Print ISSN: 1738-3110 / Online ISSN 2093-7717
http://dx.doi.org/10.15722/jds.16.5.201805.61

Cyber Insurance and Distribution Channels

Young-Arm Kwak*, Young-Sang Cho**

Received: April 15, 2018. Revised: May 10, 2018. Accepted: May 15, 2018.

Abstract

Purpose - These days, an individual user, private entity, hears everyday news of hacking and personal information leakage in the era of a most-connected society. This study investigates cyber attack, cyber insurance and distribution channels for insurance goods in South Korea by analyzing various cases of cyber attacks in domestic and overseas case.
Research design, data and methodology - This study adopted various study cases instead of the one large case for deep quality analysis, and focused on various cases of domestic and overseas cyber attacks with insurance.
Result - As a result of analyzing the cases that were hacked, types of massive losses and damages arising out of internet blackout due to cyber risks are paralyzation of public and private website and portal, electronic administrative system, public infrastructure, and consequently a normal operation of nation is impossible. These losses and damages however can be coverable under cyber insurance.
Conclusions - This paper suggests insurance carriers, as suppliers, should provide multiple channels to sell to the customer and should expand the strategy of advertisement and promotion in order for them to change their mind and compare the price and value of the information of individual users and private entity in view of cost savings.

Keywords: Internet of Things, Internet Blackout, Cyber Risk, Information Leakage, Distribution Channel.

JEL Classifications: K20, G22. G28, O34.

1. Introduction

Our world is progressing very quickly to digital life based on internet of things(IOT). Recently one of the popular words out of the most hottest terminologies is a cryptocurrency with blockchain. The core of cryptocurrency with blockchain is a security together with responsibility and indemnification of financial accidents as well as credit and stability on cryptocurrency transaction.

Cyber risk is rapidly increasing due to the hyperconnectivity of the IoT in the intelligent information society (Lee, Jun, & Kim, 2017). Menashri and Baram (2015) stated that “the growing use of information technology, monitoring, and control through computerized control systems, together with the increasing dependence of the free market on products and services supplied through infrastructure, have increased interdependency between infrastructures. Consequently, an attack on critical infrastructure is liable to have a decisive effect on the functioning of other infrastructures”.

Also, Abdo, Kaouk, Flaus, and Masse (2018), stressed that "The introduction of connected systems and digital technology in process industries creates new cyber-security vulnerabilities that can be exploited by sophisticated threats and lead to undesirable safety accidents. Thus, identifying these vulnerabilities during risk analysis becomes an important part for effective industrial risk evaluation."

Personal data leak incidents(Hwang & Yoo, 2016) could occur 12 times in a year on average. “Therefore cyber insurance has been attracting attention as a new risk management countermeasure by transferring cyber risk.” However, cyber insurance is still a new concept in South Korea (Lee et al., 2017). Companies dealing with personal information, such as game companies, mobile communication companies, portals, credit card companies, brokerage houses, insurance companies, etc all are at risk of leakage of personal information of their customers (Kim, 2014).

* First Author, Professor, Department of Global Trade Management, Shinhan University, Korea.
Tel: +82-31-870-3542, E-mail: yakyak@shinhan.ac.kr
** Corresponding Author, Professor, Department of Retail Management, Kongju National University, Korea.
Tel: +82-41-330-1424, E-mail: choskr1@kongju.ac.kr

Personal information leakage even has an adverse effect on the national economy (Kim, 2014). The personal information leakage is far unabated, and rather, continues to grow. In addition, the number of leakages, contents and methods of information leakage are reaching increasingly serious and sensitive levels (Kim, 2014).

This study aims to propose any distribution plans for cyber insurance with cyber risks in South Korea analyzing cases of cyber attack and insurance as a tool of risk transfer for the interest of individual user or private entities or subscribers.

In terms of terminology, a word of 'cyber risk' is only used in this study, where the same word has wide meanings, for example cyber attack, cyber terror, cyber war, cyber crime and hacking under this research. Also this study did not mention both word of war and terror from cyber attack, and exclude a suspect, offender and terrorist in the analysis. A scope of this study is limited to the individual user or private entities or subscriber of an application, portal on cyber world for the sake of protecting all kinds of priceless data.

2. Theoretical Background

2.1. Review of literature

Review of literature was conducted as following one-by-one, distribution channels, sales channel of insurance market, legal issues of insurance on liability, information leakage liability insurance, concept of cyber insurance, cyber attack to financial firm, investigation of risk and security risk analysis.

