RHUL-KU workshop
“Cyber Insurance as an Actuary Economics”
A Study of Security Management with Cyber Insurance

Kyushu University

Tomohisa Ishikawa (CISSP, CISA, CISM, QSA, CFE)
Kouichi Sakurai (Ph.D)

1. Introduction

2. About Cyber Insurance

3. Simulation Analysis

4. Wrap-Up

1. Introduction

2. About Cyber Insurance

3. Simulation Analysis

4. Wrap-Up

Research Background

■ Motivation

- Security Investment Model, The Modeling of Security Behavior and Response

■ Problem

- Many companies recognize the necessity of security investment.
- However, there is not a practical method to consider the appropriate security investment value, and it is very difficult to know the cost-benefit

■ Solution

- We propose the cost-benefit analysis using simulation model.
- By using above analysis, we are going to evaluate the cost-benefit of “Cyber Insurance” as security investment.

Related Works

■ Related works for the estimation of appropriate security investment

- Including damage cost estimation, there are 4 approaches.

■ 1. Mathematical Modeling Approach

- By building the mathematical model, this approach estimates security investment condition under the particular condition

- **Gorden & Loeb Model（2002）**
- If the information leakage probability function S(v,z) is defined by a particular mathematical function with the vulnerability v and security investment z, the security investment should be less than 1/e (= 36.79%)
  - Gordon, L.A. ,Loeb, M.P, *The Economics of In-formation Security Investment*, ACM Transactions on Information and System Security, Vol. 5, No. 4,November 2002, Pages 438-457.

- It is a very clear model, but it is an abstract model, and it is hard to apply practical situation.

Related Works

■ 2. Analytical Framework Approach

- This approach is for damage cost estimation, and this approach provide the viewpoints and items for calculating damage cost
- By the calculation of damage cost, the security manager can know necessary limitation for the investment.

COUNTRY	Org.	Analytical Framework
Japan	IPA	• （2001）Damage Cost Estimation Model • （2004）Security Accounting Model
	JNSA	• （2002）Security Incident Cost Estimation Model • （2002）JO Model
Korea	KISA	• （2006）KISA Model
	KAIST	• （2010）Internet Incident Damage Evaluation Model（※１）
U.S. EU	-	• （-）ROSI Model（Return On Security Investment）
	The Economist	• （2014）CyberTab

- （※１）KAIST security researcher team estimates that 867.2 billion won in 3.20（Korean Cyber Terrorism Attack）

Related Works

■ 3. Statistical Data Approach

- This approach provides the statistics by using the data from the service and the survey by security vendors.
- Since it is very clear figures, many companies use them as the benchmarks.

- **Incapsula（2014）**
- DDoS Attack Cost is $40,000 per hour.
  - Incapsula, *Incapsula Survey : What DDoS Attacks Really Cost Businesses*, 2014, https://www.incapsula.com/blog/ddos-impact-cost-of-ddos-attack.html

- **Ponemon Institute（2015）**
- The average information leakage cost per record is $157
  - Ponemon Institute, *2015 Cost of Data Breach Study*, 2015, http://www-03.ibm.com/security/data-breach/

Related Works

■ 4. Simulation Approach

- Based on the data from the statistical data approach, this approach calculates more realistic data by using Monte Carlo approach
  - Conrad, J.R., Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations, IEEE, March 2005
  - Burtescu, E., Decision Assistance in Risk Assessment Monte Carlo Simulations, Informatica Economica, Vol.16, No. 4, (2012).
  - Lyon,D., Modeling Security Investments With Monte Carlo Simulations, SANS Institute: Reading Room, 2014

- As long as the security managers have data, they can evaluate the cost-benefit of security investment, and it is very easy to apply the actual case.
- In this research, our team would like to evaluate the effects of cyber insurance.

