Insuring big losses due to security breaches through Insurance: A business model

Arunabha Mukhopadhyay
Indian Institute of Management Calcutta
D H Road
Calcutta -700104
arunabha@iimcal@ac.in

Samir Chatterjee
Claremont Graduate University
California-91711-6190,
samir.chatterjee@cgu.edu

Rahul Roy
Indian Institute of Management Calcutta
D H Road Calcutta -700104
rahul@iimcal.ac.in

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

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

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

Abstract

Security breaches deter e-commerce activities. Organizations spend millions of dollars on security appliances to make online transactions more secure. Nonetheless, a new virus or a clever hacker can easily compromise these deterrents and cause losses of millions of dollars annually. To reduce the impact of such losses, e-risk insurance is a viable complement to the security devices. Currently, e-risk insurance is in its developmental stage and small claim coverage is only available. In this paper, we provide a framework, for insurance companies to duly accept large e-risk. Splitting a large risk across layers reduces the overall variance of the loss. Also in case of a contingency the loss indemnification is shared. The inputs to the proposed model are the risk transfer proportion, overloading for premium, expected return on capital and undistributed risk at each layer. The model outputs the optimal number of layers in which the risk needs to be spilt by the insurance company and the interlayer relationships.

Keywords: e-commerce, security breach, e-risk, E-risk insurance, cyber-insurance, re-insurance

1. Introduction

A study by Forester Research states that online retail sales is expected to grow to $329 billion in 2010, from $172 billion as in 2005, registering a 14% compound annual growth rate (CAGR) for the next five years. This projected revenue would account for 13% of the total US retail sales in 2010. The travel industry is expected to be the main contributor to this pie. It is expected to grow from $63 billon to $119 billion in 2010. A study by Interactive Media in Retail Group, opines that e-commerce volumes have grown by 31% from August 2004 and reached £1.54 Billon in August 2005.All these clearly indicate a booming future for e-commerce.

On the contrary, studies by Gartner Research point out that, due to *online fraud*, 33% of online shoppers are buying fewer items. Similarly, according to studies by TRUSTe, 40% of consumers avoid buying from small online retailers due to *identity theft* concerns.

Gartner report adds that, during the period May 2004 to May 2005, about 73 million consumers have received *phishing attacks* through e-mails. Of which 2.4 million users have reported losing money. Companies up in arms after being targeted include Paypal, eBay, Citizens bank, bank of America, MSN, Amazon.com, VISA, Citibank, Lloyds TSB, Yahoo, US Bank, Microsoft and AOL. According to Forester Research, 0.6 million Internet banking customers turned away from online financial transactions due to fear of keystroke logging Trojans and phishing mails.

This clearly reveals that growth of e-commerce is greatly deterred by malicious activities like hacking, virus / worm or phishing attacks.

To counter these threats companies resort to extensive use of security appliances. IDC study shows worldwide spending on security appliances grew by

Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)
0-7695-2755-8/07 $20.00 © 2007 IEEE

17% to $613 million in 2005. Similarly, according to a study by Gartner, the spending on Global IT security would reach $24.6 billon by 2009. Results of Economist Intelligence and AT&T poll of executives of 50 countries reveal that 26% of consider security as their top concern [1].

In this backdrop, we define e-Risk as the possibility of an electronic event, whose occurrence causes loss to e-businesses. A list of e-risk [3] and their causal mechanism is shown in Table 1.

Table I: List of e-risk

Event	Mechanism
Compromise	a) Network security components
	b) organization web server, and posting of incorrect or indecent material on the web site (commonly called graffiti)
Failure	a) Application Service Provider (ASP)
	b) Internet Service Provider (ISP)
"identity theft"/ "cyber-extortion"	a) Hacking.
	b) Phishing
	c) Pharming
Denial of Service (DoS)	by making malicious calls to the router
Attack by wireless devices	a) sniffing b) snooping

It is a common knowledge that no computer system in this world is totally secure or free from vulnerabilities [3, 4, 5, 6, 7,8,10], especially, the ones connected to the Internet. Information Security is more than a technical issue. Information Security studies can be broadly grouped into four categories according to [10], a) technical defenses, b) Intrusion detection systems c) behavioral aspect d) economic aspect.

