Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

Tiered Approach for Mitigating Big Security Losses: A Variance Reduction Model

Arunabha Mukhopadhyay
Indian Institute of Management Lucknow

Samir Chatterjee
Claremont Graduate University

Debashis Saha
IIM Calcutta

Ambuj Mahanti
IIM Calcutta

Samir Sadhukhan
IIM Calcutta

Recommended Citation

Mukhopadhyay, Arunabha; Chatterjee, Samir; Saha, Debashis; Mahanti, Ambuj; and Sadhukhan, Samir, "Tiered Approach for Mitigating Big Security Losses: A Variance Reduction Model" (2007). *AMCIS 2007 Proceedings*. 260.
http://aisel.aisnet.org/amcis2007/260

Tiered approach for mitigating big security losses: A variance reduction model

Arunabha Mukhopadhyay
Indian Institute of Management Lucknow
Lucknow -226013
arunabha@iiml@ac.in

Samir Chatterjee
Claremount Graduate University
Claremont, CA 91711-6190
Samir.Chatterjee@cgu.edu

Debashis Saha
Indian Institute of Management Calcutta
Calcutta -700104
ds@iimcal.ac.in

Ambuj Mahanti
Indian Institute of Management Calcutta
Calcutta -700104
am@iimcal.ac.in

Samir K Sadhukhan
Indian Institute of Management Calcutta
Calcutta -700104
samir@iimcal.ac.in

ABSTRACT

In the next five years, revenues from e-commerce are predicted to grow immensely. Yet, the fear of transactions being spied by smart hackers and phishers is deterring users. Online organizations are equally vulnerable to Denial of Service attacks, hacking, virus attacks and graffiti. Organizations implement the latest security technologies and policies, to deter malicious attackers. Yet, security breaches are common. Organizations lose millions in terms of opportunity cost, market capitalization and brand equity. We propose e-risk insurance as a supplement to security. In this paper, we propose two variance slicing models (variance reduction technique (VRT) and an integer linear program (ILP)) for finding out the optimal number of layers, into which e-risk needs to be sliced. The input to the model is the original variance of the e-risk and the e-risk variance retention strategy. Slicing of e-risk will encourage insurance companies to except risks with large variance, as the probability of ruin reduces.

Keywords

E-commerce, security breach, variance reduction, e-risk insurance, slicing of e-risk.

INTRODUCTION

E-commerce revenues have shown a phenomenal growth in the recent past. The retail or Business to Customer (B2C) transactions are on the rise. Neilsen /NetRatings study states that, in September 2005 alone, 49.3 million people visited websites, such as Yahoo!shopping, Shopzilla, Shopping.com, Froogle.com, PriceGrabber, Nextag and ShopLocal. Shopzilla and Shopping.com alone had 15 million hits in September 2005. Similarly, a study by Interactive Media in Retail Group, opines that e-commerce volumes had grown by 31% from August 2004 and reached £1.54 billon in August 2005. All these clearly indicate a booming future for e-commerce (Dataquest 2006; Johnson and Brian, 2006).

A study by Forester Research shows that in spite of the huge prospects of e-commerce, 0.6 million Internet banking customers turned away from online financial transactions due to fear of keystroke logging Trojans and phishing mails (Dataquest, 2006)**.** Hacker groups worldwide are always experimenting with the limitations operating systems and databases. They exploit the “zero-day” advantage to crack into financial institutions (such as banks, insurance companies, credit card issuing bodies) that cause immense loss to business (Schneier, 2000). Many, “old-economy” organizations have implemented enterprise resource planning (ERP) software for enhancing operational efficiency. But disgruntled employees can break into these systems and create immense loss for the organization. Online companies should ensure confidentiality, integrity, availability and non-repudiation for every transaction.

We define *e-risk* as the possibility of a malicious activity (hacking, virus attack, phishing etc), which can create loss for an organization, in terms of (i) opportunity cost (OC), (ii) market capitalization (MC) and (iii) brand equity. (Mukhopadhyay, Chatterjee, Saha Mahanti, Chakrabarti and Podder, 2005; Mukhopadhyay,2007b). Malicious attackers, exploit the inherent weakness (i.e., e-vulnerability) of information assets (e.g., servers, information systems) and communication channel (such as sniffing, snooping, repudiation etc) to create a successful denial of service attack (DoS), identity theft and graffiti (i.e., e-threat). For example a DoS attack on e-bay on 11th Jun 1999 had resulted in drop of its share price by 20%. Too many adverse impacts tarnish brand image of an organization, and customers fear to transact with it (Campbell, Gordon and Loeb, 2003).

E-risk, as per the above definition, comprises four components, (i) *Conventional Information technology (IT) risk*, (ii) *Internet related risks*, (iii) *Risk from wireless media,* and (iv) *Legal risks* (Mukhopadhyay et al., 2005; Mukhopadhyay 2007b). IT related risks can be classified into four eras. Firstly, the *pre internet age* (1990 - 1995), when personal and main frame computers dominated. Loss was confined to the software or hardware failure or data loss. Secondly, *the internet era* (1995 - 2000), when e-commerce took off. This era saw an immense increase in interconnectivity. It brought along with it malicious attacks, such DoS, graffiti and identity theft. These affected e-commerce the most. A single malicious attack can compromise thousands of machines in a few minutes. Thirdly, the *post internet era* (2000 - 2005), this saw the threat from mobile devices. These turned organizations more vulnerable. Finally, the *current period* (2005 -), now issues, related to non-compliance of standards and legal arbitration due to party losses, are of major concern. Table 1 lists the types of *e-risk*, their causal mechanism, and impact to business (i.e., OC, MC and brand) (Mukhopadhyay,Chatterjee, Saha, Mahanti and Podder, 2005a, 2005b; Mukhopadhyay, 2007b)

