KiRi 리포트 2018.5.8.
포커스

일반손해보험에 내재된 사이버 리스크 관리

변혜원 연구위원

요약

■ 기업 사업모형의 클라우드 서비스 의존도 확대, 사이버공격 증가, 정보보안 및 개인정보보호 관련 규제 강화 등으로 사이버 리스크에 대한 노출이 확대되고 있음
- 컴퓨터 운영체계나 마이크로프로세서의 보안취약점을 이용한 사이버공격은 정보유출 외에도 광범위한 피해를 초래함
- 한편 정보통신 기술이 사회에 미치는 영향이 심화되면서 사이버 리스크를 직접적으로 보장하는 사이버 보험 이외에도 전통적인 손해보험상품의 사이버 위험에 대한 노출도 확대됨

■ 임원배상책임(D&O)보험, 전문배상책임(E&O)보험, 재산보험 등 기존 손해보험은 사이버 리스크로 인한 손실에 대해 면책 여부가 분명하지 않은 경우 사이버 사고에 따른 손실에 직면할 수 있음
- 보험회사가 직면하는 사이버 리스크에는 약관에서 보장하고 있는 명시적(affirmative) 사이버 리스크와 약관상 면책 여부가 분명하지 않아 보험회사가 손실을 보장해야 하는 묵시적(silent) 사이버 리스크가 있음

■ 최근 영국의 보험회사 건전성감독당국은 손해보험회사에 묵시적 리스크를 포함하는 사이버 언더라이팅 리스크를 관리할 것을 요구함
- 감독당국은 손해보험회사에 보험료 조정이나 명확한 면책조항 등을 통해 묵시적 사이버 리스크를 관리할 것을 제안함

■ 국내 보험산업도 보험회사가 직면한 묵시적 사이버 리스크의 노출 규모 파악을 포함한 적극적인 모니터링과 적절한 대응방안 마련이 필요함
- 손해보험시장의 경우 묵시적 사이버 리스크 노출 규모는 제한적일 것으로 보이나, 빠르게 변화하는 사이버 환경을 고려할 때 보험회사와 감독당국의 적극적인 관리가 필요한 시점임

1. 검토배경

■ 최근 정보통신 기술이 사회에 미치는 영향이 심화되면서 사이버 사고의 피해는 정보유출뿐 아니라 영업정지, 물리적 피해 등으로 광범위하게 나타남

- 작년 5월 WannaCry 랜섬웨어 공격, 6월 NotPetya 말웨어 공격, 9월 Equifax의 정보유출사건, 올해 초 발표된 컴퓨터 마이크로프로세서에 드러난 보안취약점[1] 발견 등 사이버 리스크는 빠르게 증가하고 있음
- WannaCry 랜섬웨어 공격은 영국의 공공 의료서비스 시스템을 마비시켰으며, NotPetya 공격은 수송업체, 건강관리업체, 제약회사 등의 조업중단을 가져와 기업의 영업 손실을 초래함

■ 따라서 사이버 관련 손실을 보장하는 보험계약을 인수함으로써 보험회사가 직면하는 언더라이팅 리스크를 관리하기 위해서는 사이버보험에서 직접적으로 보장하는 리스크뿐만 아니라, 일반손해보험이 보장하는 관련 리스크도 관리해야 할 것임

- 사이버 사고는 사이버 보험이 보장하는 개인정보유출, 정보유출 대응 비용, 사이버 사고와 관련한 배상책임을 발생시키는 것은 물론, 임원배상책임(D&O)보험, 전문배상책임(E&O)보험, 재산보험 등 전통적 손해보험의 보장 영역에도 피해를 초래할 수도 있음

■ 본고는 최근의 사이버 사고와 사이버 리스크 현황을 살펴 본 후, 이와 관련된 보험회사의 언더라이팅 리스크 관리에 대해 살펴보고자 함

1) 컴퓨터 마이크로프로세서의 보안취약점인 Meltdown과 Spectre를 이용한 해킹을 방지하기 위해 소프트웨어 보안패치가 제공되어 해킹 위협은 경감되었으나, 보안전문가들은 여전히 위험은 존재한다고 보고 있음

