanced security software or controls to protect IS assets, such as advanced access control, intrusion detection, firewall, surveillance mechanisms, and the generation of exception reports* [11].

With the increased use of electronic connections and web integrated systems, preventive efforts in the form of security software are likely to be vital. Based on previous research studies, it can be said that security software can provide basic (embedded in operating systems), intermediate (embedded in database management systems), and advanced (specialized security software of access control to IS) levels of security [18], [11], [34]. Deploying advanced security software is regarded as crucial because it offers both better access protection and intrusion detection through more sophisticated firewalls, and unauthorized IS activities detection [11].

Although empirical studies found preventive efforts create more obstacles for people to engage in IS abuse [11], other findings show that it can impede business functions [33] and even decrease a firm's profits [9]. Hence, [22] suggests that there are strategic uses of prevention efforts that can minimize the impact on a firm's operations while affording the firm a desired level of protection.

Awareness; With the development of various networks, the Internet and web enabled services, the rapid rise of threats from viruses, worms and the like has illustrated the need for increased awareness by users. It is an obvious need for increased awareness of the threats to information security not only among security and systems administrators, but also among the users of information in organizations [33].

Employee awareness is recognized as one of the greatest challenges in implementing security in general [13]. Information security awareness (ISA) is defined as an employee's general knowledge about information security and his cognizance of the information security policy of his organization [2]. This definition is consistent with the view security awareness is a state in which employees are aware of and are ideally committed to the security objectives of their organizations [24].

[24] Conceptually analyzed information security awareness and suggested methods to enhance awareness based on several theoretical perspectives. [5] suggested that organizations can use three security countermeasures—user awareness of security policies; security education, training, and awareness (SETA) programs; and computer monitoring—to reduce user's IS abuse. They showed that users' awareness of countermeasures impacts perceptions on organizational sanctions, which in turn reduces users' IS misuse intention [2].

Information security awareness is one vital aspect that forms part of information security management and awareness is about making sure that all employees in an organization are aware of their role and responsibility towards securing the information they work with [14].

[15] Highlighted that awareness of information security is one of the key factors of successful self-implementation of information security systems. Latest empirical study of [2] highlighted that information security awareness can directly and indirectly alter employees' belief sets about compliance with the ISP. Information systems (IS) can be useful only if people use them [17]. Similarly, information security awareness is of crucial importance, as information security techniques or procedures can be misused, misinterpreted or not used by end-users, thereby losing their real usefulness [24], [29], [30].

Hence, creation of security-aware culture within the organization will improve information security effectiveness [2], [9], [11], [24], [29], [30].

Threat; Threat is broad range of forces capable of creating adverse consequences [16] and an external incentive that exists whether or not it is perceived by an individual [35]. If an individual perceives the threat, that individual can be described as having awareness of a threat. A properly constructed fear serves to convey the severity of the threat and its target population's susceptibility to the threat [21], [35].

Nowadays, threats are dynamic, constantly changing overtime to adjust to the various deterrent and preventive efforts [22], [37]. For example, empirical study of 109 Taiwanese companies revealed that threats trough the network were rated as contributing the most severe threat and yet had the lowest level of protection [37]. IS threats such as access of systems by competitors, inadequate control over media [16], [33], interruption, interception, modification, and fabrication force organizations to more enhanced IS security modeling, developing security strategies and policies [37].

Previous studies differentiate mainly two kinds of threats [10], [21], [35], [36]:

- Perceived threat severity is establishing a belief to the seriousness of the threat and probability of personally experiencing the threat, as well as an ability to enact anti-spyware protection.
- Perceived threat susceptibility is an end user's perceptions of the probability of encountering the threat.

TABLE I
LITERATURE OVERVIEW

Focus	Definition	Previous Studies
DETERRENT EFFORTS	Attempts to discourage deliberate attacks against a system through dissemination of information and threat of sanction in the form of penalties for violations of security policies and security awareness training. These efforts directed towards reducing IS abuses and affecting the probability that IS abusers will be caught.	[11] [15] [26] [28] [29] [33] [37]
DETERRENT SEVERITY	Corresponds to severity of sanctions which can dissuade people from IS security abuses because they will be severely punished when they are caught, such as reprimand by management, suspension of duties, dismissal from appointment, and prosecution in court.	[2] [11] [29] [33]
PREVENTIVE EFFORTS	Efforts warding off illegitimate activities via more advanced security software and sophisticated access control to impede unauthorized access and make it difficult for people to engage in IS abuses.	[9] [11] [18] [22] [29]
SECURITY AWARENESS	Information security policy awareness, knowledge and understanding of their responsibilities, negative consequences of noncompliance with ISP and potential costs.	[2] [3] [14] [15] [24]
SECURITY THREAT	An external stimulus that exists whether or not it is perceived by an individual, beliefs and fear towards the significance of the threat.	[10] [36] [37]

