On the development of cyber insurance market: a legal aspect

1.Introduction

Cyber insurance is one of the effective tools to transfer cyber and IT security risk and minimize potential financial losses. Take the example of Sony's personal information security breach, Sony made a cyber insurance claim to mitigate the losses. In Taiwan, the cyber insurance market demand was driven by Taiwan's Personal Information Protection Act (PIPA) which was passed in April 2010 and implemented in Oct 2012. According to PIPA, a non-government agency including the natural persons, juridical persons, or group shall be liable for the damages caused by their illegal collection, processing or using of personal information or other ways of infringement on the rights of the individual whose personal information was collected, processed or used. The non-government agency may thus pay each individual NT$500 to NT$20,000 and the total compensation amount in each case may be up to NT $200 million if there is no evidence for actual damage amount.

However, the cyber insurance market does not prosper as expected one hand because of the absence of incentives of insurance companies to develop and promote the cyber-insurance products and on the other hand because of the unaffordable price that deters many companies from buying the insurance. Some countries have tried to identify the incentives and barriers for the cyber insurance market and have taken some measurements to kick start its development. In this paper, the barriers for the cyber insurance market were addressed and how American government promoted this market was mentioned. Finally, suggestions on how to stimulate the cyber insurance market growth were proposed for reference.

2.What is cyber insurance?

Insurance means the parties concerned agree that one party pays a premium to the other party, and the other party is liable for pecuniary indemnification for damage caused by unforeseeable events or force majeure1. Thus, the cyber insurance means the parties concerned agree that one party pays a premium to the other party, and the other party is liable pecuniary indemnification for damage caused by cyber security breach. The cyber insurance usually covers the insured's losses (or costs) and his liabilities to the third party. For example, the insured was to be liable for the damages caused by the unlawful disclosure of identifiable personal information belonging to the third party resulted from the insured's negligence. 2Typically, cyber insurance covers penalties or regulatory fines for data breaches, litigation costs and compensation arising from civil suits filed by those whose rights are infringed, direct costs to notify those whose personal data was illegal collected, processed or used and so on. 3

3.What are the barriers for cyber insurance market?

Per the report made by European Network and Information Security Agency in2012, the following issues have significant influence on incentives of insurers to design and provide cyber –insurance products, including uncertainty about the extent of risk and lack of robust actuarial data, uncertainty about what risk is being insured, fast-paced nature of the use of technology, little visibility on what constitutes effective measures, absence of insurer of last resort to re-insure catastrophic risks, and perception that existing insurance already covers cyber-risks 4. In Taiwan, insurance companies face the same issues as mentioned above when they tried to develop and promote the cyber-insurance products. However, what discourages the insurance and re-insurance companies from investing in the cyber-insurance market most is the lack of accurate information to figure out the costs associated with different information security risk and thus to price the cyber insurance contract precisely.

Several cases involving personal data breach did happened after Taiwan's PIPA became effective on Oct 1th 2012, but few verdicts have been made. It is not easy to master the direct costs or losses resulting from violation of PIPA, including penalties or fines from regulator,, compensation to the parties of the civil suit who claim their personal data were unlawfully collected, processed or used, litigation costs and so on. Otherwise, indirect costs or losses such as media costs, costs to regain reputation or trust of consumers, costs of deployment of proper technical measures to prevent the data breach from happening again etc. are difficult to calculate. Therefore, it is not easy to identify the costs of information security risk and thus to calculate the premium the insured has to pay precisely.

The rapid development of technology also has a negative impact on the ability of the insurers to master the types of the information security risk which shall be insured and its costs. Accompanied with the convenience and efficiency of applying new technologies into the working environment, security issues arise, too. For example, the loss or theft of mobile or portable devices may result in data breaches. In 2012, an unencrypted laptop computer with personal information and other sensitive information of one of NASA's employees was stolen from his locked vehicle and this led to thousands of NASA's workers and contractors at risk. 5And, per the report made by a NASA inspector, similar data breaches had been resulted from the lost or theft of 48 NASA laptops and mobile computing devices between April 2009 and April 2011. 6