Many previous studies in the point of distribution channels were found in many research. Chinomona (2012) studied that "managers can utilize expert, referent and traditional legitimate powers to attain channel cooperation with manufacturing SMEs in addition to garnering their trust, relationship satisfaction and commitment." Quan and Youn (2016) studied that "comparative analysis on the characteristics from those of the theories are shown, and the explanation for the power in consumers' store-choice behaviors and their limitations are examined. Also, plans for improving commercial sphere analysis are explored." Lee and Kim (2017) explained that "retail companies are turning from one type of retailer to multiple business categories through various reasons, such as taking advantage of existed types of retailers'channel distribution, information and know-how, and entering into new types of retailers. However, there is few research conducted about multiple type of retailers." Kim, Lee, Kim, Nam, and Youn (2010) studied that "drugstores need to have price competitiveness to have multiple shop opening strategy and to satisfy consumers and to supply high quality services that is future subject to solve." Choi, Kim, and Lee (2011) studied that "this research looks at the concept of major market' private brand, the strategy, the success example and the prospects, and views the globally rapid-growing private brands, not only having the limited role of distributing the products as retailers, but also having a control of the distribution channel as a manufacturing company." Kim and Kim (2017) explained that "loyalty factors were important. In particular, consumers' perception of behaviors such as local specialties and community service that can be distinctly differentiated from other distribution agencies was very low."

With regard to sales channel of insurance market, Kazemi, Javanmard, and Mohammadi (2017) explained that "Our research has demonstrated the effect of employees' engagement on the strategic-driven behavior, emphasizing the role of employees' engagement in health-care service firms. Although previous service research has focused on the factors that drive employees' performance, it seems that most of this research has been inspired by the idea of the service profit chain, focusing on the effect of employees' satisfaction on performance." Haicheng (2012) studied that "the article studied on the contribution role of essential factor market of insurance in financial industry development to economic growth in Chongqing by the way of demonstration analysis." Joo (2017) studied that "the findings of the paper will provide a guideline for understanding on firm's attributes and its effects towards introduction of Corporate Pension Insurance products."

In regard to legal issues of insurance on liability, Hong (2013) studied that in recent years, various E-Commerce related accidents are occurring frequently due to the increase of E-Commerce in Korea. Consumer's damage caused by these has become a serious problem. Laws relating to E-Commerce has been revised to the strengthen responsibility of E-Commerce merchants for consumer protection (Hong, 2013).

In view of information leakage liability insurance, Kim (2014) studied companies dealing with customer information across all industries wherever personal information is being leaked such as game companies, mobile communication companies, portals, credit card companies, brokerage houses, insurance companies, etc. The personal information leakage is far unabated, and rather continue to grow. In addition, the number of leakages, contents and methods of information leakage are reaching increasingly serious and sensitive levels (Kim, 2014). Kwak (2009) also stressed insurance utilization for recent events of personal information leak in view of risk management by insurance goods related both commercial company and customer on e-commerce. In order to verify the pattern of personal data leak incidents (Hwang et al., 2016) searched the personal data leak incidents reported by the media from 2011 to 2014. "This study can be useful for organizations to predict a loss of personal data leak incidents and information security investments and furthermore, this study can be a data for requirements of the cyber-insurance."

With regard to the concept of cyber insurance, Lee et al. (2017) previously studied that cyber insurance has been attracting attention as a new risk management countermeasure by transferring cyber risk. However, cyber insurance is still a new concept in South Korea. Research results suggest that most requisite cyber insurance types are business interruption and liability(Lee et al., 2017). In respect of Cyber Risk Exposure and Prospects for Cyber Insurance, Adeleke et al. (2011) studied that this study draws attention to the ubiquitous and borderless nature of cybercrime. It examines the prospect of introducing customized cyber insurance policy in the Nigerian market. Findings also show that the traditional policies have limitations with respect to protection against cyber risks and that there is a prospect for marketing a specifically designed cyber insurance policy in Nigeria (Adeleke, Ibiwoye, & Olowokudejo, 2011).

As for Cyber attack to financial firm, Yang(2011) studied that "due to country's high dependence on computer system in managing and operating the critical infrastructures, it's becoming a primary target from the 'cyber terrorists'. In the 12th of April 2011, Korea's National Agricultural Cooperative lender, Nonghyup or NH bank, has experienced a system-wide crash that halted all of its banking transaction. This outage was the results of "unprecedented act of cyber terrorism" by the cyber terrorists."

When it comes to investigation of risk, Kim (2009) studied that as a result of this study only a few Korean firms have certain management methods designed to predict the possibility of risk occurrence and establishment of systematic countermeasures. Accordingly, in order to accurately recognize and manage, the firms need to not only specialize risk management department but also outsource by using a consulting firm (Kim, 2009). Hayward (2017) evaluating “Imminence” of A Cyber Attack, studied that "While there is broad agreement that some cyber attacks will satisfy Article 51’s “armed attack” requirement, the question of how to evaluate whether such an attack is “imminent”—based on an analysis of the technology of cyber weapons—has received little attention. This note applies existing theories of imminence to the technological aspects of how cyber weapons are developed and launched, providing considerations for determining when the “last possible window” to stop a prospective cyber attack is likely to close —or whether it has already passed." About cyber attack properties, Halloran, Robinson, and NeilBrock (2017) studied that "there is little chance of performing a top down development or anticipating all critical requirements such devices will need to satisfy individually and collectively.

