Abstract

A NOVEL FRAMEWORK FOR MITIGATING e-RISK THROUGH INSURANCE

Arunabha Mukhopadhyay

“New” economy organizations are solely reliant on the Internet for their top lines. The “old” economy organizations use Internet as an effective distribution channel, to reduce costs and enhance bottom lines. The critical success factors for these organizations are secure, robust, scalable communication channels and creation of a sense of trust in the minds of their users (customers and suppliers). But, these communication channels are prone to threats like snooping and sniffing and other malicious attacks.

E-risk is defined as a probability of a malicious electronic event that cause disruption of business and monetary loss. We define e-risk as a collection of four risks namely (i) Conventional risk: hardware failure, software failure and data loss, (ii) Internet related risks: Virus or worm attack, Denial of service, graffiti, identity theft, cyber extortion, phishing.(iii) risk of wireless media : PDAs, mobile phones etc are used to hack organizational databases and (iv) legal risks: non compliance to legal standards like BS7799, COBIT etc. Hackers and disgruntled employees, exploit both the security and application level vulnerabilities to break into organizational databases and gather confidential customer information (like pin numbers of credit cards from a bank). E-risk disasters have direct impact on the bottom line of the organization, in terms of loss of opportunity cost. The organization’s brand equity and market capitalization too are adversely impacted.

To secure these online transactions, and to ensure confidentiality, integrity and availability of information, organizations spend millions of dollars on perimeter and core security like firewalls, anti-virus, intrusion detection systems, digital signature and encryption. They even resort to building in redundancy of servers and security appliances into their systems. Uses of stringent technology policies (such as authentication and authorization rules) are common. Nonetheless, a new virus or a clever hacker can easily compromise these deterrents, resulting in losses to the tune of millions of dollars annually.

To cope up with the problem, of security management and securing e-commerce, this study proposes, to invest in e-risk insurance products as a viable complementary method (over and above the perimeter security appliances). E-risk insurance would help reduce the financial losses of e-business organizations, in lieu of payment of a premium. It would also give a competitive advantage to the e-business organization in terms of its strategic positioning. The e-risk insured organization would be differentiated from its competitors in terms of its security management. This would help create a greater user base (customers and suppliers), as it would create a sense of trust in the minds of its users. This in turn would lead to greater economic value for the organization vis-à-vis its competitor.

To substantiate this proposition of e-risk insurance, this study is broadly addresses the following issues, namely: (i) e-vulnerability assessment and e-risk quantification, (ii) preferential premium computation for online business organizations, (ii) a tiered framework for e-risk mitigation for e-risk insurance companies and (iii) strategies for funded self-insurance of e-risk through options, for online business organizations.

We propose an e-vulnerability metric based on two parameters namely, (i) technological issues and (ii) organizational issues. This provides a basic understanding about the level of the level of e-vulnerability present in an online business organization. If the e-vulnerability is an online business organization is above a threshold, we propose immediate e-risk mitigation. We have developed a Copula based Bayesian Belief Network for quantifying the e-risk of an online business organization. The basic premise of this model lies on the fact that information security failure in an organization occurred due to either a technological failure (like firewall, proxy servers, anti virus) or to a security policy failure. The basic input to the model are (i) a causal diagram showing the problems of a security breach, (ii) the log data of security appliances (like firewall, proxy servers, anti virus) and (iii) correlation existing amongst the nodes comprising the causal diagram. The output from this model is a joint probability table comprising of the nodes of the causal diagram. The model is used to arrive at the frequency (or probability) of loss for each of the causal variables (like firewall, proxy servers, anti virus or policy failure), that could lead to a security breach. The claim distribution for each of the causal variables is assumed. The *loss expectancy* for each of the causal variables is the product of frequency of loss times the claim distribution. An e-business organization would use the loss expectancy as the baseline to understand its vulnerability. Similarly, an insurance company would use this loss expectancy to set the premium for e-insurance product.

This study develops a utility based preferential pricing model for e-insurance product. This model takes as input the expected loss so computed and the risk profile (i.e., averse, neutral and seeker) of its customers and outputs preferential premium for an e-business organization. The launch of the e-insurance product would be a competitive advantage for an insurance company. An insurance company providing e-insurance would be distinctly differentiated vis-à-vis its competitors.

We have developed a framework of e-risk sharing amongst e-risk insurance companies. This thesis focuses on developing a business model for the insurance companies, by which they can mitigate the e-risk that they accept and does not go ruin. The study proposes that multiple insurance companies share the e-risk amongst themselves. This is based on the premise that sharing of e-risk amongst multiple tiers reduces the variance of e-risk. The framework proposes a framework, to minimize loss of data in case an eventuality strikes a member in the chain. It is proposed that a canonical form of the data would be stored at each tier, with the help of Internet Data Center's (IDC). So, as a contingency measure, some amount of data could be retrieved and handed over to the customer, in addition to indemnification for the loss, in monetary terms. We have developed two models, to find out the optimal number of layers into which the e-risk should be split. The first is a variance reduction model and the second is a return on capital technique. In the former model the variance of the e-risk is sliced till there is sufficient reduction in variance. In the latter model, the mean e-risk is sliced till the net cash flow exceeds the return of capital. Net cash flow is arrived at by computing the amount of premium received for retaining e-risk less the costs namely (i) investment in technology to retain the e-risk,(ii) premium to be paid for passing the e-risk and (iii) the cost of indemnifying the loss in case of a claim. The revenue of an e-risk insurance company depends on the amount of e-risk it retains. The study simulated a number of market scenarios (varying the risk transferred fraction, the premium overloading factor, the frequency of occurrence of security breaches).

We also propose two strategies for funded self e-risk insurance. In the exchange traded strategy we propose that the online organization, invest the pooled fund in combination of (i) stock index, (ii) long put and (iii) short call. The stock index grows the fund, the long put prevents any downslide and the short call retrieves a part of the premium paid for the long put contract. In the over the counter strategy we suggest that the online business organization invest in long call, with a strike equal to the expected loss.

The e-insurance product market is presently at an emergent stage. With the predicted increase in online retail, there exists a ready demand for e-risk insurance products. The immediate subscribers of these e-insurance products would be mainly risk averse e-business organizations. The indemnification guarantee by the e-risk insurance company would create a sense of security in the minds of the e-business organization and e-commerce would prosper.