EU 의 사이버보험 활성화 정책

- ENISA 의 사이버보험에 대한 권고를 중심으로 -

송은지 오남호*
한국인터넷진흥원 주임연구원
한국인터넷진흥원 팀장 *

Ⅰ. 서론

점차 진화하는 사이버 위협에 대응하는 안전장치로서 사이버보험이 부상함에 따라 이를 지원하려는 해외 주요국의 정책 검토 움직임이 활발하다. 대표적으로 EU 는 2017 년 10 월 6 일 ENISA 에서 사이버보험 워크숍을 개최하여 정책 당국과 업계를 대상으로 하는 권고안과 업계의 시장 현황을 통한 향후 과제 등을 검토하였다.

이어서 ENISA 는 11 월에 "사이버보험의 위험평가 언어의 공통성(Commonality of risk assessment language in cyber insurance)"이라는 제목과 사이버보험의 권고안(Recommendations of Cyber Insurance)이라는 부제로 도출된 보고서를 발표한 바 있다.

전통적으로 세계 사이버보험 시장은 미국 기업들이 85%를 차지하고 있으며 시장 규모도 미국을 중심으로 지난 10 년간 크게 성장하였다[1]. 또한, EU 도 2018 년 5 월 25 일부터 개인정보보호 규정(General Data Protection Regulation: GDPR)이 발효됨에 따라 사이버보험 시장이 급성장할 것으로 예측되고 있다. EU 는 사이버보험 사업을 육성하기 위해 개정된 NIS 지침을 활용하여 사고 데이터를 축적하려는 전략적인 행보를 보이고 있다.

본 고에서는 EU ENISA 에서 개최한 워크숍의 주요 내용과 발표된 권고안을 상세히 살펴봄으로써 글로벌 사이버보험 시장의 최신 시장 현황을 알아보고 EU 의 향후 사이버보험 관련 지원 정책 방향을 알아보고자 한다.

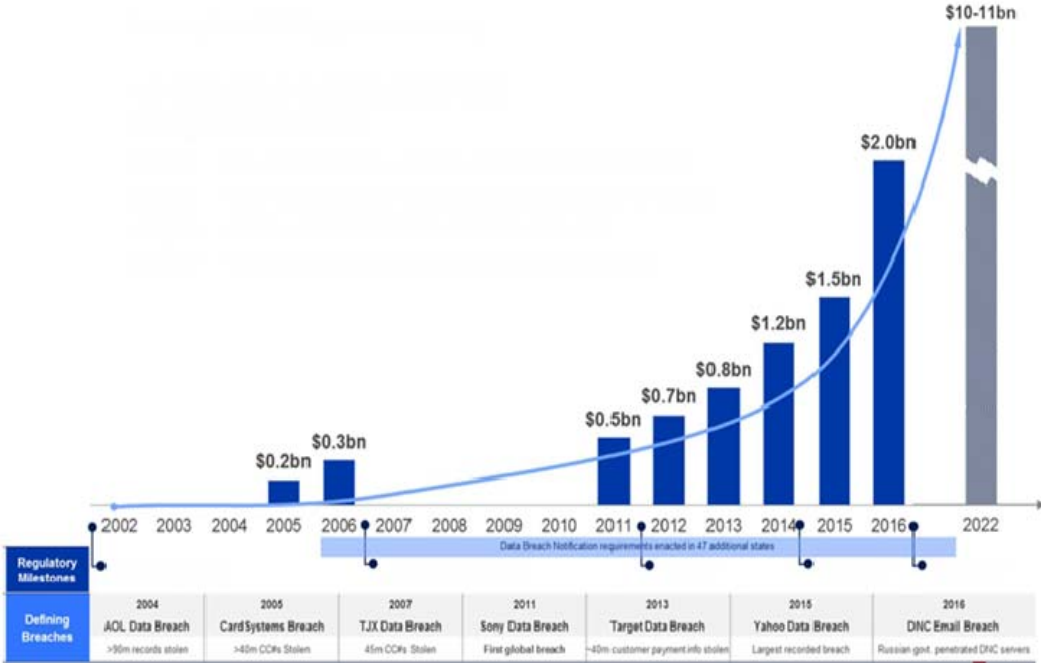
* 본 내용은 송은지 주임연구원(☎ 061-820-1207, songeunji@kisa.or.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP 의 공식적인 입장이 아님을 밝힙니다.

