8-6-2011

Towards a Managerial Decision Framework for Utilization of Cyber Insurance Instruments in IT security

Tridib Bandyopadhyay
Kennesaw State University, tbandyop@kennesaw.edu

Snehal Shidore
Kennesaw State University, sshidore@kennesaw.edu

Towards a Managerial Decision Framework for Utilization of Cyber Insurance Instruments in IT security

Tridib Bandyopadhyay
Kennesaw State University
tbandyop@kennesaw.edu

Snehal Shidore
Kennesaw State University
sshidore@kennesaw.edu

ABSTRACT

Organizations live with residual IT security risk since technological controls are imperfect. This underlines the importance of cyber insurance in the management of IT security risk. Despite the obvious advantages, cyber insurance instruments are scarcely utilized in practice. Extant research mostly considers the economic aspects of the rational purchase of cyber insurance. In contrast, we take an organizational perspective and attempt to isolate the paradigms, contexts and constituent forces that shape the organizational decision making process towards utilization of cyber insurance. Prescriptive and descriptive decisional models are analyzed, organizational decision constituencies are explained and domain specific contexts are included before we propose an integrated decision framework for organizational utilization of cyber insurance.

Keywords

Cyber insurance, IT security, Decision model, Integrative utilization of cyber insurance, Failure of cyber insurance market.

INTRODUCTION

Utilization of information assets and networks has permeated all major business processes. As a result, managing IT security risks of an organization is of paramount importance today. Management of IT security risk involves one or more of the avenues, namely risk reduction, risk appropriation and risk transfer. Complex decision processes must precede in an organization as one of more of these avenues are explored, and appropriate risk management vehicles are selected to combat IT security risks. In this research, we focus on the decision process that precedes the selection of cyber insurance as the vehicle for the risk transfer strategy in an organization's IT security management. The specific goal of this research is to propose an initial decisional model for the utilization of cyber insurance in the organizational IT security risk management initiatives and programs.

Technological controls lag innovation of the hackers. IT security is essentially a game of reactive defense that must face the uncertainties in the contexts of attack as well as the unknown variants in threat vectors. Even after implementing robust technological controls; superincumbent security policies and governance; and organization-wide IT security awareness, training and educational initiatives; an organization must live with residual IT security risk that remains unmitigated. IT security economists suggest that organizations should first utilize technological controls to minimize the likelihood of successful hacking attacks, and then use *cyber insurance*[1] to mitigate the residual risk in the realm of cyber security (for example, refer Gordon et. al. 2003). In resonance, the original market expectation of cyber insurance stood high. However, earlier projections of a multibillion dollar market in cyber insurance have largely proved elusive: current premium volume in US is somewhere at $400-500 million (The Betterley Report, 2010).

Researchers have attempted to isolate the reasons for such lackluster performance of the cyber insurance market in US. The generally argued reasons center on *a*) correlation of cyber risk among organizations (Bohme et al., 2006), *b*) information asymmetry in contract design (Bandyopadhyay et. al., 2009) and c) difficulty in appreciation and evaluation of cyber loss, paucity of actuarial data and pricing anomalies (Industry press and governmental sources[2]). As such, the field of cyber insurance is nascent and scantly researched, leaving numerous questions unanswered.

---

[1] '*Cyber insurance'* refers to the insurance contracts that cover both first and third party cyber risks arising from disuse, abuse and misuse of the IT and network assets integrated in the value chain and other business processes in an organization.

[2] For example, visit http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf

One major area in cyber insurance that requires in-depth research is the organizational processes that guide the managers toward favorable/unfavorable decision on the utilization of cyber insurance instruments. Once we understand the paradigm, context and decision making process that govern the organizational utilization of cyber insurance in their integrated cyber risk management programs, targeted instruments can be designed and requisite proportions of cyber risk can be efficiently transferred to the insurer. Since information and network assets add value and enable most business processes in today's networked world, understanding the decisional complexities leading to integrative use of cyber insurance in the management of cyber security risk is critical and worthy of rigorous analysis. This research, to the best of our knowledge, is the very first attempt in that direction.

