International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 10 | Oct 2019 www.irjet.net p-ISSN: 2395-0072

Deterrence Theory for Evaluating Information Security Factors in E-Health Systems

Lazarus Kwao [1], Richard Millham [2], Wisdom Xornam Ativi[3]

[1]Ghana Baptist University College, Kumasi,
[2]Durban University of Technology, South Africa,
[3]University of Electronic Science and Technology of China

Abstract - *This paper analyzed the determinants of information security affecting adoption of E-Health. We introduced E-Health Systems which are designed to formulate strategic plans for Health Service. 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 E-Health Systems. Our empirical study results highlight that deterrent efforts and deterrent severity have no significant influence on the proactive use intentions of E-Health Systems, whereas, preventive efforts play an important role in proactive use intentions of E-Health Systems. 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.*

Key Words: Deterrence Theory, E-Health Information Security, Developing Countries, Ghana Health Service

1. Introduction

The implementation and use of Information and Communication Technologies (ICT) for health (E-Health) in the last 20 years, has transformed the way healthcare services are delivered (Andreassen, Kjekshus, & Tjora, 2015). Influenced by this transformation; health errors and cost of delivering care have been reduced, while physician's efficiency has been improved with fewer duplicative treatments and tests. These identified benefits and many others have influenced several governments not only in developed countries but also in many developing countries to reserve huge amount of money for stimulating its adoption (Omary, Lupiana, Mtenzi, & Wu, 2009). However, the attractive advantages of E-Health Systems entail many scientific challenges (Shortliffe, 2005; Williams, 2016). One of the foremost of these are the security issues raised by adopting electronic storage and communication, and the sensitive nature of health data. In addition, citizens' willingness to accept, use and adopt E-Health services raises important political, cultural, organisational, technological and social issues which must be considered and treated carefully by any government contemplating its adoption. (Delone & McLean, 2003).

1.1 Problem Statement

One major barrier to successfully implementation of E-Health Systems reported by many (Dünnebeil, Sunyaev, Blohm, Leimeister, & Krcmar, 2012; Mair, et al., 2012) is whether users accept the new system and the potential security challenges and changes that follow (Ahmadian, Khajouei, Nejad, Ebrahimzadeh, & Nikkar, 2014). This tendency is much more serious in developing countries where computer anxiety is very high (Li, Talaei-Khoei, Seale, Ray, & MacIntyre, 2013). A significant barrier in e-Health adoption can be found in the growing problems of user behavior, (end-user perspective) as picked up by both the research community and Information Systems (IS) security practitioners in recent times (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Mair, et al., 2012; Dünnebeil, Sunyaev, Blohm, Leimeister, & Krcmar, 2012; Cresswell & Sheikh, 2013).

From previous literatures, it could be said that, in implementing E-Health Systems, Stanton et al, (2003), Humaidi and Balakrishnan, (2012), Thingbø., & Flores., (2015) also admits, concentrating on technical and procedural aspects of information security alone is inadequate as E-Health system users may not follow technical and procedural measures. Johnston, A. C., & Warkentin, M (2010) also suggests, security efforts that fail to consider how humans react to and use technology often do not deliver intended benefits. Boujettif (2010), Kreicberge (2010) and Brady (2011) also adds, although technical efforts are important, major internal and external threats are due to the poor security behavior of the users who are also internal employees. Many information security incidents and successful intrusions could be prevented if people acted differently. Thus, to manage behavioral information security in E-Health adoption, it is important to understand what drives existing security behaviors of employees and how these behaviors can be improved to influence the adoption and use of E-Health Systems.

1.2 Objective of the Study

The purpose of this study is to explore the determinants of behavioural information security that affects the adoption and use of E-Health Systems.

2. General Deterrence Theory

The term "general deterrence" refers to the practice of instilling fear in people in the hopes that such fear will prevent them from committing crimes in the future (Beccaria C. , 1764; Devine, 1981; Beccaria C. , 2016). An organization using a deterrence security model imposes sanctions, penalties, disincentives, or any combination of them. D'Arcy & Hovav, (2005) asserts that GDT's disincentives and sanctions against IS breaches or deviant behavior, effectively hinder individuals from such involvements. GDT has been applied in preventing deviant acts in various areas, such as drug abuse (Anderson et al., 1977; Meier and Johnson, 1977), drug sales (Miller and Anderson, 1986), employee theft (Hollinger and Clark, 1983; Miller and Anderson, 1986), school delinquency (Jensen et al., 1978), school misbehavior (Pestello, 1989), tax evasion (Miller and Anderson, 1986; Wenzel, 2004), underage drinking (Paternoster and Iovanni, 1986), and vandalism (Paternoster and Iovanni, 1986).