Also, Hongxu, Rui, and Fenfei (2015) analyzed Causes and Actual Events on Electric Power Infrastructure Impacted by Cyber Attack, that is, "With the development of electric power technology, information technology and military technology, the impact of cyber attack on electric power infrastructure has increasingly become a hot spot issue which calls both domestic and foreign attention. First, main reasons of the impact on power infrastructure caused by cyber attack are analyzed from the following aspects: The dependence of electric power infrastructure on information infrastructure makes cyber attack issues in information field likely to affect electric power field." Guerrero-Higueras, DeCastro-Garcia, and Matellan (2018) studied that "Cyber-security for robotic systems is a growing concern. This article shows that cyber-attacks on Real Time Location Systems can be detected by a system built using supervised learning. Furthermore it shows that some type of cyber-attacks on Real Time Location Systems, specifically Denial of Service and Spoofing, can be detected by a system built using Machine Learning techniques". Leszczyna (2018) studied about Cybersecurity and privacy in standards for smart grids, that "The purpose of this paper is to bring in all smart grid standards that describe cybersecurity issues and to provide the information regarding their contents. In order to achieve this goal, a systematic study was conducted that led to the identification of thirty six publications on security and eleven on privacy." Faga (2017), for Analysing The Distinction Between Cybercrime, Cyber Attack, studied that "This paper is an attempt to draw distinctive lines between the concepts of cybercrime, cyber-attack, and cyber warfare in the current information age, in which it has become difficult to separate the activities of transnational criminals from acts of belligerents using cyberspace. It concludes that current international law constructs are inadequate to address the implications of transnational cyber threats; the author recommends consequential amendments to the laws of war in order to address the challenges posed by transnational cyber threats." Polatidis, Pavlidis, and Mouratidis (2018) studied that, in view of 'Cyber-attack path discovery in a dynamic supply chain maritime risk management system, “Maritime port infrastructures rely on the use of information systems for collaboration, while a vital part of collaborating is to provide protection to these systems. Attack graph analysis and risk assessment provide information that can be used to protect the assets of a network from cyber-attacks. Menashri et al. (2015) about 'Critical Infrastructures and their Interdependence in a Cyber Attack' studied that "The growing use of information technology, monitoring, and control through computerized control systems, together with the increasing dependence of the free market on products and services supplied through infrastructure, have increased interdependency between infrastructures. Consequently, an attack on critical infrastructure is liable to have a decisive effect on the functioning of other infrastructures."

Abdo et al. (2018) regarding A safety/security risk analysis approach of Industrial Control Systems, studied that "The introduction of connected systems and digital technology in process industries creates new cyber-security vulnerabilities that can be exploited by sophisticated threats and lead to undesirable safety accidents. Thus, identifying these vulnerabilities during risk analysis becomes an

important part for effective industrial risk evaluation (Abdo et al., 2018).

From what we analyzed as above, the author found that previous studies mainly dealt with in terms of cyber attack, information leakage, cases analysis based on technical advance and introduction of cyber insurance with insurance market size. No study on relationship of and/or distribution plans for cyber insurance with cyber risks in South Korea was found, the summary of which is a differentiation of this study in comparison with previous studies.

2.2. Loss Categories and Definitions

Incident types by cyber attack are far various like as Assistance coverage -psychological support, Bodily injury and death, Breach of privacy, Business interruption(Interruption of operations), Communication and media, Contingent business interruption(CBI) for nonphysical damage, Cyber ransom and extortion, Data and software loss, D&O [Directors' and officers' liability], Environmental damage, Financial theft and/or fraud, Fines and penalties, Incident response costs, Intellectual property theft, Legal protection(Lawyer fees), Network security/Security failure, Physical asset damage, Professional services E&O(Professional indemnity), Regulatory & legal defense costs(excluding fines and penalties), Reputational damage(excluding legal protection) and Tech E&O as shown <Table 1>. In terms of Cyber's loss categories and definitions, OECD (2017) defined incident types of cyber attack as follows :

<Table 1> Loss Categories and Definitions

Incident Type Group	Coverage Scope
Assistance coverage -psychological support	Assistance and psychological support to the victim after a cyber-event leading to the circulation of prejudicial information on the policyholder without his/her consent
Bodily injury and death	Compensation costs for bodily injury or consecutive death through the wrongdoing or negligence of the observed company or related third parties (e.g., sensible data leakage leading to suicide)
Breach of privacy [compensation]	Compensation costs after leakage of private and/or sensitive data, including credit-watch services, but excluding incident response costs
Business interruption Interruption of operations	Reimbursement of lost profits caused by a production interruption not originating from physical damage
Communication and media	Compensation costs due to misuse of communication media at the observed company resulting in defamation, libel or slander of third parties including webpage defacement as well as Patent/Copyright infringement and Trade Secret Misappropriation
Contingent business interruption (CBI) for nonphysical damage	Reimbursement of the lost profits for the observed company caused by related third parties (supplier, partner, provider, customer) production interruption not originating from physical damage
Cyber ransom and extortion	Costs of expert handling for a ransom and/or extortion incident combined with the amount of the ransom payment (e.g., access to data is locked until ransom is paid)
Data and software loss	Costs of reconstitution and/or replacement and/or restoration and/or reproduction of data and/or software which have been lost, corrupted, stolen, deleted or encrypted
D&O [Directors' and officers' liability]	Compensation costs in case of claims made by a third party against the observed company directors and officers, including breach of trust or breach of duty resulting from cyber event
Environmental Damage	Coverage scope: compensation costs after leakage of toxic and/or polluting products consecutive to a cyber-event
Financial theft and/or fraud	Pure financial losses arising from cyber internal or external malicious activity designed to commit fraud, theft of money or theft of other financial assets (e.g., shares) It covers both pure financial losses suffered by the observed company or by related third parties as a result of proven wrong-doing by the observed company
Fines and Penalties	Compensation for fines and penalties imposed on the observed company Insurance recoveries for these costs are provided only in jurisdictions where it is allowed
Incident Response Costs	Compensation for crisis management/remediation actions requiring internal or external expert costs, but excluding regulatory and legal defense costs Coverage includes: (i) IT investigation and forensic analysis, excluding those directly related to regulatory and legal defenses costs; (ii) public relations and communications costs; (iii) remediation costs (e.g., costs to delete or cost to activate a "flooding: of the harmful contents published against an insured); (iv) notification costs