2. 사이버 리스크의 진화

■ 사이버 리스크는 정보기술 체계의 고장으로 인한 재무적 손실, 파괴, 또는 한 기관의 명성에 손해를 초래할 수 있는 모든 리스크로 정의할 수 있음[2)]

- 사이버 손실의 주된 원인은 I) 의도된 사이버 범죄나 테러리즘, ii) 시스템 오류나 고장에 의한 데이터 손실, iii) 화재, 자연재해, 전기사고, 산업 사고 등으로 인한 사회기반구조의 물리적 손실, iv) 손해배상을 초래하는 온라인 활동의 배상책임 등임

■ 작년에는 WannaCry와 NotPetya의 공격에 의한 정보유출이나 데이터파괴 사건들이 발생했으며, 피해는 공격을 받은 기업뿐만 아니라 유출된 정보와 관련된 개인에게도 영향을 미침

- 2017년 5월에 있었던 WannaCry는 150개국의 20만 대의 컴퓨터에 감염되었으며, 약 천만 달러의 인질비용, 80억 달러의 영업정지 관련 비용이 발생한 것으로 추정됨(2017년 5월 중순 기준)[3)]
- NotPetya 공격으로 수송업체, 건강관리업체, 제약회사 등의 조업이 중단됨

■ 한편 올해 초에는 컴퓨터의 마이크로프로세서에 존재하는 두 가지 보안약점인 Spectre와 Meltdown이 알려졌는데, 이는 정보보안 사고의 가능성이 높아짐을 의미함[4)]

- 해커는 보안취약점들을 이용하여 마이크로프로세서 칩의 메모리 핵심에 저장되어 있는 모든 데이터에 접근할 수 있음
- Apple, Microsoft, Linux 등에서 제공한 소프트웨어 보안패치가 취약점을 상당 부분 보완하였지만, 보안전문가들은 하드웨어의 취약점이 여전히 존재한다고 보고 있음[5)]

■ 아울러 디지털 정보량과 클라우드 컴퓨팅 사용이 증가하면서 사이버 리스크에 대한 노출이 확대되고 있음

---

2) "any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems"(Institute of Risk Management)
3) https://www.propertycasualty360.com/2017/05/16/insurance-experts-wannacry-calls-for-tougher-cyber/
4) Greenberg(2018. 1. 7), "Triple Meltdown: How So Many Researchers Found a 20-year-old Chip Flaw at the Same Time", Wired
5) Aon Benefield(2018. 3), *Cyber Threat Insights*

- 미국의 상위 3개 클라우드 서비스가 3일에서 6일 동안 중단되는 사이버 사고가 발생할 경우, 총 손실은 69~147억 달러, 그 중 15~28억 달러가 보험에서 보장되는 것으로 추정됨[6)]
- 우리나라에서도 작년 6월 인터넷호스팅 업체인 인터넷 나야나가 랜섬웨어의 공격을 받아 5일 동안 서비스가 중단되었으며, 13억 원을 해커에게 지불한 바 있음[7)]

■ 유럽은 개인정보보호규정(GDPR: General Data Protection Regulation)을 2018년 5월부터 시행하고 있으며, 이로 인해 EU에서 활동하는 기업의 배상책임 부담이 높아질 것으로 예상됨[8)]

- GDPR은 데이터보안과 관련하여 데이터유출통지(제33조, 제34조), 집단 및 공익소송(제80조), 보상청구권(제82조), 과징금(제83조) 등의 내용을 담고 있음
- 미국의 경우에도 개인정보보호와 사이버 리스크 관리를 강화하는 규제들을 도입하고 있으며, 이러한 경향은 다른 국가들에도 나타나고 있음

3. 묵시적 사이버 리스크

■ 사이버 사고는 정보유출 사고를 명시적으로 보장하는 사이버보험과 더불어 이미 판매되었거나 판매되고 있는 손해보험의 사이버 리스크에 대한 노출도 증가시키고 있음