There is no singe formula which could guarantee 100% security, but some international organizations have promulgated best practices for information security management, such as ISO 2700x standards. 7In Taiwan, Bureau of Standards, Metrology and Inspection (BSMI) which belongs to the Ministry of Economic also consulted ISO standards and announced Chinese National Standards on information security. For example, BSMI consulted ISO 27001 "Information technology – Security techniques – Information security management systems – Requirements" and then promulgated CNS27001. Theoretically, if the company who tries to buy cyber insurance policy that covers data breaches and damages to customers' data privacy can show that it has adopted and do implement the suite of security management standards well, the premium could properly be reduced because such company shall face less security risk. 8 However, it is still not easy to

price the cyber insurance contract rightly because of no enough data or evidence which could approve what constitutes effective information security measures as well as no impartial, controversial or standard formula to value intangible assets like personal or sensitive information. 9 Finally, the availability of re-insurance programs plays an important role in the cyber insurance market because insurers would appeal to such program as a strategy of risk management. The lack of solid and actual data as mentioned above would discourage re-insurers from providing insurance policies that covers the insured's losses and liabilities. Therefore, insurers may not be keen to develop and offer cyber insurance products.

4.The USA experience on developing cyber insurance market

4.1Current market status

Due to the increase of the number of data breaches, cyber attacks, and civil suits filed by those whose data were illegal disclosed to third parties, more and more enterprises recognize the importance of cyber and privacy risks and turning to cyber insurance to minimize the potential finical losses. 10 However, the increased government focus on cyber security also contributed to the rapidly growth of the cyber insurance market. 11 For example, US Department of Homeland Security has been aware of the benefits of the cyber insurance, including encouraging better information security management, reducing the finical losses that a company has to face due to the data breach and so on. 12

Compared to other lines of insurance, cyber insurance market is not mature yet and is small in USA. For example, the gross premiums for medical malpractice insurance are more than 10% of that for cyber insurance market. However, the cyber insurance market certainly appears to grow rapidly. Per the survey made by Corporate Board Member & FTI Consulting, 48% of corporate directors and 55% of general counsel take highly of the issue of data security. 13And, per the report made by Marsh, there are more and more companies buying cyber insurance to cover financial losses due to the data breach or cyber attack, and the number of Marsh's US clients purchasing cyber insurance increased 33% in 2012 over 2011. 14

4.2What contributed to the growth of the cyber insurance market in USA?

Some measurements taken by the government or regulatory intervention had impacts on the incentives of companies to carry cyber insurance. CF Disclosure Guidance published by U.S. Securities and Exchange Commission in Oct 2011 mentioned that except the operation and financial risks, public companies shall disclose the cyber security risks and cyber incidents for such risks and incidents may result in severe finical losses and thus have a board impact on their financial statements. 15 And, according to the guidance, appropriate disclosures may includes risk factors and this potential costs and consequences, cyber incidents experienced or expected and theirs costs and consequences, undetected risks related to cyber incidents, and the relevant insurance coverage. 16 Such disclosure requirements triggered the demands for the cyber insurance products because cyber insurance as an effective tool to transfer financial losses or damages could be an evidence that firms are managing cyber security risks well and properly. 17

The demand for cyber-insurance products may be created by government by means of requiring government contractors and subcontractors to purchase cyber insurance under Federal Acquisition Regulations (FAR) which mentions that contractors are required by law and FAR to provide insurance for certain types of perils 18. Also, in order to sustain the covered critical infrastructure (CCI) designation, the owner of such infrastructure may need to carry cyber insurance, too. 19

On the other hand, referring to Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 which requires those who provides Federal and non-Federal Government customers with a qualified/certificated anti-terrorism technologies shall obtain liability insurance of such types but the amount of such insurance shall be reasonable and will not distort the sales price of such technologies 20, the federal government tried to draw and enact legislation that provides limitations on cyber security liability 21. If it works, this could raise the incentive of insurers because amounts of potential financial losses which may be transferred to insurers are predictable.

