ACIS 2009 Proceedings

Australasian (ACIS)

12-2009

Assessing Business Value of IT and IS Risk: Security Issues

Brian Cusack
School Mathematics & Computer Science, AUT University, brian.cusack@aut.ac.nz

Assessing Business Value of IT and IS Risk: Security Issues

Brian Cusack
School Mathematics & Computer Science
AUT University
Auckland, New Zealand
brian.cusack@aut.ac.nz

ABSTRACT

Enterprise systems have taken full advantage of Information Technology (IT) and Information Systems (IS) to innovate and to create business value. The principal business value for system is utility. System utility is a complex factor that has many contributing variables and the resultant of business value. The metrics of utility are measures such as up-time, customer satisfaction, and so on. In this paper the concern of security as the protection of information assets is discussed in relation to managing the risk of utility. Risk modeling has come under greater scrutiny since the collapse of global financial markets in 2008. A common criticism is that risk models disengage business layers and foster surrogates that anesthetize prudent virtues within the enterprise system. The discussion in this essay proceeds by elaborating current risk modeling trends and concludes by promoting an awareness of the changing scope and expectations for effective business security risk analysis.

Keywords

IT & IS Security, Risk, Modeling, Utility, Business Value

INTRODUCTION

The collapse of global financial markets in 2008 has made visible the modeling and assumptions of financial risk management. The key problem area identified is the relationship between business and the risk models. The systemic collapse of markets has highlighted weaknesses in modeling the external system environment and the inability of models to deliver relevant controls for the management of the internal system environment. Key criticisms are targeted towards the role of computer generated risk modeling systems and audit within the information system. "Skepticism about the complicated, computer-driven modeling systems that many financial giants rely on to minimize risk has grown. 'All I can say is, beware of geeks...bearing formulas.' " (Gordon, 2008, p.3). The intermediation of enterprise system goals and objectives by models is consistent with the van Bon (2004) architecture for enterprise systems. The architecture for enterprise systems has an abstract layer, an intermediating layer for models and a peripheral layer of empirical realities. These layers correspond respectively with roles for Boards and their agents (the C layer agency), managers and implementers who are involved in a real world. The van Bon architecture for an enterprise system highlights the differentiation within system by layering but also dynamic issues regarding the governance, the management and control of system.

Information systems and information technology are intimately embedded within business enterprise architecture as the enabler of business process. The van Bon (2004) decomposition of IS to IT elemental mapping encapsulates the relationship of IT to IS as a Venn diagram of two intersecting but distinct circles. Discussions of enterprise system attributes such as risk and security consequently involve the interaction of variables (such as applications, hardware and so on) and the mutual independence of others (such as documents, people and so on). In this paper an assumption is made that IT and IS comply with the van Bon (2004) definition and that the debate necessarily includes the ambiguity of two mutually dependant conceptual frameworks. To address the problem of risk assessment of business system utility value a number of other assumptions are also made. It is assumed that risk is defined as the degree of uncertainty about an event, that security is defined as the protection of enterprise assets and that security has a mitigating relationship with risk.

This paper is structured to provide definition of the objects and then to explore specific relationships within a generic enterprise system. The first discussion section reviews the current state of financial risk modeling to identify weaknesses in the modeling theory that may have implications for other system modeling applications. The second discussion section draws out the implications of current financial risk modeling for mitigation activities in an increasingly electronic business world. The third discussion section reviews system utility value in relation to system risk. Finally the learning from these reviews is applied to the systems utility value model (Varadharajan, 2000) for mobile business to recommend improvements.