Broadly Information Security has been focused to the development of a) checklist b) Risk Analysis models c) Formal methods and d) Soft approach [7].

Earlier studies states that Information System should be viewed as a security risk planning problem comprising of the five stages: a) recognition of the security problem b) risk Analysis c) alternate generation d) planning decision and e) security implementation [7].

Recent studies [2, 3, 4, 5, 8,10] recommend the use of financial instruments, like cyber insurance or e-risk insurance, to hedge the losses due to security breaches.

In this work we wish to provide a business model for insurance so that they can optimally slice the accepted e-risk amogst themselves. This would reduce the variance of e-risk accepted by any insurance company.

This paper comprises 6 sections. In Section 2 we present a brief overview of e-risk insurance. Section 3 we describe the proposed tiered apparaoch for e-risk mitigation. In Section 4, we formulate the problem and also provide an algorithm for arriving at the optimal number of layers into which e-risk should be optimally sliced. In section 5, we discuss the results of the simulation by taking various values of e-risk and retain of capital (ROC). Section 6 provides the concluding remarks

2. e-risk insurance

e-risk insurance is a risk transfer mechanism, by which an organism can exchange its uncertainty for certainty. The organization is uncertain about: a) timing of the event b) frequency of the event per year c) the financial implications of the event. These uncertainties make budgeting difficult for an organization. Insurance offers a mechanism, by which an organization can exchange uncertain loss for a fixed yearly loss (i.e. premium). The organization pays a premium for which the insurance company indemnifies for the loss, whenever it occurs.

An e-risk event is defined in terms of the frequency (low, high) of the event and the impact (low, high) of the event to an organization. The expected loss is arrived by the product of the frequency times the impact of the event.

Let us assume *E (N)* denotes the expectation of the loss frequency distribution. While *E(X)* is the expectation of the loss amount distribution. The expected loss *E* (S_N) and its variance $Var(S_N)$ is given by (1)

$$E\ (S_N)\ = E\ (N)\ {*}E(X)$$

$$Var(S_N) = E(N){*}Var(X) + \{E(X)\}^2{*}Var(N) \qquad (1)$$

We propose a two stage framework for large e-risk mitigation. The first stage is to do a security risk analysis of the e-business organization. The inputs to the system are log files of the network security appliances (Firewall, Intrusion detection system, Antivirus etc) and the security policy information (authentication rule). These are supplied to a *Copula aided Bayesian Belief Network* [2], which provides the probability of occurrence of a security breach due to failure of any of these. Based on expert opinion, a loss distribution (impact) of the e-Risk is assumed (i.e. Binomial, Poisson).

There are four cases as follows: a) low frequency, low impact e-Risk to be mitigated by "self-insurance". This mechanism ensures "loss protection" and reduces the "size/impact of a loss". Companies set aside amounts in their budget as contingent liability and use it whenever a loss occurs in reality. Companies chalk out Business Continuity Plans (BCP) with focus on Disaster Recovery (DR) issues to meet such contingencies. b) Low frequency, High impact e-Risk can be tackled by using "cyber-insurance". Pass the risk to a third part in lieu of a premium. c) For high frequency, low impact e-Risk, it is best to go for "self-protection", with the aim to reduce the frequency of occurrence of the event (i.e. "loss prevention"). These include installation of technical defenses like antivirus, firewalls, encryption and also policy decisions like passwords, authentication etc. A proper "self-protection mechanism" helps in reducing the premium for "cyber-insurance" policies. d) High frequency, high impact, best to avoid it [2, 10]

