https://doi.org/10.48009/2_iis_2012_21-25

Issues in Information Systems

Volume 13, Issue 2, pp. 21-25, 2012

IMPACT OF SECURITY COUNTERMEASURES IN ORGANIZATIONAL INFORMATION CONVERGENCE: A THEORETICAL MODEL

Ganesh Vaidyanathan, Indiana University South Bend, gvaidyan@iusb.edu
Neamen Berhanu, Ivy Tech, South Bend, nberhanu@ivytech.edu

ABSTRACT

Organizations need to understand the specifics of the security countermeasures in order to deploy a successful security program. Given the large number of security breaches that occur, organizations have to customize their security models and sharpen their security policies in order to be considered in the organizational information convergence. Such an information convergence of security policies and other security programs along with the user awareness of security deterrence methods of certainty and severity of sanctions may bring fruition to the success of the security programs. This study uses the theoretical lenses of the General Deterrence Theory to explore how the security countermeasures impact security information flow in an organization and how they in turn impact the security performance of the organization moderated by awareness of security.

Keywords: Information technology, convergence, theoretical model, security, General Deterrence Theory

INTRODUCTION

Organizations invest to obtain information and spend a lot of time, effort, and money to accumulate that information in order to remain competitive. As the manufacturing and the marketing operations of organizations make way through the global business world, use of the accumulated information and the technologies associated with the use of such information becomes more and more vital to organizations. Moreover, the advent of new flexible and affordable technologies is influencing the organizations to increased use of information thereby increasing their reliability of those accumulated information. Therefore, information is a key resource of an organization. While this importance of information has been recognized for a very longtime as possibly the most critical resource in the post-industrial age[20], the downside of facing security threats to the accumulated information has increased dramatically as well. Increased reliability has prompted organizations to invest more and more to prevent those security breaches. While organizations have invested in capabilities for prevention, detection, and Web-related security initiatives using security countermeasures, a recent survey reveals a troubling degradation in core security-related capabilities[17] Moreover, a study illustrated the need for increased levels of policy in information security[26]. To strengthen the security, organizations must understand how their security countermeasures and the information flow of security countermeasures influence the success and performance of security. In this study, a research model will be proposed that may lead to testing the impacts of security countermeasures on the success of organizational information convergence in organizations through the lens of a general deterrence theory. We anticipate the results to be of great importance to information systems security managers.

GENERAL DETERRENCE THEORY

The General Deterrence Theory (GDT) assumes that potential violators are made aware of efforts to control anti-social behaviors and people respond to "policing" and the punishment that is associated with effective policing [1,2,7]. The main theme of GDT is based on the belief that businesses are especially concerned with making profit and therefore they are “amoral calculators”[14]. Hence severe consequences that surpass the cost of compliance have the potential to compel businesses to adhere to rules and regulations[25]. Schuessler[19] suggested that GDT posits that individuals can be dissuaded from committing antisocial acts through the use of countermeasures such as strong disincentives and sanctions relative to the act. Harsh actions taken against violators, it is believed, send a clear message in the community of regulated industries. This theory has been applied to Information systems to investigate in monitoring security, enforcing company policy, and executing guidelines. GDT has been used to argue that information security actions can deter potential computer abusers from committing acts that violate organizational policy[11,22,23,24]. Schuessler[19] also noted that when using GDT as a guideline, countermeasures could be put in place to eliminate security threats or at least mitigate some of the risk. D'Arcy et al. [4] introduced and tested an extended GDT model that posits that user awareness of security policies, security education, training, and awareness programs, and computer monitoring directly impacts user perceptions of the certainty and severity of sanctions associated with IS misuse, which in turn have a direct effect on Information Systems (IS) misuse intention. In IS, the "policing" activity occurs when, for instance, security officers use deterrents to monitor and enforce policy and distribute information about organizational guidelines for acceptable system usage. Enforcing severe penalties for serious security violations is thought to dissuade potential offenders, especially less motivated potential offenders, from illicit behaviors[24].