B. A Case of Web-based IIS

In Peru, CEPLAN (National Center Strategic Planning) which is a agency attached to the Presidency of Council of Ministers is responsible for formulating and executing strategic plans for harmonious and sustainable development of the country, and strengthening democratic governance [4]. It is necessary for CEPLAN to gather and share information from SINAPLAN (National Systems of Strategic Planning) entities which are public sectors including national government, regional government, and local government. Thus, CEPLAN is developing a Web-based information system integrating many information systems of SINAPLAN entities to achieve the objective of CEPLAN.Fig. 1 shows a conceptual architecture of the Web-based IIS. The IIS consists of four core components such as MIPE, SIME, SINPLE, and BANPPLE as described in Table II. Three departments of CEPLAN including DNSE (National Office of Monitoring and Evaluation), DNPE (National Office of Forecasting and Strategic Studies), and DNCP (National Office of Coordinating and strategic Planning) play important roles in developing and managing the Web-based IIS.

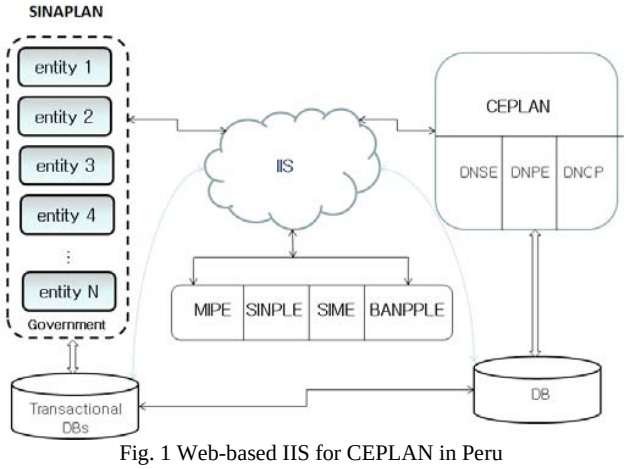

Fig. 1 Web-based IIS for CEPLAN in Peru

TABLE II
FOUR MODULES AND OVERVIEW

Modules	Overview
MIPE (Module Information for Strategic Planning)	Collecting data from SINAPLAN entities and distributing guidelines and policies about strategic plans
SINPLE (National System of Plans)	Supporting enrollment of strategic plans being formulated by SINAPLAN entities
SIME (Module Information for Strategic Planning)	Supporting processes of monitoring and evaluating strategic plans
BANPPE (Bank of Programs and Strategic Projects)	Repositories of a variety of programs, strategic projects, strategic development plans, etc.

III.RESEARCH DESIGN AND ANALYSIS

A. Research Model and Hypotheses

What kinds of information security factors have influence on intentions to proactively use the Web-based IIS? [11] suggested deterrent efforts, deterrent severity, and preventive efforts as determinants of information systems security. According to their empirical study, deterrent efforts and preventive efforts are positively related to information systems security effectiveness. Deterrent efforts are defined as certainty of sanctions such as efforts directly affecting the probability that information security abusers will be caught [11]. Deterrent severity means severity of sanctions dissuading people from IS security abuses because they will be severely punished when they are caught. Preventive efforts are attempts to ward off criminal behavior through controls [8]. More advanced security software tends to provide more sophisticated access control, thereby making it more difficult for people to engage in IS abuses [11].In this study, we identify deterrent efforts, deterrent severity, and preventive efforts as organizational factor, and security awareness and security threats as individual as shown in Fig. 2 and Table III.