Organizational decision on the utilization of cyber insurance is an inherently difficult task. The constituencies of decision makers belong to different knowledge domains. IT managers are domain experts and understand the specificities of cyber risks relating to the information and network assets that they manage. However, their appreciation of insurance contracts as an organizational tool to manage cyber risks is minimal. On the other hand, the risk managers are trained professionals in risk management, which includes efficient use of insurance contracts. Even so, their appreciation of cyber risk and its ramifications are incomplete. Adding to the complexity are the uncertainties of a fledgling cyber insurance market, where products are untested, pricing appears arbitrary and experimentation in contract writing is commonplace. It is not clear, how these two diagrammatically opposite capability sets in an organization approaches the question of utilization of cyber insurance in the cyber defense programs and initiatives. In this research, we attempt to provide a first-cut model that may enable us to look inside and analyze this specific decision making process in detail through an empirical approach.

The rest of the paper is as follows. First we survey representative prescriptive/normative and descriptive decision models including those of industrial purchase/buying behavior. Second, we analyze the constituencies of decision makers and their skill sets to identify the process of selection of IT security initiatives. Third, we analyze the cyber insurance market and the available products to understand the dynamics of consumption. Fourth, we present our proposed model. Finally, we discuss the high point of the research, explain goals and expectations from this research and provide our concluding remarks.

DECISION MODELS

We consider several descriptive and prescriptive models in organizational decision making in order to create the backdrop of our fundamental framework, which subsequently lead to our proposed decisional model for utilization of cyber insurance instruments in the management of organizational IT security risk management. In what follows, we first rationalize our utilization of decisional elements from multiple models, and then we describe those specific models which are incorporated in our decision framework.

Descriptive model of decision making focuses on improving managerial decisions, and involves intelligence (identification of the need for a decision making), design (developing domain of the problem and the exhaustive set of alternatives) and choice (actual selection of one or more of the alternatives from the candidate set). Since descriptive decision making is based on the principle of limited/bounded rationality, an expansive organizational decision model for cyber insurance must consider several descriptive models of decision making. This is further underscored by the requirement that an appropriate model for cyber insurance utilization must appreciate and include critical limitations or boundaries of the domain - asymmetric information, the evolving nature of cyber risk and the emerging capabilities of the provider of such services and products. On the contrary, the prescriptive models are valuable for their ability to help decision makers make better choices, and have high pragmatic value in an organizational set-up.

Webster and Wind (1972) examine a general model of organizational buying behavior noting that an organizational buying behavior generally remains influenced by budget, cost and profit considerations. Their model presents a comprehensive view of organizational buying to evaluate relevance of specific classes of variables viz. organizational, social, individual, environmental etc. In turn, each class has 2 broad categories of variables: a) the *task variables* are directly related to the buying problem and b) the *non-task* variables which are extended beyond the buying problems. Environmental factors, e.g., economic, technological, political, geographical and cultural, which influence the buying process are also inclusive in their model. The article provides special importance for the environmental factors and explains how these factors may impact a

decision in 4 different ways: they define a) availability of goods and services, b) general business condition, c) interpersonal relation between organization, sellers and their competitors and d) information flow into the buying organization.

Nutt (1975) explains models of decision making in a descriptive fashion. Various decision models such as Bureaucratic, Normative, behavioral, group decision and open system decision making are explained in this article, which we summarize and present in Figure 1. The article emphasizes that decision making depends upon not only the number and types of dependencies and adjustment patterns between and within the organizational units, but it also depends on the assessment of primary, managerial and institutional layers in the organization in the right perspectives in order to induce shared norms and values of the constituencies in the decision process.

Grandori (1984) explains prescriptive contingency network where decision making strategies depend upon 2 factors, namely the cause and effect relation and organizational actors' preferences. He finds when a) preferences and cause and effect relation are clear, actors are likely to adopt a computational strategy, b) preferences are not clear but cause and effect relation is clear then actors adopt a compromising strategy, c) cause and effect relation is unclear but preferences are clear then actors follow judgmental strategy and d) if both the conditions are unclear then actors follow inspirational strategy. The decision strategies included in this article have certain commonalities: they depend on the rules of search, rules of choice and rules of learning; which are essentially the rational, cybernetic approaches of an organizational decision making process. In order to facilitate decision making process and to handle uncertainty and conflict of interest, this work identifies 5 decision models: optimizing, heuristic, incremental, cybernetic and random which further expands and elaborates the normative model of Nutt for practicable translation in organizational set up. The attributes of each of these models have been isolated and presented in Figure 2 below.