LEARNING FROM FINANCIAL MODELLING DILEMMAS

The potential for an entire system to collapse and thereby deliver unintended outcomes is a scenario that risk assessors evaluate. In regard to the 2008 collapse of financial markets this is one possible outcome associated with risk modeling and the application of risk management software that presupposes a degree of uncertainty about future net returns. According to Manganelli & Engle (2001), "The increased volatility of financial markets during the last decade has induced researchers, practitioners and regulators to design and develop more sophisticated risk management tools" (p. 5). One of the principal constructs has been the value at risk models (VaR) that reduce conceptual complexity to a single numerical output of probability. These tools work on the philosophy that the calculation of the maximum potential loss in a portfolio schema is the assessable risk that best reflects system risk to market. The resultant numerical outputs are used for both regulatory and managerial decision-making. The enterprise system impact of the calculation is to deliver estimators that determine the outcome of decisions regarding future returns. Finance intuitions are vulnerable to many risks (including credit, operational, liquidity, market and so on). VaR is a preferred indicator as it estimates the maximum economic loss that market volatility may cause portfolios. The implication is for the allocation of capital, stability and the profitability of finance institutions. In the market events of 2008 clearly the VaR indicator proved inadequate to prevent systemic collapse. The definition of VaR suggests that systemic collapse is an unintended outcome and that VaR was designed to minimize the chance of the occurrence. A fair judgment would be that VaR underestimated residual risk, it did not properly assess underlying risk, and/or the decision-makers responsible had dis-interested complicity. In simple terms the theory and software risk management tool were only effective as a forecasting tool for managerial control within a conditioned set of parameters.

An evaluation of VaR is a useful analysis to illustrate the limits of risk theory and the potential for unintended outcomes in practice. In the following section the effect of risk mitigation strategies (eg. System Security implementation) is discussed to moderate the propositions developed in this paragraph. The two matters of concern with VaR calculation are the subjective judgments a user can make and the variation that is apparent when different approaches are taken to calculating VaR. The calculation of VaR varies by selection of methodology and editor choices. Mangenelli & Engle (2001) point out that in empirical studies of different approaches to calculating VaR to the same portfolio there is a variation of up to 14 times between the calculations. The theory models underlying VaR calculation can be loosely grouped into parametric, non-parametric and hybrids that are semi-parametric. All models adopt specific assumptions, math models and quantitative techniques, and aim to create quasi-stable data sets in order to generate the VaR estimator. The guiding framework is that of statistics and the underlying assumptions are both consistent and limited by the framework. As a consequence the question of relevance to the empirical world arises and the problem of potential loss in the real world using VaR as a risk indicator. Each approach to calculation has particular assumptions and hence strengths weaknesses and particular conditions under which the estimator works best. For example in the semi-parametric method of extreme value the upper and lower Hill estimators are derived subjectively as there is no current statistical method and in the parametric methods data are conditioned by distribution choices. Other researchers (such as Artzner, 1999) have been skeptical of the generality of VaR applicability in the real world and proposed alternative risk models that use VaR estimators as the threshold for other risk models such as the Expected Shortfall model.

The general adoption by finance institutions and regulators of VaR for risk management emphasizes a dilemma. The assessment and estimation tools for risk have theoretical limitations and yet the market opportunity and the drive to create profit demand proactive decision-making. The decision-maker is thrown back into a simple cost – benefit trade-off situation. On one horn of the dilemma is the opportunity for benefit and on the other the perceived cost (risk) of the opportunity. Risk management tools offer mitigation comfort to the decision-maker once the limitations are accepted. Similarly security strategies provide mitigation but not complete solutions. In the worst case scenario risk decision support tools can enhance the appetite for risk and insulate a manager from relevant data that falls outside of the conditioned sets. In this way the system becomes self destructive and over accumulated periods of time based data processing there is the potential for systemic collapse. The analysis of VaR also shows that collusion between estimations and estimators is an internal system weakness and the acceptance of the VaR metric by both institutions and regulators as a principal metric is an external system weakness. The embedded assumptions of models bring theoretical limitations on the material applicability of a model but there is often little guidance for compliant users of errant systems.