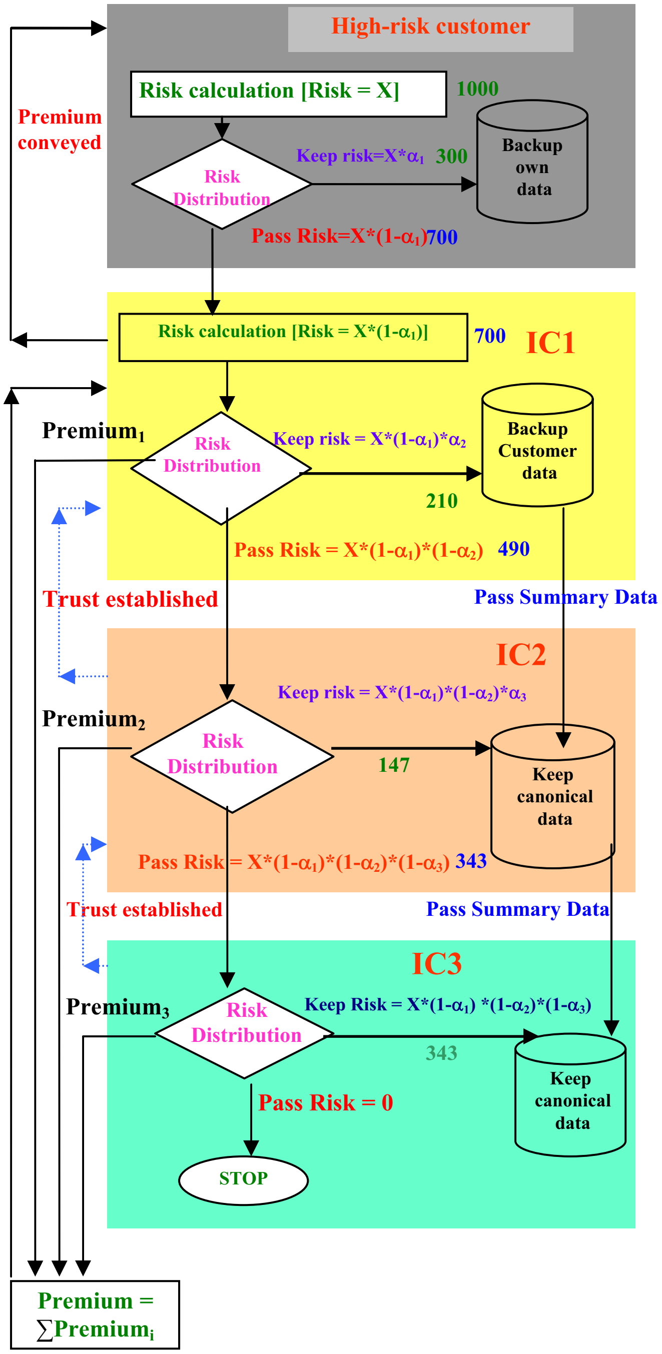
Cyber-insurance solutions can help "enhance trust and promote e-commerce in the market space" The role of insurance of would be substantial, as governments are taking a back seat in most countries. [1].

Cyber-insurance policies have been launched by AIG (netadvantage), Chubb (Cyber Security), Lloyds (e-comprehensive) etc. These provide a maximum coverage $50millon. A sale of $200 million cyber-insurance has been reported in 2002 [1].

3. Tiered approach for e-risk mitigation

The insurance company decides on a strategy, to adequately distribute the e-risk passed to by the e-business organization [4].

In figure 1, an online organization has an e-risk of $1000 million. It decides to keep $300 M and buy insurance for $700 M. A ceding office (the prime insurer) accepts the e-risk. It then decides to re-insurance the same, across 3 layers, according to the rule, retain 30% and pass 70% of the e-risk. At each tier, a canonical data is also stored by the concerned insurance company. The frequency of the data being stored varies from daily, weekly to monthly. This would ideally be stored by an Internet Data Centre at varying localities. At each layer a trust relationship is established amongst the insurance companies and each agrees to indemnify the other in case of a contingency. In case of a loss, the e-business gets indemnified monetarily and also has some amount of data restored.


