국제심포지엄

4차 산업혁명과 사이버보험

본 자료는 2018년 11월 5일 중소기업중앙회 제2대회의실에서 개최된 국제심포지엄 『4차 산업혁명과 사이버보험』에서 논의된 내용을 정리한 것입니다.

CONTENTS

4차 산업혁명과 사이버보험

CONTENTS

Ⅰ. 개최 취지

■ 인공지능, 블록체인, 사물인터넷 등으로 대표되는 4차 산업혁명에 의해 우리 주변의 모든 것이 빠르게 디지털화되고 있음

○ 또한 인터넷과 결합되면서 과거와 비교할 수 없을 정도로 사물과 사물 간에, 그리고 사물과 사람 간 연결성이 확대되고 있음

■ 이처럼 초연결사회(Hyper-connected Society)로 진화해감에 따라 사이버위험의 성격도 변화하고 있음

○ 과거에는 개인정보 유출에 의한 프라이버시 피해가 주를 이루었으나 점차 물리적 피해를 수반하는 형태로 변화하고 있음

■ 사이버 사고가 물리적 피해를 수반할 경우 정상적인 영업활동이나 일상적인 생활의 영위가 어려워져 빠른 피해복구가 중요해졌음

○ 이로 인해 피해복구 재원조달을 위한 위험재무 수단의 하나로 사이버보험의 중요성이 점차 증대하고 있음

■ 그러나 아직 국내에서는 사이버보험의 역할에 대한 논의가 충분히 이루어지지 못하고 있음

○ 국제심포지엄 개최를 통해 주요국의 경험에 대해 듣고 국내 보험산업 및 정책당국에 주는 시사점에 대해 논의하고자 함

Ⅱ. 보험의 사이버 - 피지컬 시장으로의 전환

권욱진 (St. John's 대학 교수)

1. 사이버위험의 특성

■ 세계경제포럼(World Economic Forum)의 2018년 글로벌 위험 보고서에 의하면, 사이버위험은 가능성(Likelihood) 측면에서는 3위, 영향(Impact) 측면에서는 6위를 기록하였음

○ 한편, 로이즈는 사이버 공격에 의한 전 세계 피해규모가 약 365억 달러에 이를 것으로 추정하였음

■ Romanosky(2016)가 미국의 사이버 사고 자료를 토대로 분석한 결과에 의하면, 평균 피해비용은 약 784만 달러였음

○ 반면, 중간값은 약 25만 달러로 평균값과 중간값 간에 상당한 차이를 보였음

○ 평균값과 중간값이 큰 차이를 보이는 이유는 사이버 사고의 분포가 다수의 소규모 피해와 소수의 대규모 피해로 구성되어 있기 때문임
- 분석 대상 샘플의 최대 피해액 규모는 약 7억 5천만 달러였음

