Integrated Cyber Security Risk Management-Insurance and Investment Cost Analysis

By

THOMAS Y.S. LEE

Information and Decision Sciences Department

College of Business Administration

University of Illinois

Chicago, Illinois

USA

Broad Outline of Presentation

1. Insurable Cyber Risks
    - What is Cyber Risk?
    - Examples of Recent Cyber Attacks/Problems
    - Key Insurable Cyber Risks
2. The Model
    - Hacker Model
    - Software monoculture (correlated) Risks
    - Defense Level
    - Loss; Cyber Insurance & Premium

Broad Outline of Presentation

3. Numerical Analysis

- Comparative Statics
- Mean-Standard Deviation approach to finding an Optimal level of cyber security investment
- Balancing defense level and cost approach to finding an optimal level of security investment
- Target defense level approach to finding an optimal level of security investment

What is Cyber Risk ?

Any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems (includes networks & the internet).

Key Insurable Cyber Risks

- Theft
- Business interruption
- Legal suits alleging trademark/copyright infringement
- Malware (Malicious Software)
  - Software that is intended to damage or disable computers (systems)

Pricing Cyber Risk

Frequency

- Strength of Security System
  - Likelihood of intrusion
- Risk Management Culture
  - Control in place & role of compliance & audit
- Rating of Service Providers
  - Reliability of cloud providers, backup providers, website, etc
- Disaster Recovery
  - Ability to recover from attack

Pricing Cyber Risk

Severity

- Extortion
- Legal Fees & Fines
- Lost Income
- IT Staff Costs
- PR & Marketing Costs
- Customer Support

Defender Capabilities

Defensible Actions:

- **Detect:** verify that some attacker is looking around
- **Deny:** prevent the attacker from gaining information
- **Disrupt:** stop or change outbound traffic (to attacker)
- **Degrade:** attack attacker's command & control
- **Deceive:** interfere with command & control
- **Contain:** network segmentation changes

The Hacker Model

A multi-firm, multiple-event, single-period (say a year) cyber security breach model.

An insurer's portfolio of *w* firms (policyholders) exposed to the considered type of cyber risk incidents.

Let $T = \{s, 1,2, \ldots, h\}$ be the set of all possible hackers and let $T_k \subseteq T$ be the set of hackers face by firm k for k=1,…,w.

N_{ki} = the numbers of type *i hac*kers attack firm *k* for each $i \in T_k$.

$\{N_{ki}\}$ are independent *Poisson process* with parameter λ_{ki}.

The Hacker Model

To model the software monoculture risk, we assume type s (i.e., *special*) hacker attacks all *w* firms simultaneously upon arrival; while other (i.e., non-special) types of hackers/threats attack only one firm upon arrival.

[e.g., a *special* type of software that is used by all firms.]

- By definition $N_{ks} = N_s$ for all *k=1,2,…,w*.
- The total number of hackers attack firm *k* is given by

$$N_s + \sum_{i \in T_k \setminus \{s\}} N_{ki} .$$

The Hacker Model

m_k = the level of counter measures implemented by firm *k*.

$$D_{kvij} = \begin{cases} 1 & if\ the\ v^{th}\ type\ j\ hacker\ breach\ counter\ measure\ level\ j\ of\ firm\ k \\ 0 & Otherwise. \end{cases}$$

$P(D_{kvij} = 1) \equiv d_{ij};\ 0 \le d_{ij} \le 1$ for all *k, i, j* and *v*.

The v^{th}type *i* hacker breach all firm k's counter measures

$$D_{kvi}(m_k) = \prod_{j=0}^{m_k} D_{kvij}$$

The probability that a type *i* hacker successfully breach firm *k*

$$d_i(m_k) \equiv P(D_{kvi}(m_k) = 1) = \prod_{j=0}^{m_k} d_{ij}\,.$$

The number of security breaches for each firm *k,*

$$B_k(m_k) = \sum_{v=1}^{N_s} D_{kvs} + \sum_{i \in T_k \setminus \{s\}} \sum_{v=1}^{N_{ki}} D_{kvi}$$

is a Poisson random variable with parameter $\lambda_s d_s(m_k) + \sum_{i \in T_k \setminus \{s\}} \lambda_{ki} d_i(m_k)$.