Masuch and LaPotin (1989) examine *garbage can* model and *artificial intelligence* model in detail. The garbage can model considers organizational decision making on 3 elements: problem, solutions and choice opportunities. He argues if problems meet the right solutions, a rational outcome is made else non decisions ensue. On the other hand, AI indicates 3 directions for possible improvement in modeling techniques. *First*, it provides continuous solution space for non trivial aspects of human decision making, *second*, AI uses object oriented design technique as a replacement for procedure driven designs and *third*, it provides better understanding of epistemological, i.e. philosophical theory of knowledge conditions, of modeling.

Puto and Qualls (1989) examine integrated approach for decision making. According to them, behavioral decision making process can be divided into 2 parts, a) riskless choices where outcomes are known with certainty and b) risky choices which involves probabilistic outcomes. They argue that a choice process consists of 2 distinct stages. The first stage is the editing phase where the decision makers restructure the problems into simplified forms by comparing each outcome with certain reference points that the decision makers hold in their mindset. On the other hand, the second stage is the evaluation phase where the hypothesized form of the value function shows that individuals make risk adverse choices for gain and risk taking choices for losses.

Akdere and Altman (2009) explain the action research model which involves gathering information, applying to an organizational problem and then collecting additional data based on the results of action taken which predict future actions. According to their model, decision makers choose decision making strategy based on cost/benefit compromise, i.e. they balance the costs of decision making strategy in time and other resources with the benefits of quality decision. In addition to the above balancing strategy, contextual factors such as significance of the decision, importance of the commitments relating to the decision, leader expertise, likelihood of commitment, goal alignment, group expertise and team competence are also mentioned/considered.

McKendrick (2010) describe how large companies plan towards management of information for future. The emphasis in their research is on the size of the problem and the breadth and extent of the impact of the decision that will be taken by the decision makers. The article explains that, decision process which must utilize substantial data, normative decision making processes should be augmented with analytical processing and other automated supports, for quality outcomes.

Gordon, Loeb and Sohail (2003) investigate organizations' concerns about protecting information and maintaining integrity of their data assets due to increased vulnerability through the internet attacks. They suggest taking advantages of cyber insurance in order to handle internet related risks which cannot be fully mitigated by the use of technological controls.

Ogut, Raghunathan and Menon (2005) look at the organizational utilization of cyber insurance from the perspective of optimal risk management and discuss the strategic aspects of such utilization in conjunction with regular technological controls. They also discuss how the interdependence between the risks of the firms and their suppliers of technology controls affects firms' decision to invest in cyberinsurance instruments.