High-risk customer
Risk calculation [Risk = X]
1000
Premium conveyed
Risk Distribution
Keep risk=$X*\alpha_1$
300
Backup own data
Pass Risk=$X*(1-\alpha_1)$
700
Risk calculation [Risk = $X*(1-\alpha_1)$]
700
IC1
Premium$_1$
Risk Distribution
Keep risk = $X*(1-\alpha_1)*\alpha_2$
Backup Customer data
210
Pass Risk = $X*(1-\alpha_1)*(1-\alpha_2)$
490
Trust established
Pass Summary Data
IC2
Keep risk = $X*(1-\alpha_1)*(1-\alpha_2)*\alpha_3$
Premium$_2$
Risk Distribution
147
Keep canonical data
Pass Risk = $X*(1-\alpha_1)*(1-\alpha_2)*(1-\alpha_3)$
343
Trust established
Pass Summary Data
IC3
Premium$_3$
Risk Distribution
Keep Risk = $X*(1-\alpha_1)*(1-\alpha_2)*(1-\alpha_3)$
343
Keep canonical data
Pass Risk = 0
STOP
Premium = $\sum$Premium$_i$

IC= Insurance Company

Fig 1: A tired approach of risk mitigation

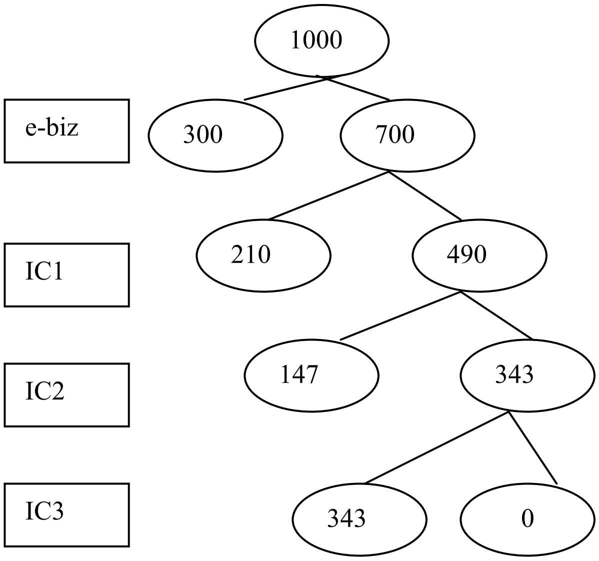


Fig 1a: A schematic diagram of risk distribution across layers

The root node in Fig 1a is the amount of e-risk (e-R) to be hedged using insurance. The left arm of the tree shows the amounts of e-risk retained (e-RR$_i$), and the right arm shows the amount of e-risk transferred (e-RTi) at each layer. It is assumed that the e-business organization would also share a part of the e-risk itself.

The basic premise of this tiered approach is to spread the risk amongst a number of players. This reduces the variance of the loss to be suffered by each player in case of contingency [11].

4. Problem Formulation

In this section, we propose a mechanism, for finding out the optimal number of layers (L), insurance companies, would like distribute a given e-risk (e-R). The inputs are total e-risk (e-R), e-risk transfer fraction (e-RTF$_i$) policy, and expected return on capital (ROC$_i$), for each layer. We assume that the ROC$_i$ and e-RTF$_i$ are same at each tier. It is also assumed that the e-business company, itself would also keep a slice of the risk.

The decisions taken by each insurance company are: (i) amount of e-risk retained (e-RR$_i$), (ii) amount of e-risk transferred (e-RT$_i$) and (iii) Investment in technology (IT$_i$).

The summation of e-risk retained (e-RR$_i$), gives the total e-risk absorbed (e-TRA). While residual e-risk (e-RS) is expected Loss amount(R) less the total e-risk absorbed (e-TRA).