■ 데이터의 부족 등에 의해 사이버 사고 원인 및 피해 유형별로 세분화된 분석이 이루어지지 못하고 있음

2. 미국의 사이버보험 시장 현황

■ 단독형(Stand-alone) 사이버보험의 수입보험료는 2011년 5억 달러에서 2015년 15억 달러로 증가하였음

○ 현재 46개 주에서 정보유출사고 신고 의무화를 도입하고 있는데, 2015년 기준 신고 건수는 1,370건임

■ 산업별 사이버보험 시장 규모를 살펴보면, 금융, 유통, 의료 등의 분야가 높은 비중을 차지하였음

○ 2015년 수입보험료를 기준으로 할 때, 금융 분야가 29%, 유통 분야가 21%, 그리고 의료 분야가 15%를 기록하였음

■ 사이버보험 손해율은 2016년 기준으로 약 61.4% 정도임

3. 사이버보험 시장 전망 및 과제

■ 주요 기관들은 향후 전 세계 사이버보험 시장이 빠른 속도로 성장할 것으로 전망하였음

○ PWC는 2020년까지 연평균 성장률이 21%에 이를 것으로 예측하였고, Aon은 44%에 이를 것으로 전망하였음

■ 향후 보험상품의 발전방향과 관련해서는 사고 원인 및 피해 유형별로 세분화된 보험상품이 등장할 것으로 보임

○ 현재는 모든 유형의 사이버위험을 하나의 상품을 통해 보장하고 있는데, 전통적인 보험의 경우처럼 점차 세분화될 것임

■ 한편, 사이버보험 활성화를 위해서는 보험약관의 용어 등을 표준화하는 작업이 필요함

○ 보험회사, 브로커 등을 대상으로 인터뷰 조사한 결과에 의하면, 보험회사별로 보험약관의 용어 정의가 상이하였음

Ⅲ. 일본의 사이버보험

도이 다케시 (MS & AD 시니어 매니저)

1. 사이버 사고 동향

■ 일본 경찰청의 사이버 범죄 보고서에 의하면, 2013년 약 8만 4,863건이던 사이버 범죄 건수가 2017년 약 13만 건으로 증가하였음

○ 사이버 범죄 유형 가운데 인터넷 사기(Fraud)가 가장 큰 비중을 차지하였음

■ 인터넷 뱅킹 관련 불법 송금(Illegal Remittance) 규모는 감소추세에 있음

○ 2014년 상반기 약 18.51억 엔에서 2018년 상반기 3.72억 엔으로 감소하였음

■ 특정 대상을 목표로 한 사이버 공격(Targeted Attacks)은 2013년 이후 지속적으로 증가하고 있음

○ 2013년 492건에서 2017년 6,077건으로 증가하였음

2. 사이버보험 시장 현황 및 MS & AD의 사이버위험 평가 시스템

■ 일본의 사이버보험 시장 규모는 2014년 이후 지속적으로 증가하였음

○ 2014년 약 105억 엔이던 사이버보험 수입보험료가 2017년 약 188억 엔으로 증가하였음

■ MS & AD는 여러 기업과의 제휴를 통해 사이버보험 가입 기업에 사이버위험 평가 및 관리와 관련된 다양한 서비스를 제공하고 있음

○ 사이버위험 평가와 관련해서는 Verizon, Bitsight 등과 협력하고 있고, 사이버위험 통제 및 예방과 관련해서는 NEC, Insights 등과 협력하고 있음

■ MS & AD는 사이버보험 가입 단계에서 가입 기업의 사이버 위험을 평가하기 위해 Verizon에서 개발한 설문지를 활용하고 있음

○ 또한, 인터넷상의 다양한 정보를 활용해 가입 기업의 사이버위험을 평가하고 있는데, 이러한 작업은 Bitsight의 도움을 받아 이루어지고 있음

3. 중소기업 대상 사이버보험 설문조사 결과

■ 2018년 9월 26일부터 10월 12일에 걸쳐 일본 중소기업을 대상으로 사이버보험 관련 설문조사를 실시하였음

○ 약 1만 개의 기업에 설문지를 보냈으나 664개 기업만이 설문지에 응답하였음

■ 조사 대상 기업 가운데 12.3%만이 현재 사이버보험에 가입하고 있었음

○ 10.4%는 가입 계획을 가지고 있었고, 나머지 77.3%는 가입 계획조차 없었음

■ 사이버보험 가입 계획이 없는 기업을 대상으로 조사한 결과 약 35.6%가 사이버보험에 대해 전혀 모르고 있었음

○ 중소기업을 대상으로 사이버보험 관련 홍보를 보다 적극적으로 할 필요가 있다는 사실을 알게 되었음

■ 중소기업이 희망하는 사이버보험의 담보 1순위는 배상책임(Liability)으로 63.0%의 기업이 원했음

○ 두 번째는 복구비용으로 58.6%를 기록했는데, 중소기업의 규모가 클수록 복구비용의 상대적 중요성이 증가하였음

Ⅳ. 중국의 사이버보험 시장 현황 및 발전전략

프랭크 왕 (Gen Re China 언더라이팅 디렉터)