The model in figure 1 includes three organizational disincentives that criminology research has shown to be important in determining potential immoral activities (Gray & Martin, 1969):

1) Certainty of sanction or the perceived likelihood of the perpetrator being caught in a deviant act (Burns, Nanayakkara, Courtney, & Roberts, 2012),

2) Severity of sanction or the gravity of the ramifications a violator faces for such involvement if caught (D'Arcy & Hovav, 2005), and

3) Celerity of sanction or swiftness in punishing the perpetrator once caught (Antia, Bergen, Dutta, & Fisher, 2006).

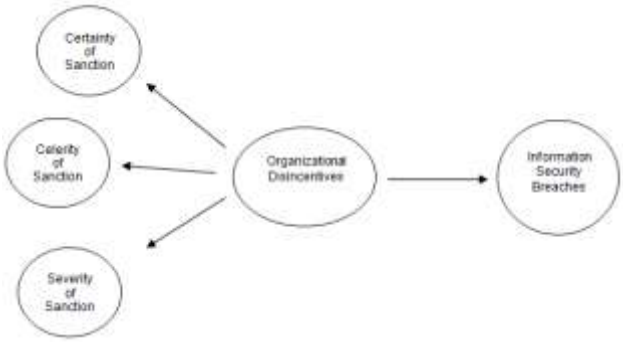

Figure 1: General Deterrence Theory Model

2.1 Related Literature

Deterrence theory is extensively advocated by IS scholars (Gray & Martin, 1969; Jervis, 1979; Achen & Snidal, 1989). In the Information System (IS) security context, deterrent efforts correspond to certainty of sanctions affecting the probability that IS abusers will be caught (Siponen, Pahnila, & Mahmood, 2010). 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 (Vance & Siponen, 2012). The following examples from previous studies were found to be effective:

Administrative policies, employee training, and visible security functions (Padayachee, 2012),

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 (Knapp & Ferrante, 2012),

Multiple methods to disseminate information about penalties and acceptable systems usage, statements of penalties for violations (Siponen, Pahnila, & Mahmood, 2010).

Straub, (1990) while studying (Blumstein, 1978; Bulgurcu, Cavusoglu, & I., 2010; Kankanhalli, Teo, Tan, & Wei, 2003) organizations found out that fewer IS abuses were achieved through deterrent efforts. (Straub & Welke, 1998) 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, (Kankanhalli, Teo, Tan, & Wei, 2003) and (Whitman, 2004) 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. Spicer, (2004) 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.

Enforcing more severe penalty for IS abusers, who are caught in their act, does not seem to dissuade IS abuses. Indeed, Silberman, (1976) 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, (Kankanhalli, Teo, Tan, & Wei, 2003) 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.

2.2 Research Constructs

Certainty of sanction. In general context, certainty of sanction 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 (Siponen, Pahnila, & Mahmood, 2010; Gottfredson, 2011). Certainty and harshness of punishments for such illegal or unethical acts of behavior increase the effectiveness of sanctions (Joo, Kim, Normatov, & Kim, 2011). Hence, many scholars distinguish sanctions as deterrent measures into

certainty and severity of sanctions even in E-Health systems (Park, Kim, & Park, 2017).

Severity of sanction. Scholars agree upon the fact that deterrent efforts are particularly effective if the punishment for IS abuses is also severe. Severity of sanction corresponds to ramifications violators face 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 (Kankanhalli, Teo, Tan, & Wei, 2003).

Celerity of sanction*;* When potential abusers choose to ignore the severity of sanction, one of the main options is the hardening of systems against these threats, via countermeasures known as preventive measures, constitute the next line of defense (Straub & Welke, 1998), (Whitman, 2004). In general, celerity of sanction are attempts and safeguards to ward off criminal behavior through controls Forcht, (1994) as well as enforce policy statements and guidelines (Gopal & Sanders, 1997). In other words, these safeguards impede security violations by actively enforcing aspects of the organization's security policy (Spicer, 2004).