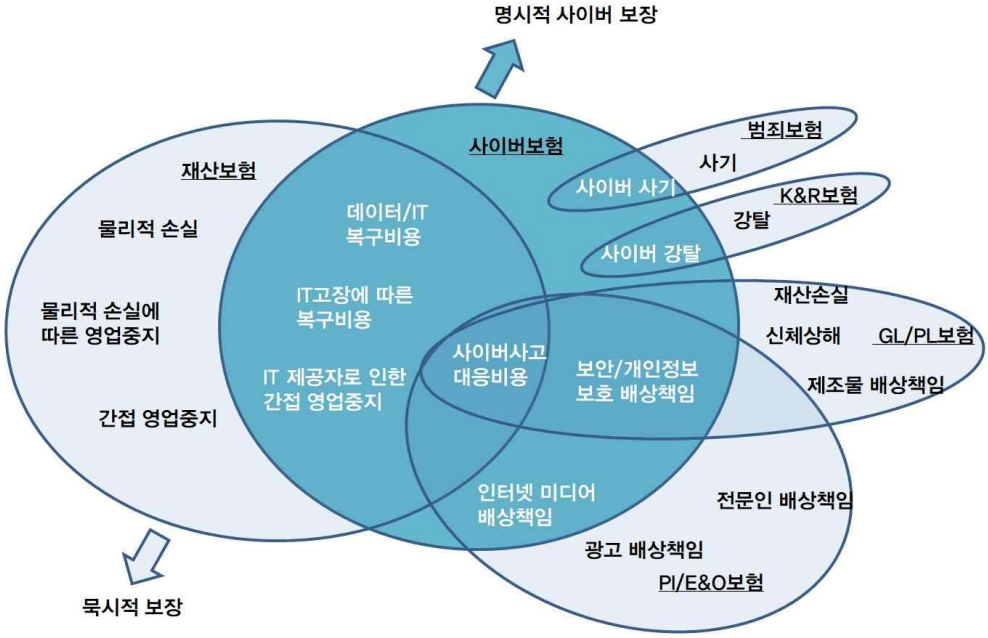
■ 한편 보험회사가 사이버 관련 손실에 노출된 보험계약의 인수에 따른 위험의 집합을 사이버 언더라이팅 리스크라고 함[9)]

- 사이버 사고는 사이버공격, 악성코드를 이용한 IT 체계의 감염 등과 같은 악의적인 행동에 기인할 수도 있으나, 데이터손실, 사고에 의한 행동이나 태만 등과 같은 비악의적인 행동에 의해 발생할 수도 있음

6) AIR(2018), "Cloud Down: Impacts on the US Economy", Emerging Risk Report 2018
7) 인터넷 나야나는 3천 4백 여 중소기업에 웹호스팅 서비스를 제공하고 있었음(http://www.hani.co.kr/arti/economy/it/798812.html)
8) http://ec.europa.eu/justice/data-protection/reform/index_en.htm
9) Prudential regulation Authority(2017. 7), "Cyber Insurance Underwriting Risk", Supervisory Statement SS4/17

■ 사이버 언더라이팅 리스크는 명시적(affirmative) 사이버 리스크와 묵시적(non-affirmative 또는 silent) 사이버 리스크에 기인함[10)]

〈그림 1〉 명시적 사이버 보장과 묵시적 사이버 보장



주: K&R(kidnap and ransom): 납치보험, GL(general liability): 제3자 배상책임보험, PL(product liability): 제조물배상책임보험, PI(professional insurance): 전문인배상책임보험, E&O(Error & Omission): 전문배상책임보험
자료: Parsorie(2018)

■ 명시적 사이버 리스크란 사이버 리스크에 대한 보장을 명시한 보험계약과 관련된 리스크임

- 사이버 보험계약에서 명시한 과학수사, 법률비용, 알림 및 신용 모니터링, 제3자 배상책임 등과 같은 유출대응 비용 보장은 명시적 사이버 리스크에 해당됨

■ 묵시적 사이버 리스크는 사이버 리스크에 대한 보장을 포함하는지, 제외하는지에 대해 명확히 하지 않은 보험계약과 관련된 리스크를 의미함

- 사이버 사고는 임원배상책임보험(D&O), 전문배상책임(E&O)보험, 재산보험, 전위험(all risks)보험 등과 같은 전통적 손해보험에서 보장여부를 명확히 하지 않은 손실을 야기할 수 있음