Ⅱ. 사이버보험 시장

글로벌 사이버보험 시장의 보험료 규모는 약 34 억 달러로 추정되고 있으며, 그 중 70%인 약 23 억 달러는 독자적 사이버보험 상품으로 구성된다. 또한, 85%의 보험사가 미국에서 유래하고 있다[1].

1. 미국의 사이버보험 시장

[그림 1]과 같이 미국 사이버보험 시장은 2011 년부터 2016 년까지 연간 32%의 증가율을 보이며 성장하고 있다. 최근 이렇게 시장이 급성장한 데는 여러 가지 요인이 있지만 2011 년 발생한 최초의 글로벌 규모의 침해사고였던 Sony 의 데이터 유출 사고, 4,000 만 건에 달하는 고객 지불 정보가 유출된 2013 년의 Target 사의 사고, 2015 년 발생한 최대 규모의 Yahoo 의 데이터 유출 사고, 2016 년 러시아 정부의 민주당 전국위원회 서버 해킹 사건 등을 전후로 해서 큰 폭으로 시장이 성장한 것을 볼 수 있다.



<자료> ENISA 워크숍 자료, 2017.

[그림 1] 미국 사이버보험 시장 규모 현황 및 전망

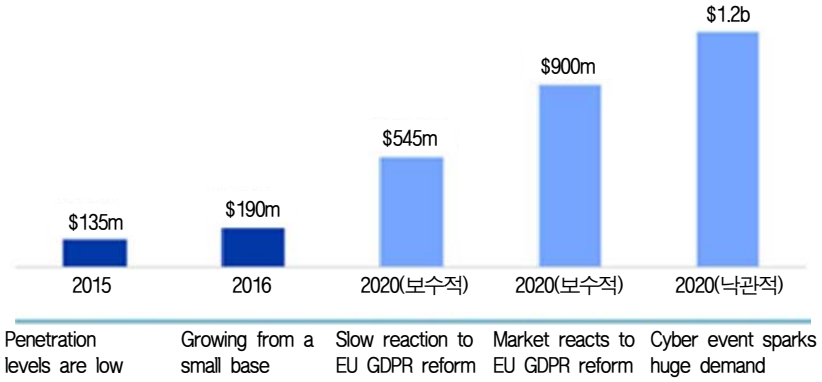
또한, 2002 년에서 2017 년 사이에 미국 48 개 주에서 데이터 침해에 관한 법률이 제정되면서 2006 년부터 2015 년 사이 사이버 침해 신고 건수가 325% 증가하기도 하였다. 이에 따라 2006 년부터 2015 년 사이 데이터 침해 비용도 60% 늘어난다. 이러한 여러 가지 요인들이 복합적으로 작용하면서 미국 사이버보험 시장이 고속 성장하였으며 2022 년까지 약 100 억에서 110 억 달러로 시장 규모가 크게 증가할 것으로 예상되고 있다.

이와 같이 성숙한 단계에 접어든 미국 사이버보험 시장의 주요 수요자는 대형 금융 기관, 소매상, 의료 기업 등이다. 10 억 달러 이상의 매출을 창출한 기업이 시장의 38%, 1 억에서 10 억 달러의 매출을 기록한 기업이 43%, 매출 1 억 달러 이하의 기업이 19%로 비교적 균등하게 분포하고 있다.