1. Introduction

2. About Cyber Insurance

3. Simulation Analysis

4. Wrap-Up

Cyber Insurance

■ Cyber Insurance

- It is one of the risk management strategies
  - Avoid, Mitigate, Accept, Transfer
- The market size in the U.S. is 1 billion dollars in 2013
- Target leaks massive customer information, and the 1/3 of total costs for security incidents were covered by cyber insurance.

■ Target (2013)

● By POS Malware, Company leaks 40M card info. and 70M Personal Information.

Countermeasure Cost **$252M**

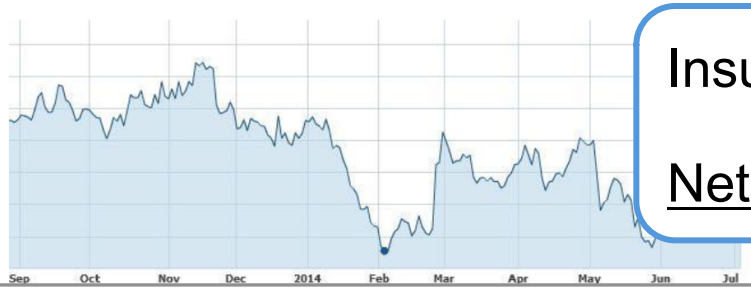
→ It is calculated with IR report published in 2014 4Q

Class Action **$10M**

→ In 2015 March, Target agree to pay $10M as the compensation in one class action

Stock Decrease **-8$/stock**

→ the stock price after the announcement of information leakage



Insurance	90 million dollars
Net Cost	162 million dollars

Cyber Insurance

The Recognition of Cyber Insurance

- According to IPA research, only 28.2% knows the details of cyber insurance.
  - IPA, Cyber Risk Management Survey 2015
    https://www.ipa.go.jp/files/000045629.pdf

The Characteristics of Cyber Insurance（Japan）

- Several insurance companies provide cyber insurance service. All insurance SLA and the benefit by insurances is almost same, and they covers all perspectives in security incident.
- （Ex）Tokio Marine Nichido, Mitui Sumitomo Insurance, AIU

- （Ex）AIU Insurance
  - The cost for the compensation
  - The cost for administrative procedure
  - The cost for incident response

Cyber Insurance

■ The Characteristics of Cyber Insurance（International）

- There are no difference of the coverage between Japanese insurance and foreign insurance, but foreign insurance tends to cover the compensation for class actions and penalty.

- Ex）Data Protection Law in U.K.
  - The government penalized the organizations which do not provide adequate information security countermeasures.
  - Ex）Sony Computer Entertainment Europe(2011)　Penalty 250,000 £

- Ex）PCI-DSS（Payment Card Industry Data Security Standard）
  - The security guideline formulated by card brand companies
  - All organizations treating credit cards should follow this guideline
  - The compliance violation causes the penalty ($5,000 ~ $100,000)

- Ex）HIPAA（Health Insurance Portability and Accountability Act）
  - The compliance violation causes the penalty
  - Ex）WellPoint（2013）　Agree to pay $170M penalty

Cyber Insurance

■ The Characteristics of Cyber Insurance（International）

- SEC (OEIC(Securities and Exchange Commission) recommendation
  - Also, some organization such as SEC OCIE (Office of Compliance Inspections and Examinations) recommended to have Cyber Insurance to financial sector and 44% of scoped company join into cyber insurance.

- AIG Insurance
  - AIG announced that the coverage of cyber insurance expands the damage of human body and physical device. (It means cyber insurance starts to cover IoT cyber incident)
  - http://money.cnn.com/2014/04/23/technology/security/aig-cybersecurity-insurance/

Cyber Insurance

■ Cyber Insurance Research Trend

- Academic : Several studies from economics and mathematical modeling
- Practical : It is very hard to building the model because of lack of data
  - http://jp.reuters.com/article/2014/07/15/idJPL4N0PQ19O20140715