The main objective of celerity of sanction is to wear abusers down through implementing security software to impede unauthorized access to and use of IS assets (Straub D. , 1990). celerity of sanction includes the following:

- *Measures needed to detect, document, and counter potential threats.*
- *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.*

With the increased use of electronic connections and integrated health systems, celerity of sanction 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 (Nance & Straub, 1988; Kankanhalli, Teo, Tan, & Wei, 2003). 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 (Kankanhalli, Teo, Tan, & Wei, 2003).

Although empirical studies found celerity of sanctions create more obstacles for people to engage in IS abuse (Kankanhalli, Teo, Tan, & Wei, 2003), other findings show that it can impede business functions (Whitman, 2004) and even decrease a firm's profits (Gopal & Sanders, 1997). Hence, (Schuessler, 2009) suggests that there are strategic uses of celerity of sanctions that can minimize the impact on a firm's operations while affording the firm a desired level of protection.

Security Awareness*;* With the development of various E-Health services, 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 (Whitman, 2004).

Employee awareness is recognized as one of the greatest challenges in implementing security in general (Knapp, Morris, Marshall, & Byrd, 2009). 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 (Bulgurcu, Cavusoglu, & I., 2010). 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 (Siponen M. , 2000).

Siponen., (2000) Conceptually analyzed information security awareness and suggested methods to enhance awareness based on several theoretical perspectives. D'Arcy & Hovav, (2005) 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 (Bulgurcu, Cavusoglu, & I., 2010).

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 (Kritzinger & Smith, 2008).

(Johnson, 2006) Highlighted that awareness of information security is one of the key factors of successful self-implementation of information security systems. Latest empirical study of Maarop et., al, (2015) highlighted that information security awareness can directly and indirectly alter employees' belief sets about compliance. 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 (Siponen M. , 2000; Siponen, Pahnila, & Mahmood, 2010).

Hence, creation of security-aware culture within the organization will improve information security effectiveness (Bulgurcu, Cavusoglu, & I., 2010; Kankanhalli, Teo, Tan, & Wei, 2003; Siponen M. , 2000; Alnatheer, 2015).

Security Threat; Threat is broad range of forces capable of creating adverse consequences and an external incentive that exists whether or not it is perceived by an individual (Loch, Carr, & Warkentin, 1992). 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 (Johnston & Warkentin, 2010).

Nowadays, threats are dynamic, constantly changing overtime to adjust to the various deterrent and preventive efforts (Baskerville, Spagnoletti, & Kim, 2014). Information Systems threats such as access of systems by competitors, inadequate control over media (Loch, Carr, & Warkentin, 1992; Whitman, 2004), interruption, interception, modification, and fabrication force organizations to more enhanced IS security modeling, developing security strategies and policies (Jung, Han, & Lee, 2001; Joo, Kim, Normatov, & Kim, 2011).

Table 1: Operationalization of Constructs and Measurement

Constructs	Definition	Measurement
Certainty of sanctions	Efforts directed toward reducing information security abuses	Understanding and adherence to information security procedures.
Severity of sanctions	Severity of sanctions to dissuade people from information security abuses	Severity of penalties for noncompliance of information security rules or regulations.
Celerity of sanctions	Efforts warding off illegitimate activities through security solutions	Number of software or solution for information security.
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.
Security Threat	Perceived threat severity and susceptibility	Three items including threats to computer viruses and their negative consequences, and their fear.

