Swiss Re

보도자료

스위스재보험 시그마보고서에 의하면, 보험사와 기업은 난해한 과제인 사이버 리스크에 대처할 수 있음. Swiss Re Institute 공식 출범

- 사이버 공격과 관련된 잠재적 비용이 빠르게 증가하고 있음. 사이버 보안 및 회복탄력성 문제는 기업에게 점점 큰 부담이 되고 있음
- 사이버 보험 전문 시장이 빠른 속도로 발달하고 있지만, 아직 담보범위가 상대적으로 좁음
- 상품 및 프로세스 개혁과 빅데이터 및 스마트 분석에 힘입어 사이버 보험 솔루션의 개선이 이루어질 수 있음
- 정부는 사이버 회복탄력성(cyber resilience) 제고를 위해 중요한 역할을 할 수 있음
- 이 보고서는 오늘 공식적으로 출범하는 Swiss Re Institute의 첫 보고서임

취리히, 2017년 3월 1일 – 사이버 리스크는 기업에 점점 큰 부담이 되고 있다. 최근에 발생한 여러 사건은, 사이버 공격에 따른 비용이 데이터 손실 또는 오류에 따르는 직접적 비용보다 훨씬 높을 수 있다는 사실을 보여주고 있다. 스위스재보험의 최신 시그마보고서 "사이버: 난해한 리스크에 대한 대처"는 기업들이 사이버 보안을 리스크 관리 계획에 통합하기 위해서는 현재보다 훨씬 많은 노력을 해야 한다고 언급하고 있다. 사이버 회복탄력성을 제고하기 위한 초기 사업이 진행되고 있다. 사이버 보험 전용 시장이 빠른 속도로 발달하고 있지만, 지금까지는 담보범위가 잠재적 익스포저에 비해 좁은 실정이다. 상품 및 프로세스 혁신, 그리고 고급 분석도구가 있어야 사이버 보험 솔루션의 개선이 이루어지고 인수 적격성 및 담보범위의 한계가 확장될 수 있을 것이다. 궁극적으로, 일부 사이버 리스크, 특히 극단적인 재해 손실 이벤트와 관련된 사이버 리스크에 대해서는 보험가입이 불가능할 수도 있다. 이러한 리스크와 관련하여, 정부가 지원하는 보호장치가 필요할 수도 있다.

세간의 이목을 끈 최근의 사이버 공격은, 사이버 보안의 침해로 인한 비용은 데이터 손실 또는 오류로 인한 후유증의 관리에 비해 훨씬 광범위하다는 사실을 보여주고 있다. 이제 기업들은 평판, 물리적 및 지적 재산권의 손상뿐만 아니라 업무 운영의 중단 가능성까지 고려해야만 한다. 사이버 사고와 관련된 잠재적 비용의 범위 및 규모의 증가세는 끊임없이 진화하는 사이버 리스크 환경을 반영하는 것이며, 이는 세 가지의 주요 원동력에 의해 좌우되고 있다:

- 점점 빨라지고 광범위해지고 있는 디지털 변화;

Darren Pain, Zurich
Telephone +41 43 285 2504

Kurt Karl, Armonk
Telephone +1 914 828 8686

Jonathan Anchen, Bangalore
Telephone +91 80 4900 2650

Investor Relations, Zurich
Telephone +41 43 285 4444

Swiss Re Ltd
Mythenquai 50/60
P.O. Box
CH-8022 Zurich

Telephone +41 43 285 2121
Fax +41 43 285 2999

www.swissre.com
@SwissRe

- 인터넷접속이 가능한 기기 및 클라우드 컴퓨팅 등이 빠른 속도로 퍼지면서, 초연결성으로 인해 취약점의 증가;
- 성공적인 사이버 공격에 따른 잠재적인 경제적 이익에 대해 인지한 해커 집단의 수단 정교화 진행.

위험에 대한 인식이 증가했음에도 불구하고, 전반적으로 기업은 사이버 리스크에 대처할 준비가 미흡한 상황이다. 상대적으로 적은 수의 기업만이 사이버 보안을 리스크 관리 계획에 통합했다. 고급 데이터 보호 장치를 구축할 것을 기업들에게 요구하는 법안이 수많은 관할권에서 발효되고 있으므로, 규제가 촉매 역할을 할 수 있다. 그 결과, “대기업과 중소기업은 사이버 보안 아키텍처에 대한 투자를 늘림으로써 강력한 손실 전 및 손실 후 리스크관리 역량을 개발할 필요가 있습니다”라고 수석 이코노미스트 Kurt Karl 은 언급했다.