Defense Level

Defense Level = probability of no breaches.

1. Breaching process for the commonly used software is the same for all firms. ***Firm independent*** **or** ***identical breaching process*** **due to software monoculture risk.**

$$d_s(m_k) \equiv P(D_{kvs}(m_k) = 1) = d_s \ \& \ D_{kvs} = D_{1vs} \text{ for all } k \ \& \ v.$$

The probability of no breach for firm *k* & all firms

$$P(B_k(m_k) = 0) = e^{-(\lambda_s d_s + \sum_{i \in T_k \setminus \{s\}} \lambda_{ki} d_i(m_k))}$$

$$P(\sum_{k=1}^{w} B_k(m_k) = 0) = e^{-\left(\lambda_s d_s + \sum_{k=1}^{w} \sum_{i \in T_k \setminus \{s\}} \lambda_{ki} d_i(m_k)\right)}.$$

Defense Level

2. Breaching process for the commonly used software depends on the level of security that the firm implemented. ***Firm dependent*** **breaching process due to software monoculture risk**

$$d_s(m_k) \equiv P(D_{kvs}(m_k) = 1) \text{ for all } k \ \& \ v.$$

The probability of no breach for firm *k* & all firms

$$P(B_k(m_k) = 0) = e^{-(\lambda_s d_{ks}(m_k) + \sum_{i \in T_k \setminus \{s\}} \lambda_{ki} d_i(m_k))}.$$

$$P\left(\sum_{k=1}^{w} B_k(m_k) = 0\right) = e^{-\lambda_s (1 - \prod_{k=1}^{w} (1 - d_{ks}(m_k)))} e^{-(\sum_{k=1}^{w} \sum_{i \in T_k \setminus \{s\}} \lambda_{ki} d_i(m_k))}.$$

Cost Model

- $g_k(m)$ = firm *k*'s cost of security investment for maintaining countermeasure level *m.*
- Let L_{kli} denote the loss due to the l^{th}type *i* hacker breaches all counter measures of firm *k*.

Firm independent or identical loss due to software monoculture risk

We assume that $\{L_{kvs} \equiv L_{vs}; \text{all } k \text{ and } v \}$ are independent and identically distributed random variables with the first two moment of L_{kvs} as $l_s \; and \; l_s^{(2)}$.

The cost function for firm *k;* $C_k(m_k)$ can be written as

$$C_k(m_k) = g_k(m_k) + \sum_{j=1}^{N_s} D_{js} L_{js} + \sum_{i \in T_k \setminus \{s\}} \sum_{j=1}^{N_{ki}} D_{kji} L_{kji}$$

Cost Model-**Firm independent or identical loss due to software monoculture risk**

- Insurer Risk Pooling arrangement

$$\bar{C} = \left(\frac{1}{w}\right)\sum_{k=1}^{w} C_k(m_k);$$

$$E(\bar{C}) = \left(\frac{1}{w}\right)\sum_{k=1}^{w}\{g_k(m_k) + \lambda_s l_s d_s + \sum_{i\in T_k\setminus\{s\}} \lambda_{ki}\, l_{ki} d_i(m_k)\};$$

$$V(\bar{C}) = \left(\frac{1}{w}\right)^2 \sum_{k=1}^{w} V\left(C_k(m_k)\right) + \left(\frac{w(w-1)}{w^2}\right)\lambda_s l_s^{(2)} d_s.$$

If the number of firms *w* is sufficiently large central limit theorem implies that $\bar{C} \sim N\left(E(\bar{C}), V(\bar{C})\right)$.