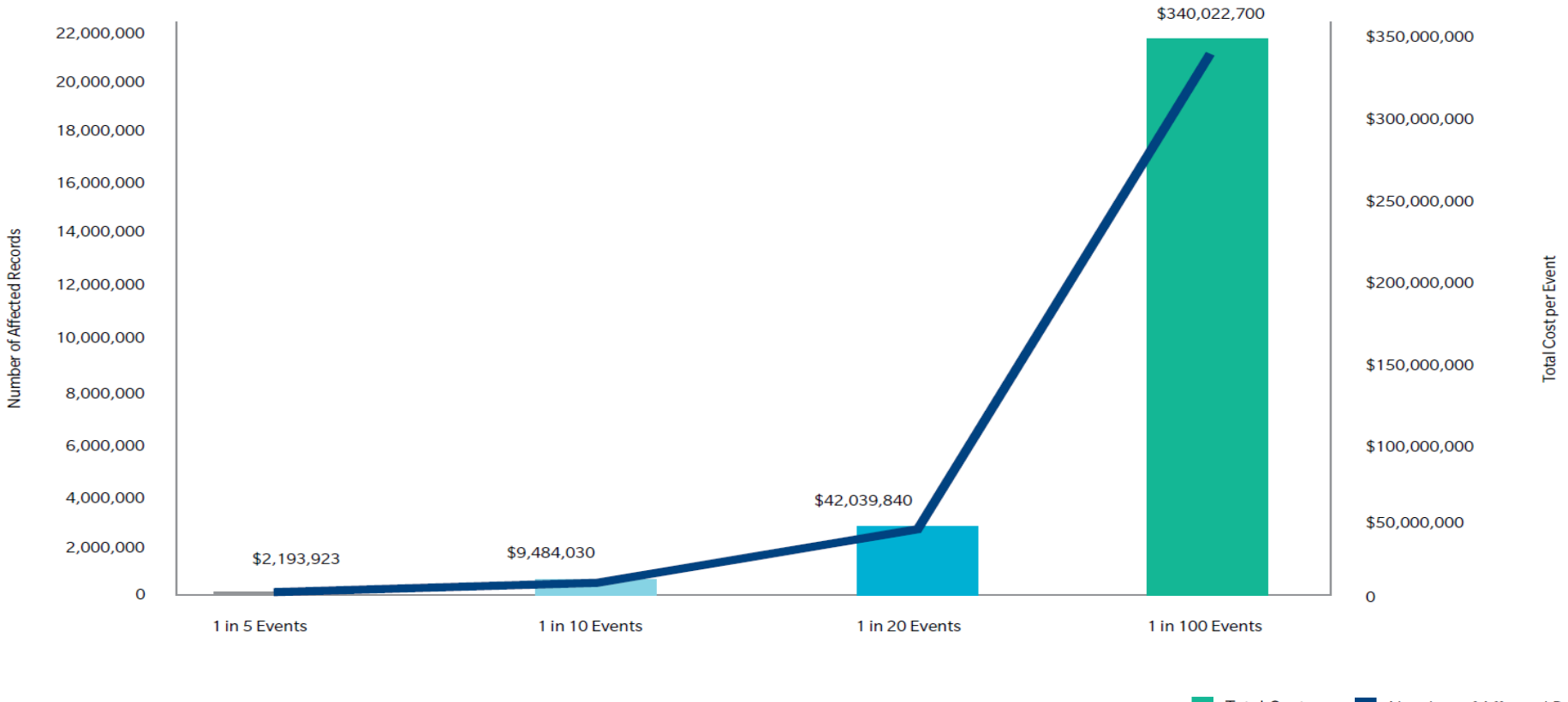
- Several Organization starts to publish the report recently.
  - NetDiligence 2015 Cyber Claims Study
  - Marsh & McLennan A Cyber Security：A Call to Action,
  - Marsh & McLennan Cyber Security Overview
  - Insurance Information Institute Cyber Risk: Threat and Opportunity

Cyber Insurance

■ Cyber IDEAL – Marsh's Model

- Marsh develop the model analysis methods to calculate risks.