The cash outflows for insurance companies, at each layer are: a) Investment in technology (IT$_i$) to backup the data in the canonical form ;(similar to [10]) b) Loss indemnification in case of claim (C$_i$) (Assumption: Claims arise randomly) c) Payment of premium to the next tier (P$_{i+1}$) for e-risk transferring (e-RT$_i$). The cash inflows are premium received (P$_i$) at each layer, in lieu of e-risk retained (e-RR$_i$). An overhead factor (OV) is charged on the e-risk (e-RR$_i$ or e-RT$_i$) for arriving at the premium (P$_i$ or P$_{i+1}$). The net cash flow (NCF$_i$) of the ith layer is follows:

$$\mathrm{NCF}_i = (\mathrm{P}_i – \mathrm{P}_{i+1}) – \mathrm{IT}_i – \mathrm{C}_i \qquad (2)$$

If NCF$_i$ is less than the ROC$_i$, at any layer, then that layer and its successors do not enter into business.

For a optimal number of layers (L), if the percentage of e-risk undisturbed (e-RU=e-RS/e-R), is within a bound (Min_RU, Max_RU) we accept the solution as feasible.

The mathematical formulation is as follows:

Find L

where

$$\mathrm{L} = \mathrm{f}\,(\mathrm{ROC}_{\,i}, \mathrm{NCF}_{\,i}, \mathrm{e\text{-}RU}, \mathrm{e\text{-}R})$$

$$\mathrm{NCF}_{\,i} = \mathrm{g}\,(\mathrm{e\text{-}RR}_i, \mathrm{e\text{-}RT}_i, \mathrm{e\text{-}RTF}_i, \mathrm{OV}, \mathrm{C}_i, \mathrm{IT}_i)$$

$$\mathrm{C}_i = \text{Random Number} * \ \mathrm{e\text{-}RR}_i * \mathrm{e\text{-}RTF}_i$$

$$\mathrm{IT}_i = \mathrm{h}(\mathrm{e\text{-}RR}_i)$$

$$\mathrm{e\text{-}TRA} = \sum_{i=1}^{L} \mathrm{e\text{-}RR}_i ; \mathrm{e\text{-}RS} = e - \mathrm{R} \ \ \mathrm{\text{-}TRA} ; \mathrm{e\text{-}RU} = \frac{\mathrm{e\text{-}RS}}{\mathrm{e\text{-}R}}$$

4.1 Algorithm

In order to obtain the optimal number of layers, we suggest the following algorithm:

Input e-R, ROC, e-RTF, Loss_amount, ROC

```
Procedure Optimal_Layers ( )
Max_layer = 0
For RTF = Min_e-RTF, Max_e-RTF, Step_e-RTF
        Sum = 0
        Count = 0
  For OV = Min_OV, Max_OV, Step_OV

      If Layer (ROC, e-RTF, OV) == -1
         Exit Procedure Optimal_Layers ( )
      Else
        Sum = Sum + Layer (ROC,e-RTF, OV)
         Count = Count + 1
      End If
  End For
       Avg_layer = Sum/Count
      If (Avg_layer > Max_layer)
```

```
                Max_layer = Avg_layer
            End If
End For
Output: Range of e-RTF & e-RU in neighborhood of Max_layer.

End Optimal_Layers Procedure

Function Layer (ROC, e-RTF, OV)
i = 1
NCF_i = (P_i - P_{i+1}) - IT_i - C_i
        While (NCF_i > ROC)
                i = i + 1
                NCF_i = (P_i - P_{i+1}) - IT_i - C_i
        End While
Layer = i-1

Calculate e-RU_layer

        If Validate (e-RU_layer)
                Return Layer
        Else
                Return -1
        End if
End Layer Function

 Function Validate (e-RU)
                If(Min_e-RU ≤ e-RU ≤ Max_e-RU)
                        Return Success
                Else
                        Return Failure
                End if
 End Validate Function
```

For an e-RTF$_i$, we vary the OV, in small steps, till a layer is reached where NCF$_i$ is less than ROC. We then average it, to obtain the optimal number of layers, for that given e-RTF$_i$.

In effect the output is an optimal number of layers for a given e-risk occur within a bound of e-RTF and e-RU.