1. 사이버 사고 동향

■ 미국의 정보보안 회사인 시만텍(Symantec)에 의하면, 2017년 랜섬웨어 공격 건수를 기준으로 할 때, 중국은 미국에 이어 2위를 차지하였음

○ 또한, 이메일 가운데 스팸 이메일이 차지하는 비중으로 볼 때도 중국은 사우디아라비아에 이어 2위를 기록하였음

■ 모바일 사이버 사고의 경우에는 전체 사고의 절반 이상이 미국에서 발생하여 가장 큰 비중을 차지하였음

○ 인도가 11%, 독일이 9%였으며, 중국은 2%의 비중을 차지하였음

■ 사물인터넷에 대한 공격은 2016년 약 6천 건에서 2017년 약 5만 건으로 증가하여 약 600%의 증가율을 보였음

○ 공격의 근원지로는 중국이 21%로 가장 높은 비중을 차지하였으며, 이어서 미국이 11%, 브라질이 7%, 러시아가 6%의 비중을 차지하였음

2. 법적 환경

■ 2017년 6월 1일부터 사이버보안법(Cybersecurity Law)이 시행되었는데, 사이버 공간에서의 프라이버시 및 보안을 포괄적으로 규제하는 첫 번째 법률임

○ 사이버보안법에는 네트워크 사업자의 의무 및 책임, 개인정보 및 중요정보에 대한 보호 규칙, 주요 정보통신기반시설의 보안 규칙 등이 명시되어 있음

■ 중국의 경우 개인정보보호와 관련된 포괄적인 법률인 개인정보보호법은 아직 존재하지 않음

○ 현재 개인정보보호법 관련 논의가 진행되고 있으며, 빠르면 2020년경에 제정될 것으로 보임

■ 2017년 8월 16일 사이버 법원이 설립되었으며, 주요 업무는 사이버 공간에서 발생한 사건의 소송을 처리하는 것임

○ 접수 건수는 2018년 10월까지 약 1만 1,600건 정도 되었으며, 건당 평균 처리 시간은 약 28분 정도 되었음

3. 가계성 사이버보험

■ 개인은행계좌손실보험(Individual Bank Account Loss Insurance)

○ 계좌 및 비밀번호가 도용, 불법복제, 협박에 의해 유출되어 발생하는 손실을 보장함

○ 배상한도는 3만 위안부터 88만 위안이고, 보험료는 1년에 48~1,408위안임

■ 사이버가상재물손실보험(Cyber Virtual Property Insurance)

○ 온라인게임의 계정, 장비, 아이템 등이 도용 및 해킹에 의해 손실을 볼 경우 보상함

○ 중국태평양손해보험회사가 중국온라인게임서비스연맹과 함께 개발하였음
- 온라인 플랫폼에서 판매되고 있으며, 보험금 청구도 온라인을 통해 이루어지고 있음

■ 모바일결제보상보험(Mobile Payment Protection Insurance)

○ 모바일결제서비스 이용자 대상 보험으로, 2014년 처음으로 출시되었음
- 모바일 바이러스에 의한 금전적 손실을 보상함
- 사고 건당 보상한도는 3천 위안이고, 1년간 총 한도는 10만 위안임

○ 중안보험회사와 모바일결제서비스 사업자인 바이두가 공동으로 개발하였음
- 보험료는 모바일결제서비스 사업자인 바이두가 부담함

Ⅴ. 한국의 사이버보험 현황 및 정책과제

임준 (보험연구원 연구위원)