Intellectual property theft	Loss of value of an Intellectual Property asset, resulting in pure financial loss
Legal protection - Lawyer fees	Costs of legal action brought by or against the policyholder including lawyer fees costs in case of trial Example: identity theft, lawyer costs to prove the misuse of victim's identity
Network security/ Security failure	Compensation costs for damages caused to third parties (supplier, partner, provider, customer) through the policyholder/observed company's IT network, but excluding incident response costs The policyholder/observed company may not have any damage but has been used as a vector or channel to reach a third party
Physical asset damage	Losses (including business interruption and contingent business interruption) related to the destruction of physical property of the observed company due to a cyber-event at this company
Products	Compensation costs in case delivered products or operations by the observed company are defective or harmful resulting from a cyber-event, excluding technical products or operations (Tech E&O) and excluding Professional Services E&O
Professional services E&O, Professional indemnity	Compensation costs related to the failure in providing adequate professional services or products resulting from a cyber-event, excluding technical services and products (Tech E&O)
Regulatory & legal defense costs (excluding fines and penalties)	A: Regulatory costs: compensation for costs incurred to the observed company or related third-parties when responding to governmental or regulatory inquiries related to a cyber-attack (covers the legal, technical or IT forensic services directly related to regulatory inquiries but excludes Fines and Penalties) B: Legal defense costs: coverage for own defense costs incurred to the observed company or related third parties facing legal action in courts following a cyber-attack
Reputational damage (excluding legal protection)	Compensation for loss of profits due to a reduction of trade/clients because they lost confidence in the impacted company
Tech E&O	Compensation costs related to the failure in providing adequate technical service or technical products resulting from a cyber-event

Source: Adapted from OECD (2017).

2.3. Cyber Insurance Market Size

Concerning market size of cyber insurance, the following is requoted: "While the cyber insurance market has reached a significant size since its inception, in comparison to the overall insurance market, cyber remains a small component. As of 2015 in which the cyber insurance market reached $2 billion, the net premiums in the commercial insurance market was $247 billion, or $1.2 trillion net premiums in the U.S. insurance industry, generated by close to 6000 insurance firms (Insurance Information Institute, n.d.-a, n.d.-b). Relative to the insurance numbers to the cybersecurity market, Gartner reported that the worldwide cybersecurity market was $75.4 billion in 2015 and forecasted to growth to $170 billion by 2020" (Morgan, 2015; Romanosky, Ablon, Kuehn, & Jones, 2017).

By OECD (2017), it was reported that "A number of studies have suggested that limited awareness of cyber risk - and particularly, awareness of the potential cost of cyber incidents - among companies is an important impediment to broader take-up of cyber insurance coverage. Close to 80% of the respondents to the OECD questionnaire indicated that the level of awareness of cyber security risk among potential policyholders was an important or moderately important driver of the level of cyber security risk. In the PwC 2016 Annual Survey of Corporate Directors, board engagement on cyber security differed widely depending on firm size. For example, 68% of directors at mega-sized companies indicated that their board is very engaged in overseeing/ understanding the risks of cyber-attacks, compared to 32% of directors at smaller companies." quoted.

3. Cases Analysis of Cyber Risks

In order to carry out this research, the author used and adopted various case studies instead of one large case study for deep quality analysis, where the author focused on various cases of cyber attacks in domestic and overseas case with cyber insurance matter. From these cases, the author found that cyber attacks irrespective of type and mode of attack are various and huge and then routinized for life, which recall a necessity of cyber risk's control and cyber risk's transfer.

3.1. Precedent of Cyber Attack in South Korea

In the world today, South Korea is a most-connected society in that most of its citizens takes very well advantage of handling personal computer and mobile phones at home, workplace and on the road with walking/moving. While this fact of well organized/developed most-connected society is extremely weak to cyber attack from inside/outside 24 hours

in a day, on the other hand, a least-connected society is paradoxically safe from cyber attack.

3.1.1. In case of computer networks of government and entities

In South Korea, a number of cyber attack have been taken place in places, such as e-mail hacking to Department of Foreign Affairs and Security from January to June 2016, where accounts with password were robbed, as well as customer's personal information hack of InterPark on July 11th, 2016.