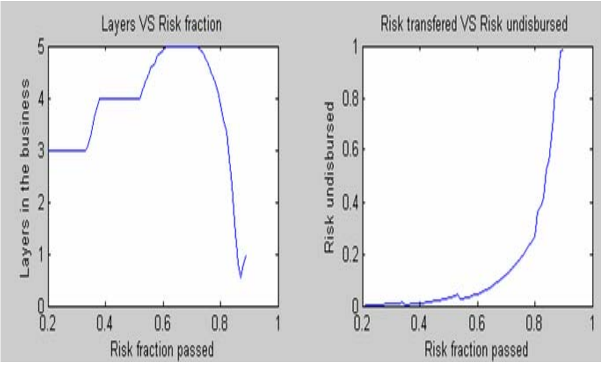
5. Experimental Results

We simulate a number of scenarios using software developed in MATLAB. The basic assumptions of the model are as follows: a) e-Risk distribution as per Quota share [11] method. Each insurance company, have to pass a fixed proportion of e-risk to the next layer, as agreed in the treaty. No layer (except the last) can "retain all" of the e-risk. This prevent insurance companies from, retaining high proportion of good risk or low proportion of bad e-risk; b) Minimum e-risk retention fraction at each layer is 0.1; c) Maximum risk retention is 0.9; d) e-Risk retention is increased in steps of 0.01; e) Minimum overload is 1.0; f) Maximum overload is 1.5; g) Overload factor increased in steps of 0.02. The premium at each layer is arrived as follows:

$$Premium=(1+q)*E(S_N)+k*\sqrt{Var(S_N)} \qquad (4)$$

here q is the overload factor and k is the contingency factor (we assumed k=1); h) for optimal technology investment, we used eq (6) from [10] where alpha = 0.00001, beta=100; i) claims arise from a uniform random distribution.

Case I: ROC =\$2 x 10^5; Loss =\$8 x 10^5.



.

Fig 2a: Optimal Layers. Fig2b:Undisbursed e-risk

A maximum of 3 layers needed to distribute the \$8 x 10^5, if the expected ROC is \$2 x 10^5, and e-risk transfer (e-RTF) is 0.2.

From figure 2a, it is evident, that for a loss of \$8 x 10^5 with, expected ROC of \$2 x 10^5, it is ideal to choose a e-RTF policy, between 0.2(min) to 0.4(max).

Figure 2b reveals that, in the e-RTF$_i$ range of 0.2(min) to 0.4(max), the risk left undistributed (RU) is the lowest. For the e-RTF$_i$ policy of 0.6, a maximum of five layers are needed, for the risk distribution. .But for an e-RTF$_i$ policy beyond 0.6, the amount of risk proportion undisbursed (e-RU) increases sharply.

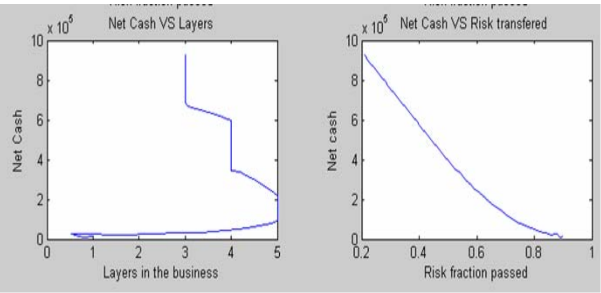


Fig 3a: Net cash VS Layers   Fig 3b: Net Cash VS Risk

Figure 3a, shows that, for e-RTF$_i$ policy 0.2, the ideal number of layers is three, since the NCF$_i$ is the maximum there. Then NCF$_i$ slowly decreases to the right (i.e. layer 5).

Premium (P$_i$) is directly related to the amount of e-risk retained e-RR$_i$ (i.e. eq 4) at any layer. If e-RR$_i$, is less, then premium inflow (P$_i$) is low for the insurance company. Yet, the insurance company has a high outflow of premium (P$_{i+1}$) to the next insurance company. So, beyond layer 5, the net cash decreases sharply.

Figure 3b, similarly shows, that net cash flow (NCF) is max, for e-RTF$_i$=0.2.Then it drops gently between e-RTF policy 0.4 to 0.6 and reaches to zero after e-RTF policy 0.8. This is in line with the result of Fig 3a.