1. 기업시장

■ 국내 사이버보험 시장은 공급 측면 및 수요 측면의 여러 제약요인에 의해 보험가입률이 저조한 상황임

○ 이러한 문제에 대해 제3자 피해보상수단 마련 의무화를 중심으로 사이버보험 정책이 추진되어 왔음

■ 주요국의 경우에는 공급 측면은 사이버 사고 데이터 표준화 및 집적, 수요 측면은 사이버위험 인식 제고를 위한 홍보 중심으로 추진되고 있음

○ 아직까지는 보험 가입률 제고를 위한 의무화 도입이나 직·간접적인 보험료 지원 제도의 시행 사례가 존재하지는 않음

■ 향후 시장상황의 변화 등으로 인해 의무화만으로는 한계에 부딪힐 경우 재보험풀이나 인센티브제도 도입과 같은 대안을 검토할 필요가 있음

○ 사이버위험과 비슷하게 LPHI(Low Probability and High Impact)의 특성을 보이는 홍수보험의 경우 보험제도의 건전성도 유지하면서 보험 가입률을 제고할 수 있는 방안으로 세제지원 등의 인센티브제도 도입이 논의되고 있음

2. 가계시장

■ 설문조사 결과에 의하면, 대다수의 소비자가 가계성 사이버보험 상품의 판매 사실을 인지하지 못하고 있음

○ 사이버 금융범죄 관련 보험상품의 경우 응답자의 약 8.4%만이 판매 사실에 대해 인지하고 있었음

■ 현재는 가계성 사이버보험이 주로 특약 형태로 판매되고 있는데, 설문조사를 통해 단독형에 대한 잠재적 수요가 존재함을 확인할 수 있었음

○ 사이버 금융범죄 보험상품의 구입 의향을 밝힌 응답자 가운데 약 47.9%가 특약형 대신 단독형 상품을 선호하였음

■ 단독형 상품의 경우 수수료 문제로 인해 설계사 채널을 통해 판매하기는 어려운데, 부가상품의 형태로 판매하는 것이 하나의 전략이 될 수 있음

○ 이 경우 소비자가 인식하지 못한 상태에서 보험에 가입되는 등의 소비자보호 이슈가 제기될 수 있기 때문에 투명한 정보 제공 등의 소비자보호 장치 마련이 필요함

3. 공공부문

■ 공공부문의 경우 대량의 데이터를 보유하고 있으나 혁신적인 활용에 있어서는 미흡했다는 비판이 제기되면서 전 세계적으로 공공데이터 개방 운동이 전개되었음

○ 국내에서도 2013년 '정부 3.0'이라는 제목으로 공공데이터 개방 운동이 추진되었음

■ 그동안의 국내 공공데이터 개방 정책을 평가해보면, 개방 및 활용 측면에 비해 위험재무 전략 측면의 논의는 상대적으로 미흡하였음

○ 2015년 11개 분야의 공공데이터 개방을 시작으로, 2017년에는 29개 분야로 확대되었음

■ 보다 적극적인 개방을 위해서는 위험재무 전략이 병행되어야 하는데, 민영보험회사로의 위험 전가가 어려울 경우 위험의 일부 또는 전부를 공공부문이 보유하는 방안을 검토할 필요가 있음

○ 공공부문의 위험보유 방안으로 자가보험과 정부지원 재보험풀을 생각해볼 수 있음

Ⅵ. 토론내용 요약

「강용석」 (SK인포섹 글로벌사업본부 본부장)

■ 보험산업에서 사이버위험 평가 툴을 만들 때 정보통신기반시설(Critical Information Infrastructure) 사례를 참고하면 좋을 듯함

○ 정보통신기반시설의 경우 법에 의해 취약점을 점검하고 조치하도록 되어 있는데, 이와 관련하여 매우 상세한 프로세스가 이미 만들어져 있음

■ 보험회사가 사이버위험 평가 프레임워크를 만들 때 점검항목에 예방활동 뿐만 아니라 탐지활동도 포함시킬 필요가 있음

○ 예방은 사전에 취약점을 점검하여 위험관리 시스템의 미비점을 보완하는 활동을 의미하고, 탐지는 모니터링을 통해 사이버 공격을 조기에 발견하여 신속히 대응하는 활동을 의미함

