2012

Organizational Adoption of Cyber Insurance Instruments in IT Security Risk Management– A Modeling Approach

Tridib Bandyopadhyay
Coles College of Business, Kennesaw State University, tbandyop@kennesaw.edu

ORGANIZATIONAL ADOPTION OF CYBER INSURANCE INSTRUMENTS IN IT SECURITY RISK MANAGEMENT– A MODELING APPROACH

Tridib Bandyopadhyay
Coles College of Business, Kennesaw State University
tbandyop@kennesaw.edu

ABSTRACT

Cyber insurance can be an effective instrument to transfer cyber risk and complement the benefits from technological controls that guard the IS (information and network) assets in organizations. This research attempts to identify the factors that could explain the proclivity of adoption of cyber insurance in managing cyber risk of an organization. Grounded on the context based TOE framework of adoption of innovation, we propose a research model that integrates technology, organizational and environmental factors surrounding the adoption of cyber insurance. We begin with the insights from TOE literature, and contextualize them with the specificities of cyber insurance in order to formulate a set of relevant hypotheses, empirical validation of which could provide valuable insight into organizational adoption (or the observed lack) of cyber insurance. This research attempts to explain the contextual factors that affect successful organizational adoption of cyber insurance and extend the TOE adoption of innovation theory in the area of IT security risk management.

Keywords

Cyber insurance, IT security risk, cyber risk, organizational cyber risk management, residual IT security risk

INTRODUCTION

Organizations are exposed to cyber risk in terms of hardware failure, vulnerability in configurations, bugs in software, remote standard software exploit, data and information loss including other threats and attacks from computer virus and propagating worms. Organizations face an increased mix of these risks as more and more business processes become automated, more IT assets are acquired and the IT assets are utilized more intensely. Facing increased rate of hacking attacks (http://steveensley.com/2011/07/hacking-attacks-are-on-the-rise/), organizations are exposed to an ever increasing magnitude of loss from cyber risks.

Since IS security technologies provide incomplete protection against unauthorized access and misuse/abuse of data; under normal circumstances, an organization must live with residual cyber risk even after it has implemented an optimal framework of IS technology controls. One way that residual cyber risk can be mitigated is with the use of cyber insurance. Cyber insurance refers to the specific insurance contracts that provide coverage against loss from theft of data and IS assets. These specialized insurance contracts could also provide coverage for losses from other information and network assets and could also provide costs of victim notification, liability compensation and cyber extortion (Bandyopadhyay and Shidore, 2011). Companies like AEG and Chubb offer full ranges of products covering myriad facets of residual cyber risk (e.g., vide AEG NetAdvantage at www.aeg.com). Fundamental appropriateness of cyber insurance in IS security risk management can also be reasonably expected given that residual risk is overwhelmingly mitigated with the help of insurance contracts in most major aspects of business, industrial and natural perils. Belying expectations of insurance economists and other market researchers, cyber insurance has failed to be a mainstream instrument in managing cyber risk in organizations. The present volume of premium of cyber insurance contracts in US is only about $500 million (The Betterley Report, 2010)!

One important question that comes to mind is why organizations do not use cyber insurance widely for managing their residual cyber risks. The little research that has been conducted in the area of cyber insurance suggests that difficulty to assess the perils from cyber risk, existence of monoculture in computing platforms and operating systems leading to correlated losses, information asymmetry in cyber insurance contracting, and pricing issues are the major reasons for the unattractiveness of cyber insurance instruments (Bandyopadhyay, Mookerjee and Rao, 2009; Majuca, Yurcik and Kesan, 2006). In this research, we take a holistic view and a value based approach to assess the forces of adoptive utilization of cyber insurance. In particular, we attempt to identify and assess the contextual factors leading to adoption and utilization of cyber insurance as an integral measure to manage cyber risk. We consider that cyber insurance instrument - a techno-financial innovation - is poised for evaluation by an organization for its value in managing cyber risks, and use this perspective as the

backdrop of our model. In this paper we propose and present our research model that captures the context constrained view of organizational adoption of cyber insurance as an instrument in managing organizational cyber risk.
In what follows, we first provide a brief review of research on cyber insurance and the TOE framework of organizational adoption of innovation. Next, we develop an SEM model that captures the interplay between the forces of Technology, Organization and Environmental factors towards successful adoption of cyber insurance in organizational management of cyber risk. Pari-passu, we develop a set of hypotheses that, along with the SEM model, can be utilized for data collection and analysis of insights during the upcoming phases of our research. We close this report with a brief recap of the discussion on the contextual forces in the model before we summarize our concluding thoughts.