10) Affirmative cyber risk를 보험계약에서 명시적으로 인수하겠다고 동의했다는 의미에서 명시적 사이버 리스크라고 의역하였으며, non-affirmative(silent) cyber risk도 묵시적 사이버 리스크라고 의역하였음

- 랜섬웨어 사고는 납치보험(K&R: kidnap and ransom), 사이버공격이 야기한 물리적 손실은 재산보험, 의료기구 및 서비스, 가전기구, 교통 분야에서 신체부상에 대한 위험노출의 증가할 경우 일반책임보험에도 영향을 미칠 것임[11]
- 또한 말웨어 공격에 의한 영업중지나 사고에 의한 클라우드 서비스 중지 등은 기업휴지보험에서 보장하는 사고에 해당될 수 있음

■ 이와 관련하여 영국 건전성감독기관(PRA: Prudential Regulation Authority)은 보험회사가 언더라이팅 리스크 관리를 위해 묵시적 사이버 리스크에 유의해야 함을 강조함[12]

- PRA는 2017년 사이버 언더라이팅 리스크에 대한 감독성명(Supervisory Statement)을 통해 보험회사가 사이버 언더라이팅 리스크를 인지하고, 정량화하고, 관리할 것을 요구함
- 동 성명에서 PRA는 묵시적 사이버 리스크 관리를 위한 방안으로서 추가적인 리스크를 반영하고 명확한 보장을 제공할 수 있도록 보험료를 조정하거나, 명확하고 명문화된 제외 조항을 도입하는 방법, 구체적인 보장의 한계를 명시하는 방법을 제시함

■ 아울러 PRA는 보험회사의 이사회가 사이버 전략, 이와 관련된 위험 허용 한도 등을 포함하는 경영정보(Management Information)를 주기적으로 검토할 것을 요구함

- 위험허용한도(Risk Appetite Statements)와 측정을 대해 명확하게 제시
- 명시적 사이버 리스크와 묵시적 사이버 리스크에 대한 총 사이버 언더라이팅 노출 측정법
- 극단적인 빈도(최대 200년에 한 번)로 손실총합을 명확하게 고려하고, PRA가 주기적으로 행하는 일반보험 위기상황분석(Stress Test)을 따라 사이버 언더라이팅 리스크 위기상황분석 실시

4. 요약 및 결론

■ 최근 증가하고 있는 사이버공격, 클라우드 서비스에 대한 의존 심화, 정보보안 관련 규제 강화 등은 정보유출에서 오는 직접적 피해뿐 아니라 조업중단이나 배상책임 등 광범위한 피해를 초래함

11) Parsorie(2018)
12) Prudential regulation Authority(2017. 7)

- 조업중단, 물리적 피해, 배상책임 관련 사이버 피해는 기업휴지보험, 재산종합보험, 임원배상책임(D&O)보험, 전문배상책임(E&O)보험 등 일반손해보험이 보장영역에 포함된다고 볼 수 있음

■ 그러나 아직까지 국내 금융당국이나 보험회사는 사이버 언더라이팅 리스크 가운데 명시적 사이버 리스크에만 집중하는 것으로 보임

- 최근 사이버보험 활성화를 위해 명시적으로 사이버 리스크를 보장하는 사이버보험 현황 파악과 보험회사의 명시적 사이버 리스크 관리 방안 마련을 위한 많은 노력이 이루어졌으나, 상대적으로 묵시적 사이버 리스크 관련 현황에 대한 이해는 부족한 실정임

■ 빠르게 진화하는 사이버 리스크를 고려할 때, 보험회사는 묵시적 사이버 리스크의 노출 정도를 측정하고 이에 대비해야 할 필요가 있음

- 첫째, 사이버보험이 보장하는 명시적 사이버 리스크와 함께 현재 보유하고 있는 일반손해보험이 보장하는 묵시적 사이버 리스크의 규모를 측정하여야 할 것임
- 둘째, 보험회사의 이사회는 보험회사의 명시적 사이버 리스크와 묵시적 사이버 리스크 노출 현황을 파악하고 이를 바탕으로 한 사이버 리스크 관리전략을 수립할 필요가 있음
- 셋째, 묵시적 사이버 리스크 관리를 위해 보험료를 조정하거나, 보장이 어렵다면 명확한 제외조항이나 보장의 제한을 명시하는 등 PRA가 제시한 방안을 고려할 수 있을 것임