3.0 Research Model

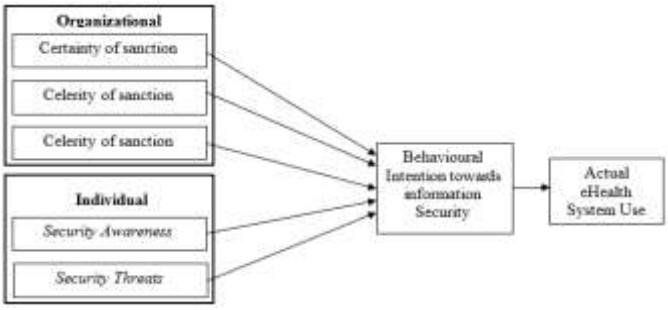

*Figure 2**: Revised GDT Model***

The purpose of this study is to explore the determinants of behavioural information security that affects the adoption and use of E-Health Systems. The term "***adoption***" in this study refers to the "initial decision made by the individual to interact with the technology" (Venkatesh, Morris, Davis, & Davis, 2003). This research adapted the General Deterrence Theory (GDT) to determine behavioural information security factors affecting the acceptance and use of e-health services in hospitals where e-health services are still being developed. The study seeks to achieve these main goals; develop a modified model by revising the General Deterrence Theory (GDT) model as shown in figure 1. The modifications are in two directions, the first direction is a regrouping of the main GDT variables (Certainty of sanction, Celerity of sanction, and Celerity of sanction) as ***organizational factor***, and adding new variables *Security Awareness* and *Security Threats* as ***individual factors*** as shown in Figure 2. This model will help health agencies improve decision making to understand the information security factors that influence health workers adoption of e-health hospitals.

3.1 Research Hypotheses

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

Hypothesis 1: The more personnel understands and adhere to information security procedures, the greater intentions to proactively use E-Health Systems.

Hypothesis 2: The greater the severity of sanctions, the greater the intentions to proactively use E-Health Systems.

Hypothesis 3: The more security software an organization introduces as preventive efforts (celerity of sanctions), the greater intentions to proactively use E-Health Systems.

Hypothesis 4: The higher information security awareness, the greater intentions to proactively use E-Health Systems.

Hypothesis 5: The perceived information security threats have negatively influence on intentions to proactively use E-Health Systems.

3.2 Study Population

The population for the collection of data for the research was 217 purposively from administration record specifically the medical officers, community health nurses, Health Insurance Officers and Records Officers of their respective units. Selected government hospitals in the Ashanti Regional Health Directorate were chosen as the case study.

3.3 Data Analysis and Results

Table 2: Analysis and Hypothesis test

	Type	No. of Responses (ratio, %)
Certainty of sanctions How does your organization measure /monitor whether its security controls are working?	• Internal risk analysis • Internal compliance audit • External risk analysis • External compliance audit • Hire outside firm to attempt to gain unauthorized access to systems • Use internal metrics to monitor operation and effectiveness of controls • Assign IT staff to attempt to gain unauthorized access to systems	59 (40.7%) 38 (26.2%) 6 (4.1%) 0 (0.0%) 12 (8.3%) 30 (20.7%) 0 (0.0%)
Severity of sanctions	• No actions are taken • Reprimand by management • Suspension of duties • Dismissal from appointment • Prosecution in court • Others	12(8.3%) 29(20.0%) 82(56.6%) 8(5.5%) 10(6.9%) 4(2.8%)
Celerity of sanctions (What type of authentication does your organization use to gain access and Efforts warding off illegitimate activities at one of your facilities?)	• Data loss prevention and backup systems • Username and password • Digital certificate • One-time password with two-factor authentication (token) • Device ID/risk-based authentication (authentication risk measure based on factors such as the device, IP geo-location and user behavior) • Biometrics • No authentication	54(37.2%) 32(22.1%) 48(33.1%) 54(37.2%) 91(62.8%) 121(83.4%)

Table 3: Information Security Awareness, Threats, and Use Intentions of E-Health

Using a five-point Likert's scale, in which 1 indicates strongly disagree, 3 does neutral, and 5 means strongly agree. * 1: Strongly disagree 3: Neutral 5: Strongly agree

Dimension	Items of questionnaire	Mean (standard deviation)
Information security awareness	I have sufficient knowledge and understanding regarding Information Security (IS) 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	3.07 (0.5099)
Information security threats	It is likely that my computer will become infected with various viruses (malwares, spyware, adware, worms, Trojan horses) 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	3.46 (0.901)
use intentions of E-Health Systems	I intend to use E-Health Systems I predicted that I will use E-Health Systems I plan to use E-Health Systems	4.18 (0.647)

Table 4 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 4: Regression Analysis between Organizational Characteristics and Use Intentions