LITERATURE REVIEW

Cyber insurance is an IS innovation that involves utilization of specialized insurance instrument which covers cyber risk. Very few researchers consider IS adoption over the whole organization with the notable exceptions of Chau and Tam, 1997 and Rai and Howard, 1993. While Chau et al., 1997 discusses organizational adoption of open systems, Rai et al., 1993 discusses an organization's contextual issues regarding innovation in Computer Aided Software engineering (CASE). Our research, like Chau et al., 1997 extends the theoretical TOE framework of innovation by Tornatzky and Fleischer, 1990. However, although both begins with the same theoretical framework, our research is detail oriented and identifies a total of 9 factors as integrated in the fundamental 3 elements of context propounded by Tornatzky et al., 1990. Few researchers have investigated different aspects of utilization of cyber insurance. A framework of using cyberinsurance in mitigating information risk that may not be addressed through technology has been proposed by Gordon, Loeb and Sohail, 2003. Ogut, Raghunathan and Menon, 2005 discuss how the interdependence between the risks of the firms and their suppliers of IS technology controls may affect decision to invest in cyberinsurance. Majuca et al., 2006 study the evolution of cyberinsurance market and analyze the impacts of impediments of moral hazard and adverse selection. Bandyopadhyay et al., 2011 discusses apparent unattractiveness of cyber insurance to the IS managers, while Bandyopadhyay et al., 2011 presents and analyze a strategic model of organizations' internal decision processes towards integration of cyber insurance in IS security risk management. To the best of our knowledge, this research is the first one that attempts to isolate the contextual factors leading to adoptive utilization of cyber insurance in integrative management of cyber risk in an organization.

MODEL PRELIMINARIES

Our goal in this work is to provide an adequate model for organizational adoption of cyber insurance in IS risk management. However, before we develop our model, it is important that we explain the divergent perspectives of innovation that cyber insurance may represent. Further, we also bring to the fore a dichotomy in decisional complexity that may complicate an organization's proclivity to adopt cyber insurance instruments in their cyber risk management program.

Cyber Insurance as an Innovative IS Security Measure

Looking from the providers' perspective, cyber insurance may be considered as an innovation in financial instrument - a special type of insurance contract meant to protect losses from a specific type of asset (the IS assets). However, from the utilization perspective, cyber insurance is appropriated as an innovative instrument to manage IS security risk of an organization. In the consumption side, cyber insurance helps protect proper functioning of business processes by ensuring reparation of losses from abuse and misuse of IS assets. Specifically, cyber insurance is an innovation in organizational IS security initiatives and is utilized to support and augment the functionalities and benefits of IS security technology controls. In this work, we view cyber insurance as an innovation in the way it is implemented to enhance the IS security in particular and lower organizational cyber risk in general.

Decisional Complexity in Cyber Insurance Adoption

Cyberinsurance mitigates IS security risks and falls in the professional area of IS managers. However, since it is a financial instrument, the professional experience and theoretical underpinnings regarding cyber insurance is not one of the forte of the IS managers. On the other hand, cyber insurance is much akin to many other types of insurance, which the traditional Risk managers deal regularly in their professional life. Moreover, since cyber insurance tends to cover risk areas which may overlap/compensate gaps in traditional property loss and liability insurances, organizational risk managers are made privy to the decision process for the adoption of cyber insurance. This gives rise to an important dichotomy in the decisional complexity that cyber insurance faces in terms of adoption decision. We take special care to accommodate the above challenges in the way we review and argue the factors contributing successful adoption of cyber insurance.