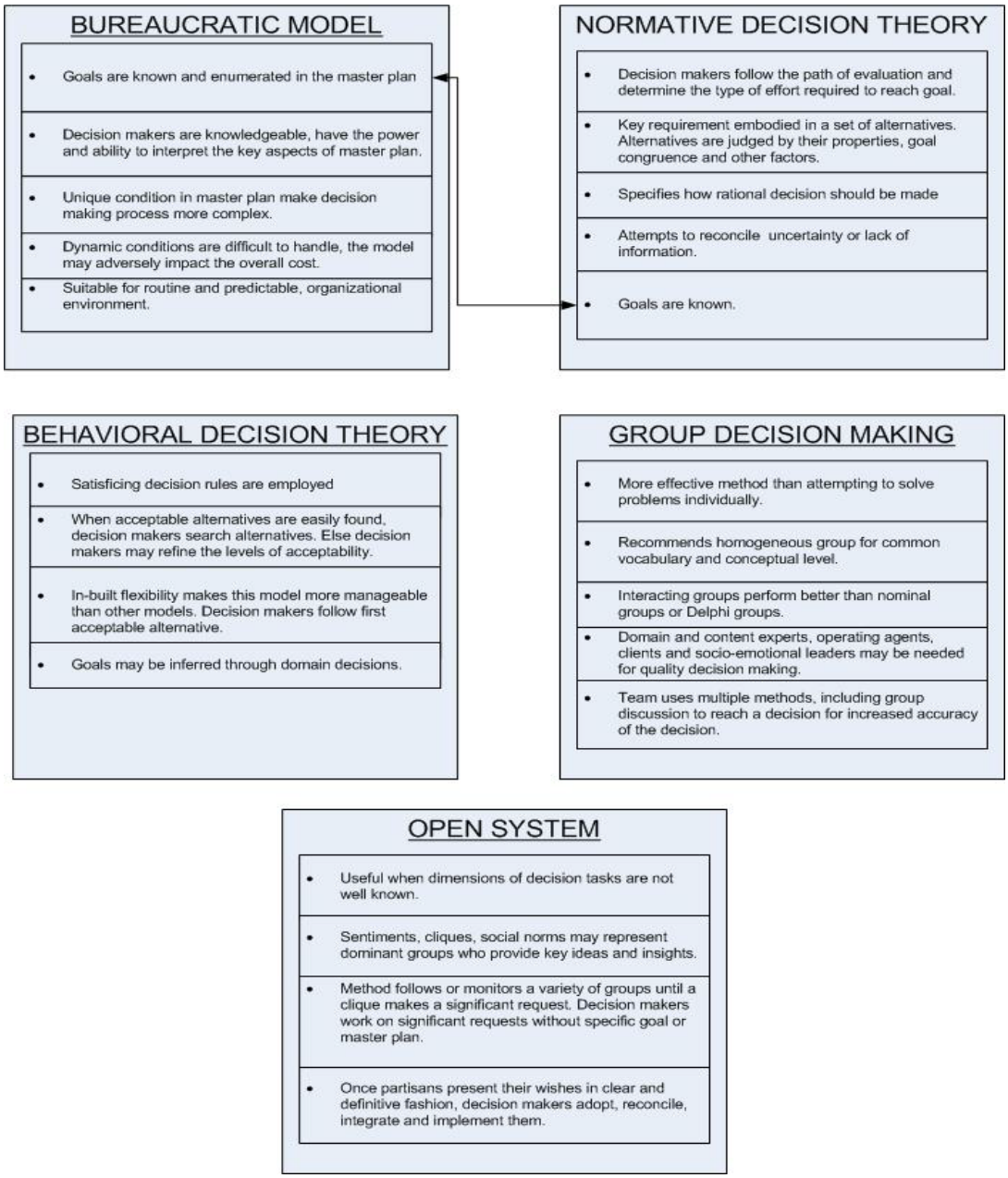

Figure 1. Descriptive Models in Organizational Decision Making

Majuca, Yurcik and Kesan (2006) study the evolution of the market for cyberinsurance and analyze the effects of classical impediments like moral hazard and adverse selection that affect the organizational decision processes, finally leading to inadequate utilization of cyber insurance in the risk management programs of the organization.

Standardized assets and systems of computing, monoculture in applications and platforms coupled with the general interconnectivity of the systems over the Internet together ensure that threat vectors, once successful, may create cyber hurricane and propagate fast over the Internet. Since correlation in cyber risk creates difficulty for insurers to provide efficient insurance contracts, the organizational consumption decisions are much impeded. With this backdrop, Bohme and Kataria (2006) study the effect of correlation in cyber risks and attempts to explain the (under) development of cyberinsurance market.