2. EU 의 사이버보험 시장

2016 년 EU 의 독자적 사이버보험 시장은 약 1 억 9,000 만 달러로 추정되며, GDPR 이 구매자 인식 및 수요에 미치는 영향에 따라 2020 년까지 약 9 억 달러(현실적 성장) 규모로 성장할 것으로 예상되고 있다. 한편, 느리게 성장한다면 2020 년 5 억 4,500 만 달러 규모로 보수적인 전망을 할 수 있으며, 거대한 사고 발생으로 수요가 더욱 촉발된다면 12 억 달러의 규모로 보다 낙관적 전망을 할 수 있는 상황이다.

EU 의 사이버보험 시장이 성장하는 데는 크게 네 가지의 원인을 들 수 있다. 첫 번째는 법안의 제정이다. GDPR 발효로 인해 위반하는 기업은 글로벌 총 매출의 2~4%에 달하는



<자료> ENISA 워크숍 자료, 2017.

[그림 2] EU 사이버보험 시장 규모 현황 및 전망

과징금을 부담해야 하고, 이는 범 EU 차원으로 집행된다. 또한, NIS 지침으로 데이터 침해 통지 의무가 부과된다. 두 번째는 인식 제고이다. GDPR 로 인해서 사이버보안 강화의 중요성에 대한 인식이 향상되었고 기업들도 심각하게 인식하고 있다. 세 번째는 침해 사고 건수의 증가이다. 2011 년 이후 사이버사고 침해 건수는 36% 증가했다. 이는 사고가 늘어난 절대적 수치의 증가도 있겠지만 통지를 의무화함에 따라 건수가 더욱 증가한 것으로 추측된다. 네 번째는 침해사고로 인한 비용의 증가이다. 유럽의 데이터 침해 비용은 미국에 비해 35% 낮게 책정되는 수준이지만, GDPR 로 인해 비용이 상승할 가능성이 높다. 이는 앞에서 살펴본 미국 선례와 마찬가지로 데이터 침해 통지 의무화 법안의 시행 후 시장 규모가 상승할 것이라고 추정할 수 있다.

미국에 비해 미성숙한 단계인 EU 의 사이버보험 시장은 매출 10 억 달러 이상의 기업이 85% 이상, 매출 5,000 만 달러에서 10 억 달러의 기업이 10%, 매출 5,000 만 달러 이하의 기업이 5%를 각각 차지하고 있다. 대부분 대기업의 수요를 중심으로 시장이 형성되어 있으며 중소기업의 수요나 매출 기여는 미미하다고 볼 수 있겠다.

Ⅲ . 사이버보험 위험평가

1. 개요

사이버보험 위험평가는 보험사가 보험 정책과 관련된 위험을 평가하고 사정하는데 사용하는 방법론을 통칭한다. 이는 피보험자의 보험료 산정에도 도움이 된다. ENISA 의 “사이버보험의 위험평가 언어의 공통성(Commonality of risk assessment language in cyber insurance)”에 따르면 사이버보험의 위험평가는 대부분 보험 질문지를 통해 수행되며, 정보보호 및 개인정보보호 관련 업계 표준을 참고하기도 한다.

위험 평가 과정은 위험 식별 및 평가(Risk identification and evaluation)→프로그램 마케팅(Marketing of programme)→옵션 제시(Present option)→프로그램 실행(Programme executions) 등의 단계를 포함한다. 위험 식별 및 평가 단계에서는 시장 상황과 손실 등을 분석하며 현재 위험을 평가한다. 이어서 프로그램 마케팅은 단계에서는 데이터를 수집하여 보험사에 제출하며 언더라이터 회의 등을 거치고 예비 견적을 받는 작업을 수행한다. 옵션 제시 단

계에서는 견적과 커버리지 조건들을 평가 및 비교해보고 담보 협상, 최종 협상 등을 진행하게 된다. 마지막 프로그램 실행단계에서는 선택한 프로그램을 결합하여 청구서를 작성하고 보험 증권을 취득한다.