■ 금융당국도 보험회사가 보유하고 있는 일반손해보험에 내재하는 묵시적 사이버 리스크의 수준을 파악하여 보험회사의 묵시적 사이버 리스크 관리를 촉진해야 할 것임 KiRi

〈별첨 표 1〉 최근 사이버 사고

년도	대상	구분	내용
2017. 5	영국, NHS	WannaCry 랜섬웨어 공격	의료기관, 80개 이상의 NHS(세금으로 운영되는 영국의 공공 의료 서비스) 기관의 컴퓨터 정지
2017. 6	유럽, FedEx(TNT Express 유럽)	NotPetya 말웨어 공격	수송업체, 수송량 감소에 따른 수입감소와 IT 체계 복구비용으로 3억 달러의 손실(2017. 9 기준)
2017. 6	미국 Merck & Co	NotPetya 말웨어 공격	제약회사, 말웨어 공격에 의한 생산정지로 약 3억 천만 달러로 추정(2017. 10 기준)
2017. 6	덴마크, Maersk	NotPetya 말웨어 공격	콘테이너 수송업체, 컴퓨터 시스템 오작동으로 수익의 3억 달러 손실(2017. 9 기준)
2017. 6	미국, Nuance Comms	NotPetya 말웨어 공격	2017. 6. 27 건강관리 고객이 사용하는 시스템 이상, 2017년 6천 800만 달러의 수입 손실 + 복구 비용으로 2천 4백만 달러 2017. 12 기록(transcription) 플랫폼에 있는 리포트를 접속하려는 시도
2017. 9	미국, Equifax	개인정보 유출	신용정보업체, 1억 4천 3백만여 명의 미국고객의 개인정보(이름, 주소, 사회보장번호), 영국과 캐나다 고객의 정보, 20만 명의 신용카드 정보가 유출
2017. 12	사우디아라비아, 산업설비	Triton 말웨어 공격	산업제어시스템(ICS)을 조작하기 위한 말웨어 장착을 시도했으나 실패 동 공격은 주요 사회간접시설을 대상으로 한 공격으로서, 물리적, 인적 피해와 조업중단손실 등을 가져올 수 있었음

자료: 1) Woolf(2016. 10. 26.), “DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say”, The Guardian.com
2) Novet(2017. 8. 16), “Shipping Company Maersk Says June Cyberattack Could Cost It up to $300 Million”, CNBC
3) Palmer(2017. 9. 20), “NotPetya Cyber Attack on TNT Express Cost FedEx $300m”, ZDNet.com
4) Cheetham and Heon(2018.3.6), “Triton Cyber Attack: Hackers Target the Safety Systems of Industrial Plants”, SCOR.COM

〈별첨 표 2〉 PRA의 사이버 언더라이팅 리스크 관련 보험산업조사 결과

· 묵시적 사이버 리스크는 중요함
· 묵시적 사이버 손실 가능성은 시간이 흐름에 따라 증가함
· 특종보험(Casualty Line)은 잠재적으로 침묵 사이버 리스크에 상당히 노출되어 있음
· 해상, 항공, 교통 및 재산보험의 묵시적 손실 가능성
· 재보험 계약의 노출 및 대응의 불확실함
· 대부분의 보험회사들은 명시적 사이버 리스크 관리와 묵시적 사이버 리스크 관리 모두에 대한 명확한 전략이나 리스크 성향이 부족함
· 사이버전문가를 개발하는 데에 대한 투자가 부족
· 보험회사는 명시적으로 보장하는 리스크조차도 잘 이해하지 못하고 있음
· 사이버 리스크 관리 능력이 제한적
· 재해모형 개발자의 사이버재해(Cyber Catastrophe) 모형은 개발 초기 단계
· EU Data Directive는 긍정 사이버 노출을 증가시킬 예정

주: PRA는 2015. 10~2016. 6 사이 보험산업을 대상으로 사이버 리스크 관리 현황을 조사하였으며, 이를 바탕으로 언더라이팅 리스크에 대한 감독성명을 발표함

자료: https://www.bankofengland.co.uk/prudential-regulation/letter/2016/cyber-underwriting-risk