EBUSINESS SECURITY RISK MITIGATION CHALLENGES

The use of theoretical models in practice is a process that is guided by conditions and exceptions. IS and IT security modelling is embedded in contexts that undergo continuous structural change. System security concerns the protection of enterprise assets that are both material (hardware) and abstract (informational), and concerns all enterprise processes (Anderson, 2001). Underlying the security requirements is the calculation of costs and benefits (CBA) and the associated dilemma. The economic model provides a limit to systems security (Eddie, 2002, Oz, 2004, p. 694) and that has implications for degrees of protection. In addition the context in which enterprise systems exist changes in ways that a requirement, such as security, also changes. The questions of what is worth securing?, and at what cost? constantly undergoes revision. Not surprisingly the adoption of enterprise security models has also undergone change. The relationship between security modeling and risk modeling has converged to a point where security standards are described as "risk based" (see ISO/IEC/JTC1 27000 series). The assessment of system risk provides a fundamental foundation on which security decisions can be based. Whether the cost benefit analysis engages utility, alignment or financial metrics risk assessment has different outcomes from different security modeling systems. In an enterprise system complexity arises when security risk is calculated for sub-systems and the interaction between systems. In an online ebusiness system for example it is not feasible to lock down all the ports in an epayment sub system to ensure 100% protection of information (and hence preventing beneficial transactions) nor to use protection procedures that consume excessive resources (and hence frustrate the customer who may cancel the transaction). Rather a compromise is calculated where utility, alignment and financial benefits are maximized against loss and potential loss. Such security architecture has evaluated IT and IS security risk against and for business value compliance.

The upsurge and continued use of the Internet as a medium for doing business has exacerbated ontological problems in the fundamentally different worlds of business, and IT. eBusiness has focused on the strategic co-ordination of business objectives, customer-centric management, and the exploitation of technology. In contrast to the eCommerce model, eBusiness has shifted the control of business processes from IT experts and to business managers and executives (Kalatoa & Robinson, 2001). The business leadership of all enterprise processes is a shift in emphasis from technologies shaping business purposes and technical developers determining business possibilities. The shift is to the retention of the control of business processes by the business for business purposes. The IT & IS are the enabler of business objectives. The eBusiness environment consequently presents a new set of challenges for enterprise security. Specifically the measured alignment of business objectives and IT/IS objectives is a critical condition for system security. For example the best formed practices for protecting information and system in the IT world may be unacceptably slow, expensive or customer frustrating to the business world. Similarly the assumptions made in the design of eBusinesses that may not hold in practice. For example up time, efficiencies and application performances that have best case representation in the business world may have worst case delivery in the IT/IS world.

A more vexing problem is the potential for the semantic decoupling of IT/IS objectives from the business objectives (and visa versa). In this instance the execution of an objective lapses into interpretative alternatives that are framed by the preferred ontology. Consequently the potential for slippage in meaning is high and the effect of execution ambiguous. The consequences of slippage for securing IT and IS are far reaching. The problem of aligning business objectives with those of IT (and visa versa) have been well developed in the literature. Various strategies and tactics are advocated (for example the balanced score card (Kaplan & Norton, 1996); matching (Van Grembergen & De Haes, 2009), and so on) to address the alignment problem. Current modelling of eBusiness system security is caught in a tension of IT requirements and business demands. The move of system security towards customer centred enterprise development requires a rethinking of security service supply against business demand. Significant challenges arise in negotiating a seamless, effective security web to minimise the likelihood of business process vulnerability in unauthorised uses, sabotage, or criminal activity. The reworking of the issue views negotiation between the ontologies as being critical to progress in eBusiness system security. Imposition by force of alignment mandates or abdication of responsibility in cultural constructs falls short of achieving the level of confidence a caring customer may trust. Considerable trust has been lost through the underperformance of current IT and Business system security models.

The alignment of IT and business objectives is a problematic that invites debate. The empirical work of van Grembergen & de Haas (2009) shows that alignment of business strategy and IT strategy will lead to the best business performance. It is assumed that objectives (measurables) can be treated in some way so that one measure shares contingencies with another. In practice, however, metrics are the result of theoretical undertakings that have shaped and produced a measure in keeping with a particular ontology. Van Grembergen and de Haas (2009) discuss five measurement techniques that may be used to quantify the alignment relationship. Each metric system contributes a perspective view on the relationship and measures for decision making. As in other literature (for example, ITGI, 2005) priority is given to the business objectives and it is assumed the IT / IS objectives are formulated in keeping with the business priority. Reconciliation at the abstract layer remains a problem for effective alignment and prioritising the business objective is a partial solution. Strategic alignment has a medium impact on IT effectiveness. The implication again is that IT / IS can benefit from aligning the objectives with the business objectives. A method for managing the process is termed the cascading balanced score card (Van Grembergen, 2002). In this process technology, operational excellence, business contexts, the customer, and future orientations, are integrated into a hybrid set of control objectives (p.2). Objectives in this sense contain considerations of the different ontologies and are internally consistent and externally coherent with the business strategic purposes. A more general method proposes cascading scorecards that cluster variables consistent with the different eBusiness stakeholder interests for objective alignment. The alignment is achieved by exercising the Governance capability of risk management and adopting the assumption (a weaker position than case 1) that sufficient financial performance gain equates with sufficient security.