Impact of correlated hackers' arrival process

$$V^{corr} - V^{ind} = l_s^{(2)} d_s(m_1)\lambda_{1s}\left(\frac{w-1}{w}\right) > 0.$$

Cyber Insurer Risk Pooling-**Firm dependent loss due to software monoculture risk**

We assume that $\{L_{kvs}$; all k and $v\}$ are independent and identically distributed random variables with the first two moment of L_{kvs} as l_{ks} and $l_{ks}^{(2)}$.

The cost function for firm k; $C_k(m_k)$ can be written as

$$C_k(m_k) = g_k(m_k) + \sum_{v=1}^{N_s} D_{kvs}\, L_{kvs} + \sum_{i \in T_k \setminus \{s\}} \sum_{v=1}^{N_{ki}} D_{kvi}\, L_{kvi}\,.$$

$$E(\bar{C}) = \left(\frac{1}{w}\right) \sum_{k=1}^{w} \{g_k(m_k) + \sum_{i \in T_k} \lambda_{ki}\, l_{ki} d_i(m_k)\}$$

$$V(\bar{C}) = \left(\frac{1}{w}\right)^2 \sum_{k=1}^{w} \sum_{i \in T_k} l_{ki}^{(2)} d_i(m_k) \lambda_{ki} + \left(\frac{1}{w^2}\right) 2 \sum_{1 \le k < r \le w} \lambda_s l_{ks} d_s(m_k) l_{rs} d_s(m_r)\,.$$

Impact of correlated hackers' arrival process

$$V^{corr} - V^{ind} = \left(\frac{1}{w}\right)^2 2 \sum_{1 \le k < j \le w} \lambda_{1s} l_{ks} l_{js} d_s(m_k) d_s(m_j) > 0.$$

Optimal level of cyber security investment

Cyber insurance premium formula

$$p(\theta_\alpha) = E(\bar{C}) + \theta_\alpha\sqrt{V(\bar{C})} = E(\bar{C})(1 + \frac{\theta_\alpha\sqrt{V(\bar{C})}}{E(\bar{C})})$$

where θ_α represent the weight that measure our attitude towards risk and is an appropriate critical value for confidence level $1 - \alpha$ of the normal distribution.

- $\frac{\theta_\alpha\sqrt{V(\bar{C})}}{E(\bar{C})}$ is the loading associated with the cyber insurance contract.
- Let $p^{FISBP}(\theta_\alpha)$ (respectively, $p^{FDSBP}(\theta_\alpha)$) denote the pricing formula obtain by assuming firm independent of security breaching process (respectively, firm dependent of security breaching process) for the commonly used software.

Comparative Statics

For each *k* and *i* we have

- $\frac{\partial p^{FISBP}(\theta_\alpha)}{\partial \lambda_s} > 0$; $\frac{\partial p^{FDSBP}(\theta_\alpha)}{\partial \lambda_{ki}} > 0$; $\frac{\partial p^{FISBP}(\theta_\alpha)}{\partial l_{ks}} > 0$; $\frac{\partial p^{FDSBP}(\theta_\alpha)}{\partial l_{ki}} > 0$;
- $\frac{\partial p^{FISBP}(\theta_\alpha)}{\partial d_s} > 0$; $\frac{\partial p^{FISBP}(\theta_\alpha)}{\partial l_{ki}^{(2)}} > 0$; $\frac{\partial p^{FDSBP}(\theta_\alpha)}{\partial l_{ks}^{(2)}} > 0$;
- $\frac{\partial p^{FDSBP}(\theta_\alpha)}{\partial d_s(m_k)} > 0$; $\frac{\partial p^{FDSBP}(\theta_\alpha)}{\partial d_i(m_k)} > 0$; $\frac{\partial p^{FISBP}(\theta_\alpha)}{\partial d_i(m_k)} > 0$.
- These results justify our intuition: $p^{FISBP}(\theta_\alpha)$ and $p^{FDSBP}(\theta_\alpha)$ are *increasing function of number of hackers/attacks, breaching probabilities* and *the first two moments of loss*.
- Provide justification for the insurer to *offer premium discount* if the firm *actively engages in reducing* these sources of risks.