2. 기존 위험평가 프레임워크

보험사가 위험 평가의 수단으로 사용하는 보험 질문지의 분석 전에 사용 가능한 위험 평가 및 표준화 이니셔티브의 검토가 필요하다. 이와 관련하여 캠브리지 위험 연구센터가 보험사 Lloyd's 와 공동으로 개발한 "사이버 축적 위험 관리(Managing Cyber Accumulation Risk)"와 Lloyd's 가 개발한 "사이버 핵심 데이터 요구사항(Lloyd's Cyber Core Data Requirements)"을 들 수 있다.

먼저 캠브리지의 이니셔티브는 표준화된 방식으로 사이버 위협을 정의하기 위해 시도하고 있는데 총 19 개의 손실 커버리지를 식별하는 스키마를 생성하며 각각 직접 손해 및 제 3 자 손해 등을 구분하여 설명하고 있다[2]. 이 연구는 사이버 사고의 축적 위험에 대한 불확실성을 해결하기 위해 수행되었고 이러한 위험으로 인해 보험사가 사이버보험의 인수를 주저하게 된다는 사실을 강조한다. 캠브리지의 연구 결과는 손실 커버리지의 식별 및 표준화 작업을 통해 사이버 보험에 대한 축적 위험을 이해하고 관리하기 위한 프레임워크를 제공한다는 데에 큰 의의가 있다. 이러한 접근 방법은 위험 평가에 대한 기초를 제공하고 있지만 분류한 스키마들에서 요청하는 정보들은 회사가 산정하기 어려운 요소들이 많아 현실적으로는 실용적이지 못한 것으로 간주될 수 있다. 예를 들어, 보험사는 조직의 시간당 손실을 산출하면 비즈니스 중단 비용을 평가할 수 있지만 현실적으로 시간당 손실 산출은 거의 불가능하다.

표준화를 위한 업계 주도의 이니셔티브인 Lloyd's 의 사이버 핵심 데이터 요구사항은 사이버 노출 데이터를 위한 공통 핵심 스키마 및 시장의 사이버 위험 도구에 사용되는 입력 데이터에 대한 공통 핵심 기능을 정립하고자 한다. 이 두 가지는 모두 사이버 위험을 평가할 때 고려해야 하는 핵심 속성 및 정보가 기존의 업계 표준과 일치해야 하는 방법이다. 전문가들은 이런 노력이 공통 보험 정책 언어를 개발하도록 장려함으로써 보험사 및 재보험사가 위험을 좀 더 정확하게 측정할 것이라고 평가한다.

3. 보안 표준과 사이버보험

앞에서 설명한 것과 같이 보안 표준은 피보험자의 사이버 보안 성숙도나 인식의 지표로 사용되며 위험 평가 프로세스를 식별하는 기준점으로 활용된다. 사이버보험 업계에서 가장 자주 사용되는 보안 표준은 ISO 27001/2, NIST 의 CyberSecurity Framework, Cobit 5, NCSC 10 Steps 등이다.

보험사는 보다 정교하게 피보험자의 위험을 평가하기 위해 보안 표준의 항목들을 질문지의 내용에 포함시킬 수 있다. 그러나 사이버보험 전반에서 채택된 보안 표준이 없기 때문에 보험사마다 질문지와 언어 모두 상이할 수 밖에 없다. ENISA 는 본 연구에서 위에 언급한 보안 표준들을 서로 비교하는 작업을 통해 보험 상품 커버리지와 질문이 얼마나 유사