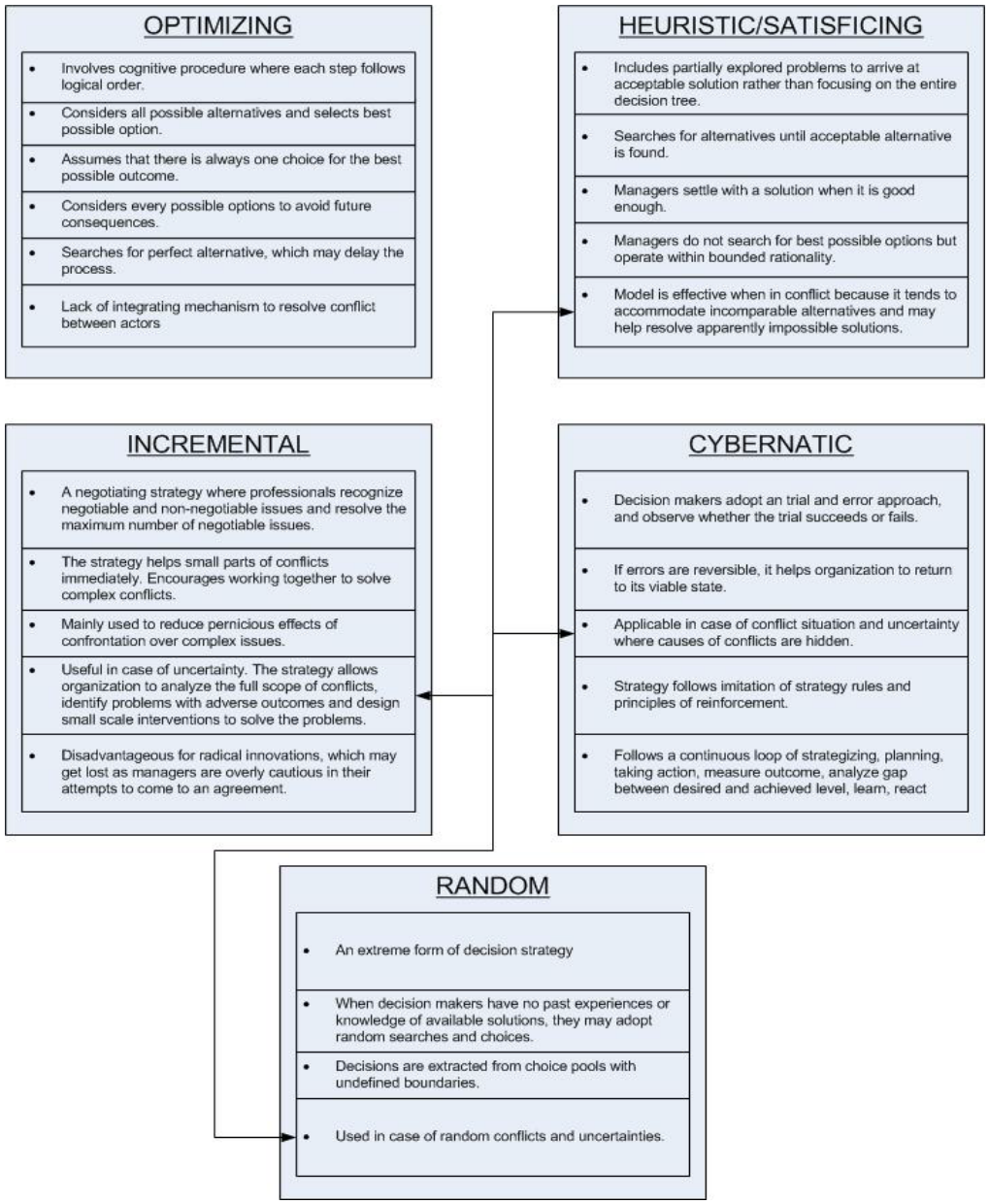

Figure 2. Prescriptive models of decision making in organization

Bandyopadhyay, Mookerjee and Rao (2009) indicate that organizational decision process regarding utilization of cyber insurance may get contaminated for certain types of breaches. This is so, because unlike regular insurance, there could be situations where a breach event incurs loss in excess of the material loss from the breach - shattered confidence of the stakeholders may affect company's competitive advantages, stock prices etc. Knowing this, the claim strategy - which is a

given assumption in the utilization of insurance contracts - becomes invalid because the type of breach cannot be exactly known in advance. When the exact type of a realized breach is known, then only a firm may decide to claim losses.

Bohme and Schwartz (2010) endeavor to provide a unified framework for the utilization of cyber insurance. They model the organizational decision processes at the center of the utilization framework. The agents at the consumption side, whose cyber risk arise out of their distributed implementation of network resources (nodes) attempt to transfer an efficient portion of their residual cyber risk to the insurer. In their framework, organizational environment creates the context of decision process in terms of how much cyber risk is transferred optimally to the insurer.