RESEARCH MODEL

Straub[22] found that IS security deterrents drastically lesson occurrences of computer abuse. The study found that the preventives and the deterrents led to success with regards to information systems security. Some researchers posit that although GDT has provided a reasonable theoretical background for understanding computer abuse, it has not led to practical successes, partly because organizations have not adequately applied it to their real environments and because the theory does not cover all the factors affecting computer abuse[16]. In this study, we use another dimension which is another important security criterion, the knowledge that is essential to evaluate the risk associated to the security attacks in order to implement appropriate countermeasures. In the deployment of smart cards, Renaudin et al.[18] emphasizes that knowledge of security approaches, both software and hardware, is essential to implement appropriate countermeasures. Up-to-date knowledge of security threats to devise security mechanisms that are effective is also essential in building secure systems[9]. Figure 1 shows the newly extended version of the GDT. The GDT can be extended to include the countermeasures of security that are generally executed in organizations. Kotulic and Clark[15] defined countermeasures as an array of organizational devices to deter, prevent, or detect security breaches. As customized security mechanisms using security knowledge is better than traditional countermeasures of detection[13], we will use security knowledge in place of detection mechanisms. The three countermeasures of security knowledge, preventions, and deterrents are used in our extended GDT model. We explore this model further in our research model.

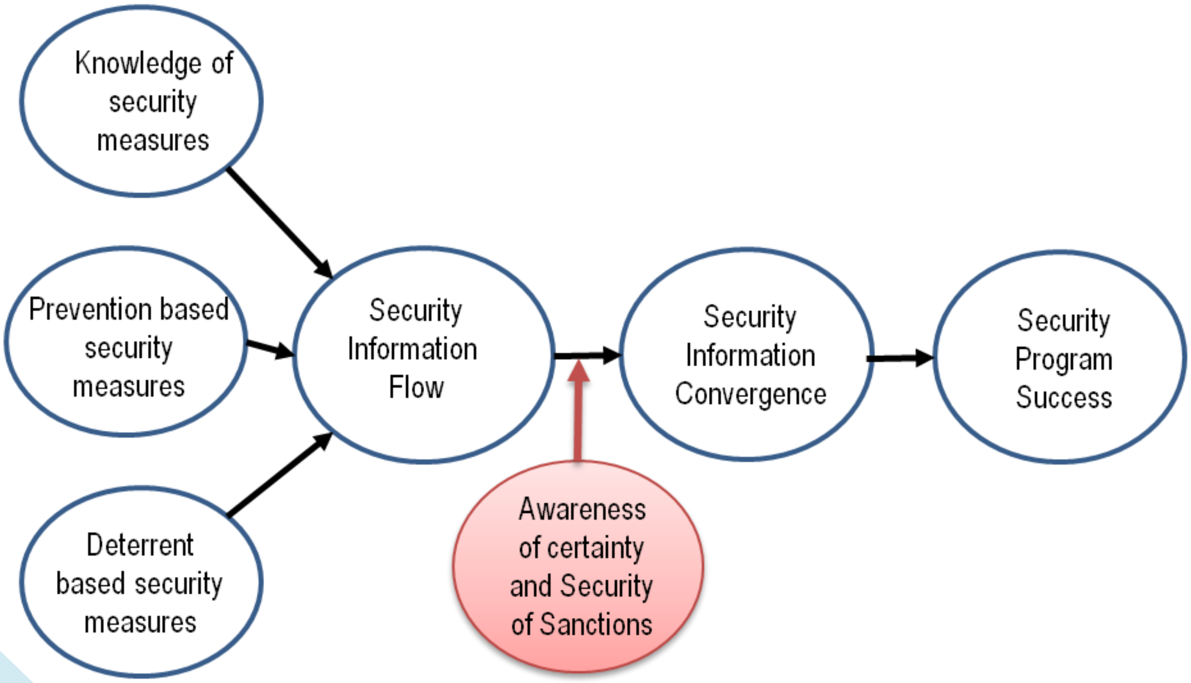
Knowledge of security measures
Prevention based security measures
Deterrent based security measures
Security Information Flow
Awareness of certainty and Security of Sanctions
Security Information Convergence
Security Program Success

Figure 1. Security in Information Convergence using an Extended GDT

In our research model, we use the theoretical lenses of the GDT to explore how the countermeasures impact the security information flow in an organization and how they in turn impact the security performance of the organization. In this section, we articulate the relationship between the security countermeasures to the security information flow and further to the success of organizational information convergence.