복잡한 리스크에 대한 관리

수많은 기업들이 사이버 리스크를 더욱 잘 흡수할 수 있는 제 3 자들에게 이 리스크를 전가할 방법을 모색하고 있다. “사이버 보험 전문 시장이 발전하고 있으며, 점점 더 많은 보험사들이 이 특수보험 종목에서의 비즈니스 기회를 모색하고 있습니다”라고 Kurt Karl 은 덧붙였다. 일반적으로 전용 사이버 보험은 데이터/네트워크 보안 위반 및 관련 손실에 대한 핵심 보장을 제공하고 있으며, 오늘날 시장에서의 보장 한도는 약 USD 500 만 - USD 1 억 사이이다. 하지만, 이외의 중대한 일부 사이버관련 리스크에 대해서는 보험가입이 거의 이루어지지 않은 상태이며, 기존 담보규모는 기업 전반의 잠재적 익스포저에 비해 미미한 상황이다.

보험 솔루션 개발에 있어 핵심적인 제약요인은 사이버 리스크의 본질과 연관되어 있다. 사이버 리스크는 복잡하며 수치화하기 어려운데, 특히 빠른 속도로 변화하는 기술적 환경 및 과거의 사이버 관련 클레임 데이터(이를 통해 미래의 손실 가능성에 대한 정보를 추정)의 부재를 감안할 때 더욱 그러하다. 보험사들과 리스크 분석도구 벤더들은 사이버 이벤트로 인한 잠재적 손실 규모를 추정해보기 위해, 사이버 리스크 모델링에 대한 각기 다른 접근방식(결정론적 시나리오 분석 및 확률모델 포함)에 대해 실험하고 있다. 자연재해 등의 기타 위험과 관련된 경험은, 기본적인 리스크 동인에 대해 이해가 증진되고 사이버 손실에 대한 더 많은 데이터가 축적되면서, 모델에 대한 지속적인 개선이 이루어질 것이라는 희망을 안겨주고 있다.

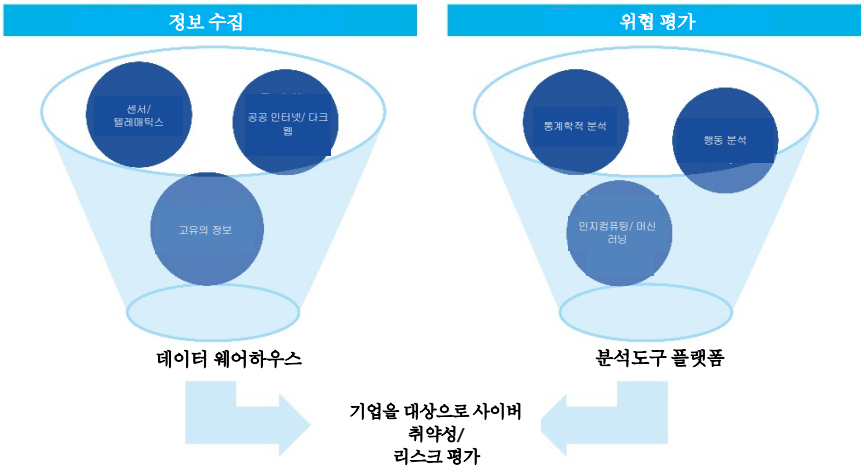
상품 및 프로세스의 혁신

한편, 보험 및 기타 리스크 전가 방법의 상품 및 프로세스 혁신은 사이버 리스크 관리 역량의 개선에 있어 중요한 역할을 하게 될 것이다. 혁신 속도에 영향을 미치는 핵심요인은, 관련 데이터의 포착 및 분석, 그리고 사이버 리스크에 대해 정확한 언더라이팅에 필요한 관련 위협 정보가 될 것이다. 정보의 수집 및 전파를 개선하기 위해 업계는 지속적으로 노력하고 있다.

예를 들어, 다양한 리스크 분석도구 벤더들은, 기업들이 사이버 익스포저를 포착 및 계량화하고 이를 보험사에게 보고할 수 있는 표준화된 접근방식을 제공해주는 데이터 도식을 구축해왔다.[1] 마찬가지로, CRO 포럼은 기업들이 사이버 위협과 취약성에 대한 핵심적 정보를 포착할 수 있는 공통적인 언어와 체계를 홍보하고 있다.