MODEL DEVELOPMENT

In this section, we first present the Technology Organization Environment (TOE) framework of Tornatzky et al., 1990 and argue its prima facie suitability as a starting point for an adequate model of adoption of cyber insurance. Having done so, we present our research model that has 3 contextual elements comprising a total of 9 factors that may determine organizational decision to adopt cyber insurance as an integral measure to combat cyber risk.

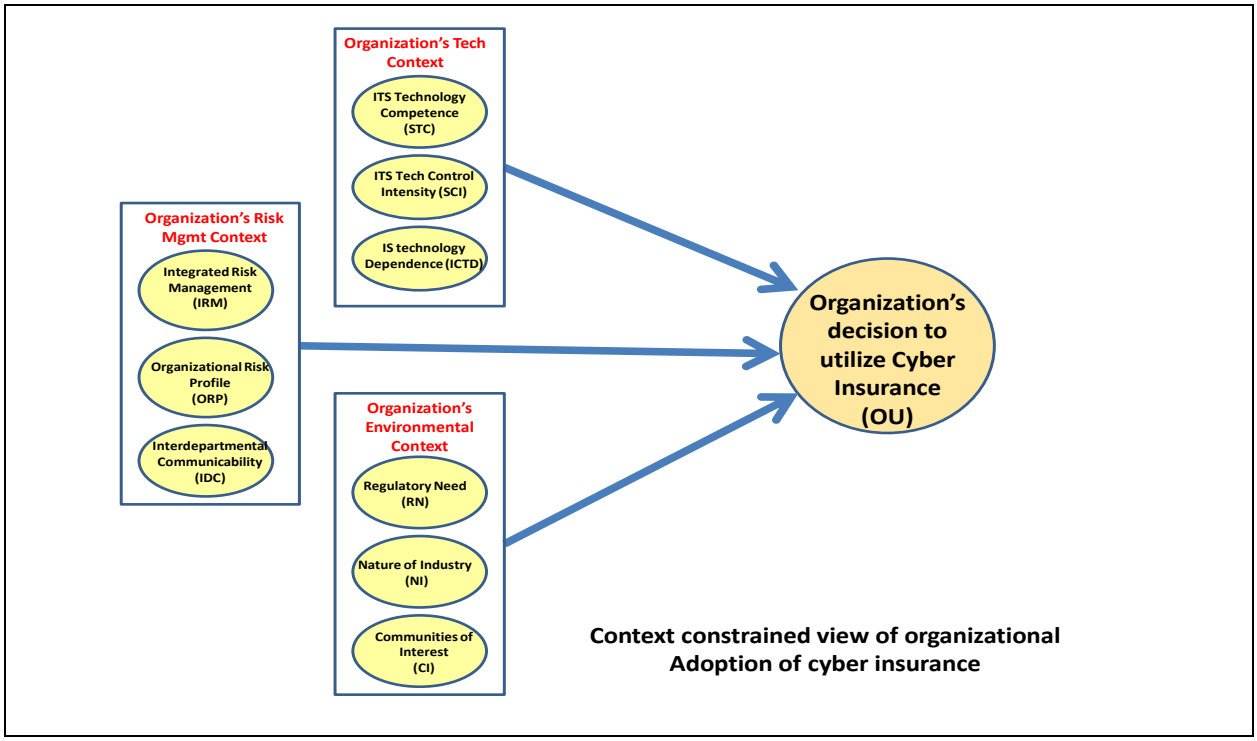
A Theoretical Framework for Adoption of Cyber Insurance

A model for adoption and utilization of cyber insurance must fundamentally include the factors that affect the perceived valuation of cyber insurance as an instrument to manage cyber risk in the organization. Since the value of cyber insurance lies in its utilization under the contextual specificities of an organization's being and functioning, the TOE framework propounded by Tornatzky et al., 1990 is of special appeal. In this paper, we adopt the TOE framework as the backbone of our structural equation model. Next, we appropriately constrain the framework to render the model suitable for our domain specific analysis of adoption decision. The TOE framework identifies the following three factors that influence organizational adoption and utilization of an innovation.