Continuously hackers, by using of account with password, makes an additional attack resulting in additional severe losses and damage of the citizen. They attack to official computers and then make a zombi computer through malicious codes, the result of which affects to the computer networks of the government and paralyzed every networks, causing massive damages to all relevant aspects on the technological world.

Personal information leaked from InterPark can be abused to open hundreds of thousands of accounts, and abused to make replies on bulletin boards with public opinion manipulations, and can rob big money from the said accounts through personal information leakage.

When personal information is leaked, victims might suffer financial damage or become targets of other crimes (Kwak, 2009). For instance, telemarketing companies send spam mail to e-mail addresses and cell phone numbers acquired illegally for sending spam message at anytime and anywhere. In fact South Korea has 5,700 phone fraud cases resulting in 57 billion won($54.6 million) in losses every year according to study of Korea Institute of Information Society and Cryptology. Many hacker attack on computer systems of South Korea's government and public agencies come from China, with the personal information stolen in the attacks mostly exploited for financial fraud (Kwak, 2009).

3.1.2. In case of law suit

A lot of law suit cases from cause of leakage due to cyber attacks as just mentioned in South Korea have been lodged as belows in <Table 2>.

Personal information means the fact, judgement, evaluation of the private mind, body, asset, social class and status. Information which can identify any person such as his/her name and identification number belongs to personal information as well.

Infringement accident in course of leakage through network means situation arising from attacks against network and information system by means of hacking, computer virus, logic bomb, mail bomb, distributed denial of service (DDoS) and high-power electromagnetic wave.

There are security technologies on protection of leakage information such as authentication using password algorithm, firewall, anti virus system, password control, and then the core is a human resource management of 'security administrator'. Possession of these security technologies is the guideline for check the liability of personal information leakage, when accidents took place.

Paradoxically, the greater the amount of information to be protected in proportion to the development of information technology (Kim, 2014). Especially if that information is trading in a particular industry is further emphasized the need for its protection. However despite the importance of such protection, frequent information leakage causes heavy losses to the industry. Because of this social distrust of enterprises is increasing (Kim, 2014).

<Table 2> Law Suit Case from Cause of Leakage (As of August 2014)

Cause of leakage	Company(plaintiff)	Case No.	Verdict	Course
negligence inside	GS Caltex Corporation	Supreme Court 2011DA59834	plaintiff defeated	final judgement
	NC soft Corporation	Supreme Court 2007DA17888	plaintiff winning (respectively KRW 100,000)	final judgement
	Kookmin Bank	Seoul High Court 2007NA33059, 33066	plaintiff winning (respectively KRW100,000 or 200,000)	final judgement
	LG Electronics Inc.	Supreme Court 2008DA96826	plaintiff winning (respectively KRW 300,000)	final judgement
attack or invasion from outside	Auction	Seoul High Court 2010NA31510	plaintiff defeated	trial at the Supreme Court
	SK Communications	Seoul Central District Court 2011GAHAP90267	plaintiff defeated	trial on an appeal
		Seoul Western District Court 2011GAHAP11733	plaintiff winning (respectively KRW 200,000)	trial on an appeal
others	SK Broadband Co., Ltd.	Seoul High Court 2011NA67493	plaintiff winning (respectively KRW 200,000)	final judgement

Source: Adapted from Kim (2014).

3.2. Overseas Precedent of Cyber Attack

3.2.1. In case of Yahoo

Internet portal, Yahoo was hacked in 2014 where 500 million personal information leaked, the details of which were subscriber's name, e-mail address, phone number, date of birth, password and electronic authentication of identity. The quantity of 500 million personal information leaked is the largest event out of personal information leaked in the world.

From this leakage it is predicted to lodge numerous suits from a lot of victims leaked. There is a case that indemnification amount estimates USD 221.00, equivalent to KRW 240,000 per data, hence total indemnification amount can be hit the astronomical costs resulted from court verdict.

Under cyber transaction over the world with no meaning of frontier, in particular a kind of recently hot issue is the cryptocurrency, Bitcoin, the some hacking cases of which are seen in <Table 3>.

<Table 3> Notable Hacking Cases on Bitcoin

Date	Contents
June 2011	Bitcoin USD 8.75million robbery at trading floor, Mount Gox, Japan
April 2013	Bitcoin USD 4.60million robbery at wallet service, Instar Wallet
November 2013	Bitcoin USD 100million robbery at Shipmarketplace, and closed
February 2014	Bitcoin USD 470million robbery at trading floor, Mount Gox, and bankruptcy
August 2016	Bitcoin USD 65million robbery at trading floor, Bitfinex, Hong Kong
April 2017	Bitcoin KRW 5.5billion robbery at trading floor, Yapizon, Korea

Source: Data was proceeded by authors.