IT SECURITY RISK MANAGEMENT AND ORGANIZATIONAL CONSTITUENCIES

Risk in IT systems is defined as the negative impact of the realization of vulnerability that can impair an information asset (NIST). Risk considers both the likelihood of an adverse occurrence as well as the impact of the occurrence. Risk is integral to any value driven business. We manage risk with the help of a multistage process: a) identification of risk, b) assessment of the probability of the risk to be realized and the adverse impact thereof and c) planning and taking conscious actions to reduce the probability or the impact (or both) of the risk to an acceptable level. For IT security risk, the actions that are available include technology controls - both in the prevention and detection regimes - as well as the cyber insurance instruments which can further help reduce risk that an organization must carry in its operations. Every organization lives with some amount of risk even after they best apply all risk mitigation and transfer strategies, such amount of risk defines the risk profile or risk appetite of an organization. An organization may face risk in myriad fashion and manner. Risks are often categorized into the following types: strategic, reputational, operational, financial, and compliance-oriented. In this research we however limit ourselves to IT security risk, which arise from the vulnerabilities that exist in the information and network assets of an organization. Specifically, IT risks include loss from unused, abused and misused information and network assets; costs of system recovery and replacement; cost of informational overhead; and third party encumbrances including liability and restitution related expenditures. However, since information and network assets now-a-days support most all business processes - elements of IT security risk may actually link to all the different categories of risk that we have mentioned here. For example, if a POS system becomes inoperable, the ensued downtime could contribute to operational risks. On the other hand, if a company suffers humiliating breaches that expose the fragile IT security health of its organization (e.g. TJMax case), then the risk may appear in the form of reputational risks. This gives rise to an additional dimension of complexity in IT security risk management: the diffusive nature of the impact of IT security risk makes the IT security risk mitigation decisions more involved and complex.

The above discussion explains why identifying every constituency of IT security risk management itself may be a difficult proposition in itself. In the rest of the paper, we thus simply dichotomize the constituencies of IT security risk decision makers at the C-level of executive deliberation. We assume that the IT security risk management decisions are taken by the CRO (Chief Risk Officer) and the CISO (Chief Information Security Officer) in a cooperative fashion, which may involve both simultaneous and sequential decision and information flows. In fact, with the implementation of the Basel Act, the Sarbanes Oxley and HIPPA directives including the Turnbull report, intense cooperative decision making is encouraged across the industry (CIO News 2008). In the next section we present our proposed model for organizational decision making relating to utilization of cyber insurance instruments, and explain the model in detail.

THE PROPOSED DECISION MODEL

The expansive model that we propose for organizational decision towards utilization of cyber insurance is presented below (Figure 3). Our model reconciles and combines elements of several decision models that we have presented in Figure 1 and 2, which we further explain below.

First, our model implements the bureaucratic elements of decision making by negotiating the decision process between two different divisions of the organizations. This is purposeful since the relevant capabilities and skill sets are distributed in the organization. The CISO is knowledgeable in technological aspects including the vulnerability of information and network assets. On the other hand, the CRO is trained in risk management including administration of insurance contracts. Moreover, since decisions to purchase and utilize cyber insurance contracts precede actual utilization of these instruments, and as cyber insurance instruments are contracted to remain in effect over long horizons, such decisions are seasonal and not much prone to sudden and dynamic conditions. Consequently, the bureaucratic element does not introduce any major risks of cost overrun.