Mean-Standard Deviation approach to finding an Optimal level of cyber security investment

- We formulate the following optimization problem to find a set of counter measures which minimizes the premium or cost incurred (OP-I)

$$\min_{(m_1, m_2, \ldots, m_w)} p(\theta_\alpha) = E(\bar{C}) + \theta_\alpha \sqrt{V(\bar{C})}$$
$$s.t.\ 0 \leq m_k \leq u \ \ for\ k = 1,2, \ldots, w$$

u is the maximum level of security level available;

θ_α is the critical value for confidence level $1 - \alpha$ of the normal distribution (i.e., the weight that measure our attitude towards risk).

Mean-Standard Deviation approach to finding an Optimal level of cyber security investment

Lemma 1: Let $m^*(\theta)$ denote the optimal solution to (OP I) as a function of θ. Then we have

$$m^*(\theta) \geq m^*(0).$$

This result confirms our intuition that mean analysis ignores the variability of loss cost and hence underestimated the level of cyber security investment.

Lemma 2: For (OP I-I), the optimal value for the case of firm independent loss due to software monoculture risk is larger than the optimal value for the case of firm dependent loss due to software monoculture risk.

Mean-Standard Deviation approach to finding an Optimal level of cyber security investment

(OP-I) simplifies substantially for the special case of mean analysis ($\theta = 0$). (OP-I) a *w* variables optimization problem reduces to *w* individual firm optimization problem with a single variable, the firm's cyber security investment level.

Lemma 3. Suppose that $\theta = 0$. Then the solution for (OP I) is the same as the individual firm solution. Let m_i^* denote the optimal solution to the firm *i*'s minimization of expected cost problem. That is, m_i^* is the solution to the following optimization problem

$$\min_{0 \le m \le u} E\big(C_i(m)\big).$$

Then, $(m_1^*, m_2^*, \dots, m_w^*)$ is the optimal solution for (OP I).

Numerical results – identical suppliers (OP I-I)

Sensitivity analysis on numerical results obtained from solving (OP I-I).

Base Case Data

- $T = T_1 = T_k = \{s,1,2,3\};$
- $1 \leq k \leq w = 30; 1 \leq i \leq 3; 0 \leq m \leq u = 70;$
- $\lambda_s = 156;\ \lambda_1 = \lambda_2 = \lambda_3 = 104; d_s = 0.25;$
- $d_1(m) = d_2(m) = d_2(m) = (0.8)^{m+1};$
- $d_s(m) = (0.25)^{m+1}; l_s = 75; l_1 = l_{ki} = 50;$
- $l_s^{(2)} = 2 * {l_s}^2 = 11250;\ l_1^{(2)} = l_{ki}^{(2)} = 2 * {l_1}^2 = 5000;$
- $g_1(m) = g_k(m) = 5m + 10m^2$

Table 1 Optimal m: sensitivity analysis of the value of $g(m)$

$g(m) = 5m + 10m^2$ **(FISBP,FDSBP)**

$g(m)$=base	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
0.1*base	(19,19)	(19,20)	(19,20)
0.5*base	(13,13)	(14,14)	(14,14)
base	(11,11)	(11,11)	(11,11)
2*base	(9,9)	(11,11)	(11,11)
4*base	(7,7)	(11,11)	(11,11)
10*base	(5,5)	(11,11)	(11,11)
15*base	(4,4)	(11,11)	(11,11)
20*base	(3,3)	(11,11)	(11,11)
40*base	(2,2)	(11,11)	(11,11)
80*base	(1,1)	(11,11)	(11,11)