Era	*e-risk*		Mechanism	Impact to business		
				OC	MC	Brand
Pre-internet Era	Conventional IT risk	Hardware failure	Mechanical failure or sabotage.	Y	Y	Y
		Software failure	Inherent or induced bugs.	Y	Y	Y
		Data loss	Loss of storage devices.	Y	Y	Y
Internet era	Internet related risk	DoS	Router flooding.	Y	Y	Y
		Virus, Trojan worm attack	Compromise of perimeter security.	Y	Y	Y
		Identity theft/ Cyber-extortion	Hacking, Phishing, Pharming.	-	Y	Y
		Graffiti	Web server Compromise	Y	Y	Y
Post Internet era	Risks from wireless media		Sniffing, Snooping	-	-	Y
Current era	Legal risk	Lawsuits and third-party claims	Sending a virus Infected mail.	-	Y	Y
		Non-compliance with regulations	Non adherence to security standards.	-	-	Y

Table 1: List of e-risks, casual mechanisms and impact to business

E-RISK MITIGATION STRATEGIES

There are various mitigation strategies followed by CTO's of online organizations to mitigate *e-risks*. We will discuss them now.

Self-protection

Most organizations use technology (such as antivirus, firewalls, encryption and also policy decisions such as passwords, authentication etc) (Gordon et al., 2003; Dhillon and Gholamreza, 2007, Dhillon and Backhouse, 2000; Anderson, 2001; Schneier, 2000) for *self-protection*. The main objective is to protect their information assets and their networks being clogged, sniffed or snooped. Self–protection helps to reduce the frequency of *e-risk.* Numerous research efforts have gone into developing systems and networks that are invincible. Yet, no system till date is fully *e-risk* proof (Schneier 2000; Schneier, 2001; Straub, 1998; and Baskerville, 1993).

E-risk Insurance

To supplement the existing security measures and to reduce the impact of loss, an effective alternative mechanism is insuring the e-risks (Gordon, Loeb and Sohai, 2003; Mukhopadhyay, Chatterjee, Roy, Saha, Mahanti and Sadhukhan, 2007; Mukhopadhyay 2007b; Mukhopadhyay et al., 2006; Mukhopadhyay et al., 2005). This would help reduce the financial burden on the organizations, as the insurance company would indemnify the loss. In effect, an organization's risk is being passed on to another party on paying a premium. Mostly, e-risk with a low frequency and high severity are insured. This reduces the companies concern about "self insuring" i.e., keeping aside huge amounts for contingency purpose. The other advantages of e-risk insurance are as follows: (i) create a sense of trust in the minds of the user, (ii) e-commerce companies will exert pressure on software developers to ensure that the code they supply is bug free to a large extent, (iii) the insurance companies would develop expertise in tracking hackers and invest in the development of technologies to curb the rouge activities.

Self e-risk Insurance

It is ideal to go for *self-e-risk insurance*, if the e-risk of low frequency and low severity type. *Self e-risk insurance* is used to ensure "loss protection" (Mukhopadhyay, Chakrabarti, Saha and Mahanti, 2007a). It helps in reducing the "size of a loss". To accomplish this, online organizations need to set aside amounts in their budget as contingent liability and use it whenever a loss occurs in reality. To reduce the size of the loss, companies chalk out Business Continuity Plans (BCP) with focus on Disaster Recovery (DR) issues.

Self e-risk insurance and *e-risk insurance* are substitute goods. An organization can choose to go for either, depending on its wealth and the nature of the e- risk. Similarly, *self protection* and *self insurance* are substitutes. Investment in more security elements reduces the requirement of setting aside capital for self-insurance. *Self-protection* and *e-risk insurance* are complementary goods. It is prudent to invest in *self protection* to reduce the initial e-risk and pass the residual e-risk to an insurance company.

Our proposed e-risk mitigation strategy

Technological security measures can only bring down the frequency of the impact, but not reduce the impact of the financial loss. We propose, a combination of technology and e-risk insurance would help minimize the loss, this help minimize the impact of brand image, MC and OC (Mukhopadhyay, 2007b). In this framework, we propose that an e-commerce organization, with high frequency and high severity of loss, should go in for *self protection*. This would help to reduce the frequency of the malicious event, though the impact would remain as before. The online organization will take a decision to self-insure or go for e-risk insurance based on the wealth and risk profile of the organization. A wealthy and risk seeking online organization would opt for *self-insurance.* A low wealth organization would opt for *e-risk insurance*. A wealthy *self –insured* organization can further slice a part of its risk to an insurer.

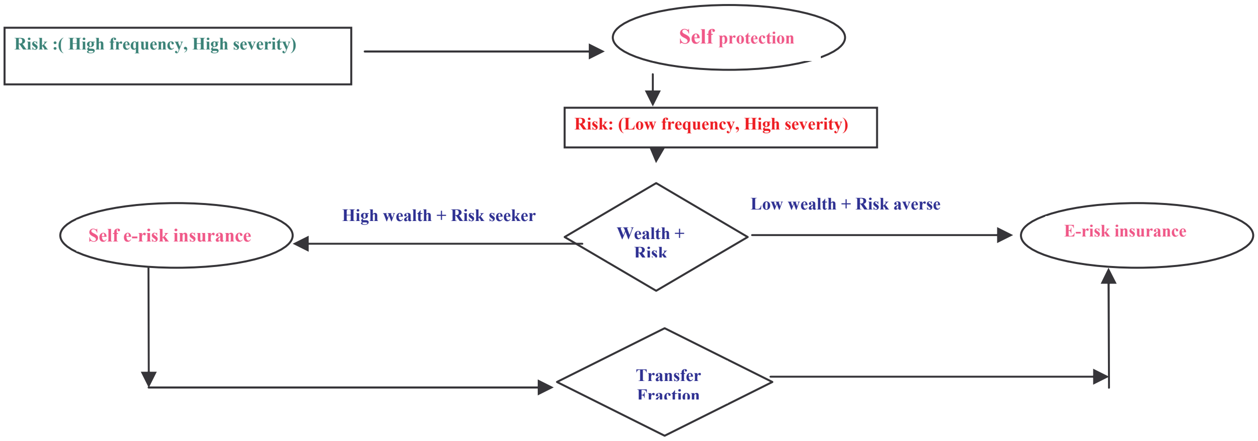


Figure 1: Proposed e-risk mitigation strategy

Insurance products

A list of e-risk products are shown in Table 2. The coverage's are small (i.e., in millions) compared to the turnover (i.e., billion) of the online business organizations. The prime reasons are (i) types of the e-risk are unknown and (ii) the associated losses have not been clearly worked out. Insurance companies fear that they would go bankrupt, if large claims arise. Another possibility could be the lack of proper business models. Each of the insurer necessitates proper *self–protection* and proper network security review for risk assessment, prior to acceptance of the risk (Reid and Stephen, 2001).The e-risk insurance products till date have remained concentrated to the UK, USA and Japan markets only.