보험사들은 간단하고 더욱 유연한 보험상품의 개발을 모색하고 있다. 특히 대기업에 비해 사이버 리스크에 대응할 준비가 미흡한 경우가 많은 중소기업을 위한 상품이 포함된다. 또한, 일부 보험사/ 재보험사들은 지식격차를 해소하고, 고객들에 대한 서비스를 개선하고, 추가적인 서비스를 제공하기 위해 사이버 보안 회사 및 데이터 분석도구 벤더들과의 협업을 모색하고 있다. 더 일반적으로, 고급 분석도구는 보험사/재보험사들의 전통적인 언더라이팅 툴을 확장해주고, 빠르게 변화하는 기초 리스크 요인들에 신속하게 대응하도록 지원할 수 있다.

그림 1: 보완적 언더라이팅 툴로서의 스마트 분석도구



출처: Swiss Re Economic Research & Consulting.

사이버 리스크에 대한 전반적인 손실흡수 능력을 개선하기 위한 또 하나의 방법은, 자본시장 투자자들이 일부 익스포저를 인수하도록 하는 상품을 개발하는 것이다. 현재, 사이버 등의 운영 리스크를 담보하는 보험연계증권(ILS)을 개발하기 위한 몇몇 계획이 있다. 사이버 리스크에 대한 ILS 시장은 초기 단계이지만 성장 가능성이 있다.

[1] 예를 들어, 다음 자료 참조: "RMS Launches New Data Standard for Managing Cyber Insurance", *rms.com*, 2016.01.19. 및 *Verisk Cyber Exposure Data Standard and Preparer's Guide* , AIR, 2016.

정부의 지원 역할

인수 적격성 범위를 확장함에 있어, 기업은 거래 보험사와 협업을 통해 지속 가능한 시장을 생성할 필요가 있다. 또한 정부도 사이버 회복탄력성의 제고에 있어 중요한 역할을 담당하고 있는데, 이에는 사이버 정보의 수집 및 공유를 개선하기 위한 조치, 그리고 사이버공간이 활용 및 보호되는 방식에 대한 법과 규제의 도입이 포함된다. 인센티브를 제공을 점검하고 사이버 위협에 대한 인식을 제고함으로써, 정부는 민간이 더 나은 시장주도적 솔루션을 개발하도록 계속 유인할 수 있다. 하지만, 궁극적으로는 일부 사이버 이벤트로 인한 잠재적 손실 규모는 민간 보험/재보험 섹터가 흡수하기에는 지나치게 클 수도 있는데, 특히 핵심 인프라 또는 네트워크의 대대적인 파괴 등과 같은 대규모 손해 이벤트가(그 결과 상당 규모의 누적손실이 발생할 수 있음) 이에 해당한다.

이 시그마 보고서는 "Swiss Re Institute" 이름으로 처음으로 출간되는 보고서입니다. Swiss Re Institute 은 재보험업계의 연구 리더로서의 스위스재보험의 위상 제고라는 임무를 부여 받고 2017 년 3 월 1 일에 정식으로 출범하게 되어, 그 결과 당사의 다양한 고급 리서치 및 정보제공 역량이 하나로 통합됩니다. Swiss Re Institute 은 재보험업계의 선도적인 리서치 간행물인 시그마를 포함하여, 스위스재보험의 리서치중심 보고서를 발간할 계획입니다.

Notes to editors

Swiss Re

The Swiss Re Group is a leading wholesale provider of reinsurance, insurance and other insurance-based forms of risk transfer. Dealing direct and working through brokers, its global client base consists of insurance companies, mid-to-large-sized corporations and public sector clients. From standard products to tailor-made coverage across all lines of business, Swiss Re deploys its capital strength, expertise and innovation power to enable the risk-taking upon which enterprise and progress in society depend. Founded in Zurich, Switzerland, in 1863, Swiss Re serves clients through a network of around 70 offices globally and is rated "AA-" by Standard & Poor's, "Aa3" by Moody's and "A+" by A.M. Best. Registered shares in the Swiss Re Group holding company, Swiss Re Ltd, are listed in accordance with the International Reporting Standard on the SIX Swiss Exchange and trade under the symbol SREN. For more information about Swiss Re Group, please visit: www.swissre.com or follow us on Twitter @SwissRe.

How to order this *sigma* study:

The English, German, French, and Spanish versions of the *sigma* No 1 /2017, *Cyber: getting to grips with a complex risk* are available electronically on Swiss Re's website: www.swissre.com/sigma