TABLE 2 OPTIMAL M: SENSITIVITY ANALYSIS OF THE VALUE OF l_1

l_1 **(FISBP,FDSBP)** $\{{l_1}^{(2)} = 2(l_1)^2\}$

l_1	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
50	(11,11)	(11,11)	(11,11)
150	(15,15)	(15,15)	(15,15)
300	(17,17)	(17,18)	(17,18)
600	(20,20)	(20,20)	(20,20)
1500	(23,23)	(24,24)	(24,24)
3000	(26,26)	(26,27)	(27,27)
6000	(29,29)	(30,30)	(30,30)
10000	(31,31)	(32,32)	(32,32)
15000	(32,32)	(34,34)	(34,34)
20000	(33,33)	(35,35)	(36,36)

Table 3 Optimal m: sensitivity analysis of the value of d_s

d_s (FISBP,FDSBP)			
d_s	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
0.01	(11,11)	(11,11)	(11,11)
0.05	(11,11)	(11,11)	(11,11)
0.1	(11,11)	(11,11)	(11,11)
0.25	(11,11)	(11,11)	(11,11)
0.4	(11,11)	(11,11)	(11,11)
0.5	(11,11)	(11,11)	(11,11)
0.65	(11,12)	(11,12)	(11,12)
0.8	(11,13)	(11,13)	(11,13)
0.95	(11,16)	(11,17)	(11,17)
0.99	(11,13)	(11,13)	(11,13)

Table 4 Optimal m: sensitivity analysis of the value of λ_1

λ_1 (FISBP,FDSBP)			
λ_1	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
52	(9,9)	(9,9)	(9,9)
104	(11,11)	(11,11)	(11,11)
156	(13,13)	(13,13)	(13,13)
208	(13,13)	(13,13)	(13,13)
260	(14,14)	(14,14)	(14,14)
312	(15,15)	(15,15)	(15,15)
364	(15,15)	(15,16)	(15,16)

Balancing defense level and cost approach to finding an optimal level of security investment

Our objective is to maximizes defense level subject to a given constraint of budget allocated for security investment ***K*** (OP II)

$$\max_{(m_1,m_2,\ldots,m_w)} P\left(\sum_{k=1}^{w} B_k(m_k) = 0\right)$$

$$s.t. \quad E(\bar{C}) + \theta_\alpha \sqrt{V(\bar{C})} \leq \boldsymbol{K}$$

$$0 \leq m_k \leq u \;\; for\; k = 1,2,\ldots,w.$$

Let us define for the case of identical firms

$$m^d(K) = argmax\{m | E(\bar{C}(m)) + \theta_\alpha \sqrt{V(\bar{C}(m))} \leq \boldsymbol{K}; 0 \leq m \leq u\}.$$

Then we have $m^d(K)$ as the optimal solution for (OP II).

Maximum Defense Level achieves given budget K

Firm independent breaching process due to software monoculture risk

$$\mathrm{P}\left(\sum_{k=1}^{w} B_k\left(m^d(K)\right)=0\right)=e^{-\lambda_s d_s - w\sum_{i\in T_1\setminus\{s\}}\lambda_{1i}d_i\left(m^d(\boldsymbol{K})\right)}$$

Firm dependent breaching process due to software monoculture risk

$$\mathrm{P}\left(\sum_{k=1}^{w} B_k\left(m^d(K)\right)=0\right)$$

$$=e^{-\lambda_s\left(1-\left(1-d_s\left(m^d(K)\right)\right)^{w}\right)-w\sum_{i\in T_1\setminus\{s\}}\lambda_{1i}d_i\left(m^d(\boldsymbol{K})\right)}.$$

Target defense level approach to finding an optimal level of security investment

Our objective is to seek a level of cyber security investment that minimized cost and achieved certain target defense level. Let δ be the firm's minimum acceptable or targeted defense level. The resulting optimization problem is (OP III)

$$\min_{(m_1,m_2,\ldots,m_w)} p(\theta_\alpha) = E(\bar{C}) + \theta_\alpha \sqrt{V(\bar{C})}$$

$$s.t. \quad P(B_k(m_k) = 0) \geq \delta \qquad \text{for } 1 \leq k \leq w$$

$$0 \leq m_k \leq u \;\; for \; k = 1,2,\ldots,w$$

Numerical results – identical suppliers (OP III)

Base case data: it is not feasible for the FISBP model to achieve the targeted service level, δ = 0.95 and 0.98.