1. The first factor isolates the *technological context*. In this, identified are the relevant technologies that are in current use in the organization as well as the capabilities and skills of the personnel who implement these technologies in order to create organizational value.
2. Second, the *organizational context* indicates the internal forces that impact the organization's being and functioning. For example, organizational attributes like size and operational specificities like decisional hierarchy and internal strategy and planning structures are instrumental in this set of factors (Chau et al., 1997).
3. The environmental context for the organization includes the conditionalities and forces that exist in the environment of business. Thus industry structure, competitive landscape, regulatory environment and global presence are important considerations. In general, the environmental context includes opportunities, threats and uncertainties that shape the strategies of the organization.

Our Research Model for Adoption of Cyber Insurance

Based on the TOE framework of Tornatzky et al., 1990, as explained above, a model for cyber insurance - as an adoption of IS innovation - is proposed below.



The model closely follows the fundamental (3) elements of the adoption model of Tornatzky and Fleischer (1990). However, all the elements have been labeled differently to suit present research. First, we label technology context as *organization's technology context* and holistically include both productive and security technology contexts of IS as implemented in the business processes of the organization. Second, the organizational context has been labeled as *organization's risk management context*. We conceptualize that generic organizational factors such as size and decisional structures are implied in the way the risk management environment of the organization is established and operationalized. Finally, the environmental context has been labeled as *organization's environmental context*.

These nine factors of adoption decision, specific to the case of cyber insurance, now integrate the impact of the 3 fundamental environmental elements on the adoption decision of cyber insurance. In the following, we define and explain each of these nine factors under the 3 fundamental elements of adoption.

RATIOCINATION OF THE INTEGRATIVE FACTORS IN MODEL AND FORMULATION OF HYPOTHESES

The goal of this section is to explain each of the 9 factors that constitute the 3 contextual elements of our research model. We simultaneously develop a set of hypotheses that we propose to utilize during the analysis phase of this ongoing research.

Organization's Risk Management Context

We define risk as the impact of undesirable events that affect the functionality and performance parameters of a business in an adverse fashion. As such, all businesses with profit motive must bear attendant risks that accompany their revenue and cost models. One recent addition to the pool of the traditional organizational risks is the risk of misuse and abuse of IS assets (e.g., databases, servers, routers, etc.) – henceforth *cyber risk*. Cyber risk is technical in nature, inadequately understood (Amoruso, 2006), and often characterized by its idiosyncratic recalcitrance against accurate assessment of loss[1]. Since cyber risk is predominantly technical in nature, many organizations tend to mitigate these risks with technical measures (e.g. IS security technology controls like the Firewall and Intrusion Detection devices). In such cases, the primary decisional constituency comprises the IS managers, who are experts in IS technologies and methods but have scant knowledge in insurance. When cyber risk is integrated and managed centrally from the risk management center of the organization, an integrated risk management paradigm emerges. Under such an arrangement, two fundamentally disparate decisional constituencies tend to emerge. In the integrated paradigm, the risk managers provide the lead in the area of risk mitigation with insurance prudence, while the IS managers lead the areas of coordinated cyber defense that essentially include leaving an optimal amount of cyber risk for onward transfer to the insurer with the help of cyber insurance instruments. This integrated approach promises a balanced outcome and a more favorable environment for adoption of cyber insurance (Gordon et al., 2003), but it is challenged by the requirement of high level of effective coordination between the two disparate decisional constituencies. We now posit our 1st hypothesis:

Hypothesis H1: Organizations which manage cyber risk centrally as an implementation of integrated risk management paradigm are more likely to adopt cyber insurance than those who manage cyber risk in a decentralized fashion