Provider	**Policy**	**Min Premium**	**Coverage** (Million)	**Controls or Self Protection**
Cigna Property and Casualty	Secure Systems Insurance	$25,000	$25	Security assessment by approved vendor
ICSA	TruSecure	$20,000	$25	ICSA security review
J &H Marsch	NetSecure	$5000	$200	(i)E-business security assessment. (ii)AT &T Internet datacenter and web hosting facilities.
Lloyds	CIDSI e-comprehensive	$10,000	$50	(i) Review by IRG. (ii)Tripwire's Integrity security software
Reliance National or NRMS	Insure Trust	variable	$10	NRMS review
Zurich Financial Services group	E-risk Protection Program	$4,000	$25	IBM security certification

Table 2: e-risk insurance products

Note: ICSA=International Computer Security Association; NRMS=Network Risk Management Services of Atlanta; IRG =Information Risk Group

TIERED APPROACH OF E-RISK MITIGATION

To encourage e-risk insurance companies to provide large e-risk coverage, we propose a tier approach of e-risk mitigation. In this method, the insurer absorbs a large e-risk and slices it across multiple layers. In the process the variance retained at each tier is kept low. This prevents each of the individual insurance companies from going bankrupt. The basic assumption is that the quantification of the expected loss and variance is done accurately. E-risk can be quantified using the Copula based Bayesian Belief Network model for e-vulnerability assessment and quantification (CBe-VA & RQ) model (Mukhopadhyay, Chatterjee, Saha, Mahanti and Sadhukhan, 2006).

Slicing of variance increases stability

We would now show how slicing of e-risk reduces variance. Let us assume that an online business organization arrives with an e-risk of mean of $1000 and variance $5000. The e-risk insurance company(IC) can follow two strategies: (i) insure the entire e-risk itself, and (ii) slice the e-risk across multiple tiers. We assume that the expense and contingency loading for premium setting are 10%. The online organization initially keeps to it self an e-risk 30% too.

Case 1: e-risk is sliced amongst multiple tiers.

The primary insurer decides to share the e-risk amongst three insurance companies (i.e., IC1, IC2 and IC3). The e-risk retention proportion for each tier is set at 30%. The last tier (IC3) retains the residual risk. Table 3 shows (i) the amount of e-risk retained (ii) variance retained at each tier and (iii) the net cash outflow (insurance premium and self –insurance). Using the *Collective Risk Model* (Hossack,Pollard and Zehnwirth, 1983), we construct the combined distribution of the loss. The frequency of failure for each ith tier is denoted as E (N_i) and the associated loss distribution in terms of the mean (E (L_i)) and variance V (L_i). Both the frequency of the attack and the associated loss of are stochastic variables. The central tendencies (mean E (S_i) and variance Var (S_i)) of the combined distribution are defined as follows:

$$E\ (S_i) = E\ (N_i\ ) *E(\ L_i\ )\ ;\ Var\ (S_i) = E\ (N_i\ )*Var\ (\ L_i\ )+\{E\ (L_i)\}^2*Var\ (N_i\ ) \qquad (1)$$

Based on the expected loss arrived at in equation (1) the premium is defined as the expected loss E (S_i) times the overhead loading (OV) plus the variance (V(S_i)) times the contingency loading (k). The premium is arrived at by using equation (2):

$$Premium= (1+OV)*\ E\ (S_i) + k*\ \sqrt{}Var\ (S_i) \qquad (2)$$

The total cash outflow for the online organization is $1105. The online business pays a premium of $773 and incurs $332 as self-insurance. The total variance retained in the process is $831.

Layers	Mean e-risk retained ($)	Variance of e-risk retained ($)	Net cash outflow ($)	
e-biz	300	450	332	*Self-insurance*
IC1	210	221	232	*Insurance*
IC2	147	108	163	
IC3	343	53	378	
Total	1000	831	1105	

Table 3:e-risk sliced across 3 tiers

Case 2: e-risk kept with a single e-risk insurance organization

Let us consider a scenario where the insurance decides to insure the full e-risk alone. The premium arrived at using equation (2). The premium in this case works out to be $1107, while the variance of the e-risk remains as high as $5000.

Figure 2 illustrates (i) the mean e-risk and variance retained at each tier, (ii) net cash outflow for the online business and (iii) the amount of premium received by the insurance company, for both the above discussed cases. In case of a single insurer, the premium received is $1107. In case of 3 insurers, the cash inflow is $1105 (i.e., premium $773 and self insurance $332). Slicing across 3 tiers reduces the total variance by 83% as opposed to a single insurer. It also retains a very low variance at each tier too. This prevents e-risk insurance companies going bankrupt even if a major contingency arises. So it is advisbale for e-risk insurance companies to go for a slicing of e-risk to reduce the variance.

VARIANCE REDUCTION TECHNIQUE (VRT)

In this paper we will develop a VRT model to find out the optimal number of layers (for e-risk insurance companies), which an e-risk should be sliced into such that the overall variance of the of the participating e-risk insurance companies reduces. The splitting stops when there is not much substantial decrease in variance from the previous to the next layer. The VRT concept has its base in *Portfolio optimization theory* which states that the variance of the risk is reduced by splitting it into smaller fractions (Mukhopadhyay, 2007b). Thus, investors are advised to invest into a portfolio of assets, as opposed to investing in a single asset. The common analogy is “never put all your eggs in the same basket”.