[표 1] 보안 표준 및 사이버보험 커버리지

커버리지 유형	보험 적용 대상	커버리지 제공비율(%)	보안 표준 비율(%)	중요 보안 표준
최초 대응	핫라인, IT 및 법률 고문	100%	100%	사건 대응 및 관리
이벤트 관리	법률/PR, 기술 법의학 및 통지	100%	100%	사건 대응 및 관리
데이터 보호 및 사이버 책임	책임 청구 및 벌금	100%	100%	몇 가지 보안 표준
네트워크 중단	사이버 사건(예: 맬웨어)으로 인한 소득 손실	100%	100%	몇 가지 보안 표준
네트워크 중단: OSP	외부 서비스 공급자 보안 또는 시스템 장애로 인한 손실	-	100%	몇 가지 보안 표준
네트워크 중단: 시스템 고장	시스템 고장 또는 인간의 실수로 인한 손실	40%	100%	보안 기술 평가 및 격차 해소를 위한 적절한 훈련
사이버 갈취	랜섬 지불 비용 및 사이버 전문가	90%	100%	몇 가지 보안 표준
전자 데이터 사건	컴퓨터 시스템의 뜻하지 않은 손상으로 인한 손실(예: 홍수)	20%	100%	몇 가지 보안 표준
미디어 책임	전자 콘텐츠의 지적 재산권 침해에 따른 손해 및 방어 비용	80%	100%	몇 가지 보안 표준
사이버 도난	사기성 전자 자금 이체로 인한 금전적 손실	20%	100%	권한의 통제된 사용 및 꼭 필요한 경우만 허락하는 방식의 통제된 액세스
형사 보상 기금	체포 및 유죄 판결로 이어지는 정보의 지불 비용	10%	0%	없음

<자료> ENISA Commonality of risk assessment language in cyber insurance 자료, 2017.

한지를 살펴보았다. 먼저 보안 표준들을 20 개의 중요 보안 통제 요소들을 중심으로 비교한 결과 거의 모두 주요 보안 표준에 언급되어 있는 사항임을 확인하였다.

이어서 보험 상품의 커버리지에 보안 표준의 통제 항목들이 반영되는지도 비교해보았다. [표 1]과 같이 보안 표준과 사이버보험 상품의 커버리지는 약간의 상관관계가 있는 것으로 결과가 확인되었다. 그러나 커버리지 유형과 보안 표준의 항목들이 긍정적인 상관 관계가 있더라도 보안 표준이 광범위하기 때문에 주의가 필요하다. 보험회사가 제공하는 12 개의 가장 일반적인 커버리지 유형과 보안 표준이 호응하는지를 분석하고 적용되는지를 확인하기 위해 통계적인 ANOVA 방법론을 사용하였다.

ENISA 는 추가로 글로벌 보험사 10 개가 사용하는 사이버보험 질문지와 보안 표준 간에도 이러한 긍정적인 상관관계가 있는지를 분석하였다. 그 결과, 모든 보안 표준이 포함하는 항목이 설문지에 일부만 반영되어 있는 경우가 많았다. 이는 특정 사이버보안 통제를 권고하는 보안 표준의 비율이 높을수록 해당 항목을 포함하는 설문지의 비율이 낮다는 음의 상관관계가 밝혀짐으로써 보안 표준과 사이버위험 평가에 사용하는 보험사의 설문지 항목은 조화되지 않는 것으로 분석되었다.

정리해보면, 전반적으로 보안 표준과 커버리지 구성 요소는 조화되어 있으나 보험 질문지는 조화되어 있지 않다는 연구 결과를 확인할 수 있다.

Ⅳ. EU 의 사이버보험 활성화 정책방안

1. 업계 대상 권고

ENISA 는 연구결과를 통해 최종적으로 사이버보험 활성화를 위한 권고안을 도출하였다[3]. 사이버보험 업계를 대상으로 하는 권고 사항은 크게 여덟 가지 방안을 제시하고 있다. 첫 번째는 정책 언어 및 보험 설문지의 표준화이다. 명확하고 단순화된 문구를 제공하기 위해 정책 언어와 커버리지를 표준화하고 동일한 위험을 다루는 보험 인수 방법도 표준화하는 것을 의미한다. 업계의 모범 사례를 기반으로 사이버 위험을 평가하는 질문지를 도출하고 공통적인 정책 문구나 보험 인수 언어를 개발하는 것을 포함한다.