Security in the eBusiness context is distributed across different stakeholders (principally the customer, the aggregator, and the supplier), all of whom have different expectations for protection. The customer expects privacy and protection from fraud but at the same time speed of transaction and an accurate match in expectation and experience. The aggregator also requires protection from fraud (in this instance customer fraud) and the non disclosure of business intelligences. The supplier has a greater concern with the material protection of goods and service delivery. Together the three principal parties in eBusiness agree formally and informally on a trust model in which they may do business. Traditionally security has been a loose fit policy folder that that has impacted variably on the different entities within an enterprise system. However the eBusiness scenario requires a tight fit of security and policy to assure a common sense of trust. Tight fit lessens the potential for violation between entities and manages the IT/IS supply intensity in the eBusiness environment.

The implications of the eBusiness paradigm are far reaching for enterprise design and the subsequent system security architectures. The potential for the customer to shape the business and to redefine businesses security expectations also requires the development of models that can better bridge the gaps between current dominant ontologies. New integrative models are required for seamless and effective security webs that minimize the likelihood of business process vulnerability. Consideration of the fundamental building blocks of system as well as participant motivations and intentions, underpin aligned objectives that can deliver the common sense of trust. Integrative models that bridge the divides in previous enterprise model approaches to security can deal effectively with specific risks within the preferred working frameworks. Other attempts to reconcile differences between the frameworks are many and varied, and in general fail to adequately redress risks introduced between the ontologies. The IT Governance approach relies on alignment as the key linking mechanism, the Business approach attempts to generalise by putting unknowns into black boxes, and the IT approach has promoted discrete layered protective models that do little to cue customers into freer transacting. Attempts to introduce security culture have over extended beliefs about trust and treated key security objects descriptively. What remains is a broad range of partial solutions to a problem that requires further understanding if system security may be redressed within the eBusiness paradigm.

MBUSINESS SYSTEM UTILITY RISK CHALLENGES

System utility is a complex factor that may be reduced to a single numerical representation of system performance. Similar to the VaR estimator utility measures provide metric value across the divides of enterprise culture for decision-makers. In the case of mobile business (mBusiness) applications are characterized by their high degrees of uncertainty about the identity and intention of the interacting parties (Varadharajan, 2000). Risk assessment hence must consider trust (and not just security) as a mitigating factor. Other IT constraints such as bandwidth play a critical role in system risk mitigation possibilities. The uncertainty element in the interactions and the restricted bandwidth resource can often violate the fundamental assumptions of a conventional security management system. Traditionally binary models (for example Grant and Deny) have been used to allocate permissions and to resource system use. However these models become ineffective and inefficient in mobile business applications. A more recent innovation has been to separate the security and trust models and then to enhance the assessment of beneficial actions post authorization (Cusack & Ling, 2007). These innovations are not with out objection but provide sets of partial solutions to the problem of systems utility in constrained conditions. Trust authorization enhanced with risk management produces better systems utility across different levels of security violation (see figure1). The approach possesses the ability to use trust evaluation to not only "weed out" malicious entities, but also allocate appropriate access permissions to the benevolent entities according to the risk levels. The development and application of the risk management tools is still a challenge for mobile network operators. An effective risk management tool is able to 'weed out' high percentages of potential threats and to learn from past experiences. Learning about agent behaviors is one factor missing from traditional system security models (Lee & Turban, 2001).