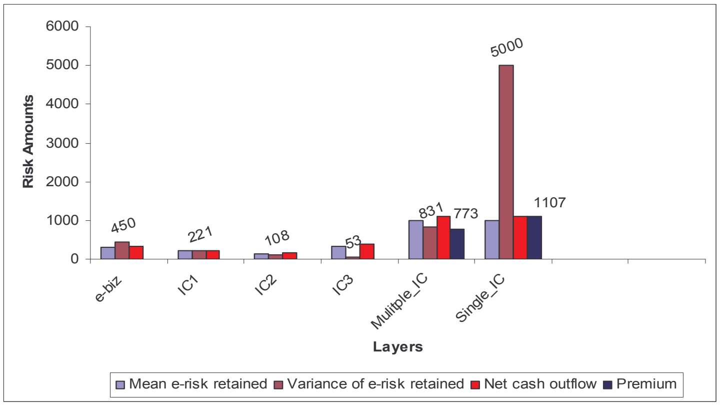


Figure 2: Impact of slicing e-risk

Let us assume that an online business organization has an e-risk of variance V and wishes to insure it. The primary insurance company accepts that risk and splits it across multiple tiers. It is assumed that each company retains α^2 proportion of the variance and passes $(1-\alpha)^2$ fraction to the next layer. This is so, as we know $V(\alpha X) = \alpha^2 V(X)$ (Das, 1996). The α lies between zero and one. This, in turn, determines the amount of variance retained (VR_i) and variance transferred (VT_i) at each tier. Figure 3 shows the splitting of the variance into multiple tiers. The root node is the variance (V) to be hedged using insurance. The left arm of the tree shows the amounts of variance retained (VR_i), and the right arm shows the variance transferred (VT_i) at each layer.

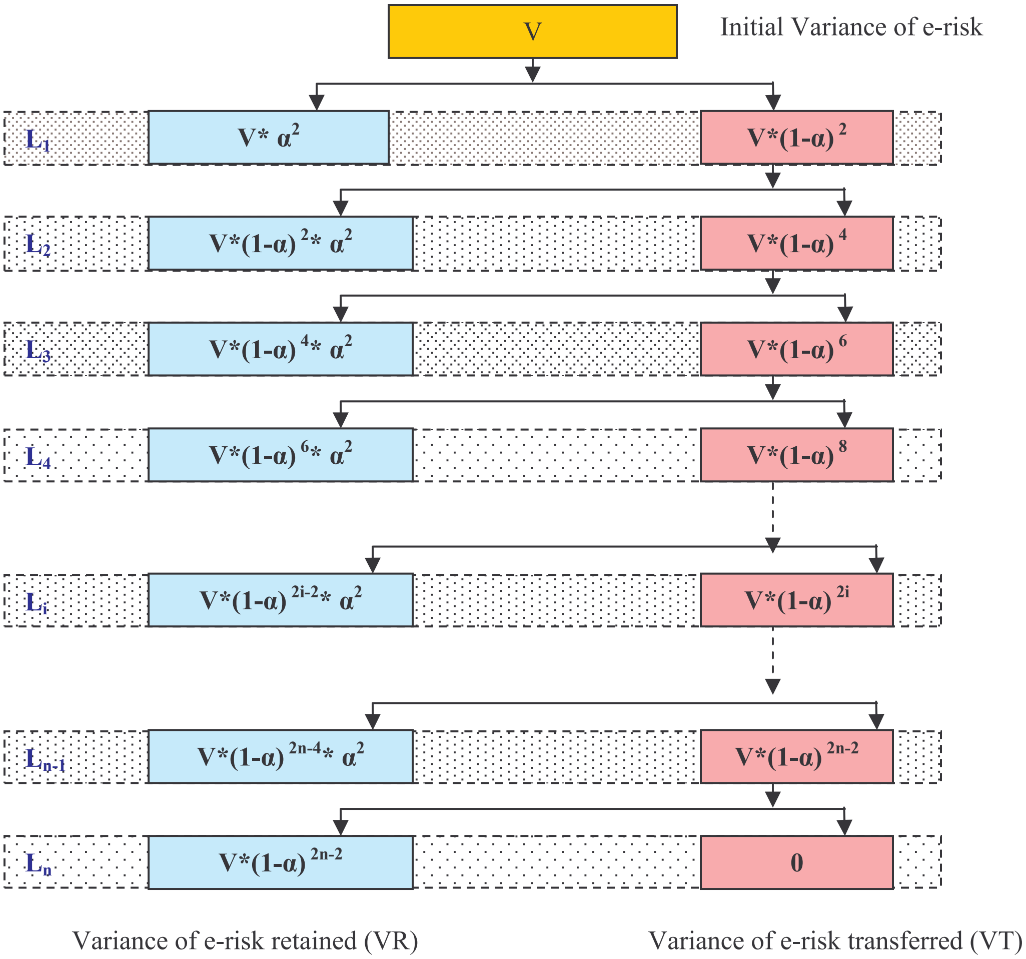

V
Initial Variance of e-risk
L_1
$V^* \alpha^2$
$V^*(1-\alpha)^2$
L_2
$V^*(1-\alpha)^{2} * \alpha^2$
$V^*(1-\alpha)^4$
L_3
$V^*(1-\alpha)^{4} * \alpha^2$
$V^*(1-\alpha)^6$
L_4
$V^*(1-\alpha)^{6} * \alpha^2$
$V^*(1-\alpha)^8$
L_i
$V^*(1-\alpha)^{2i-2} * \alpha^2$
$V^*(1-\alpha)^{2i}$
L_{n-1}
$V^*(1-\alpha)^{2n-4} * \alpha^2$
$V^*(1-\alpha)^{2n-2}$
L_n
$V^*(1-\alpha)^{2n-2}$
0
Variance of e-risk retained (VR)
Variance of e-risk transferred (VT)