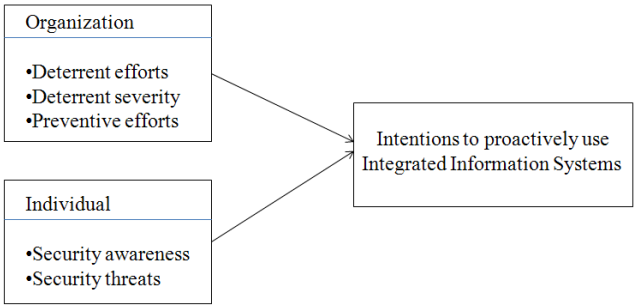

Fig. 2 A research model

TABLE III
BRIEFLY DESCRIBES OPERATIONALIZATION OF CONSTRUCTS AND MEASUREMENT

Constructs	Definition	Measurement	Sources
Deterrent efforts	Efforts directed toward reducing information security abuses	Total hours per week spending for information security activities	[11] [29]
Deterrent severity	Severity of sanctions to dissuade people from information security abuses	Severity of penalties for noncompliance of information security rules or regulations	[11]
Preventive effort	Efforts warding off illegitimate activities through security solutions	Number of software or solution for information security	[11] [29]
Information security awareness	Information security policy awareness, knowledge and understanding of their responsibilities, negative consequences of noncompliance with information security policy and potential cost	Six items including awareness on general information security and information security policy	[2]
Information security threats	Perceived threat severity and susceptibility	Three items including threats to computer viruses and their negative consequences, and their fear	[37]

Five hypotheses are derived from the research model shown in Fig. 2.

Hypothesis 1: The more personnel working in information security areas, the greater intentions to proactively use the Web-based IIS.

Hypothesis 2: The higher deterrent severity, the greater intentions to proactively use the Web-based IIS.

Hypothesis 3: The more security software an organization introduces as preventive efforts, the greater intentions to proactively use the Web-based IIS.

Hypothesis 4: The higher information security awareness, the greater intentions to proactively use the Web-based IIS.

Hypothesis 5: The perceived information security threats have negatively influence on intentions to proactively use the Web-based IIS.

B. Analysis and Hypothesis test

145 samples of data were collected from SINAPLAN entities. Table 4 shows current status of information security in respondents' organization. As shown in table 4, only one percent of organizations introduced authentication systems based on the public key infrastructure.

TABLE IV
USER ORGANIZATIONS: STATUS OF INFORMATION SECURITY IN SINAPLAN ENTITIES

Dimension of Information security	Type	No. of personnel (ratio, %)
No. of personnel working in information security	0-5	111(76.6%)
	6-10	26(17.9%)
	11-20	6(4.1%)
	21-50	2(1.4%)
Work-hour for information security per week (excluding physical security)	Less than 5 hours	59 (40.7%)
	6-15 hours	38 (26.2%)
	16-25 hours	6 (4.1%)
	26-35 hours	0 (0.0%)
	26-45 hours	12 (8.3%)
	More than 46hours	30 (20.7%)
Deterrent severity	No actions are taken	12(8.3%)
	Reprimand by management	29(20.0%)
	Suspension of duties	82(56.6%)
	Dismissal from appointment	8(5.5%)
	Prosecution in court	10(6.9%)
	Others	4(2.8%)
Preventive efforts	Advanced security software embedded in operating systems	54(37.2%)
	Advanced security software embedded in database management systems	54(37.2%)
	Vaccine antivirus	130(89.7%)
	Firewalls	121(83.4%)
	Intrusion detection systems	89(61.4%)
	Vulnerability check	48(33.1%)
	Data loss prevention and backup systems	91(62.8%)
	Encryption and Digital signature systems	32(22.1%)
	Authentication based on the public key infrastructure	2(1.4%)

Each questionnaire item of Table V was asked by using a five-point Likert's scale, in which 1 indicates strongly disagree, 3 does neutral, and 5 means strongly agree. The level of information security awareness is not high. However, most organizations are willing to use proactively the Web-based IIS.

TABLE V
INFORMATION SECURITY AWARENESS, THREATS, AND USE INTENTIONS OF IIS

Dimension	Items of questionnaire	Mean (standard deviation)
Information security awareness	I have sufficient knowledge and understanding regarding Information Security (IS)	3.07 (0.5099)
	I have sufficient knowledge about the cost of potential information security problems and threats	
	I fully understand the concerns related to IS and potential risks they pose to organization	
	I know and understand the regulations prescribed by IS policy of my organization	
	I know my liabilities as prescribed in the IS policy to improve IS of my organizations	
	I have full knowledge of my responsibilities and costs of noncompliance with IS policy in my organizations	
Information security threats	It is likely that my computer will become infected with various viruses (malwares, spyware, adware, worms, Trojan horses)	3.46 (0.901)
	If my computer will become infected by viruses, the resulting negative consequences are hazardous and bring severe causes to my organization	
	I am afraid of various threats to information security under open network environment like Internet	
Proactive use intentions of IIS	I intent to use Web-based integrated information systems (IIS)	4.18 (0.647)
	I predicted that I will use Web-based integrated information systems (SII)	
	I plan to use Web-based integrated information systems (IIS)	