FIGURE 3: RETAIL EXPOSURE FOR A 1-IN-100 EVENT (US$)



引用：MARSH & McLENNAN Companies, A CYBERSECURITY: CALL TO ACTION, (Nov 2014)

Cyber Insurance

■ Actual Example - Cyber Insurance Claims

- Target (2013.12)
  - POS Malware breach (40M card info, 70M PII)
  - The countermeasure costs are $ 252M (@ 2014 financial report)
  - The insurance covers $ 90M (35.7% of countermeasure costs)

- Home Depot (2014.09)
  - 56M card info leakage
  - The countermeasure cost would be $62M, but $27M returns by cyber insurance.
  - It means 43.5% will be covered by cyber insurance

- Sony Picture (2014.11)
  - Sony pictures hacking damage are estimated as more than $100M
  - However, this damages are covered by the insurance

1. Introduction

2. About Cyber Insurance

3. Simulation Analysis

4. Wrap-Up

The Cost-Benefit Analysis by the Simulations

■ This study methods

- In this research, we analyze the cost-benefit analysis by using the simulation. We will seek optimal security investment value, and we will solve the problems of the uncertainty of security investment criteria and cost-benefit.

- In this study, we assume virtual model company(e-commerce) and we will discuss the investment and cost-benefit. We will use the data from “statistical data approach” and the data disclosed by “SOUND HOUSE” as necessary data for simulation.

- **What is “SOUND HOUSE”?**
  - E-commerce company dealing with audio and instrument
  - In 2008, this company leaks 97,500 customer records by SQL Injection
    - Customer Records: name, e-mail address, password, the date of birth
    - Credit card information is also leaked for some customers.
  - Presidents take the policy to disclose the details of security incidents
    (→In this research, we used this data for some parameters)

What is SQL Injection?

SQL Injection is a high risk problem that allows the attacker to retrieve data accumulated in a database or execute an arbitrary command on the server by executing an illegal SQL statement on a web application.