Security Information Flow

An organization needs to take several steps concerning information systems security. One, managers who realize they need to improve security, have to first institute clear policies detailing what is acceptable and what is not. This is the first step in having successful deterrents. The policy needs to be explicit and attempt to address all foreseeable scenarios. The second step is to educate users. Users should be thought on what is acceptable and what is unacceptable in accordance to the policy set in step one. Users should clearly understand the harsh consequences for violators depending on the severity of the violation. Third, Information systems security officers should focus on data security. This includes observing suspicious activities, monitoring passwords and classification of data. Fourth, the study also implies that to discourage computer misuse, utilization of security software plays a role[22]. Information sharing inside organizations forms the real basis of all organizational processes and activities. The information sharing is also essential in streamlining all processes and decision-making capabilities inside an organization. Moreover, organizations process information internally to reduce uncertainty and equivocality or ambiguity[5]. The processed information is used to accomplish internal tasks, coordinate activities, and interpret external environment. Such processed information includes controls (rules and regulations) which are established to provide a known response to problems that have arisen in the past. Those established rules, procedures, standards, and policies provide a fixed, objective knowledge base from which employees can learn to respond to routine organization phenomena[5]. That information is ingrained in the security controls and are accomplished as part of an organization-wide information security program that involves the management of organizational risk that includes the risk to information, individuals, and the organization as a whole. Such information has to be transferred to the employees of the organization. This information transfer is often attained by various organizational programs and security policies. The security policy is the most important layer of security available to an organization and they define the security philosophy and the organizational security activities are the basis for all subsequent security decisions and implementations. Also, a fundamental part of an organization's security function is the implementation of a security education, training, and awareness (SETA) program. Both the security policy and the SETA program are relatively low-cost protection mechanisms with the potential for high returns-on-investment[6,27]. The organization security information consists of the countermeasures including the detection, the deterrence, and the prevention methods. This information flow is accomplished through the security and SETA programs in an organization.

> ***Preposition 1:***
> *Customized countermeasures of security and user understanding of those countermeasures through the security and SETA programs are positively associated with increased organizational security information flow.*

Awareness of Certainty and Severity of Sanctions

Deterrence refers to the fear inflicted by a previous experience of inspection, a warning, or a reprimand on a business. Informal social and economic sanctions are more successful in deterring crime than the risk of legal penalties. Negative publicity can drive away customers and could lead to loss. GDT focuses on consequences of carrying out a malicious act and how these consequences deter others from committing illicit acts. This theory draws attention to two categories including certainty of sanctions and severity of those sanctions. If there is a high major threat of punishment (deterrent certainty), in addition to having the security violation be severe, GDT states that those who are planning to commit criminal acts will be reluctant to do so. Therefore, the theory assumes that if those who are planning to commit malevolent acts will stop and think twice if there are significant consequences to their actions. The main idea here is for the users to be aware of those sanctions and most importantly the certainty and severity of those sanctions. We use the awareness factor of GDT as a moderator in our research model.

Security Information Convergence

Convergence is the approach toward a definite value, a definite point, a common view or opinion. Organizational information convergence in security relates to the convergence of security measures and the operational element of the security measures. Security policies consist of detailed guidelines on the proper use of organizational IS resources[28] and provides knowledge of acceptable and unacceptable conducts that can deter punishment[16]. SETA programs also have similar deterrent effects that are achieved through meetings and seminars to reinforce consequences of misuse[4]. Although a research points out that security policies was not associated with diminished quantity or severity of medical record security incidents[29], other research are more successful with the introduction of policies in organizations to thwart misuse of IS resources. We look at the security incidents in an organization with the security information convergence and we posit that this information convergence is vital to the deterrence and prevention of security incidents.

> ***Preposition 2:***
> *Organizational security information flow consisting of countermeasures moderated by the awareness of certainty and severity of sanctions is positively associated with the security information convergence*.

Security Program Success

The success of a security program depends upon how well an organization converge their security information to the users. Security programs focus on protecting information present in business processes and organizations that articulate and enforce their policies benefit immensely. This is accomplished by establishing a security program[12] and enforcing the program[22]. A successful security program can be measured by how well its community members are engaged in its development; how well they understand the roles and responsibilities; and most importantly, how well the organization can minimize damage from malicious attacks and unauthorized access to their systems. The ultimate measure of success in a program is its value to the organization. Deterrent certainty uses the measure of success of the security effort[22]. Moreover, if the certainty is merged with appropriate measures that the users are aware and if there is an information convergence that exists in an organization, the security program may be successful. Hence,

> ***Preposition 3:***
> *Organizational security information convergence is positively associated with the success of the security program in organizations.*

CONCLUSION AND FURTHER RESEARCH

This study proposes a model through the theoretical lens of GDT to investigate security. We look through the theoretical lenses of GDT to explore how the countermeasures impact the security information flow in an organization and how they in turn impact the security performance of the organization. We also articulate the relationship between the security countermeasures to the security information flow and further to the success of organizational information convergence. A set of prepositions are proposed in this study that forms the basis of our study and using these prepositions, we are making progress to understand the success of security programs in organizations. We are well underway in gathering data using a survey instrument and we will use an empirical method to further this study.