Case II: ROC =\$2 x 10^5; Loss = (\$8 x 10^5, \$16 x 10^5, \$24 x 10^5, \$32 x 10^5, \$40 x 10^5)

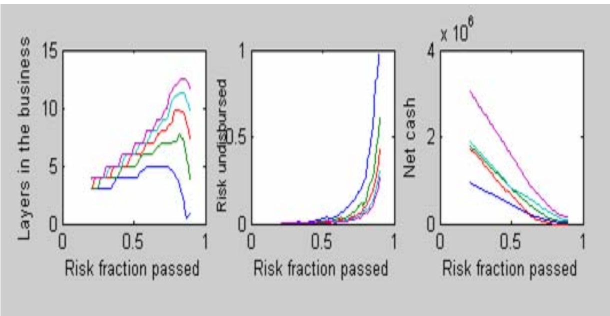


Figure 4: e-Risk distribution when ROC=\$2 x 10^3

Note the loss amounts (e-R) are depicted as follows: blue line (\$8 x 10^5); green line (\$16 x 10^5); red (\$24 x 10^5); cyan (\$ 32 x 10^5); pink (\$40 x 10^5).

For each of the loss (e-R), Table I, shows the number of layers (max and min), the range of e-risk transfer policy where the lowest left undistributed e-risk occurs, the policies which gives highest net cash inflow.

Table I: Summary of Results, when ROC =\$2 x 10^5

Loss (10^5)	***Min Layer***	***Max Layer***	***e-RTF range***	***Net Cash Flow (highest)***
8	3	5	0.2 to 0.5	0.2
16	3	8	0.2 to 0.6	0.2
24	4	10	0.2 to 0.5	0.2
32	4	11	0.2 to 0.5	0.2
40	4	12	0.2 to 0.5	0.2

In this case a risk transfer fraction (e-RTF$_i$) in the range of 0.2 to 0.5 is ideal. 4 players can handle the risk adequately.

Case III: ROC =\$6 x 10^5; Loss = (\$8 x 10^5, \$16 x 10^5, \$24 x 10^5, \$32 x 10^5, \$40 x 10^5)

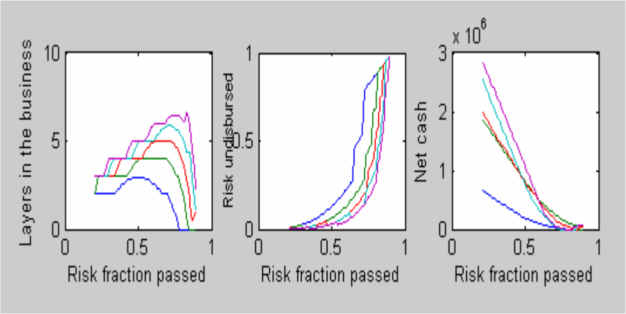


Figure 5: e-Risk distribution, when ROC =\$6 x 10^5

Note the loss amounts are depicted as follows: blue line (\$8 x 10^5); green line (\$16 x 10^5); red (\$24 x 10^5); cyan (\$ 32 x 10^5); pink (\$40 x 10^5).

For a given loss, Table II shows the number of layers (max and min), the range of e-risk transfer policy(e-RTF$_i$) where the lowest left undistributed e-risk(e-RU) occurs, the policies which gives highest net cash inflow.

Table II: Summary of Results, when ROC =$6 x 10^5

Loss (10^5)	*Min Layer*	*Max Layer*	*e-RTF range*	*Net Cash Flow (highest)*
8	2	3	0.2 to 0.47	0.2
16	2	4	0.2 to 0.45	0.2
24	3	5	0.2 to 0.45	0.2
32	3	6	0.2 to 0.44	0.2
40	3	6	0.2 to 0.37	0.2

In this scenario, a e-risk fraction transfer (e-RTF$_i$) strategy in the range of 0.2 to 0.45 is ideal. A maximum of 3 players can handle the risk adequately.