Dependent variable: proactive use intentions

Independent variables	Standardized coefficient	t-value (significance level)	Hypothesis result
Certainty of sanctions	0.044	0.519 (0.605)	Rejected
Severity of sanctions	0.113	1.371 (0.172)	Rejected
Celerity of sanctions	0.245	2.920 (0.004)	Accepted

Table 5 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 5: 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

4. Conclusion

In summary, we identified determinants of proactive use intentions of E-Health. Deterrent efforts and deterrent severity have no significant influence on the proactive use intentions of E-Health Systems. Preventive efforts play an important role in proactive use intentions of E-Health Systems. 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 E-Health Systems. The level of information security awareness is positively related to the proactive use intentions of the E-Health Systems, 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. Survival of the project: a case study of ICT innovation in health care. **Andreassen, H. K., Kjekshus, L. E. and Tjora, A.** 2015, Social Science & Medicine, pp. 132, 62-69.

2. Challenges to E-healthcare adoption in developing countries: A case study of Tanzania. **Omary, Z., et al.** s.l. : IEEE, 2009. In 2009 First International Conference on Networked Digital Technologies. pp. 201-209.

3. Strategic action in health information technology: why the obvious has taken so long? **Shortliffe, E. H.** 2005, Health affairs, pp. 24(5), 1222-1233.

4. Why is it difficult to achieve e-health systems at scale? **Williams, R.** 2016, Information, Communication & Society, pp. 19(4), 540-550.

5. The DeLone and McLean model of information systems success: a ten-year update. **Delone, W. H. and McLean, E. R.** 2003, Journal of management information systems, pp. 19(4), 9-30.

6. Determinants of physicians' technology acceptance for e-health in ambulatory care. **Dünnebeil, S., et al.** 2012, International journal of medical informatics, pp. 81(11), 746-760.

7. Factors that promote or inhibit the implementation of e-health systems: an explanatory systematic review. **Mair, F. S., et al.** 2012, Bulletin of the World Health Organization, pp. 90, 357-364.

8. Prioritizing barriers to successful implementation of hospital information systems. **Ahmadian, L., et al.** 2014, Journal of medical systems, pp. 38(12), 151.

9. Health care provider adoption of eHealth: systematic literature review. **Li, J., et al.** 2013, Interactive journal of medical research, pp. 2(1), e7.

10. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. **Boss, S. R., et al.** 2009, European Journal of Information Systems, pp. 18(2), 151-164.

11. Organizational issues in the implementation and adoption of health information technology innovations: an interpretative review. **Cresswell, K. and Sheikh, A.** 2013, International journal of medical informatics, pp. 82(5), e73-e86.

12. Fear appeals and information security behaviors: an empirical study. **Johnston, A. C. and Warkentin, M.** 2010, MIS quarterly, pp. 549-566.

13. **Beccaria, C.** On crimes and punishments. 1764.

14. Cesare Beccaria and the Theoretical Foundation of Modern Penal Jurisprudence. **Devine, F. E.** 1981, New Eng. J. on Prison L, pp. 7, 8.

15. **Beccaria, Cesare.** On crimes and punishments. s.l. : Transaction Publishers, 2016.

16. Deterring Information Systems Misuse: The Impact of Three Security Countermeasures. **D'Arcy, J. and Hovav, A.** Las Vegas : NV, 2005. In The Fourth Security Conference.

17. Punishment And Deterrence: Another Analysis Of Gibbs' Data. . **Gray, L. N. and Martin, J. D.** 1969, Social Science Quarterly, pp. 389-395.

18. Complex Adaptive Systems. **Burns, A., et al.** 2012, Agent-Based Modeling and Information Assurance.

19. How does enforcement deter gray market incidence? **Antia, K. D., et al.** 2006, Journal of Marketing, pp. 70(1), 92-106.

20. Deterrence theory revisited. **Jervis, R.** 1979, World Politics, pp. 31(2), 289-324.

21. Rational deterrence theory and comparative case studies. **Achen, C. H. and Snidal, D.** 1989, World politics, pp. 41(2), 143-169.

22. Compliance with information security policies: An empirical investigation. **Siponen, M., Pahnila, S. and Mahmood, M. A.** 2010, Computer, pp. 43(2), 64-71.

23. IS security policy violations: A rational choice perspective. **Vance, A. and Siponen, M. T.** 2012, Journal of Organizational and End User Computing (JOEUC), pp. 24(1), 21-41.