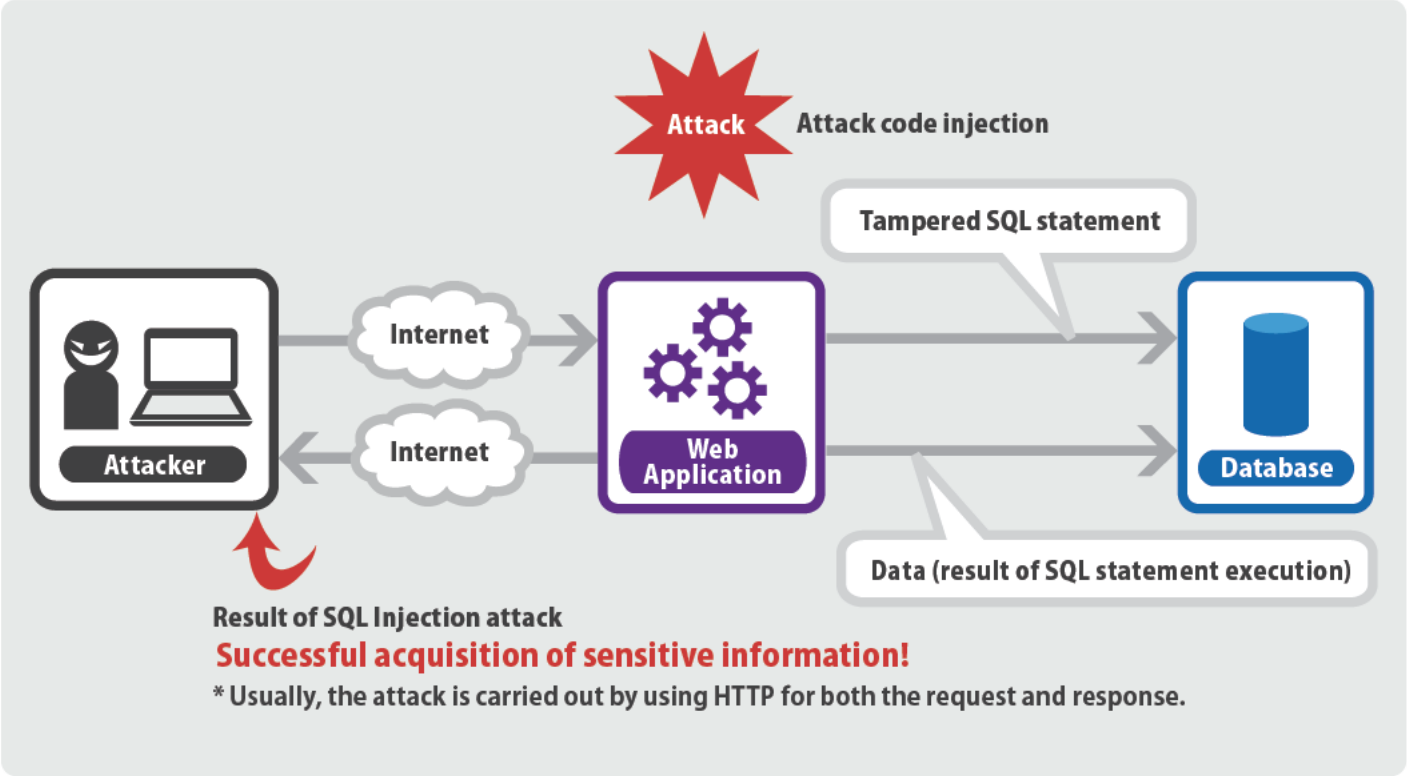


Figure 9. Image of SQL Injection

The Cost-Benefit Analysis by the Simulations

■ The conditions for the simulations are followings.

- Virtual model company is e-commerce company, and we use data from “SOUND HOUSE” and “Statistical Data Approach”
  - Web sites have only “SQL Injection” vulnerability, and the model company does not know whether or not owned websites have the vulnerability.
  - The targeted data is only customer information data, and the number of leakages should be determined by the data from Ponemon Institute and triangle distribution
  - We assume two security investments, “security assessment” which decrease the existence of SQL Injection, and “cyber insurance” that compensate the parts of damage costs.
  - We define the damage costs as the total of following.
    Investment Cost + Incident Response Cost + Compensation Cost + QA Cost

The Results and Analysis

■ The Results and Analysis （1 Million Case）

- The comparison of average cost can show the benefits of investments
- In CASE 4, ROSI will be four times bigger.
  - ROSI（Return on Security Investment）is the ratio how much returns the security investment will brings. In CASE 2, by investing 4 million yen as the security assessment, the average cost decrease 13.624 million yen. Therefore, ROSI should be 3.406.

Cyber Insurance

Table 10: Simulation Scenarios

		Investment 2	
		No	Yes
Investment 1	No	CASE 1	CASE 3
	Yes	CASE 2	CASE 4

Security Assessment

Table 11: Result （Unit Price : case, million Yen）

	CASE1	CASE 2	CASE 3	CASE 4
SQLI Ratio	16.72%	5.00%	16.72%	5.00%
Cyber Insrance	No	No	Yes	Yes
Sucess of Attack	167,141	50,136	167,232	50,215
Total Cost (Min)	0.000	4.000	0.500	4.500
Total Cost (Max)	301.083	304.739	171.834	175.726
Total Cost (Ave)	25.172	11.548	8.829	6.999
Average Relative Cost	1	0.459	0.351	0.278
ROSI	-	3.406	32.686	4.038

1. Introduction

2. About Cyber Insurance

3. Simulation Analysis

4. Wrap-Up

Wrap-Up

■ Wrap-Up

- We need to build the model that provides the practical investment criteria and cost-benefit analysis.
- In order to solve above problems, we proposed the cost-benefit analysis methods by using the simulation, and we verified them.
- By the result of the simulation, the ROSI by “Security Assessment” and “Cyber Insurance” became 4 times.

Questions ???

Thank you for your time & attention

Feel Free to Contact Me