For the matter of 'emerging cyber threats', Crawford et al., 2014 stressed that financial institutions have developed innovative mobile applications that enable mobile payment transactions for their customers. While these applications represent innovation, the institutions never planned on supporting mobile banking. Consequently, digital exchanges via the mobile transaction network are at a higher risk of compromise and/or manipulation by exploiters with increasingly sophisticated tools and skills (Crawford et al., 2014). Moreover, infrastructure and storage outsourcing efforts supporting these applications put organizations further at risk as unregulated cloud service providers have highly differentiated security mechanisms that may not address threats to their customers (Crawford et al., 2014). There is a stunning gap between the nature of new threats and the capabilities available to detect attacks, monitor(and stop) unauthorized infiltration and secure information. Many do not have the tools to provide the direct real-time awareness necessary to calculate risks to insured digital assets stored by cloud service providers or enterprise networks. There is increased awareness that companies should be accountable for private records and the security of data collected from their customers (Crawford et al., 2014).

Also in respect of anatomy of a data breach, data integrity standards can play a role in policy wording and risk assessments: Before breach incident [Reasonable and appropriate measures to manage future data breach incident] → Data breach incident [Alerting for rapid response and damage limitation] → After breach incident (short-term) [Forensic analysis] → After breach incident (long-term) [Subrogation mitigation and e-discovery] (Crawford et al., 2014). Moreover, people have digital fingerprints via their mobile devices that identify them uniquely, and social media websites have turned this into an advantage in the sales process. Applying a unique data security signature associated with that fingerprint is bolstered with the data integrity standard. Another important role for data integrity standards will be in the broker risk assessment process. Brokers can include these standards in their risk process to educate their customers and direct them to compliant carriers. One aspect of a data integrity standard is keyless signature infrastructure (Crawford et al., 2014).

3.3. Findings and Discussions

In connection with the above cases, impact of cyber attack elicits from internet paralyzation what we called 'internet blackout', which means that everybody can be faced panic unexpected between human and things on earth.

With causing a chain reaction, types of massive losses and damages arising out of internet blackout due to cyber attack are paralyzation of public and private website and portal, electronic administrative system, public infrastructure like as powerhouses, interruption of CCTV and security system, stock market, internet banking, credit service and ATM, internet shopping and online transaction, transportation system, online games, movies and music streaming service, SNS service, email, e-learning service, and patients control systems, to name a few.

This is because everything that exists today can be faced with paralyzation or interruption by internet of things(IOT) or internet of everything(IET), and consequently a normal operation of a nation is impossible. There is nothing more dangerous than internet blackout on the entire world.

Number and amounts of personal information leakage in the world is rapidly increasing, and as time goes by, there is no doubt that exposure of cyber risks resulted from cyber attacks to the individual user and private entities will be also definitely inflated.

Consequence of internet blackout overwhelms the imagnation of the individual user and private entities,. By this reason, individual user, private entity and nations should duly prevent their own personal information and data from cyber attack, breaking through the easy going attitude in an

era of information-based and 4th industrial revolution.

From the economical point of view, individual user, private entity and nation might as well insure cyber insurance so that cyber risks caused by computer and phone may be covered under insurance umbrellas in consideration of cost effectiveness as a alternative.

The insurance is one of the most useful assistant systems that help enterprises to act reliably (Kim, 2014). In particular, to be relatively free from responsibility for issues related to the damage to third parties in the course of leading, a company must use the insurance system. The introduction of information leakage liability insurance is required in order to compensate for the damage caused by a third party information leakage during the company's operating activities (Kim, 2014). Individual user might as well buy cyber insurance in view of organization with cost as well as they have to always protect themselves and to back-up data. Private entity has to take a desperate act of defense of customer's information in order that they may maintain their own business because one cyber attack may just strike a entity and then may sink forever.

Korean government should consider to increase the budget of cyber defense in point of national defense in order that they can always prevent people and entities form inside, outside and invisible attack 24 hours a day. Further to this, for the purpose of overcoming cyber disaster, Korean government should give priority to 'policy insurance of cyber risk' and should develop a recovery strategy.

From the above findings, the authors suggest the ideal distribution schemes of cyber attack and insurance so that individual user and private entities may make a readiness against cyber attack and/or cyber invasion occurred anytime and anywhere for 24 hours a day.

Measures of cyber risk management are risk avoidance, risk retention, risk reduction and risk transfer. Individual users and private entities are always using the computer and mobile phone for 24 hours a day and it is not possible for them that they are not taking computer and mobile phone in the course of normal life and work place. By this reason, risk avoidance on cyber risk management is not also possible for their living and works, which means that the size of cyber risk is expanded as well as burden of risk retention simultaneously expanded.

With a view to responding expansion of cyber risk with information security, individual user and private entities should take care of their own risk management and should consider measure of risk transfer by insuring the cyber insurance as a alternative way.

Under the above circumstance on precedent of cyber attack in South Korea and overseas, the authors suggest distribution schemes of cyber attack and cyber insurance as a reasonable tool of risk transfer from individual user and private entities to insurance carrier.

3.3.1. In case of Role of Insurance Carrier

Insurer as supplier should consider to aggressively sell cyber insurance irrespective of name of insurance goods for all kinds of customer. In the beginning of selling business, limit of liability in cyber insurance should diminish in order for insurer to reduce the burden of insurance payment, and deduction(what we call 'self insurance') in cyber insurance should elevate in order for the insured not to fall into moral risk or moral hazard. It is very enough that the insurer in South Korea has a operation skill form variable experience.