Organizations manage business risk through multiple initiatives. For example, organizations attempt to (i) prevent and reduce the likelihood of occurrence of undesirable events that cause adverse outcomes on performance parameters, e.g., Firewalls reduce the chances that an unauthorized user will be able to access sensitive organizational information and (ii) reduce the impact of realized undesirable events, e.g., IDS helps identify presence of ongoing unauthorized access and helps reduce the extent of damage or loss and Incidence Response and Disaster recovery (IRDR) reduces the downtime through alternate routes of business continuity (Whitman and Mattord, 2002). Further, organizations can also transfer a part of the risk to a willing party with the help of appropriate financial instruments, e.g., cyber insurance can transfer a part of residual cyber risk (Gordon et al., 2003). However, even after all these measures; every organization must live with the remaining risk that is left out of these equations. This remaining risk that the organizations accepts and accommodates in its business processes defines the *organizational risk appetite* (by definition, ISO 31000)[2]. Different organizations exhibit different levels of risk appetite. Certain businesses are more risky by nature (e.g., oil exploration) whereas certain others are not (e.g., commodity retail). However, even in a given industry category, certain firms may exhibit higher risk profile than other comparable firms in the industry. Firms which accept higher degree of risk in their business processes typically justify it with traditional risk return paradigm (an attempt to increase return typically accompanies higher risk). We thus arrive at our 2nd Hypothesis:

Hypothesis H2: Organizations with higher risk appetite are less likely to be interested in adopting cyber insurance in the management of cyber risk in their organization

Decision to buy and integrate cyber insurance in the organizational risk management initiatives requires high level of communication between the risk managers and the IS managers of the organization (Bandyopadhyay et al., 2011). There are several reasons for this. First, the need to buy cyber insurance can be complex to realize. For example, a laptop insured with standard property loss insurance (e.g., home insurance) will cover the physical loss of the computer but will not cover the loss of data from the same laptop[3]. Such needs are difficult to understand without high levels of communications because the seats and realization of these losses are likely to impact and trigger disparate departmental processes. Second, evaluation of requisite or optimal coverage from cyber insurance is hard without proper communications between the IS and the risk

[1] See *CRS report* for Congress (2004). Available at: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf

[2] See *Protecht Report* (2011) at http://www.protecht.com.au/media/content/brochures/newsletters/Protecht%20Quarterly%20Newsletter%20-%202011%20Q1.pdf

[3] Refer http://www.linux-on-laptops.com/laptop-insurance.html

management constituencies. This happens because the cost and coverage of cyber insurance (the procurement process is likely governed by the risk management constituency) depend on the degree of IS technology security controls in place (these decisional intricacies involve multiple parameters and they are governed by the IS constituency). Third, the procurement of cyber insurance follows an audit process that assesses the residual risk of the organization as well as the IS security readiness of the organization[4]. This includes, to the least, administration of a detailed questionnaire and for larger contracts may involve actual third party specialist audit of the prospect firm. The audit process cannot be successfully executed without high level of communication between the IS and Risk management constituencies. Finally, even after a breach of an information asset is realized, the reporting procedure can be complex and involve multiple departments especially because of the privacy concerns and sensitivity to stock prices of information breaches. As a result, multiple channels of organizational communications are needed in the claiming process (Bandyopadhyay et al., 2009). This underscores the importance of inter constituency communication in the initial decision to adopt utilization of cyber insurance. We now posit hypothesis 3:

Hypothesis H3: Organizations with functionally efficient communication channels between the decisional constituencies involving utilization of cyber insurance are more likely to adopt cyber insurance in their cyber risk management

Organization's Environmental Context

Certain breaches into information assets constitute privacy and other liabilities for the organization. For example, a loss of credit card and other personally identifiable data of consumers may constitute privacy breach while a loss of consumer health data may constitute breach of HIPPA standards. Facing liabilities of such nature, organizations attempt to ensure a regime of due diligence in its cyber security domain (Whitman et al., 2002). Cyber insurance contracts can effectively augment the due diligence efforts in cyber security and can even compensate for liability payments. As the regulatory environment surrounding organizational cyber risk management approaches higher sophistication, and the legal and regulatory needs to protect information assets and the need to disclose cyber security breaches become onerous, the beneficial impact of utilization of cyber insurance in the management of cyber risk is amplified. Hypothesis 4 is now ready to be posited:

Hypothesis H4: When regulatory needs to protect information assets become comprehensive and disclosure of data breaches become encompassing, cyber insurance is more likely to be adopted in organizational cyber risk management

The nature of industry where the organization operates becomes critical for the decision process leading to adoptive utilization of cyber insurance. Industries where the intensity and/or role of (a) intellectual property - e.g., patent, (b) pecuniary transactions - e.g., e-commerce, (c) volatility of operation - e.g., Internet stock brokerages, (d) global dispersion in clientele and suppliers - e.g., Amazon Market Place, and (e) high competitiveness (e.g., loan agencies) are of higher order; much higher levels of utilization, higher needs for protection of information assets and increased liability from breaches of information assets result. In other words, the belongingness to a specific industry directly or indirectly impacts the perceived need and benefit from utilization of cyber insurance. This leads to our hypothesis 5:

Hypothesis H5: The degree of volatility in the business environment and industry landscape positively impact the organization's likelihood of adoption and utilization of cyber insurance.