- 사이버 공격의 경우 외부에서 공격하는 방법도 있으나 요즘은 내부에 에이전트를 심어 놓고 공격하기도 함

■ 사이버보험의 경우 민간 자율에 맡길 것인지 아니면 의무화할 것인지가 이슈가 되고 있는데, 병행할 필요가 있다고 생각됨

○ 북한발 해킹과 같은 경우처럼 국가 혼란을 야기할 목적의 사이버 사고와 관련해서는 공공성에 입각한 접근이 필요함

「김성호」 (보험개발원 손해보험부문 부문장)

■ 미국의 사이버보험 시장은 매년 고성장을 지속해 가고 있으나 한국은 약 300~400억 원 수준에서 정체되어 있음

○ 한국의 보험수요는 의무보험 위주이고, 담보의 범위 역시 사이버 리스크의 다양성에도 불구하고 의무보험의 영역인 개인정보 유출로 인한 배상책임 중심임

○ 다만, 2018년 정보통신망법 개정으로 보험 의무가입 대상이 확대된다는 점에서 사이버보험 시장이 한 단계 더 커지므로, 이를 통해 제3자(3rd Party)와 당사자(1st Party)를 아우르는 보험수요의 진작 가능성도 예상해볼 수 있음

■ 사이버보험 공급 측면에서 사이버 리스크에 대한 객관적인 평가는 해외나 우리가 공히 겪고 있는 공통적인 난관임

○ 경험 데이터가 부족하고 위험의 형태나 침해를 야기하는 방법이 다양할 뿐만 아니라 위험의 양상과 관련 기술이 끊임없이 변화하고 있음

○ 이러한 문제를 해결하고자 학계, 인터넷진흥원 등과 협업을 통해 사이버 리스크 평가모델 구축을 진행해오고 있으나 손해정보와 리스크를 분석하는 데 어려움이 있는 것이 현실임

○ 일본 사례의 경우 보안업체인 BitSight나 Version社와 협력을 통해 내·외부 위험요인을 평가하고 활용하는 점이 흥미로움

- 다만, 보안 쪽의 관점은 공격 속성과 시스템 취약점을 파악해서 사고 재발을 방지하는 것이 주된 목적일 텐데, 협업에 따른 운영성과와 과거 데이터(Historical Data)가 어떻게 활용되었는지에 대해 추가로 벤치마킹해보았으면 함

■ 미국 NetDiligence나 ISO 사례, 유럽의 Insurance Europe의 사례와 같이 우리도 민관이 협력해서 사고 경험 데이터 활용의 관점에서 사고 데이터를 표준화하고 집적·활용할 수 있는 체계를 구축하는 것이 필요함

「김종현」 (한국전자통신연구원 정보보호연구본부 프로젝트리더)

■ 국제 표준화기구 ITU-T SG17 회의에서 사이버위험에 대한 표준화 개발이 논의되고 있으며, 사이버보험에서 표준화 이슈는 중요하다고 생각함

■ 가입자 입장에서 사이버위험뿐만 아니라 사이버보험의 용어, 약관 등 관련 보험 질문지 등의 표준화 역시 필요하다고 생각함

○ 업체마다 질문지가 다르고 내용을 이해하기 어렵기 때문에, 보상 범위, 사고 유형 등을 정의하는 업계 표준이 필요하다고 생각함

■ 두 번째로는 사이버보험 활성화를 위해 업계 이해관계자 간의 데이터 공유가 필요해보임

○ 보험회사가 사이버보험 판매를 고려할 때, 직면하는 어려움으로는 경험 데이터의 부족, 사이버 공격의 진화, 잠재적인 추가 손실, 사이버위험에 대한 협소한 시각 등이 있음