Figure 3: Schematic diagram of variance split

The objective of the e-risk insurance companies is to carry on splitting the e-risk across layers, till the difference in variance (V_i) of the ith layer and the (i+1) th layer (V_{i+1}) is within some predefined value of threshold (ϵ). Reduction in variance reduces the chance of e-risk insurance companies going ruin. The mathematical formulation of the above problem is as follows:

$$
\begin{aligned}
&\text{Find} \quad i \\
&\text{subject to} \\
&\qquad V_i - V_{i+1} > \varepsilon \\
&\text{where} \\
&\qquad V_i = (VT_i + \sum_{j=1}^{i} VR_j) \\
&\qquad VR_i = V(1-\alpha)^{2i-2}\alpha^2 \quad \text{and} \quad VT_i = V(1-\alpha)^{2i-2}
\end{aligned}
\tag{3}
$$

We propose a continuous algorithm to find a solution for the above problem. Figure 4 illustrates the VRT algorithm. The VRT algorithm computes (i) The proportion of e-risk retained (e_RRF), (ii) the e-risk transferred (e_RTF) at each layer, (iii) (iv) VR and (v) VT for each of the layers. The e-risk variance retained policy (e-VRP) and e-risk variance transferred policy (e-VTP) are supplied to the system. It also computes the total variance of the slicing activity. Total variance (V_i) is defined as the sum of VR_i, VT_i for the ith layer. n_L denotes the assumed maximum of layers. The VRT algorithm keeps checking whether the difference between the total variance between two successive layers has fallen below threshold. If true, it exits and outputs the number of layers into which e-risk needs to be sliced for a given e_VRP.

```
Input : e_RRF, e_RTF, e-VRP, e-VTP, n_L, epsilion
Output: i
Procedure VRT( )
For i = 1 to n_L
        Calculate  $e\_RR_i$ ,  $e\_RT_{i,,}$ $VR_i$ ,  $VT_{i,}$
        For j = 1 to $i_,$
            $V_i = VT_i + VR_j$
        End For
        If  ($V_i$- $V_{i+1}$>  epsilion)
            Break
        End if
End For
End Procedure VRT
```

Figure 4: VRT Algorithm

Performance metric

To check the viability of the solution we have developed two tests, namely:

(i) Percentage overall reduction in variance (PVR).

$$PVR_i = \frac{V - V_i}{V} \times 100$$

A high PVR indicates that there has been substantial reduction in variance due to slicing.

(ii) Percentage of undisbursed (PUD) e-risk after slicing.

$$\mathrm{PUD} = \frac{e\_R - \sum_{i=1}^{i} e\_RR_i}{e\_R} \times 100$$

Here e_R is the original amount of e-risk of an online business accepted and e_RR$_i$ is the mean e-risk absorbed till the optimal layer arrived at by VRT model. A low PUD is indicates that the e-risk has been well distributed amongst the participating e-risk insurances companies.

INTEGER LINEAR PROGRAMMING MODEL

We also develop an integer linear programming (ILP) models corresponding to VRT strategy. The problem can be formulated as an ILP. The primary e-risk insurance company, which has accepted the e-risk from the online business organization, has to take a decision about the number of tiers (i.e., dv_layers) into which the e-risk should be split. The objective is to find out the optimum number of layers subject to the constraint that the difference in variance between the two subsequent layers is above a particular threshold (ϵ). In other words, it is to optimally split the e-risk, till the variance reduces substantiality. n_L denotes the assumed maximum of layers. The ILP formulation of the above problem is as follows:

$$\text{Max} \qquad \text{Layers} = \sum_{i=1}^{n\_L} dv\_layers_i$$

Subject to

$$\varepsilon * dv\_layers_i \le V_i - V_{i+1}$$

$$dv\_layers_i \text{ is binary, for } i = 1,2,3.....\,.....n\_L$$

where

$$V_i = (VT_i + \sum_{j=1}^{i} VR_j)$$

$$VR_i = V(1-\alpha)^{2i-2}\alpha^2 \quad \text{and} \quad VT_i = V(1-\alpha)^{2i-2} \qquad (4)$$

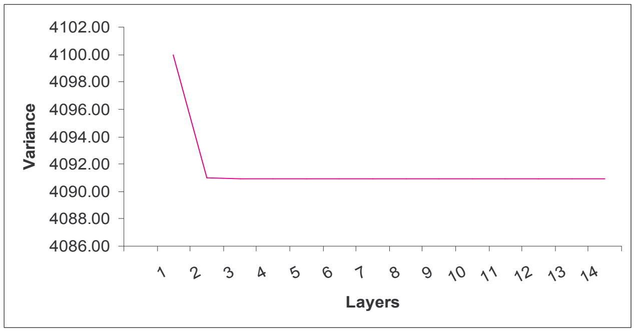
RESULTS

The basic objective is to arrive at the optimal numbers of e-risk insurance companies amongst whom the e-risk needs to be split, such that the variance is minimized. We also look at the monetary implications to both the online business and insurance company as an aftermath of variance sharing.

Case 1: e-risk of mean $100 and variance $5000

Let us assume that an e-risk insurance company wishes to hedge an e-risk with mean $100 and variance $5000. We assume that the e-risk insurance company decides on an e-risk variance retention policy (e-VRP) of 10%. In other words, it decides to pass 90% of the e-risk variance to the next tier. We decide that the splitting of e-risk variance should continue till the threshold value to be 1 is reached.

Figure 5a and 5b shows that for both the VRT and ILP model we get that the optimal number of layers needed to absorb the e-risk with mean $100 and variance $500, is 2. This clearly shows that VRT and ILP support each other. It also ensures a cross validation of the result.