Communities of interest (e.g., SOA – Society of Actuaries) play an important role in bringing state of the art thoughts, methodologies and initiatives to the fore of discussion among managers from multiple organizations, and often work as the germinator and precursor for best practices, industry standards and regulatory needs. Of special interest in relation to cyber insurance are the communities of interest relating to the profession and practices of organizational risk management. When risk managers and IS managers with special interest in IS security risks meet beyond organizational boundaries, meaningful discussions, analyses and roadmaps emerge in terms of innovative and effective initiatives that could minimize the losses from realization of cyber risks, including cyber insurance. Organizations which see value of the creativity and the state of the art approaches of their managers tend to encourage and reward their managers likewise by providing support for participating in professional and practice oriented communities of interest[5]. Accordingly, we present our 6th hypothesis below.

Hypothesis H6: Organizations that identify value, encourage collaboration and reward meaningful participation of its managers in communities of interest in areas of risk management are more likely to adopt and utilize cyber insurance

[4] See *Cyber risk insurance* (2004) at http://www.sans.org/reading_room/whitepapers/legal/cyber-risk-insurance_1412

[5] *UNDP conference paper (2006)*, available at http://lencd.com/data/docs/233-Concept%20Note_Incentive%20Systems.pdf

Organization's Technology Context

One highly influencing factor in the organizational technology context towards adoption of cyber insurance is its acquired capability and sophistication in implementing and managing IS Security Technology controls, which may bias their preferences for technology against other plausible non-technology avenues. When IS managers and their technicians are highly trained and proficient in designing and implementing efficient IS security technology controls, a biased environment towards technology dependence may pervade (VanderLeest, 2004). Under such circumstances, incremental resource allocation towards management of cyber risk could be preferentially routed to more sophisticated technology controls rather than the financial instruments like cyber insurance. While a higher degree of proficiency and technology skills available in the IS managers and technicians may ensure higher than industry average return specific to the incremental technology investments, the fundamentally myopic perspective of fund allocation hinders adoption of a time tested and effective financial instrument like cyber insurance in the management of organizational cyber risk. We now have hypothesis 7:

Hypothesis H7: Organizations high on the experience curve in IS Security technology and possessing trained and experienced technology personnel are less likely to adopt and utilize cyber insurance in managing cyber risk

In case an organization has an effective, state of the art array of technology controls in a layered cyber defense program in place, the impacts of additional investment on cyber risk are important to consider. First note that any additional gain to achieve with a higher density or intensity of technology control in a given layer of cyber defense is increasingly less cost effective[6]. In other words, reducing the likelihood of breach with the help of additional firewalls or increasing the chances of detection by implementing denser IDS schemes are increasingly less cost effective. On the contrary, the alternate avenue for managing the residual cyber risk of the organization with the help of non-technical controls of cyber insurance may becomes more attractive. This happens because high utilization of IS security technology control reduces cyber risk substantially, which reduces the expected indemnity payment of the insurer from implemented cyber insurance contracts. This in turn incentivizes the providers to attractively price cyber insurance contracts for purchase by those organizations which have already implemented a robust, state of the art technology regime in IS security[7].