* 1: Strongly disagree 3: Neutral 5: Strongly agree

Table VI shows the result of multiple regression analysis between organizational characteristics and use intentions. Hypotheses 1 and 2 were not supported. Hypothesis 3 was supported at the significance level of 1%.

TABLE VI
REGRESSION ANALYSIS BETWEEN ORGANIZATIONAL CHARACTISTICS AND USE INTENTIONS
Dependent variable: proactive use intentions

Independent variables	Standardized coefficient	t-value (significance level)	Hypothesis result
deterrent efforts	0.044	0.519(0.605)	Rejected
deterrent severity	0.113	1.371(0.172)	Rejected
preventive efforts	0.245	2.920(0.004)	Accepted

Table VI shows the result of multiple regression analysis between personal characteristics and use intentions. Hypothesis 4 was supported at the significance level of 5% and hypothesis 5 also accepted at the significance level of 1%.

TABLE VI
REGRESSION ANALYSIS BETWEEN PERSONAL CHARACTERISTICS AND USE INTENTIONS
Dependent variable: proactive intentions

Independent variables	Standardized coefficient	t-value (significance level)	Hypothesis result
Information security awareness	0.164	2.047(0.042)	Accepted
Information security threats	-0.240	-2.996(0.003)	Accepted

IV. Conclusion

In summary, we identified determinants of proactive use intentions of the web-based IIS. Deterrent efforts and deterrent severity have no significant influence on the proactive use intentions of IIS. Preventive efforts play an important role in proactive use intentions of IIS. In other words, the more organizations introduced a variety of information security solutions as preventive efforts, the more proactively users are willing to use the web-based IIS. The level of information security awareness is positively related to the proactive use intentions of the Web-based IIS, whereas the level of information security threats is negatively related to it. Thus, organizations need to do preventive efforts by introducing various information security solutions, and try to increase information security awareness while reducing the perceived information security threats.

References

[1] A. Blumstein, "*Introduction in deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*," National Academy of Sciences, Washington, DC, USA, 1978.

[2] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, vol. 34, no. 3, pp. 523-548, 2010.

[3] H. Cavusoglu, J. Son, and I. Benbasat, "*Information security control resources in organizations: A multidimensional view and their key*