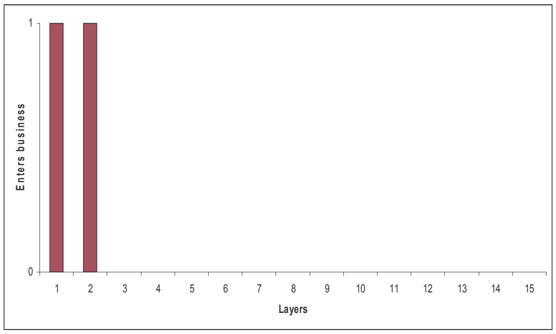
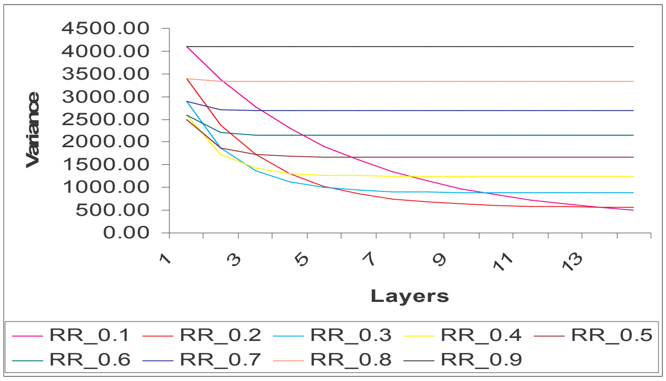


Figure 5a: VRT model

Figure 5b: ILP model

Case 2: e-risk of mean $100 and variance $5000, across multiple e-risk retention fractions

We change the e-VRP from 10% to 90% and note the optimal layers. RR_0.1 indicates that 10% of the e-risk variance has been retained. Similarly, RR_0.9 indicates that 90% retention. The threshold is set at 1.



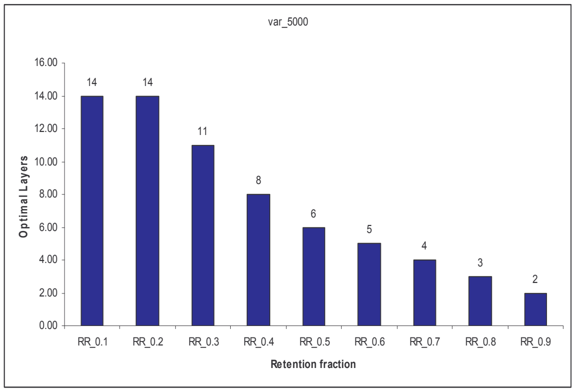


Figure 6a

Figure 6b

We get the optimal number of layers required to absorb the given e-risk for each e-VRP (RR_0.1 to RR_0.9), as 14, 14, 11, 8, 6, 5, 4, 3 and 2 respectively, as shown in Figure 6a and 6b. The optimal number of layers required to absorb an e-risk of mean $100 and variance $500, across all the e-VRP (i.e., RR_0.1 to RR_0.9) are same for both the ILP and the VRT techniques.

In Figure 7 the x-axis depicts the e-VRP and the y-axis represents PUD and PVR respectively. The blue line depicts the optimal number of layers into which the e-risk needs to be split, for a given e-VRP. The red line shows the amount of overall PVR that occurs for splitting the e-risk into the given number of optimal layers. The pink line illustrates the PUD e-risk in the system, as an aftermath of implementation of an e-risk retention strategy. For e-VRP 10% to 90%, the corresponding PVR are 90%, 89%, 82%, 75%, 67%, 57%, 46%, 33% and 18%, respectively. If an e-risk insurer chooses an e-VRP of 0.70, we can say from Figure 7 that the e-risk organization should split optimally into 4 layers, which will result in a PVR of 46% and a PUD of 0.81%.

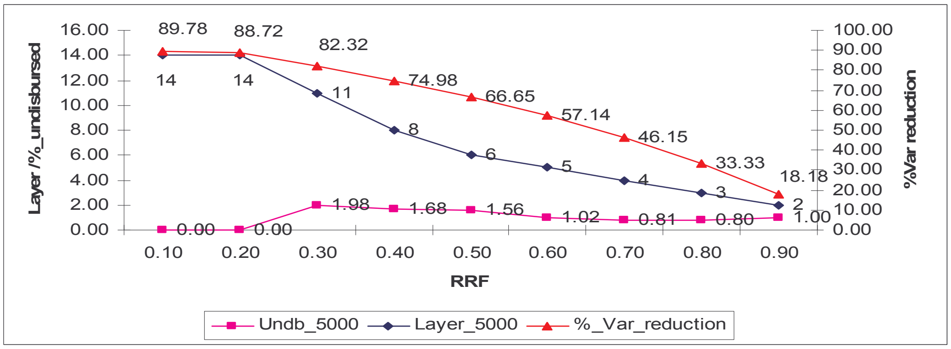


Figure 7: Slicing Mean $ 100 and variance $5000

Case 3: e-risk of mean $100 and variance $100

We now assume an e-risk of mean $100 and variance $ 100. We change the e-VRP from 10% to 90% (i.e., from RR_0.1 to RR_0.9) and note the optimal layers for each of the strategies. We assume the threshold as 1.