3.3.2. In case of Role of Government

Relevant authorities in South Korean Government should consider to positively assist making a legislation of cyber security with cyber defense, and execute real action like as increasing budget and monitoring cyber defense as national military service for the sake of the spirit of the constitution.

3.4 Distribution Channel for the service and goods

As insurance goods is a push goods, hence design of application for subscriber is very important, requiring demand of client along with policyholder and insured. As for Distribution Channel of insurance matter, there are various channel such as solicitor, agent, general agent(GA), bankasurance, tele marketing(TM), home shopping, martsurance and internet, etc.

General Agent(GA) is a group of specialists, who compares a lot of insurance goods from insurers and sales goods to the customer, so they are distribution channels for the insured and not for insurer, that is to say, the insurance company.

Current situation of insurance distribution channel is as follows based on year 2012. Insurance companies have a volume of 60,000 person as staffs, 320,000 person as sole solicitor, and 40,000 agents(excluding general agent). Main insurance distribution channel in life insurance is a exclusive sole solicitor, on the other hand, the channel in non-life insurance is a agent(excluding general agent). Market share of distribution channel in non-life insurance, cyber insurance is not life-insurance, is a agent(excluding general agent) 41.5%, exclusive sole solicitor 30.1%, staffs 15% and bankasurance 12.6% respectively.

Structure of insurance distribution channel in insurance company is a core, therefore they should treat multiple channel by use of real time monitoring to market situation. Insurance company should sale cyber insurance to the customer through strategy of multiple channel, and then non-life insurance carrier should aggressively appeal to customer to buy.

Unfortunately individual user, private entity hear everyday news of hacking and personal information leakage, therefore supply and purchase of cyber insurance are more than

important in an era of digital world. Also naturally non-life insurance carrier, as supplier should provide multiple channel to the customer and should expand the strategy of advertisement and promotion in order for them to change their mind. This is why a premium of the cyber insurance is very slight and meager, comparing to price and value of the information of individual user, private entity in view of cost savings.

4. Conclusion

4.1. Summary

Cyber Insurance plays a role in covering the risk of cyber attack. This paper aims to present Distribution Channel and Plans of the goods of Cyber Insurance by means of various cases analysis.

Unfortunately individual users and private entities hear everyday news of hacking and personal information leakage, and therefore supply and purchase of cyber insurances are more than important in an era of the digital world. Also naturally non-life insurance carriers, as suppliers, should provide multiple channels to the customer and expand the strategy of advertisement and promotion in order for them to change their mind. This is why a premium of cyber insurance is very slight and meager, compared to price and value of the information of individual users and private entities in view of cost savings.

This study aims to propose any distribution plans for cyber insurance with cyber risks in South Korea by use of analyzing some cases of cyber attack and insurance as a reasonable tool of risk transfer for the interest of individual user or private entities or subscribers.

Consequence of internet blackout overwhelms the imagnation of the individual user and private entities, by this reason individual users and private entities and nation should duly prevent their own personal information and data from cyber attacks, breaking through the easy going attitude in an era of information-based technological world.

As a result of analyzing cases that were hacked, types of massive losses and damages arising out of internet blackout due to cyber risks are paralyzation of public and private website and portal, electronic administrative system, public infrastructure. Everything existed on earth can be faced with paralyzation or interruption by most-connected society elicited from internet of things(IOT) or internet of everything(IET), and consequently a normal operation of nation is impossible. These losses and damages can be coverable under cyber insurance.

From the economical point of view, individual users and private entities and nation might as well insure cyber insurance so that cyber risks caused by computer and phones may be covered under the insurance umbrella in consideration of cost effectiveness as an alternative.

Lee et al.(2017) studied that Cyber insurance has been attracting attention as a new risk management countermeasure by transferring cyber risk. However, cyber insurance is still a new concept in South Korea.

4.2. Contribution, Limitation and Future Research

This study has some limitations. In chapter 3, the author showed law suit case from cause of leakage while overseas' law suit case did not present and analyze to computer any idea. Nevertheless the fact of which, suggestion of distribution plans for cyber insurance with cyber risks from either finding of accident cases or finding of law cases, either way is the same result. From this, further research of overseas' law suit case is obligated for analysis. Besides, all sorts of cyber risks resulted from cyber attacks are not covered by cyber insurance.

Contribution of this study is providing the perception and consciousness of the individual users and private entities and government, emphasizing appropriate usage of cyber insurance for the purpose of protecting personal information and data.

This study is helpful to aiding in further research of perception and needs of cyber insurance as a previous study in South Korea. In addition, researching cryptocurrency with blockchain is also very timely for relevant studies with cyber risk, cyber security, security and cryptology, digital forensic, 4th industrial revolution and so on for the future.

Reference

Abdo, H., Kaouk, M., Flaus, J. M., & Masse, F. (2018). A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – Combining new version of attack tree with bowtie analysis. *Computers & security*, *72*(1), 175-195.

Adeleke, L. A., Ibiwoye, A., & Olowokudejo, F. F. (2011). Cyber Risk Exposure and Prospects for Cyber Insurance. *International Journal of Management Business, 1*(4), 221-230.