drivers," Working Paper, Sauder School of Business, University of British Columbia, 2009.
[4] CEPLAN, "KSP mission to CEPLAN Peru," CEPLAN, 2010.
[5] J. D'Arcy, A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research*, vol. 20, no. 1, pp. 79-98, 2009.
[6] M. Fishbein, and J.N. Cappella, "The role of theory in developing effective health communications," *Journal of Communication*, vol. 56, pp. 1-17, 2006.
[7] M. Fishbein, and M.C. Yzer, "Using theory to design effective health behavior interventions," *Communication Theory*, vol. 13, no. 2, pp. 164-183, 2003.
[8] K.A. Forcht, "*Computer security management*," Boyd and Fraser, Danvers, MA, USA, 1994.
[9] R.D. Gopal, and G.L. Sanders, "Preventive and Deterrent Controls for Software Piracy," *Journal of Management Information Systems*, vol. 13, no. 4, pp. 29-47, 1997.
[10] A.C. Johnston, and N. Warkentin , "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly*, vol. 34, no. 3, pp. 549-566, 2010.
[11] A. Kankanhalli, H.H. Teo, B.C.Y. Tan, and K.K. Wei, "An integrative study of information systems security effectiveness," *International Journal of Information Management*, vol. 23, pp. 139-154, 2003.
[12] Klete, "*Some minimum requirements for legal sanctioning systems with special emphasis on detection, in Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*," National Academy of Sciences, Washington, DC, USA , 1978.
[13] K.J. Knapp, R.F. Morris, T.E. Marshall, and T.A. Byrd, "Information security policy: An organizational-level process model," *Computers and Security*, vol. 28, no. 7, pp. 493-508, 2009.
[14] E. Kritzinger, and E. Smith, "Information security management: An information security retrieval and awareness model for industry," *Computers and Security*, vol. 27, pp. 224-231, 2008.
[15] C.Y. Ku, Y.W. Chang, and D.C. Yen, "National information security policy and its implementation: A case study in Taiwan," *Telecommunications Policy*, vol. 33, pp. 371-384, 2009.
[16] K.D. Loch, H.H. Carr, and M.E. Warkentin, " Threats to information systems: Today's reality, yesterday's understanding," *MIS Quarterly*, vol. 16, no. 2, pp. 173–186, 1992.
[17] K. Mathieson, "Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior," *Information System Research*, vol. 3, no. 2, pp. 173-191, 1991.
[18] W.D. Nance, and D.W. Straub, "*An Investigation into the Use and Usefulness of Security Software in Detecting Computer Abuse,"* in *Proc.9th Annu. Conf. on Information Systems*, Minneapolis, MN, 1988.
[19] D.D. Parker, "*Fighting computer crime,"* Scribner's, New York, USA, 1983.
[20] F.S. Pearson, and N.A. Weiner, "Toward an Integration of Criminological Theories," *Journal of Crime and Criminology*, vol. 76, no. 1, pp. 116-150, 1985.
[21] R.W. Rogers, "A protection motivation theory of fear appeals and attitude change," *Journal of Psychology*, vol. 91, pp. 93-114, 1975.
[22] J.H. Schuessler, "*General deterrence theory: Assessing information systems security effectiveness in large versus small businesses*" [online], University of North Texas, Available from: < http://joseph.schuessler sounds.com/Research/Dissertation/Schuessler_Dissertation.pdf >, [Last Accessed March 29, 2011], 2009.
[23] M. Silberman, "Toward a Theory of Criminal Deterrence*,"* *American Sociological Review*, vol. 41, pp. 442-461, 1976
[24] T. Siponen, "A conceptual foundation for organizational information security awareness", *Information Management and Computer Security*, vol. 8, no. 1, pp. 31-41, 2000.
[25] M. Siponen, and A.O. Vance, "Neutralization: New insights into the problem of employee systems security policy violations," *MIS Quarterly*, vol. 34, no. 3, pp.487-502, 2010.
[26] G.D. Spicer, "*Information systems management maturity and information technology security effectiveness*," University of Lethbridge, Alberta, Canada, 2004.
[27] D.W. Straub, "Computer abuse and computer security: Update on an empirical study," S*ecurity, Audit, and Control Review*, vol. 4, no. 2, pp. 21-31, 1986.
[28] D.W. Straub, and W.D. Nance, "Discovering and disciplining computer abuse in organizations: A field study," *Management Information Systems Quarterly*, vol. 14, no. 1, pp. 45- 62, 1990.
[29] D.W. Straub, "Effective IS Security: An Empirical Study," *Information Systems Research*, vol. 1, no. 3, pp. 255-276, 1990.
[30] D. W. Straub, and R.J. Welke, "Coping with systems risk: Security planning models for management decision making," *MIS Quarterly*, vol. 22, no. 4, pp. 441-469, 1998.
[31] D.W. Straub, "Coping with systems risk: Security planning models for management decision making," *MIS Quarterly*, vol. 22, no. 4, pp. 441-469, 1998.
[32] K.R. Williams, and R. Hawkins, "Perceptual Research on General Deterrence: A Critical Review," *Law and Society*, vol. 20, no. 4, pp. 545-572, 1986.
[33] M. E. Whitman, "In defense of the realm: Understanding the threats to information security," *International Journal of Information Management*, vol. 24, no. 1, pp. 43-57, 2004.
[34] R. Weber, "*EDP Auditing: Conceptual Foundations and Practice*," McGraw Hill, New York, NY, 1988.
[35] K. Witte, "Putting the fear back into fear appeals: The extended parallel process model," *Communication Monograph*, vol. 59, pp. 329-349, 1992.
[36] K. Witte, K.A. Cameron, J.M. McKeon, and J.M. Berkowitz, "Predicting risk behaviors: Development and validation of a diagnostic scale," *Journal of Health Communication*, vol. 1, pp. 317-341, 1996.
[37] Q.Y. Yeh, and A.J.T. Chang, "Threats and countermeasures for information system security: A cross-industry study", *Information and Management*, vol. 44, no. 5, pp. 480-491, 2007.