Case IV: ROC = ($2 x 10^5, $6 x 10^5, $10x 10^5), Loss =$8 x 10^5

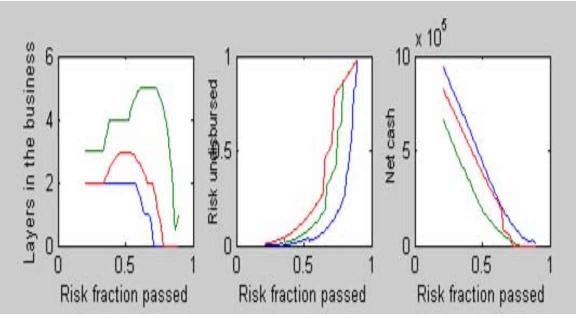


Figure 6: e-Risk distribution, when ROC =$(2, 6, 10) x 10^5

Note the loss amounts are depicted as follows: blue line ($2 x 10^5); red line ($6 x 10^5); green ($10 x 10^5).

For each of the loss, Table III shows the number of layers (max and min), the range of e-risk fraction transfer(e-RTF$_i$) policy where the lowest left undistributed risk occurs, the policies which gives highest net cash inflow.

Table III: Summary of Results, when ROC =$(2, 6, 10) x 10^5

ROC (10^5)	*Min Layer*	*Max Layer*	*e-RTF range*	*Net Cash Flow (highest)*
2	2	2	0.2 to 0.3	0.2
6	2	3	0.2 to 0.33	0.2
10	3	5	0.2 to 0.45	0.2

The ideal range for e-risk fraction transfer (e-RTF$_i$) policy is in the range of 0.2 to 0.3. An optimal of 3 players can handle the risk adequately.

6. Conclusion

This study, proposes a model for insurance companies to optimally decide on the number of layers, into which they should spilt a high e-risk, in order to reduce the overall variance. These e-risk insurance solutions would help in promoting e-commerce, as it would help in reducing the impact of the loss and thus create trust in the e-market place

Acknowledgement

We would like to thank Mr. A.K Podder, Regional Manager (Actuary), LIC, Kolkata, India for his help to us.

7. References

[1] DataQuest, Cyber Media Publication, Jan15, 2006.

[2] Mukhopadhyay A, Chatterjee S, Saha D, Mahanti A, Sadhukhan S K, e-Risk Management with Insurance: A framework using Copula aided Bayesian Belief Networks, Proceedings of the Hawaii International Conference on System Sciences, January 3-7 , 2006.

[3] Mukhopadhyay A, Chatterjee S, Saha D, Mahanti A ,Chakrabarti B B, Podder A K, Mitigating Security breach losses in e-commerce through Insurance ,Proceedings of 4th Security Conference ,Las Vegas ,Nevada ,March 30-31 ,2005

[4] Mukhopadhyay A, Chatterjee S, Saha D, Mahanti A ,Podder A K, e-risk :A case for insurance ,Proceedings of the Conference on Information Systems and Technology Management ,New Delhi ,July 23-26 ,2005

[5] Mukhopadhyay A, Saha D, Mahanti A, Chakrabarti B B, Podder A, Insurance for cyber-risk: A Utility Model ,Decision, Vol 32 ,No 1, 153-170., June 2005.

[6] 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.

[7] Dhillon, G, Torkzadeh, G. (2001), Value – focused assessment of information system security in organizations, Paper presented at the International conference on Systems, New Orelans, LA, 561-565.

[8] Schneier, B. Secrets & Lies. (2nd edition), Wiley, New York, 2000Gordon and Loeb, The economics of information security investment, ACM Trans on Inf Sys Sec, 5,4,Nov 2002, 438-457

[9] .Lawrence A.Gordon, Martin P.Loeb, Tashfeen Sohail, A framework for using Insurance for Cyber-risk management**,** Communications of the ACM, March 2003,Vol.46, No.3 81

[10] .Lawrence A. Gordon, Martin P.Loeb, The economics of information security investment, ACM Trans on Inf Sys Sec, 5,4,Nov 2002, 438-457

[11] Hossack B I, Pollard J,Zehnwirth B, Introduction to Statistics with applications to general insurance , Cambridge University Press,1983.