두 번째는 정보공유분석센터(ISAC)를 통한 업계 이해관계자간 데이터 공유 촉진이다. 익

<자료> ENISA Commonality of risk assessment language in cyber insurance, 2017.

[그림 3] 업계 및 정책 당국을 대상으로 하는 권고

명화된 방식을 통해 위험 평가를 위한 충분한 데이터를 제공하고 유용한 정보 생성을 위한 업계 표준 탬블릿을 개발하는 것도 언급하고 있다. 이는 모든 업계가 자발적으로 정보를 공유하는 수단에 동의하고 동일한 플랫폼을 사용하는 것을 전제하고 있다.

세 번째는 용어, 커버리지, 사건 유형, 사용 사례 등을 정의하는 업계 표준을 개발하는 것이다. 표준은 사이버보험 상품의 전체 범위를 다룰 필요는 없지만 사이버보험의 공급자와 수요자 모두에게 기준점으로 작용할 수 있다. 이런 표준화 노력은 업계가 주도하는 것이 바람직하며 손실을 산정하고 모델링하는 기존의 작업을 기반으로 추진할 수 있다.

네 번째는 사이버보안에 대한 사내 전문지식 개발이다. 정보보안 전문가들과 사이버 위험 인수 방법을 개발하거나 사내의 사이버보험 전문가 팀을 구성하거나 전문 지식 네트워크를 구축하는 등의 작업이 이에 해당된다.

다섯 번째는 정보보안 및 개인정보보호 규정(GDPR, NIS 지침) 등을 상품 프레임워크 개

발의 기초로 사용하는 것이다. 각종 지침이나 보안 표준의 규정을 기반으로 보험 인수 및 커버리지 용어를 조화시키고 요구사항을 기반으로 질문지를 작성하는 것을 의미한다.

여섯 번째는 산업 및 부문별로 언어를 조화시키는 것이다. 이러한 작업은 특정 부문별 요구사항을 이해하기 위해 고객과 협력하고 부문별 위험 환경을 이해하는 데에 도움이 될 수 있다.

일곱 번째는 보다 유연한 보험 인수 절차로 중소기업의 시장 요구에 대응하는 것이다. 중소기업을 위해 정책 커버리지 문구를 단순화하고 보험 인수 프로세스를 단순화시켜서 보다 효율적으로 중소기업의 보험 인수를 수행할 수 있다.

마지막은 다양한 경로를 통해 사이버 사고 데이터 수집을 지원하고 데이터 품질 향상을 위해 노력하는 항목이다. 위험 분석 등을 통해 위험 평가 프로세스를 강화하고 데이터 세분화를 강화함으로써 사고 데이터 수집 프로세스도 개선한다.

2. 정책당국 대상 권고

ENISA 의 연구 보고서는 업계 대상 권고와 더불어 EU 및 회원국의 정책 입안자들을 대상으로도 크게 다섯 가지의 권고 사항을 제시하고 있다. 첫 번째는 보험사의 최소 커버리지 요구사항을 만드는 것이다. 공통적이고 비교 가능한 기준점을 제공하기 위해 최소한 각 커버리지에서 필요한 요구사항을 정의하면 제공하는 상품에 대한 소비자의 신뢰를 제고할 수 있을 것이다.

두 번째는 NIS 지침과 GDPR 을 통해 의무 사고 데이터 보고 체계를 활용하여 의미 있는 데이터들을 생산하는 것이다. 구체적으로 특정 업계의 요구사항을 유용한 정보로 활용하기 위해 사이버보험 업계 관계자들의 자문을 받고 데이터를 공유할 수 있는 익명화 기준을 정의하는 작업이 요구될 것이다. 또한, 사고 데이터 보고로 수집된 정보들은 시간이 경과함에 따라 업데이트함으로써 적절한 관리를 해주어야 할 것이다.