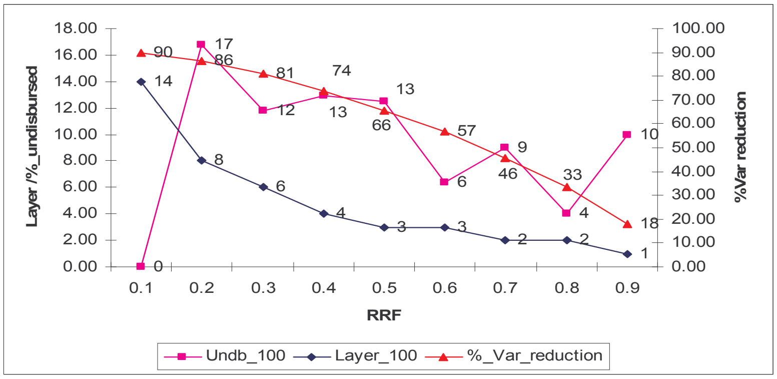


Figure 8: Slicing Mean $ 100 and variance $100

The number of optimal layers for e-VRP ranging from 20% to 90% (i.e., RR_0.2 to RR_0.9) is 8, 6, 4, 3, 3, 2, 2 and 1 respectively. In comparison to Case 2, we find that the number of layers needed to absorb the e-risk variance has decreased. This is so as the e-risk variance has decreased from $5000 to $100.This clearly shows for absorbing higher variance more number of e-risk insurance companies is needed. Figure 8 illustrates that for e-VRP 10% to 90%, the PVR are 90, 86, 81, 74, 66, 57, 46, 33 and 18 respectively. This is similar to the PVR in Case 3. The corresponding PUD e-risk is 0, 17, 12, 13, 13, 6, 9, 4 and 10 respectively. There is a marked increase in the PUD e-risk in Case 3, as opposed to case 2. This is so, as the VRT model tells us that we need only 4 layers to absorb an e-risk of variance 100, whereas to absorb a variance of 5000, 8 layers are needed. So more mean e-risk can be absorbed in the latter case as opposed to the former.

Case 4: e-risk of mean $100 and variance $500

Comparing figure 8 and 9 shows that the optimal number of layers, in Case 4 are more than in Case 3, for all e-VRP 10 % to 90%. Both VRT and ILP produce the same result. The PUD (i.e., 7, 6, 5, 6, 6, 3, 4 and 10) in Case 4 is lower than the PUD e-risk in Case 3. The PVR (88, 82, 75, 66, 57, 46, 33 and 18) in Case 3 and 4 are similar. For example, for an e-VRP of 0.2 in Case 4, we need 12 layers; where as in Case 3 we need 8 layers. So the PUD e-risk for e-VRP of 0.2 in Case 4 is 7%, whereas for Case 3 it is 17%. The PVR in Case 3 and Case 4 are similar.

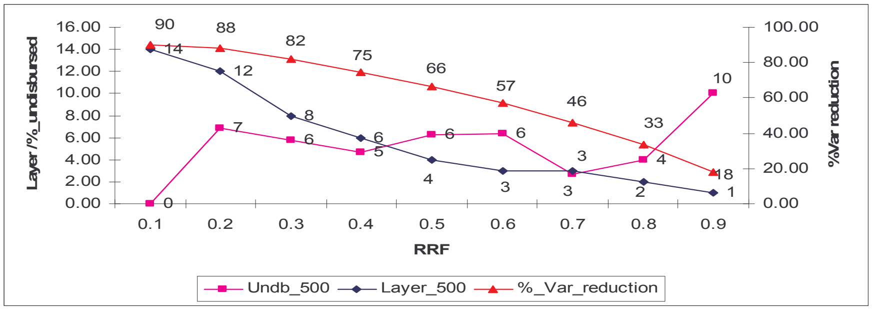


Figure 9: Slicing Mean $ 100 and variance $500

Case 5: e-risk of mean $100 and variance $2500

Figure 10 shows the optimal number of layers into which the e-risk needs to be split, for various e-VRP from 10 % to 90% (i.e., from 0.1 to 0.9). We assumed that the splitting of e-risk variance continues till the threshold reaches 1. Both VRT and ILP produce the same result.

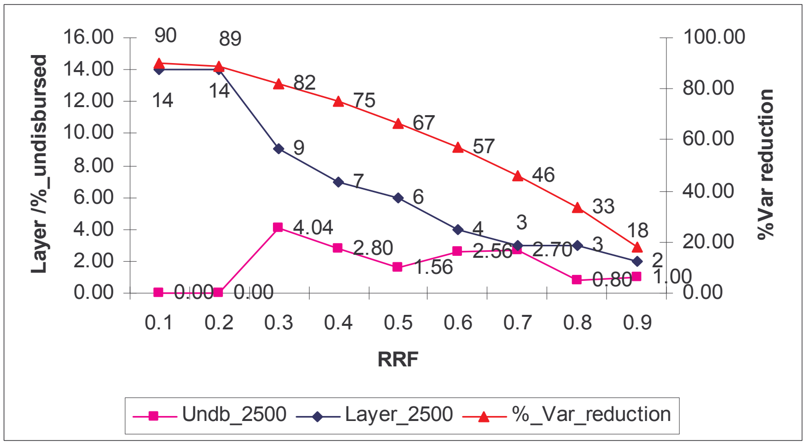


Figure 10: Slicing Mean $ 100 and variance $2500

Comparative study

Comparing Figures 7, 8, 9 and 10, we note that the PVR of Case 2, 3, 4 and 5 are more or less similar. This is so as the PVR computation is independent on the original V. It is clearly evident that the e-risk variance $5000, has the least PUD e-risk after splitting, where as e-risk variance $100, has the highest PUD e-risk. The reason, as we have already seen arises due to the fact that the e-risk variance of $5000 needs more layers, so less PUD e-risk. This makes a strong case for insuring big e-risk variance compared to e-risk with smaller variance. We thus, propose that only big e-risk should be sliced across tiers, while smaller e-risk is mitigated by self.

Choice of e-risk slicing strategy by e-risk insurance organization

The final decision about slicing of e-risk is obviously dependent on (i) risk profile of the e-risk insurance company: risk averse would prefer low risk absorption, while risk seekers would prefer large risks, (ii) size of the participating e-risk insurance companies: small or new companies would prefer to take low slices of e-risk.

PROOF OF CONCEPT

We will now derive the justification of the fact that slicing reduces variance. We will also find out the maximum possible reduction in variance that can be attained due to slicing.