○ 따라서 사이버상의 잠재적인 손해와 피해액을 예측하기 위해서 관계기관 간의 데이터 공유를 통해 어려움을 극복할 필요가 있다고 생각함

■ 세 번째로, 사이버 취약성을 정량화할 수 있는 기존의 점수화 시스템을 활용할 필요가 있음

○ 사이버 취약성을 정량화할 수 있는 표준화된 점수화 시스템이 존재하며, 이러한 시스템을 통해 사이버보험 요율을 산출하는 데 기여할 수 있을 것으로 보임

■ 마지막으로, 보험업계 종사자와 정보보안 전문가들이 협력하여 사이버 위험 인수 방법 또는 사이버보험 상품을 개발하면 좋을 것 같음

「심현우」 (한양대학교 보험계리학과 교수)

■ 사이버보험 상품 약관의 용어 등을 표준화하고 사이버위험을 세분화하여 분석할 필요가 있음

○ 현재 출시된 보험상품의 경우 약관의 용어 등에 있어서 표준화가 미흡하여 소비자가 상품을 비교·선택하는 데 어려움을 겪고 있음
- 국가 공인기관 등의 주도하에 사이버보험 상품의 약관을 표준화하는 작업이 필요함

○ 사이버위험의 경우 모든 사고가 동일한 특성을 가지고 있는 것이 아니라 여러 다양한 특성을 가지고 있으므로 유형별 위험 분석 및 위험 관리가 필요함
- 스팸이나 바이러스에 의한 사이버 사고와 해커의 침입에 의한 사이버 사고를 분석하기 위해서는 다른 접근이 필요함

■ 보험상품 개발에 활용될 수 있는 사이버 사고 데이터의 집적을 위해 다양한 분야의 전문가들이 협업할 필요가 있음

○ 컨설팅 업체, 사이버보안 업체, 경찰청 등에서 사이버 사고 관련 데이터를 수집하고 있으나 사이버보험 요율 산출 등에 활용하기에는 한계가 있음
- 컨설팅 업체와 사이버보안 업체가 수집한 데이터의 경우 전체를 대표하는 표본이 아니고 조사자의 주관적 판단이 개입되어 있으며, 경찰청의 사고 통계는 거시적인 기초통계임

○ 데이터 부족 문제를 해결하기 위한 방안의 하나로 계리사, 통계청, 보안 전문가 등의 협업을 통한 사이버상의 데이터 수집을 생각해볼 수 있음

○ 단, 데이터 수집 과정에서 개인정보보호 이슈가 야기될 수 있는데, 이와 관련하여 정보보호 규제기관의 역할 분담 및 재정립이 필요함
- 개인정보를 관리하는 기관과 개인정보를 활용하는 기관을 분리·독립시켜 역할 분담을 할 수 있게 하는 것이 필요함
- 현재 개인정보 관련 감독기관이 행정안전부, 금융위원회, 방송통신위원회 등으로 나누어져 있고, 네트워크 감식기관으로 경찰청 사이버 안전국이 있는데, 업무가 중복되는 경향이 있기 때문에 역할을 재정립하는 것이 필요함

■ 사물인터넷의 경우 전통적인 네트워크에 비해 사고 발생 가능성 및 위험 전이 속도가 증가할 것으로 예상됨

○ 사물인터넷의 위험관리 수단으로 블록체인을 사용하는 것이 효과적일 것으로 예상함

「최용민」 (한화손해보험 상무)

■ 사이버보험 시장 활성화를 위해 업계 차원에서의 다양한 노력이 필요한데, 첫 번째는 중소기업 대상 사이버위험관리 컨설팅 표준화임

○ 대기업과 달리 중소기업의 경우에는 사이버위험 평가 및 관리 능력이 부족하기 때문에 보험회사의 컨설팅이 필요함
- 예를 들어, 당장 내년에 정보통신서비스사업자가 사이버보험 의무가입 대상자가 되는데, 이들을 위한 사이버위험관리 가이드라인이 없음
- 보상한도액, 자기부담액, 예상 피해규모 등과 관련된 가이드라인을 업계가 협력하여 제시할 필요가 있음

