Information Security and Risk Management Theories

William Butler

University

Information Security and Risk Management Theory

Leaders use risk management framework to describe an organizations risk management process (Jones, 2007). There are risk management models from which organizational leaders can choose to base their risk management framework upon. All of the risk management models are based on one of several risk management theories. Bojanc (2008) presented a risk management model based on game theory. Fehle (2005) presented a risk management model based and dynamic risk management theory. Li (2007) presented a risk management model based on real option theory.

Bojanc (2008) stated that security solutions are complex (hardware, software, service) to cost and traditional costing methods such as (average rate of return (ARR), payback period (PBP), net present value (NPV), internal rate of return (IRR)) individually are not adequate. The risk management models provide organizational leadership with a framework to evaluate investment options and support decisions. Organizations have limited budgets and resources to invest in controls and protective measures and leaders must make informed decisions. Each of the risk management theories presented by (Bojanc, 2008; Fehle, 2005; Li, 2007) pose a unique set of costs and benefits to the organizational leadership applying them.

Risk Management Theories

Several information risk theories are game theory (Bojanc, 2008) and (Cox, 2009), dynamic risk management theory (Fehle, 2005) and real option theory (Li, 2007). The risk theories are the basis of major risk management models presented by (Bojanc, 2008; Fehle, 2005; Li, 2007). Each risk theory offers organizational leadership a different framework to quantify the investment in controls and to evaluate options or alternatives.

Game Theory

The Bojanc (2008) risk management model concluded with the identification of controls to mitigate identified risk and a framework to quantity investment in controls for leadership investment decisions. Bojanc identified an alternative method which analyzed the optimal information security investment based on game theory. Game theory is based on the interaction between hackers and organizational defenders. Game theory can be applied by researchers to explain situations of intrusions where the hacker has a motive to attack and cause damage to a particular organization.

Cox (2009) stated that risk analysis and game theory are complementary. Researchers use game theory to model the interaction between attackers responding to the actions of defenders (Cox, 2009). The results of such interaction s produce recommendations for the allocation of risk management resources (controls) (Cox, 2009). Cox concluded that the results of game theory analysis are more sensible than those of other risk management methodologies based on competing theories.

Cox (2009) stated that the application of game theory is useful to leader-follower and attacker-defender scenarios. For example, in the attacker-defender scenario the attacker reacts to a move by the defender and each receives an outcome based on the resource allocation of the defender. Possible game theory outcomes in the attacker-defender scenario are killed, injured or combat ineffective (Cox, 2009). The attacker-defender games can be kept simple by allowing the defender to move first then the attacker reacts to the defenders move (Cox, 2009). The results of these moves are evaluated by researchers for defender resource allocation (controls) and effectiveness against the attacker.

Game theory offered the defender the option to evaluate the results derived from different attacker-defender game scenarios and defense strategies (Cox, 2009). The attackers and defenders can make their moves in sequence or simultaneously prior to evaluating the results. Cox (2009) identified the possible move results in a loss matrix (rows and columns representing outcomes). The loss matrix, based on the moves of the attacker and defender, will yield a financial loss incurred by the defender (Cox, 2009). Game theory can be used to improve upon the standard use of the threat (T), vulnerability (V) and consequence (C) probability of occurrence threat model calculation commonly used in the UnitedStates (Cox, 2009).

Cox (2009) identified two objectives of game theory as developing predictive models and optimizing defender decisions. The development of predictive models is useful discover the causal relationship between attacker-defender choices (risk analysis). The second objective deals with optimizing the decision making of defenders by anticipating the best moves of the attacker (game theory). The objectives identified by the (Bojanc & Cox, 2009) provide defenders the means to make more effective allocation of controls. The learner believes that more scholarly research is desired in the application of game theory to risk management to increase the body of knowledge.

Dynamic risk management theory

Fehle (2005) discussed a risk management model based on a dynamic theory versus industry standard static based theory. The Fehle risk management model allowed companies to adjust their strategy to changes in the risk environment or the firm’s cash on hand. Fehle identified the inability of risk management models based on static modeling to adjust to changes in the risk environment or contracts.

Dynamic risk management theory allowed organizations to leverage risk management contracts along a continuous time line (life of the contract) versus in a moment in time (contract initiation or at predetermined set-points) (Fehle, 2005). Models based on dynamic risk management theory allow an organization to evaluate its risk management investment at anytime along the contract timeline. Fehle (2005) stated that the flexibility allowed the organization to increase, decrease or terminate the investment. The ability to conduct dynamic evaluations will yield savings for the organization and make more effective use of the organizations budget.

