KiRi 리포트 2018.10.1.
글로벌 이슈

사이버보험의 축적리스크(Accumulation Risk) 관리

문혜정 연구원

요약

대규모 기업데이터 유출, 정부 서버 해킹, 랜섬웨어 공격 등 다양한 형태의 사이버 공격이 세계적으로 빠르게 증가하면서 사이버보험에 대한 수요도 지속적으로 높아지고 있음. 사이버 보험시장의 지속가능한 성장을 위해서는 사이버 사고의 축적리스크를 관리하는 것이 핵심임. 글로벌 보험회사는 사이버보험 위험노출도 평가모형 및 축적리스크 관리시스템 등을 통해 사이버보험의 축적리스크를 관리하고 있음. 사이버보험 시장의 안정과 발전을 위한 보험회사와 정부의 역할이 함께 이행될 때 시장의 지속성장이 가능할 것으로 예상됨

대규모 기업데이터 유출, 정부 서버 해킹, 랜섬웨어[1] 공격 등 다양한 형태의 사이버 공격이 세계적으로 빠르게 증가하면서 사이버보험에 대한 수요도 지속적으로 높아지고 있음

- 2018년 세계 사이버보험의 보험료 규모는 약 40억 달러 미만으로 추정되는데, 이는 전체 보험시장의 0.5% 수준으로 아직은 낮은 보험침투율을 보이지만 연간 30% 이상 성장하고 있음[2]
  - 미국이 세계 사이버 보험시장의 85% 이상을 차지하는데, 이는 미국의 데이터보호 규제의 영향임
  - EU의 일반정보보호법(GDPR) 시행은 향후 사이버보험 수요를 더욱 촉진할 것으로 예상됨
- 우리나라도 2019년 6월 13일부터 정보통신서비스 제공자에 대해 개인정보유출 등에 대한 배상책임보험 가입 혹은 필요한 조치를 하도록 의무화[3]함에 따라 국내 사이버보험시장의 규모도 커질 전망임

사이버보험시장의 지속가능한 성장을 위해서는 사이버 사고의 축적리스크(Accumulation Risk)를 관리하는 것이 핵심임

- 축적리스크는 한 사고의 피해가 보험자 포트폴리오의 여러 사업부문으로 확산되어 발생하는 잠재적인 대규모 손실(Tail-Risk)에 대한 노출을 뜻함

1) 랜섬웨어(Ransomware)는 사용자의 디바이스 혹은 중요 데이터를 암호화하고, 암호를 푸는 대가로 사용자에게 금전을 요구하는 악성 소프트웨어의 일종임
2) The Geneva Association(2018. 8), "Advancing Accumulation Risk Management in Cyber Insurance"
3) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제32조의3(손해배상의 보장)

- 고도의 네트워크 상호연결성(Interconnectivity)으로 인해 사이버 공격은 빠르고 광범위하게 확산되어 사고 피해의 범위를 예측하기 어렵고, 이에 축적리스크는 보험회사의 주된 우려요인이 될 수 있음
- 우리나라의 사이버보험 시장은 아직 초기 단계로 많은 상품이 존재하지는 않지만, 일반 손해보험에 내재된 묵시적(Non-affirmative) 사이버리스크[4] 또한 보험회사에 예상치 못한 커다란 손실을 초래할 수 있으므로 축적리스크 평가 시 주요하게 고려해야 함

글로벌 보험회사는 사이버보험 위험노출도 평가 프레임워크 및 축적리스크 관리시스템 등을 통해 사이버보험의 축적리스크를 관리하고 있음

- Lloyd's 보험회사와 미국재보험협회 등은 RMS[5] 및 케임브리지 리스크 연구센터와 협력하여 사이버보험 위험노출도를 측정하는 표준 프레임워크인 '사이버보험 노출 데이터 스키마(Cyber Insurance Exposure Data Schema)'를 공동개발함
  - 사이버보험의 주요 담보사항을 19개 카테고리로, 비즈니스 분야를 20개 카테고리로 분류하여 커버리지별, 사업분야별 위험노출도를 측정하고 모니터링할 수 있는 틀을 제공함
  - 보험산업 내 통용가능한 표준화된 프레임워크를 제공한 것에 의의가 있음
- QBE 보험회사는 RMS(2016)[6]에서 개발한 '사이버 축적리스크 관리시스템(Cyber Accumulation Management System)'의 라이센스 계약을 체결하여 사이버위험 담보력 결정, 포트폴리오 위험 평가 등에 사용하고 있음

보험회사의 언더라이팅 규정 준수, 사이버리스크 및 축적리스크 관리 모형의 지속적인 개발, 그리고 사이버보험 시장의 안정을 위한 정부의 역할이 함께 이행될 때 시장의 지속성장이 가능할 것으로 예상됨

- 사이버보험의 역사가 길지 않으므로 현재의 낮은 손해율에 기초하여 언더라이팅 할 경우, 리스크를 과소평가하지 않도록 유의할 필요가 있음
- 사이버 사고 데이터베이스 구축 및 공유, 대형 사이버 사고 손실공유 프레임워크 구축 등 시장의 안정과 발전을 위한 정부 차원의 제도적 뒷받침이 필요함 KiRi

4) 묵시적 사이버리스크란 보험약관상 사이버 리스크에 대한 보장 혹은 면책 여부가 명확하지 않은 보험계약과 관련된 리스크를 뜻함 (변혜원(2018), 「일반손해보험에 내재된 사이버 리스크 관리」 참고)
5) 글로벌 리스크모델링 회사임 (Risk Management Solutions)
6) Risk Management Solutions, Inc. (2016), "Managing Cyber Insurance Accumulation Risk", report prepared in collaboration with and based on original research by the Centre for Risk Studies, University of Cambridge