Hypothesis H8: Organizations that implement high intensity, state of the art, dense architecture of IS security technology controls are more likely to adopt and utilize cyber insurance in managing their organizational cyber risk

Finally, the perceived need and degree of impact in reducing the residual cyber risk is proportionally higher for organizations whose business processes incorporate IS technologies more intensely. The level of dependency on IS technology may mark a major criterion in terms of a firm's perceived benefits from cyber insurance when compared to another firm in the same industry. Compare Barnes and Nobles and Amazon in their business of selling books: IS technology dependence of Amazon is much higher than that of Barnes and Noble and accordingly, Amazon likely exhibits relatively higher attraction for cyber insurance coverage. Consider the specific case where each firms suffers a DoS (Denial of Service) attack for an identical duration. Since Barnes and Noble have a brick-N-click mixed model of business, it will likely suffer a lower amount of loss than Amazon. Consequently, Amazon is likely to exhibit a relatively higher propensity for buying cyber insurance coverage.

Hypothesis H9: Organizations whose business model centers on key enablement of IS technologies and whose business processes intensely embrace IS technologies are more likely to adopt cyber insurance in managing cyber risk.

DISCUSSION AND CONCLUDING THOUGHTS

Beginning with the TOE framework of Tornatzky et al., 1990, we have developed our research model that can help explain the forces of organizational adoption of cyber insurance. We have considered cyber insurance as the adoption of an innovative instrument in the way it is appropriated in the integrated management of cyber risk. We have also explained the decisional constituencies and the resultant dichotomy that exists in the process of adoption of cyber insurance in an organization. As we argue the integrative factors of the TOE elements of adoption of cyber insurance, we formulate a set of impactful hypotheses which we can be utilize in the analysis phase of collected data. This research is in an initial stage. Our ongoing efforts include designing an adequate and appropriate set of questionnaire and operationalize the research model to collect data and infer realistic prognosis for adoption of cyber insurance. Since insurance is one of the most effective, familiar and time tested instrument for managing risk, it is confounding why cyber insurance has failed to appeal to the managers of organizations in an adequate manner. This research is an important step towards answering the conundrum. This research extends adoption of innovation theory for the case of cyber insurance instruments in management of cyber risk.

---

[6] Follows from the generalized economic concept of diminishing return on investment - an accepted modeling assumption in the literature on the economics of IT/IS security investment.

[7] See *Cyber insurance coverage decision points* at http://insurance.about.com/od/propbusiness/a/Cyber-Insurance-Coverage-Decision-Points.htm

REFERENCES:

1. Amoruso, A. J. (2006) Using real options to value losses from cyber attacks. *Journal of Digital Asset Management*, 2(3), 150-162.
2. Bandyopadhyay, T., Mookerjee, V., and Rao, R. (2009) Why IT Managers Don't Go for Cyber Insurance Products. *Communications of the ACM* Vol. 52 No.11.
3. Bandyopadhyay, T., and Shidore, S. (2011) Towards a Managerial Decision Framework for Utilization of Cyber Insurance Instruments in IT security. *Americas Conference on Information Systems*, Detroit, Michigan, USA.
4. Chau, P. Y. K., and Tam, K. Y. (1997) Factors affecting the adoption of open systems: an exploratory study. *MIS Quarterly*, Vol. 21, No. 1, pp. 1-24.
5. Gordon, L. A., Loeb, P. M., and Sohail, T. (2003) A framework for using insurance for cyber risk management. *Communications of the ACM* 46(3) 81-85.
6. Majuca, R. P., Yurcik, W., and Kesan, J. P. (2006) The Evolution of cyberinsurance. (Available at http://arxiv.org/ftp/cs/papers/0601/0601020.pdf).
7. Ogut, H., Raghunathan, S., and Menon, N. (2005) Cyber insurance and IT security investment: impact of interdependent risk. *Proceedings of the Workshop on the Economics of Information Security*. Cambridge, USA.
8. Rai, A. and Howard, G.S. (1993) An organizational context for CASE innovation, *Information Resources Management Journal* (6:3), 1993, pp. 21-34.
9. Tornatzky, L.G. and Fleischer, M. The Processes of Technological Innovation, *Lexington Books*, Lexington, MA, 1990.
10. Whitman, M and Mattord, H. (2002) Principles of Information Security, Course Technologies, KY, 2002.
11. VanderLeest S., H. (2004) The built in bias of technology. *Proceedings of the American Society for Engineering Education Annual Conference and Exposition*, Salt Lake City, Utah, USA.