Some applications of dynamic risk management theory are evaluating the effects of factors such as agency debt and other issues which could affect the leadership decision to terminate or continue a contract (Fehle, 2005). Organizations can dynamically apply current competitive information to the model to make the (continue versus terminate) contract decision (Fehle, 2005). Fehle (2005) stated that the model explored the evaluation of investment options, contract early termination fees and buyout options. The model allowed for the evaluation of associated transaction costs of contract initiation and termination (Fehle, 2005). Fehle did not specifically comment on the existing body of knowledge associated with the dynamic theory, the learner believes that more research is desired to add to the body of knowledge.

Real option theory

Li (2007) identified a risk management model which assisted decision makers in quantifying the economic value of controls. Li proposed a risk management framework based on the real option theory. Real option theory presented a framework for making security investment decisions (Junkui, 2003; Li, 2007). Li presented a step-wise process to make investment decisions: study the scenarios, determine alternatives, develop the Binomial Options Pricing Model (BOPM), determine the best alternative and implement the solution. Li contends that the real option theory method will result in the selection of more cost-effective solutions by decision makers.

Li (2008) defined the real option theory approach as a flexible framework for calculating the value of security controls under uncertain conditions. The real option model allowed practitioners to respond to environmental uncertainty and adjust their strategy to maximize the likelihood of desirable outcomes (Li, 2008). The basis of the real option theory is the practitioner can select or invest in a real option (non-financial asset) at an economic price (Junkui, 2003) and (Li, 2007). The real option theory is a more flexible capital investment evaluation framework as compared to methods such as (ARR, PBP, NPV and IRR) (Li, 2008).

Li (2008) stated that the real option solution valuing model valued options over time versus valuing options in a moment in time such as after a security incident. Li (2008) stated that the real option theory is not only useful for asset valuation but is useful in determining the most value adding option. Li (2008) presented the five step process to make investment decisions: study the scenarios, determine alternatives, develop the Binomial Options Pricing Model (BOPM), determine the best alternative and implement the solution. The possible options are postpone, abandon, scope up or down, outsource, switch, stage and growth (Li, 2008).

(Li, 2008) indicated the application of real game theory in areas such eXtreme programming; commercial off the shelf technology (COTS) based development and project investment analysis. Junkui (2003) proposed combining real options theory combined with decision tree analysis for leaders to make sounder project decisions. The real options theory evaluated cash flows and the dynamic decision tree maps the options presented to decision makers (Junkui, 2003). Li suggested the existence of pure research but also indicated the need for more case studies in real game theory. Based on the availability of peer reviewed research the learner believes that more scholarly research is warranted.

Conclusion

Bojanc (2008) presented a risk management model based on game theory. (Fehle, 2005) presented a risk management model based and dynamic risk management theory. Li (2008) presented a risk management model based on real option theory. Junkui (2003) combined real option theory with decision tree analysis. The role of each risk theory was discussed in terms of how leaders could evaluate investments and decide between competing options. The real option theory provided leaders with a five step framework to economically evaluate investments real-time and determine the alternative with the most value add (Li, 2007).

Fehle (2005) presented dynamic risk management theory which allowed organizational leadership to leverage risk management contracts along a continuous time line (life of the contract) versus in a moment in time (contract initiation or at predetermined set-points). Bojanc (2008) and Cox (2009) identified two objectives of game theory as developing predictive models and optimizing defender decisions. The three theories assist leadership with making basic investment decisions based on control valuation (dollars) and the selection of the best option. Gaming theory pits attacker against defender, dynamic theory allows one to evaluate contracts and options real time and real option theory allows leaders to evaluate the options real time.

The static versus non-static model is critical when discussing the risk posed to the organization through time. Risk posed to the organization at contract award may not remains constant throughout the life of the contract. The application of dynamic theory is complex and required the constant gathering of real time data (Fehle, 2005). Fehle (2005) did recognize the strengths of static based theory in supporting the selection of options based on available information. Organizational leadership must carefully evaluate and select the risk management theory that is right for their risk environment.

References

Bojanc, R., & Jerman-Blažic, B. (2008). An economic modeling approach to information security risk management. International Journal of Information Management, *28* (5) 413-422.

Cox Jr., L. (2009). Game Theory and Risk Analysis. *Risk Analysis: An International Journal*, 29(8), 1062-1068. doi:10.1111/j.1539-6924.2009.01247.x

Fehle, F., & Tsyplakov, S. (2005). Dynamic risk management: Theory and evidence. *Journal of Financial Economics, 78* (1) 3-47.

Jones, A. (2007). A framework for the management of information security risks. *BT Technology Journal*, *25* (1) 30-36.

Junkui Yao, F. J., & Jaafari, A. (2003). Combining real options and decision tree: An integrative approach for project investment decisions and risk management. *Journal of Structured & Project Finance,* 9(3), 53-70. Retrieved from EBSCO*host*.

Li, J., & Su, X. (2007). *Making cost effective security decision with real option thinking.* Retrieved from http://www.idi.ntnu.no/grupper/su/publ/li/icsea07-jingyue.pdf