Traditionally a binary trust model can provide a set of benefits that enhance mobile system security. It enables trust to be extracted from the security mechanism; hence it provides the opportunity to clarify the actual trust requirements of the underlying security mechanisms. These are ultimately used to make more effective security decisions and hence to determine and control the risk involved (Oplinger, 1998). It enables categorization of trust related security mechanisms using the binary trust notion, which can be applied to process and manage the binary trust information. This enables effective interaction with the underlying security model. It can enable trust management and the integration of trust with the underlying security mechanisms for security performance enhancement – by feeding the trust decisions back to the underlying security mechanisms (Youngrove, 2001).

However binary trust models are inherently hierarchical and static hence have range of drawbacks when applied to distributed systems. These include the *Security Assumption Violatio*n where the mobile agent computing model violates several basic security assumptions used by the underlying conventional security models (i.e. the assumptions of principal identity and program intentions that hinder the effectiveness of the binary trust model which relies on the underlying security models). Also the draw back of *Lack of Learning* where underlying security mechanisms have been designed to enforce various security policies in a relative static manner. They lack the capability of handling the learning task at the runtime, causing security performance to suffer due to inconsistency and time-delay in system's response to malicious behaviors. The system is left vulnerable to repetitive attacks. The *Rigid Model Structure* where since the binary trust model is inherently a hierarchical structure due to its dependence on the underlying security system making it difficult to scale up in mobile agent systems. This typically operates in an open network environment characterized by the dynamic changes of both the presence of the entities and their behavior. In addition, the lack of ability to deal with such dynamic aspects introduces uncertainties into the security decisions hence hindering the security performance. *Lack of feedback control* is the inability to process the existing system information regarding behavior and leaves the system vulnerable yet again to repetitive attacks. The weakness can be traced back to the lack of feedback control in the conventional security models (delete for review, 2007).

A new approach has been proposed that takes the concept of 'mobile agent' to be central for distributed computing. The proposal is to have mobile agents as autonomous programs that route and migrate through a network. A single agent interacts with hosts to accomplish tasks on behalf of their owners. The approach offers cost effective features such as reducing the network load, executing asynchronously and autonomously, and adapting dynamically. Conceptually the mobile agent paradigm is designed to service eBusiness applications and mBusiness architectures. The evolution of comprehensive security solutions in these contexts is reliant on the new distributed computing model and the changes it introduces. The central problem is that the definition of mobile agency violates many of the foundations in traditional security approaches. The result is that there are many proposals for system protection but in practice each has weaknesses. Attempts to protect agents and hosts through different mechanisms fall down when traditional security techniques are applied. For example, the assumptions of program identity and intention are found to be violated by mobility and open network operating environments. It is difficult to provide robust protection within the context of security mechanisms but consideration of trust and risk enhance protective capability (Siponen, 2000).

The conceptual trust enhanced security model maximizes system utility as shown in Figure 1. This architecture incorporates a novel trust model that captures risk in various security related trust relationships of a mobile agent system, and provides mechanisms for trust evaluation and trust update to aid accurate trust decisions which are in turn integrated into security decision making. It consists of four blocks or modules that inter-relate to deliver the best utility when a system is under scrutiny for information protection. The four component blocks are conceptualised to span the requirements for information protection when mobile agents are being used in a distributed system. The four component blocks are the trust model, authorization block, the interaction module and the utility response variable. The trust model manages the trust information in the system and makes trust decisions based on risk management data. The authorization block performs the standard authorization process also based on risk consideration data. The interaction component manages the mapping between behavioural evidences and the resulting updated trust value. The utility block is used to calculate the system utility at the end of each interaction. The tactic is to use trust information, managed by the trust model with risk management consideration, to refine the authorization decisions. In practice malicious entities are identified through past and current experiences and removed so that benevolent entities will be given appropriate access permissions according to the risk levels. The interactions are controlled with the benevolent entity behaviour. The authorization performance and the system utility are hence continuously improved by reducing risk and enhancing utility. (Note the innovation in the 2007 publication was to align the utility of the model with business utility value. This is a different concept than the IT system utility published in 2000).