Besides, referring to Terrorism Risk Insurance Act of 2002 which established the terrorism insurance program to provide compensations to insurers who suffered the insured losses due to terrorist attacks 22, the federal government may increase the supply of cyber insurance products by means of providing compensations to insurers who suffered the insured losses due to cyber security breach or cyber attacks. 23 Otherwise, some experts and stakeholders did suggest the federal government implement reinsurance programs to develop cyber insurance programs. 24

Finally, to solve the problem of information asymmetry, the government tried to develop the legislation that could build a mechanism for information-sharing among private entities. 25 Also, it was recommended that the federal government may consider to allow insurance firms to establish an information-sharing database together so that insurers could accordingly develop better models to figure out cyber risks and price the cyber insurance contract accurately. 26

5.Suggestions and conclusion

Compared to USA where 30-40 insurers offer cyber-insurance products and thus suggested that a more mature market exists 27, the cyber insurance market in Taiwan is still at the first stage of the product life cycle. Few insurers have introduced their cyber-insurance products covering the issues related to the personal information breach. Per the experience how US government developed the cyber insurance market, the following suggestion are made for reference. First, the government may consider requiring his contractors and subcontractors to carry cyber insurances. This could stimulate the demand for cyber insurance products as well as make cyber insurance prevail among private sector as an effective risk management tool. Second, the government may consider establishing re-insurance program to offer compensation to those who suffer the insured's large losses and damages or impose limitations of the amount insured by law. However, it is undeniable that providing re-insurance program is not feasible as the government's budget is not abundance. Finally, an information-sharing mechanism, including information on cyber attacks an cyber risks, may be helpful to solve the problem of information asymmetry.

1.Insurance Act §1 (R.O.C, 2012).

2.European Network and Information Security Agency, *Incentives and barriers of the cyber insurance market in Europe* , June 2012, at 8,

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe.
3.Ben Berkowitz, *United States: insurance-cyber insurance*, C.T.L.R. 2012, 18(7), N183.
4.*Supra* note2, at 19-25.
5.Mathew J. Schwartz, *Stolen NASA laptop had unencrypted employee data* , InformationWeek, November 15, 2012 11:17 AM, http://www.informationweek.com/security/attacks/stolen-nasa-laptop-had-unencrypted-emplo/240142160；Ben Weitzenkorn, *Stolen NASA laptop prompts new security rules*, TechNewsDaily , November 15 2012 11:35 AM, http://www.technewsdaily.com/15482-stolen-nasa-laptop.html.
6. Irene Klotz, *Laptop with NASA workers' personal data is stolen*, CAPE CANAVERAL, Nov 14, 2012 8:47pm, http://www.reuters.com/article/2012/11/15/us-space-nasa-security-idUSBRE8AE05F20121115.
7.The Government of the Hong Kong Special Administrative Region , *An overview of information security standards*, Feb 2008, at 2, http://www.infosec.gov.hk/english/technical/files/overview.pdf；*Supra* note2, at 21.
8.*Supra* note2, at 21-22.
9.*Id*.
10.*Id*.
11.*Id*.
12.U.S. Department of Homeland Security, Cyber security insurance workshop readout report, Nov 2012, at 1, http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf.
13.John E. Black Jr., *Privacy liability and insurance developments in 2012*, 16 No. 9 J. Internet L. 3, 12 (2013).
14.Marsh, *Number of companies buying cyber insurance up by one-third in 2012*, March 14, 2013, http://usa.marsh.com/NewsInsights/MarshPressReleases/ID/29878/Number-of-Companies-Buying-Cyber-Insurance-Up-by-One-Third-in-2012-Marsh.aspx.
15.U.S. Securities and Exchange Commission, *CF Disclosure Guidance: Topic No. 2 Cybersecurity*, October 13, 2011, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
16.*Id.*
17.*Supra* note2, at 6.(last visited Dec. 31, 2012)
18.Federal Acquisition Regulations §28.301.
19.E. Paul Kanefsky, *Insuring against cyber risks: congress and president Obama weigh in*, March 2012, http://www.edwardswildman.com/newsstand/detail.aspx?news=2812.
20.Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 §864.
21.*Supra* note19.
22.Terrorism Risk Insurance Act of 2002 §103.
23.*Supra* note19.
24.*Id.*
25.*Id.*
26.*Id.*
27.*Supra* note2.

Release：2013/06