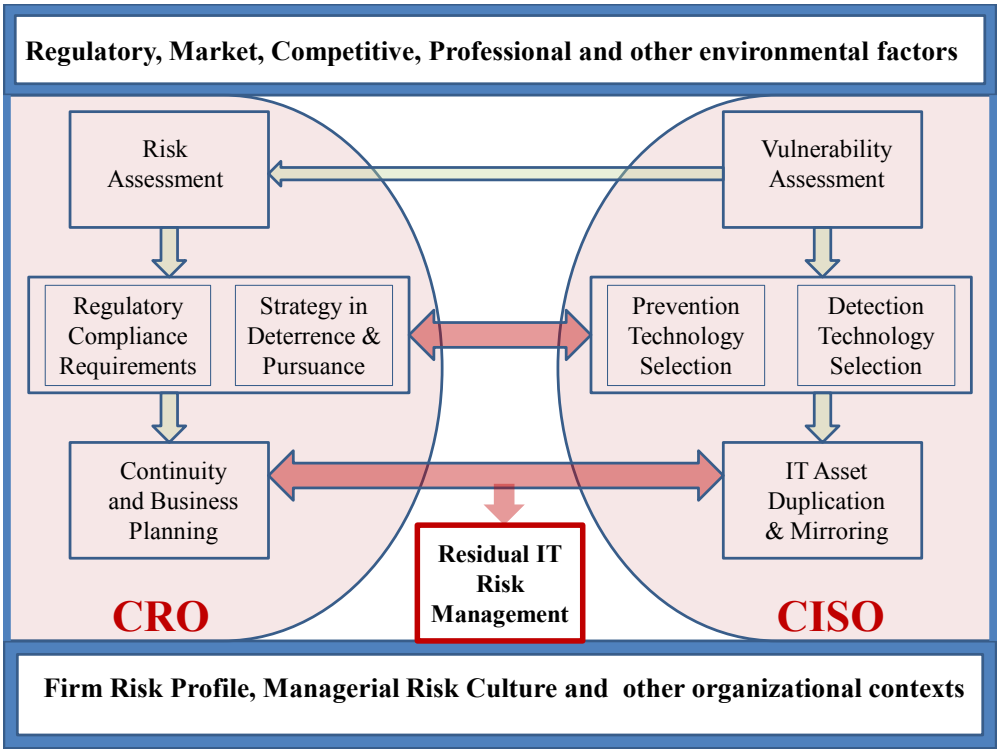

Figure 3. Decision Process towards Organizational Utilization of Cyber Insurance in residual IT security risk management

Second, this model follows the fundamental normative aspects of decision making. Evaluation of options dominates the decision scenario once the vulnerability and risk have been assessed by the respective constituencies. On one hand, the CISO and his team evaluate their options in the security technology selection process leading to available options in mirroring and duplication effort. On the other, the CRO and his group engage in evaluation of strategies in compliance, pursuance, and deterrence - finally leading to the CBP integration efforts. Our model reconciles the evaluation processes by allowing for cross communication and mutual sharing of information across constituencies.

Third, our model supports managerial optimizing behavior of the prescriptive model (Figure 2). Understanding the background and training of the constituencies represented by the CRO and CISO (from the bureaucratic element), the model ensures that both sides posses capability to objectively optimize their selection of options. Since the model imposes validation and communication requirements across the constituencies during the optimizing behavior, the two distinct decision processes must support each other in a timely fashion. Consequently, our model implicitly imposes certain behavioral decision making forces, including that of mildly bounded rationality in search and evaluation of options and also utilization of efficient heuristics while optimizing the evaluated options in an objective fashion.

Fourth, the model incorporates extra-organizational environmental *factors* as superincumbent conditionality for decisions made by the constituencies. There are multiple reasons to justify this element of the model; a) IT security risks are often realized through threat vectors which come from the business networks via the Internet connectivity, b) Data assets may contain individually identifiable information giving rise to privacy concerns - not to talk about the financial and health information, which must comply with the regulatory prescriptions, c) propagated breaches for which the firm may become a conduit, potentially give rise to liability issues defensible in the court of law, and d) correlated IT risks across organizations may govern the access, structuring and pricing of the cyber insurance contracts that the constituencies may attempt to utilize.

Fifth, the constituencies are characterized by, and their decisions are pegged onto the organizational *contexts*. Among others, important considerations that tend to influence risk management decisions in IT security relate to organizational risk profile, managers' risk culture that is supported in their reward and workload structure as well as the admissibility of the decisions in view of the general norms and culture of the organization.

DISCUSSION AND CONCLUDING REMARKS

Beginning with an exhaustive selection of theoretical models from the arena of organizational decision making, we have presented an expansive model of organizational decision process for utilization of cyber insurance as a means to manage residual unmitigated IT security risk. We have initially reviewed the theoretical models and presented the essential elements of these models in interconnected grids. Next, we have reviewed the aspects of IT security research that throw light to the motivations and economic factors for utilization of cyber insurance in an organizational context. Finally, we have combined *those* elemental attributes and characteristics of the theoretical decision models, which resonate in the context of the economic motivations that the IT security research identifies. Our model clearly appreciates the major two constituencies of the decision process by identifying their mutually variegated knowledge and skill sets. In a reconciliatory fashion, the skill sets are then dovetailed in our model through the sequence of a stepwise integrative decision making process.

An attempt to propose one unique model of utilization of cyber insurance for different types of organizations is not without limitations. There are myriad types of organizations in practice, and there are large number of variations in terms of the description and responsibilities of the decision makers in the organizational as well as the IT security risk domains. For example, in certain organizations, the differentiation between the roles and the responsibilities of the CIO and the CISO may be quite blurred. Or for that matter, the CRO may actually be a subordinated decision maker and the CFO takes the major decisions on organizational risks.