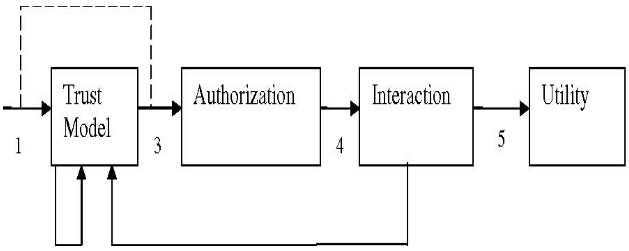

Figure 1. Trust Enhanced Risk in Mobile Business Security (Cusack & Ling, 2007)

RISK SECURITY ARCHITECTURE

The previous two sections have reviewed challenges for risk mitigation in the electronic and mobile business environments. A working solution has been portrayed as three interrelated models; one for security, one for trust and one for risk. In figure 1 these models are mapped together to show the business deliverable, that of system utility. Underpinning these propositions has been a review of the changing landscape of enterprise system models. The shift in eBusiness contexts from IT/IS dominance over business security modelling has lead to a compromise of partial solutions that are termed hybrid models. These models are characterised by negotiated principles, customer centric utility value and the prioritising of business objectives over IT/IS objectives. In the mBusiness environment innovations have allowed the review of agent interactions with a system to forecast beneficial interaction and to allocate resources to the agent accordingly. Risk models inform the trust model and allow for revision of resources by the authorisation module. Such real time system protection is an ideal in a pragmatic world and is the result of movements in traditional security models to incorporate elements of other models. The hybrid environment appears as an ideal solution and yet introduces a new set of system security issues.

Current research has provided few formal guidelines on how the risk can be integrated with the underlying security system, whereas utility has been recognized as an important factor in security system development. The general view in the literature is that every security question is an economical question concerning the utility of the underlying system. For example, it is easy to show that in a mobile agent based e-business system, both the protection of agents and hosts have a direct impact on the utility. Attacks on a host by malicious agents will cause loss of commercially sensitive data such as customer's private information, downtime to the system, loss of customers, which will eventually be counted as a utility loss. Attacks on agents will result in similar consequences that will also lead to the lost of utility. Thus utility maximization is an important issue in the design of a secure distributed system that seeks to gain maximum economic benefits from the underlying system. Risk management has always been an important aspect of security research and articulated as a limit. The risk of potential security breaches is a measure business managers require and models to accurately forecast the risk are a necessity for control in a business enterprise system. The development of these models has often been from a financial perspective and based on assumptions that tend to generalize the risk into continuums when often discrete risks may have greater impact on financial measures and the fatal issue of business continuity. Risk modeling is hence a complex undertaking and one model developed from one perspective may not maximize the utility of a system.

Hybrid risk modelling accepts that many partial solutions to be managed by an intelligent agent are often more effective than traditional security models and strategies. The intelligent agent is expected to operate in a managerial framework of controls that mitigate but don't necessarily extinguish the risk of non beneficial agent behaviour. Consequently the type of economic model for risk management appears similar to a control chart for multiple processes. The trust enhanced security framework leverages system behavioral evidences and the model integrates risk management to make optimized security decisions. In the eBusiness environment viewing risk through the eyes of a customer changes the scope of performances expected of a business and the role risk plays in transaction decisions. The modelling of risks suggests that perception of trustworthiness builds on the properties of merchant perceptions, medium perception, and context perception. Furthermore, customers seek cues that indicate the merchant's ability, integrity, and benevolence, the medium's technical competence, reliability, and utility, and, the context's certification and security (Mitchelle, 1999, Lim, 2000). Risk is hence mitigated by a basket of mediating variables (ie. The agents are persuaded towards beneficial interaction with the system) and the exploitation of the underlying technologies maximised.

The inclusion of risk management as a dependant variable in the security architecture has provided a working basis for continuous assessment of potential threats – including agents that have already been authorised. The innovation has introduced a dynamic approach to traditionally static and hierarchical models for systems protection. The utility gain obtained from honest and competent transactions from the trusted entities of the system are to be maximised while assessing the potential of threat. This risk can be defined as the possible utility loss due to the potential security policy violations by malicious behaviours of untrustworthy entities in the system. Through the enforcement of the security decisions from the proposed model the knowledge on trust relationships is leveraged to guide security decisions with risk management (allocating a particular risk level for a given interaction). This enables the underlying application to gain maximum economical benefits while keeping the security risk at a defined level.