REFERENCES

1. Blumstein. A., Cohen, J., and Nagin, D. (1978). *Introduction in deterrence and incapacitation: estimating the effects of criminal sanctions on crime rates.* National Academy of Sciences: Washington. DC.
2. Cook, P. J. (1982). *Research in criminal deterrence: laying the groundwork for the second decade.* In Morris and M. Tonry (Eds.), Crime and Justice: An Annual Review of Research. 2, 211-268, The University of Chicago Press: Chicago, IL.

3. D'Arcy, J., Hovav, A., and Galletta, D. (2008). User awareness of security countermeasures and its impact on Information Systems misuse: a deterrence approach. *Information Systems Research,* 20 (1), 79-98.
4. Daft, R.L., and Lengel, R.H. (1986). Organizational information requirements, media richness and structural design. *Management Science,* 32(5), 554-571.
5. Dhillon , G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security,* 7 (4), 171-175.
6. Ehrlich, L. (1973). Participation in illegitimate activities: a theoretical and empirical investigation. *Political Economy*, 81, 521-564.
7. Flechais, I., Sasse, A.M., and Hailes, S.M.V. (2003). Bringing security home: a process for developing secure and usable systems. *Workshop on new security paradigms,* Ascona, Switzerland: ACM Press, 49-57.
8. Hoffer, J. A., and Straub, D. W. (1989). The 9 to 5 underground: are you policing computer crimes? *Sloan Management Review,* 30 (4), 35-44.
9. ISF (2005). *The standard of good practice for information security.* Information Security Forum. Reference ISF 05-104. Pages 1-28.
10. Iyer, R.K., Kalbarczyk, Z., Pattabiraman, K., Healey, W., Hwu, W.W., Klemperer, P., and Farivar, R. (2007). Toward application-aware security and reliability. *IEEE Security and Privacy*, 5 (1), 57-62.
11. Kagan, R. A., and Sholz, J.T. (1984). *The criminology of the corporation and regulatory enforcement styles.* In Enforcing Regulation, K. Hawkins & J. M. Thomas (Eds.). Kluwer-Nijhoff: Boston, MA.
12. Kotulic, A. G., and Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management,* 41(5), 597.
13. Lee, J., and Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, 10 (2), 57–63.
14. PWC (2011). *2012 Global State of Information Security Survey.* Available at http://www.pwc.com/gx/en/information - security-survey/key-findings.jhtml; accessed on October 11, 2011.
15. Renaudin, M., Bouesse, F., Proust, P., Tual, J.P., Sourgen, L., and Germain, F. (2004). High security smartcards. *Proceedings of the conference on Design, automation and test in Europe (DATE '04)*, Volume 1, Paris, France, February 16-20.
16. Schuessler, J. (2009). *General deterrence theory: Assessing information systems security effectiveness in large versus small businesses.* Large versus Small Businesses. Denton, Texas.UNT Digital Library.
17. Sheth, J. (1994). Strategic importance of Information Technology. *Advances in Telecommunications Management*, 4, 3-16.
18. Straub, D. W., Carlson, P. J., and Jones, E. H. (1993). Deterring cheating by student programmers: a field experiment in computer security, *Journal of Management Systems,* 5 (1), 33-48.
19. Straub, D. W. (1990). Effective IS security: an empirical study, *Information Systems Research,* 1 (3), 255-276.
20. Straub, D. W., and Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study, *MIS Quarterly,* 14 (1), 45-62.
21. Straub, D.W., and Widom, C.S. (1984). *Deviancy by bits and bytes: computer abusers and control measures.* In James H, Finch and E, G, Dougall (Eds.), Computer Security: A Global Challenge. Elsevier Science Publishers B.V, (North-Holland) and IFIP. Amsterdam.
22. Thornton, D., Gunningham, N.A., and Kagan, R. A. (2005). General deterrence and corporate environmental behavior. *Law and Policy,* 25 (2), 262-88.
23. Whitman, M.E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management,* 24, 43-57.
24. Whitman, M.E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM,* 46 (8), 91-95.
25. Whitman, M. E., Townsend, A. M., Alberts, R. J. (2001). *Information systems security and the need for policy.* M. Khosrowpour (Ed.), Information Security Management: Global Challenges in the New Millennium. Idea Group Publishing, Hershey, PA, 9–18.
26. Wiant, T. L. (2003). *Policy and its impact on medical record security.* Unpublished doctoral dissertation, University of Kentucky, Lexington.