E-risk is sliced amongst finite number of layers

Fig 3 shows the amount of variance retained and passed to the next layer. It is a generalized diagram for an n-tier e-risk splitting scenario. The i$^{\text{th}}$ layer provides the generalized formula for variance retention and passing respectively. As expected, the last layer retains all the variance and passes nothing. The total amount of variance retained at each tier is as follows:

$$\text{Variance retained} = V\alpha^2 + V\alpha^2(1-\alpha)^2 + V\alpha^2(1-\alpha)^4 + V\alpha^2(1-\alpha)^6 + V\alpha^2(1-\alpha)^8 + V\alpha^2(1-\alpha)^{10} + \ldots\ldots\ldots\ldots + V\alpha^2(1-\alpha)^{2n-2} \tag{5}$$

This represents finite *geometric progression series*, with a common ratio of $(1-\alpha)^2$. The total sum of the e-risk retained in all the tiers together is given as follows:

$$\text{Total variance retained} = \frac{V\alpha^2(1-(1-\alpha)^{2n})}{1-(1-\alpha)^2} = \frac{V\alpha^2(1-(1-\alpha)^{2n})}{1-(1-\alpha)^2} \tag{6}$$

In equation (6), if (i) α is zero then the total variance retained is zero, (ii) α is set to one then the total variance retained is V (i.e., no e-risk sliced) and (iii) $0 < \alpha < 1$, the total variance retained is less than V.

E-risk is sliced amongst infinite number of layers

We now derive the lower limit of retention for each of the e-risk retention strategies. Let us assume that the passing of e-risk can occur for infinite number of layers. The sum of the amount of variance retained at each tier is as follows:

$$\text{Variance retained} = V\alpha^2 + V\alpha^2(1-\alpha)^2 + V\alpha^2(1-\alpha)^4 + V\alpha^2(1-\alpha)^6 + V\alpha^2(1-\alpha)^8 + \ldots\ldots\ldots\ldots\ldots \tag{7}$$

This also represents an infinite *geometric progression series*, with a common ratio of $(1-\alpha)^2$. Therefore, total sum of the e-risk retained in all the tiers together is given as follows:

$$\text{Total e-Risk retained} = \frac{V\alpha^2}{1-(1-\alpha)^2} = \frac{V\alpha^2}{-(-2\alpha+\alpha^2)} = \frac{V\alpha^2}{2\alpha-\alpha^2} = \frac{V\alpha^2}{\alpha(2-\alpha)} \tag{8}$$

In equation (8), if (i) α is zero, then the total e-risk retained is zero, (ii) α is set to one, then the total e-risk retained is V/2. An infinite number of insurers can attain a reduction of half the amount of the original variance.

CONCLUSION

Slicing of e-risk across multiple insurance companies reduces the probability of ruin. It also encourages insurance company to accept big security losses. This in turn helps in creating a sense of trust in the minds of the users and the organizations, and thus promotes e-commerce.

REFERENCES

1. Anderson, R. Why information security is hard—An economic perspective. In *Proceedings of 17th Annual Computer Security Applications Conference (ACSAC),* New Orleans, La. Dec.10–14, 2001
2. Baskerville, L. R. (1993) Information Systems Security Design Methods: Implication for Information Systems development, *ACM Computing Surveys*, vol. 25, no. 4, pp. 375-414.
3. Campbell, K., Gordon, A. L., Loeb, P. M. (2003) The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*, 431-448.

4. Dataquest (2006) E-commerce data, vol XXIV[1]. Cyber Media Publication.
5. Das G N (1996) Statistical methods on Commerce, Accountancy & Economics. Part I & II, M Das & Co. Calcutta.
6. Dhillon, G., Backhouse, J. (2000) Information System Security Management in the New Millennium. *Communications of the ACM, 43*(7), 125-127.
7. Dhillon, G., Gholamreza, T. (2007) *Value -focused assessment of information system security in organizations*, Information Systems Journal.
8. Gordon A, L, Loeb, P. M., Sohai, l. T. (2003) A framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3).
9. Hossack B I, Pollard J, Zehnwirth B, Introduction to Statistics with applications to general insurance , Cambridge University Press,1983.
10. Johnson Carrie A, Tesch Brian (2006) US eCommerce: 2005 To 2010: A Five-Year Forecast and Analysis Of US Online Retail Sales. Forrestor Website [On-line]
11. Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A, Chakrabarti, B. B., Podder, K. A. (2005) Security breach losses in e-commerce through Insurance*. Proceedings of 4th Security Conference*, Las Vegas, Nevada.
12. Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Podder, K. A. (2005a) e-risk: A case for insurance. *Proceedings of the Conference on Information Systems and Technology*, New Delhi, India.
13. Mukhopadhyay, A., Saha, D., Mahanti, A., Podder, K. A. (2005b) Insurance for cyber-risk: A Utility Model. *Decision, Vol 32*(1), 153-170.
14. Mukhopadhyay, A, Chatterjee, S., Saha, D., Mahanti, A, Sadhukhan, K. S. (2006) *e-Risk Management with Insurance : A framework using Copula aided Bayesian Belief Networks. Proceedings of the Hawaii International Conference on System Sciences 39*, Hawaii,USA.
15. Mukhopadhyay A, Chatterjee S, Saha D, Mahanti A, Roy R, Sadhukhan S K(2007) Insuring big losses due to security breaches through insurance: A business model, *Proceedings of the Hawaii International Conference on System Sciences 40*, Hawaii, USA.
16. Mukhopadhyay A, Chakrabarti B B, Saha D, Mahanti A (2007a) e-risk management through self-insurance: An option model, *Proceedings of the Hawaii International Conference on System Sciences 40*, Hawaii, USA.
17. Mukhopadhyay A. (2007b) A novel framework for mitigating e-risk through insurance. Phd Thesis, Indian Institute of Management Calcutta.
18. Reid, C. R., Stephen, F. A. (2001) Extending the Risk Analysis model to include market-insurance. *Computers & Security, 20*(4), 331-339.
19. Schneier, B. (2000) *Secrets and Lies: Digital security in a Networked World*: John Wiley & Sons.
20. Schneier, B. (2001). The insurance Takeover. *Information Security*.
21. Straub, W. D., J. Richard, W. (1998) Coping with Systems Risk: Security Planning Models Risk Management Decision-Making. *MIS Quarterly, 22*(4), 441-469.