ASSESSING THE BUSINESS VALUE OF RISK

The business utility of a system is a prime economic metric that translates across ontologies and interprets meaningfully in the IT/IS environment. However financial and alignment metrics also impact in the business assessment of risk. An economic model for Business performance is a tradeoff of utility, finance and alignment. Risk estimation considers the underlying assumptions embedded in these three constructs and the potential for mitigation within the context of system theory. The natural assumption is that risk (volatility) is inherent within any system and the reduction of risk is an economic problem. The implication is that risk is always apparent in a system and therefore must have an economic value for the system. In the case of a business enterprise system the continuous assessment of risk value may be reported as being more or less in quantity and calculated with the three critical economic metrics of utility, finance, and alignment. In this sense risk allocation within a system is similar to the allocation a particular number of units within a forecasting budget (IEEE, 2005).

Economic models for process control are long established in the literature (eg. Process control charts). The design of economic models starts with a set of assumptions about the behavior of processes, the characteristics of the processes, limits, and estimated parameters with respect to limits or external benchmarks. A further assumption is made that the processes are to be in control and that risk can be measured as the variation from the target value for the process. In the case of system security process the economic model assumes volatility about any given target value (Montgomery, 2007). The volatility is critical and it would be assumed in a security system that 100% of the volatility is associated with chance causes. However, in many instances assignable causes (ie. social engineering fraud, new scams, and so on) occur and management intervention is required. In the discussion above the hybrid security models for both process and management were evaluated to be useful for controlling process-failure mechanism volatility. Hybrid models in this sense were an attempt to mitigate risk and yet introduced a new set of parameters for economic evaluation (Weill, 2006).

Security measures alone are not sufficient to protect systems from malicious behaviors. The new trend is to use economical models (mainly game-theoretic models) to mitigate the risk introduced by malicious behaviors in the security context. However, often there is a lack of integration of the risk and the security models, and the effectiveness of economical models is diminished. For example, discrete decisions by security mechanisms, such as the authorization decisions in a system, can have a direct impact on the utility of the underlying system (similar arguments apply to alignment and finance risk). Risk management can be applied to maximize the utility of the underlying systems by informing the trust model to increment levels of resource allocation in the security model. In this way risk management in hybrid environments is a continuous action that compensates for potential threat by updating threat status and assigning approximate estimates for security resource allocation to status. The cost of the actions is accounted in control models. If the volatility around any target value is set to zero the costs soar out of control. Hence prudent risk management quantifies risk in unit allocations of cost and trades the cost with system benefits.

Security policy violations by malicious behaviors in a hybrid entity system are incurred by trusted agents. The risk management system is designed to continuously monitor agent behavior and to pass to the trust module updated assessments of all agent behaviors. The mapping between the risk allocation and the resultant system utility, alignment, and financial indicators is quantifiable, and provides units for assessing the business value of risk. An appropriate risk allocation can be specified if the maximum economic benefit of the underlying system is to be gained at minimal cost. The control chart can provide a continuous estimate of risk that translates into units of business value. Usually risk value is treated as an independent input parameter. By making system risk a dependent variable the micro analysis of volatility is possible and the cost calculable. The business value of security risk is hence established.

CONCLUSION

The illustration of financial market collapse in September 2008 provides learning about the limitation of system models and the intermediation effect of models in organizations. The common criticism that risk models disengage business layers and foster surrogates that anesthetize prudent virtues within the enterprise system, has been addressed by deconstructing enterprise system and enterprise decision support models to show how this may occur. Furthermore issues and problems that arise as challenges to effective risk mitigation have been discussed. The paper has concluded by reviewing and describing the moves in enterprise security architecture that compensate for electronic and mobile business expectations. The utility value solution that integrates security trust and risk models has been elaborated. The paper concludes with an evaluation of potentials for assessing the business value of risk. The solutions discussed are partial solutions to a systems economic problem that is a costly dilemma.

REFERENCES

Anderson, R. (2001). *Security Engineering*. Wiley: New York.

Artzner, (1999). “Coherent Measures of Risk”. *RISK* (10:11), pp 68-71.