Chinomona, R. (2012). The Role of Dealers' Non-Mediated Power in Fostering SME Manufacturers' Cooperation: SME Manufacturers' Perspective. *Journal of Industrial Distribution & Business, 3*(2), 5-16.

Choi, S. S., Kim, P. J., & Lee, S. Y. (2011). A Research on Private apparel Brand' Product Strategy in Discounted Stores. *Journal of Industrial Distribution & Business, 2*(2), 25-38.

Crawford, S., & Piesse, D. (2014). Cyber insurance, security and data integrity, Part 1: Insights into cyber security and risk-2014, *Ernst & Young LLP,*

2(2), 7-9.

Faga, H. P. (2017). The Implications Of Transnational Cyber Threats In International Humanitarian Law: Analysing The Distinction Between Cybercrime, Cyber Attack, And Cyber Warfare In The 21St Century. *Baltic Journal of Law & Politics*, *10*(1), 1-34.

Guerrero-Higueras, A. M., DeCastro-Garcia, N., & Matellan, V. (2018). Detection of Cyber-attacks to indoor real time localization systems for autonomous robots. *Robotics and Autonomous Systems, 99*(1), 75–83.

Haicheng, S. (2012). Study on Contribution Rate of Essential Factor Market of nsurance Development to Economic Growth: Demonstration Analysis based on Chongqing in China. *East Asian Journal of Business Management, 2*(2), 27-33.

Halloran, C. O., Robinson, T. G., & NeilBrock. (2017). Verifying cyber attack properties. *Science of Computer Programming*, *148*(1), 3–25.

Hayward, R. J. (2017). Evaluating The "Imminence" of A Cyber Attack For Purposes of Anticipatory Self-Defense. *Columbia Law Review*, *117*(399), 399-434.

Hong, J. H. (2013). Legal Issues of Insurance on Liability from Electronic Commerce. *Dong-a Law Review*, *59*(2), 325-329.

Hongxu, Y., Rui, X., & Fenfei, L. (2015). Analysis of Causes and Actual Events on Electric Power Infrastructure Impacted by Cyber Attack. *Journal of Power and Energy Engineering*, *3*(1), 77-84.

Hwang, Y. H., & Yoo, J. H. (2016). A Study on the Distribution Estimation of Personal Data Leak Incidents. *Journal of The Korea Institute of Information Security & Cryptology, 26*(3), 799-808.

Joo, H. (2017). The Impact of Corporate's Attributes on Corporate Pension Insurance Products & Type Preference. *International Journal of Industrial Distribution & Business, 8*(2), 21-31.

Kazemi, A., Javanmard, H., & Mohammadi, R. (2017). Determining the Relationship between the Effective Factors of Strategic Behavior: A Case Study for Social Insurance Company of Tehran. *East Asian Journal of Business Management, 7*(1), 5-12.

Kim, E. K. (2014). Study on Information Leakage Liability Insurance. *The Korean Journal of Financial Law, 11*(3), 149-176.

Kim, S. M., Lee, S. Y., Kim, P. J., Nam, M., & Youn, M. K. (2010). Promotional Strategies of Local Drugstores. *Journal of Industrial Distribution & Business, 1*(1), 5-12.

Kim, P. J., & Kim, H. K. (2017). The Effect of Loyalty Factors Perceived by Consumers on General Super Market. *International Journal of Industrial Distribution & Business, 8*(4), 37-46.

Kwak, Y. A. (2009). A study on insurance utilization for recent cases of personal information leak on e-commerce. *Journal of Korean Electronic Commerce Research Association, 10*(2), 21-44.

Lee, G. H., & Kim, S. C. (2017). The Growth Strategy of Retail Companies: Focusing on New Stores Expansion of E-mart. *International Journal of Industrial Distribution & Business, 8*(1), 15-22.

Lee, S. H., Jun, H. J., & Kim, T. S. (2017). Risk Management Requirements for cyber Insurance. *Journal of The Korea Institute of Information Security & Cryptology*, *27*(5), 1233~1245.

Leszczyna, R. (2018). Cybersecurity and privacy in standards for smart grids – A comprehensive survey. *Computer Standards & Interfaces*, *56*(1), 62–73.

Menashri, H., & Baram, G. (2015). Critical Infrastructures and their Interdependence in a Cyber Attack – The Case of the U.S.. *Military and Strategic Affairs, 7*(1), 79-100.

OECD Report (2017). Supporting an Effective Cyber Insurance Market. *OECD Report for the G7 Presidency*, *5*(1), 13-14.

Polatidis, N., Pavlidis, M., & Mouratidis, H. (2018). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces*, *56*(1), 74–82.

Quan, S. X., & Youn, M. K. (2016). Analysis on Preceding Study of Consumer's Store-Choice Model: Focusing on Commercial Sphere Analysis Theories. *International Journal of Industrial Distribution & Business, 7*(4), 11-16.

Romanosky, S., Ablon, L., & Kuehn, A., & Jones, T. (2017). Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk?. *Proceedings of the Workshop on the Economics of Information Security (WEIS)*, *8*(2), 1040.

Yang, J. M. (2011). A Review of NH Bank Cyber Attack. *The Journal of Legal Studies, 19*(2), 129-157.