○ 보험회사의 사이버위험관리 컨설팅 능력을 제고하기 위해서는 글로벌 사이버보안 업체로부터 도움을 받아야 하는데 막대한 비용이 소요됨
- 업계 차원에서 공동으로 비용을 분담하는 방안을 생각해볼 수 있음

○ 일정 수준까지는 중소기업의 보안체계 강화를 통해 위험을 관리하고, 그 이상의 위험은 보험업계로 전가하는 방향으로 유도해야 함

■ 두 번째는 보험가입 및 보상과 관련된 프로세스의 표준화임

○ 국내 보험회사들이 사이버보험상품 도입을 위해 글로벌 재보험사들과 접촉하였는데, 재보험사마다 가입 질문서가 질적·양적으로 상당한 차이를 보였음
- 사이버보험상품의 투명성 제고를 위해 업계 차원에서 통합하는 작업이 필요함

○ 국내의 경우 사이버보험과 관련하여 보험금 지급 경험이 거의 없으며, 보상 프로세스가 체계화되어 있지 않음
- 포렌식이나 사이버보안 전문가를 통한 체계화된 보상 프로세스의 표준화 마련을 위해 업계 공동의 노력이 필요함

■ 세 번째는, 해외 사례를 참고할 때, 기업의 사이버위험 인식 제고를 위해 협회를 중심으로 해서 업계가 공동으로 대응할 필요가 있음

「권욱진」 (St. John's 대학 교수)

■ 개별 보험회사 차원에서 사이버 사고 데이터를 집적하고 위험평가 모델을 개발하기는 쉽지 않음

○ 사이버 사고 데이터를 집적하고 사이버위험 평가모델을 가지고 있는 회사들이 많은데, 이러한 회사들과의 협업을 시도하는 것이 필요함

○ 싱가포르의 경우에는 공공기관, 통신업체, 보험회사 등이 참여하는 CyRim 프로젝트를 통해 사이버 사고 데이터베이스 구축 작업을 진행 중인데, 한국도 싱가포르 사례를 참고할 필요가 있음

「도이 다케시」 (MS & AD 시니어 매니저)

■ 사이버보안 업체인 BitSight와 Verison社와의 협력을 통해 MS & AD가 얻을 수 있었던 주요 성과 가운데 하나는 사이버보험 가입 기업에 사이버보안 관련 다양한 서비스를 제공할 수 있게 된 점임

○ 고객 기업은 사이버위험 평가 보고서를 통해 자신의 취약점에 대한 정보를 획득하고, 보완할 수 있어서 관련 서비스에 만족하고 있음

「프랭크 왕」 (Gen Re China 언더라이팅 디렉터)

■ 사이버위험 평가도 중요하지만 사이버위험 인수 전략에 대해서도 생각해볼 필요가 있음

○ 고위험군과 저위험군으로 구분하고, 저위험군부터 조심스럽게 인수하는 전략의 채택이 필요함

「임준」 (보험연구원 연구위원)

■ 오늘 발표는 주로 수요 측면에 초점을 맞추었는데, 향후 공급 측면에 대해 연구하게 된다면, 우리와 경제 규모가 비슷하거나 작은 국가에 초점을 맞출 계획임

○ 싱가포르가 하나의 벤치마킹 사례가 될 수 있음

국제심포지엄

4차 산업혁명과 사이버보험

발행일 | 2018년 12월

발행인 | 한기정

발행처 | 보험연구원

주 소 | 서울시 영등포구 국제금융로 6길 38 (여의도동 35-4)

연락처 | 02-3775-9000

인쇄처 | 경성문화사 / 02-786-2999