This work is at an early stage. The immediate goal of this research is to propose an adequate first-cut model and gather constructive feedback from knowledgeable readers. Once we are able to incorporate these comments in the model and validate it, the resultant decision model can be then be modified for amenability to data collection. Since IT security risk is a sensitive matter for most organizations, our initial foray into the decisional predicaments will likely begin with personal interviews with select managers who are readily approachable given our existing relationships with several local organizations. Later, we plan to use our interview experiences to generate survey questionnaire for data collection from CROs and CISOs of multiple organizations from an extended circle of reach. When adequate meaningful data is collected; the organizational decision process that leads to purchase and utilization of cyber insurance contracts can finally be better understood. It is indeed time that we earnestly investigate and understand why pervasive success of insurance instruments in all risk management arenas is not replicated in the new genre of IT security risks of an organization.

REFERENCES

1. Akdere, M. and Altman, B. (2009). An Organization development framework in decision making: implications for practice. Organization Development Journal, 27, 4, 47-56.
2. Allen, W. (2010). Adopting risk intelligence in today's volatile market. Journal of risk management in financial institution, 4 (1), 12-17.
3. Azizan, N., Samad, M. and Woon, L. (2011) A strategic framework for value enhancing enterprise risk management, journal of global business and economics, 2 (1), 1-26.
4. Bandyopadhyay, T., Mookerjee, V. S., Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. Communications of the ACM 52(11) 68-73.
5. Baer, W. S., Parkinson, A. (2007). Cyberinsurance in IT security management. IEEE Security & Privacy 5(3) 50-56.
6. The Betterley Report: Cyber risk and Privacy Market Survey (2010). (Available at http://betterley.com/samples/CyberRisk10nt.pdf)
7. Bohme, R. (2005). Cyber insurance revisited. Proceedings of the Workshop on the Economics of Information Security. Boston, USA.
8. Bohme, R., Kataria, G. (2006). Models and measures for correlation in cyber insurance. Proceedings of the Workshop on the Economics of Information Security. Boston, USA.
9. Bohme, R., Schwartz, G. (2010). Modeling cyber insurance: towards a unifying framework. Proceedings of the Workshop on the Economics of Information Security. Boston, USA
10. Grandori, A. (1984). A prescriptive contingency view of organizational decision making, Administrative science quarterly, 29, 192-209.
11. Gordon, L. A., Loeb, P. M., Sohail T. (2003). A framework for using insurance for cyber risk management. Communications of the ACM 46(3) 81-85.

12. Kesan, P.J., Majuca, R.P., Yurcik, W. J. (2005). The Economic case for cyber insurance. Securing Privacy in the Internet Age. Stanford University Press, California.
13. Leigh, B. (2010). Avoiding pitfall of enterprise risk management. Journal of risk management in finanacial institution, 4(1), 23-28.
14. Majuca, R. P., Yurcik, W., Kesan, J. P. (2006). The Evolution of cyberinsurance. (Available at http://arxiv.org/ftp/cs/papers/0601/0601020.pdf)
15. Masuch, M. and LaPotin, P. (1989). Beyond garbage cans: An AI Model Of organizational choice, Administrative Science Quarterly, 34, 1, 38-67.
16. McKendrick, J. (2010). The Year ahead in information management: BIG DATA, BIG ISSUES. Database Trends and Applications, 24, 4, 6-9.
17. Mikes, A. (2008). Chief risk officer at crunch time: Compliance champions or business partners. Journal of risk management in financial institution. 2 (1), 7-25.
18. Nutt, P. (1975). Models for decision making in organizations and some contextual variables which stipulate optimal use, Academy of Management Review, 84-98.
19. Ogut H., Raghunathan, S., 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.
20. Puto, C. and Qualls, w. (1989). Organizational climate and decision framing: An integrated approach to analyzing industrial buying decision. Journal of marketing research, 26, 179-192.
21. Pranee, C. (2010). Enterprise risk management. International journal of organizational innovation, 3 (2), 309-337.
22. Stoneburner, G., Goguen A., Feringal A. (2002). Risk management guide for information technology management: recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30.
23. Webster, F. and Wind, Y. (1972). A general model for understanding organizational buying behavior, Journal of marketing, 36, 12-19.
24. Yang, S. (2003). Security and trust management in collaborative computing. PhD dissertation. University of Florida, USA.