Numerical results: assume FDSBP

$$\min_{m_1} g_1(m_1) + \sum_{i \in T_1} \lambda_{1i}\, l_{1i} d_i(m_1)$$

$$+\theta_\alpha \sqrt{\left(\frac{1}{w}\right)\left(\sum_{i \in T_1} \lambda_{1i}\, l_{1i}^{(2)} d_i(m_1)\right) + \left(\frac{w-1}{w}\right)\lambda_s l_{1s}{}^2 d_s(m_1)^2}$$

$$s.t.\quad P(B_k(m_1) = 0) = e^{-(\lambda_s d_{ks}(m_1) + \sum_{i \in T_k \setminus \{s\}} \lambda_{ki} d_i(m_1))} \geq \delta;$$

$$0 \leq m_1 \leq u.$$

Table 5 Optimal m: sensitivity analysis of the value of $g(m)$

$g(m) = 5m + 10m^2$ **FDSBP-(95%.98%)**			
$g(m)$**=base**	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
0.1*base	(54,58)	(54,58)	(54,58)
0.5*base	(54,58)	(54,58)	(54,58)
base	(54,58)	(54,58)	(54,58)
2*base	(54,58)	(54,58)	(54,58)
4*base	(54,58)	(54,58)	(54,58)
10*base	(54,58)	(54,58)	(54,58)
15*base	(54,58)	(54,58)	(54,58)
20*base	(54,58)	(54,58)	(54,58)
40*base	(54,58)	(54,58)	(54,58)
80*base	(54,58)	(54,58)	(54,58)

Table 6 Optimal m: sensitivity analysis of the value of l_1

l_1 FDSBP-(95%.98%){$l_1^{(2)} = 2(l_1)^2$}			
l_1	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
50	(54,58)	(54,58)	(54,58)
150	(54,58)	(54,58)	(54,58)
300	(54,58)	(54,58)	(54,58)
600	(54,58)	(54,58)	(54,58)
1500	(54,58)	(54,58)	(54,58)
3000	(54,58)	(54,58)	(54,58)
6000	(54,58)	(54,58)	(54,58)
10000	(54,58)	(54,58)	(54,58)
15000	(54,58)	(54,58)	(54,58)
20000	(54,58)	(54,58)	(54,58)

Table 7 Optimal m: sensitivity analysis of the value of d_s

d_s **FDSBP-(95%.98%)**			
d_s	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
0.01	(54,58)	(54,58)	(54,58)
0.05	(54,58)	(54,58)	(54,58)
0.1	(54,58)	(54,58)	(54,58)
0.25	(54,58)	(54,58)	(54,58)
0.4	(54,58)	(54,58)	(54,58)
0.5	(54,58)	(54,58)	(54,58)
0.65	(54,58)	(54,58)	(54,58)
0.8	(56,60)	(56,60)	(56,60)
0.95	(infeasible,infeasible) ; (infeasible,infeasible)	(infeasible,infeasible) ; (infeasible,infeasible)	(infeasible,infeasible) ; (infeasible,infeasible)
0.99	(infeasible,infeasible) ; (infeasible,infeasible)	(infeasible,infeasible) ; (infeasible,infeasible)	(infeasible,infeasible) ; (infeasible,infeasible)

Table 8 Optimal m: sensitivity analysis of the value of λ_0

λ_0 FDSBP-(95%.98%)			
λ_0	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
52	(51,55)	(51,55)	(51,55)
104	(54,58)	(54,58)	(54,58)
156	(56,60)	(56,60)	(56,60)
208	(57,61)	(57,61)	(57,61)
260	(58,62)	(58,62)	(58,62)
312	(59,63)	(59,63)	(59,63)

QUESTION?

yslee@uic.edu