세 번째는 EU 전반의 사고데이터 중앙 집중식 저장소를 구축하는 것이다. 산업부문별 정보공유분석센터(ISAC)가 데이터 수집에 기여하고 영향을 파악할 수 있는 방법들을 정책당국이 주체가 되어 확인해야 한다.

네 번째는 사이버보안 및 사이버 위험 관리에 대한 인식을 제고하는 것이다. 정부와 정책 입안자는 사이버 보험이 사이버위험 관리의 유용한 해결책이 될 수 있다는 사실에 대

한 인식을 제고하는 이니셔티브를 시행하는 것이 필요하다. 사이버보험은 사이버 위험을 이전하는 메커니즘일뿐만 아니라 위험 예방 및 완화 수단이기도 하다는 것을 대중에게 알리는 것이 중요하다.

다섯 번째는 사이버보험 가이드라인 개발에 유럽위원회와 ENISA 의 적극적인 참여를 장려한다는 것이다. 보험회사의 설문지를 개선하는 것과 관련되는 우수사례나 위험평가에 필요한 보험 인수 정보의 유형에 대한 권고사항, 사이버보험과 관련되는 공통 분류 체계 정의 활동 등이 구체적인 활동이 될 수 있다.

Ⅴ. 결론

본 고는 EU 전역에서 사이버보험 시장의 활성화가 예상됨에 따라 그에 필요한 구체적인 사항들을 검토하고 위험 평가 언어를 표준화하는 것의 중요성을 도출하고 있다. 현재는 보험사별로 상이한 언어를 구사함으로써 동일한 커버리지의 보험료가 10 만 유로에서 30 만 유로까지 차이가 발생하고 있어 이러한 문제를 해결하기 위해서라도 위험 평가 절차의 조화가 필요하다고 보는 것이다.

또한, EU 는 사이버보험 시장이 대기업의 수요를 중심으로 형성되어 있는 것에 문제의식을 갖고 있는 것으로 보인다. 지속적으로 중소기업의 요구에 대응함으로써 보험 시장을 확대하고 성숙한 시장으로 거듭날 것을 장려하고 있다. 실제로 별다른 조치가 없더라도 차년도의 GDPR 발효로 중소기업의 사이버보험 수요가 늘어나며 EU 전반의 사이버보험 시장의 폭발적 수요가 예상된다.

물론 ENISA 에서 개최한 워크숍의 내용과 권고 사항을 담고 있는 본 연구 보고서는 EU 의 법적 조치로 해석되지 않고 ENISA 전체의 견해로 대표되지는 않는다. 그러나 EU 의 업계 전문가들과 ENISA 가 사이버보험에 대해 이러한 논의와 연구를 하고 있다는 사실만으로도 우리에게 시사하는 바가 크다고 볼 수 있다. 보고서의 권고 부분에서 언급하는 데이터 집중 저장소 구축이나 가이드라인 개발, 표준화 등은 상당히 적극적인 조치로 해석될 수 있기 때문이다. 향후에 발간될 EU 의 사이버보험 가이드라인에 어떠한 사항들이 담길지 궁금해지는 대목이다.

최근 국내에서도 정보보호 업계와 금융 업계의 신시장으로서 사이버보험 활성화 이슈

가 주목 받고 있다. 건강한 사이버보험 생태계 마련을 위한 논의에 EU ENISA 의 최근 연구와 거론되고 있는 정책(안)들이 좋은 선례가 되어 줄 수 있을 것이다.

[참고문헌]

[1] ENISA, Global Cyber Market Overview, Enisa Cyber Insurance Workshop, 2017. 10. 6.
[2] Cambridge Centre for Risk Studies, Managing Cyber Insurance Accumulation Risk, 2016. 2.
[3] ENISA, Commonality of risk assessment language in cyber insurance, 2017. 11.