24. Taxonomy of compliant information security behavior. **Padayachee, K.** 2012, Computers & Security, pp. 31(5), 673-680.

25. Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. **Knapp, K. J. and Ferrante, C. J.** 2012, Journal of Management Policy and Practice, pp. 13(5), 66-80.

26. Effective IS Security: An Empirical Study. **Straub, D.W.** 1990, Information Systems Research, pp. 255-276.

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

28. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. **Bulgurcu, H. B., Cavusoglu and I., Benbasat.** 2010, MIS Quarterly, pp. 523-548.

29. An integrative study of information systems security effectiveness. **Kankanhalli, A., et al.** 2003, International Journal of Information Management, pp. 139-154.

30. Coping with systems risk: Security planning models for management decision making. **Straub, D. W. and Welke, R.J.** 1998, MIS Quarterly, pp. 441-469.

31. In defense of the realm: Understanding the threats to information security. **Whitman, M. E.** 2004, International Journal of Information Management, pp. 43-57.

32. Information systems management maturity and information technology security effectiveness. **Spicer, G.D.** 2004, University of Lethbridge, Alberta, Canada.

33. Toward a Theory of Criminal Deterrence. **Silberman, M.** 1976, American Sociological Review, pp. 442-461.

34. Sanctions, situations, and agency in control theories of crime. **Gottfredson, M. R.** 2011, European Journal of Criminology, pp. 8(2), 128-143.

35. Determinants of information security affecting adoption of web-based integrated information systems. **Joo, J., et al.** 2011, World Academy of Science, Engineering and Technology, pp. 78, 371-376.

36. The role of information security learning and individual factors in disclosing patients' health information. **Park, E. H., Kim, J. and Park, Y. S.** 2017, Computers & Security, pp. 65, 64-76.

37. Computer security management. **Forcht, K.A.** 1994, Boyd and Fraser, Danvers, MA, USA.

38. Preventive and Deterrent Controls for Software Piracy. **Gopal, R.D. and Sanders, G.L.** 1997, Journal of Management Information Systems, pp. 29-47.

39. An Investigation into the Use and Usefulness of Security Software in Detecting Computer Abuse," . **Nance, W.D. and Straub, D.W.** Minneapolis, MN : s.n., 1988. In Proceedings of the 9th Annu. Conf. on Information Systems.

40. **Schuessler, J.H.** General deterrence theory: Assessing information systems security effectiveness in large versus small businesses. University of North Texas,. [Online] 2009. http://joseph.schuessler sounds.com/Research/Dissertation/Schuessler_Dissertation.pdf .

41. Information security policy: An organizational-level process model. **Knapp, K.J., et al.** 2009, Computers and Security, pp. 493-508,.

42. A conceptual foundation for organizational information security awareness. **Siponen, M. T.** 2000, Information Management & Computer Security, pp. 8(1), 31-41.

43. Information security management: An information security retrieval and awareness model for industry. **Kritzinger, E. and Smith, E.** 2008, Computers & Security, pp. 27(5-6), 224-231.

44. Security awareness: switch to a better programme. **Johnson, E. C.** 2006, Network security, pp. (2)15-18.

45. Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation. **Maarop, N., et al.** s.l. : World Academy of Science, Engineering and Technology, 2015. International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering. pp. 9(3), 884-889.

46. Information security culture critical success factors. **Alnatheer, M. A.** s.l. : IEEE, 2015. In 2015 12th International Conference on Information Technology-New Generations. pp. 731-735.

47. Threats to information systems: today's reality, yesterday's understanding. **Loch, K. D., Carr, H. H. and Warkentin, M. E.** 1992, Mis Quarterly, pp. 173-186.

48. Incident-centered information security: Managing a strategic balance between prevention and response. **Baskerville, R., Spagnoletti, P. and Kim, J.** 2014, Information & management, pp. 51(1), 138-151.

49. Security threats to Internet: a Korean multi-industry investigation. **Jung, B., Han, I. and Lee, S.** 2001, Information & Management, pp. 38(8), 487-498.

50. User acceptance of information technology: Toward a unified view. **Venkatesh, V., et al.** 2003, MIS quarterly, pp. 425-478.