Campbell, B., Kay, R., & Avison, D. (2005). "Strategic Alignment: A practitioner's Perspective", *Journal of Enterprise Information Management*. (18:5/6) pp 653-661.

Chai, P., Ruighaver, A. & Maynard, S. (2002). "Understanding Organisational Security", *Proceedings of the 6th Asian Pacific Conference on Information Systems*, pp 731-740.

Chaudhury, A. & Kuilboer, J. (2002). eBusiness and eCommerce Infrastructure. McGraw Hill: New York.

Cusack, B. & Ling, C. (2007). "Optimizing Information Security in Mobile Environments: Using Risk Management Tools". Proceedings of the CACS International Conference, September, Auckland, New Zealand.

Edde, D. (2002). *Security Complete*. Sybex: CA..

Forno, R., & Baklarz, R. (1999). *The Art of Information Warfare*. New York: Universal Publishers.

Gollman, D. (1999). *Computer Security*. John Wiley and Sons:NY.

Gordon, G. (2008). http://online.wsj.com/article/SB122538449722784635.html. Downloaded 22.06.09.

Hazelwood, (2006). "*Defence In depth: An Information Assurance Strategy for the enterprise*". http://www.sdsc.edu Download 10.09.08.

IEEE, editor. *IEEE Security and Privacy*, volume 3 of *Economics of Information Security*. IEEE Computer Society, 2005.

ITGI – 2005. Aligning CobiT ITIL ISO 17799 for Business Benefit. http://www.isaca.org/

Kalakota, R. & Robinson, M. (2001). e-Business Road Map for Success (2nd Ed.), Addison-Wesley: New York.

Kaplan, R. & Norton, D. (1996). "Using the Balanced Score Card as a Strategic Management System", *Harvard Business Review*, Jan. – Feb. pp 75-85.

Lee, M. & Turban, E. (2001). "A trust Model for Consumer Internet Shopping", *International Journal of Electronic Commerce*, (6:1), pp 75-91.

Lim, N. (2002). "Classification of Consumer's Perceived Risk: Sources versus Consequences", *Proceedings of the 6th Asian Pacific Conference on Information Systems*, pp 540-554.

Manganelli, S., Engle, R. (2001). "*Value at Risk models*". European Central Bank: Brussels.

Mitchelle, V. (1999). "Consumer Perceived Risk: Conceptualisations and Models", *European Journal of Marketing*, (33:1/2), pp 163-195.

Montgomery, D. (2007). Introduction to Statistical Quality Control. Wiley: NY.

Oppliger, R. (1998). Security at the Internet Layer. *Computer,*(31), pp 43-47.

Oz, E. (2004). Management Information Systems. Thompson:NY.

Seymore, B. & Kabay, M. (2002). *Computer Security Handbook*. (4th ed.). Wiley: NY.

Siponen, M. (2000). "A Conceptual Foundation for Organisational Information Security Awareness", *Information Management and Computer Security Journal*, (8:1), pp 31 – 41.

Straub D., & Welke, R. (1998). "Coping with Systems Risk: Security Planning Models for Management Decision Making". *MIS Quarterly*, (22:4), pp 441 – 464.

van Bon, J. (2004). *IT Governance a Pocket Guide Based on CobiT.*. Netherlands: Van Haren Publishing.

van Bon, J. (2007). *IT Service Management, an Introduction Based on ITIL*. Netherlands: Van Haren Publishing.

Van Grembergen, (2002). *The Balanced Score Card*, IT Governance Institute: Chicago.

Van Grembergen, W. & De Haes, S. (2009). *Enterprise Governance of IT*. Springer: NY.

Varadharajan, V. (2000). Security enhanced mobile agents. Proceedings of the 7th ACM Conference on Computer and Communication Security.

Von Solms, B, & von Solms, R., (2005). "From Information Security to Business Security". *Computer and Security Journal*, Elsevier, 272-279.

Weill, P., & Aral, S. (2006). "Generating Premium Returns on Your IT Investments". *MIT Sloan Management Review,* (47:2), pp 39-51.

Younglove, R. (2001). "IP security: what makes it work?", *Computing & Control Engineering Journal*, (12).

COPYRIGHT