KiRi Weekly
2014.9.1 제298호

KiRi 보험연구원
Korea Insurance Research Institute

서울시 영등포구 국제금융로 6길 38 (여의도동 35-4) 8층 보험연구원 (문의 : 변철성 수석담당역 / 02-3775-9115)

KiRi Weekly 2014.9.1
이슈

해외 사이버 배상책임보험시장 성장의 시사점

최창희 연구위원, 김혜란 연구원

요약

- 사이버 리스크에 의한 전 세계 연간 최대 손해액은 자연재해에 의한 손해액의 5배 규모이며 전산 시스템과 휴대용 전자기기 보급 확대로 손해액은 매년 빠르게 증가하고 있음.
- 전 세계적으로 매년 수천만에서 수억 건의 정보 유출이 이루어지고 있으며 정보 유출 사건 수와 유출 정보 건수가 급증하고 있음.
- 사이버 리스크 관련 보험사고는 발생 빈도가 높지 않으나 발생 시 피해 규모가 커 대재해와 유사한 형태의 손해를 보인다는 특징을 가지고 있으며 급속한 정보화의 진행으로 발생 가능성이 높아지고 있음.
- 외국의 보험회사들은 사이버 배상책임보험을 사이버 리스크 평가 · 관리 컨설팅, 관련 교육 프로그램 등과 함께 제공하여 사업 영역을 확대하고 매출을 증대시키고 있으나 국내의 사이버 배상책임 시장 규모는 미미한 수준임.
- 최근 들어 국내에서 개인정보 유출에 대한 배상책임이 강화될 움직임을 보이고 있어 국내의 사이버 배상책임보험 시장이 크게 성장할 것으로 예상됨.
- 국내 손해보험회사들은 사이버 배상책임보험 언더라이팅 능력을 향상시키고 관련 컨설팅 및 손해배상 소송 지원 등의 서비스를 제공하기 위하여 다음과 같은 역량을 강화하여야 함.
  - IT 시스템 관련 전문 지식, 사이버 리스크 관련 손해배상 소송 수행 능력, 사이버 리스크 관리 체계에 관한 이해, 다양한 CLI 담보에 대한 평가 능력
- 또한 손해보험회사들은 시장 성장에 대비하여 다양한 담보를 포함한 관련 상품 개발, 외국 회사의 사업모델을 벤치마킹한 사업 영역 확대, 국내에 진출한 외국 기업에 대한 마케팅 활동 강화 등의 노력을 기울일 필요가 있음.

1. 검토 배경

■ 사이버 리스크에 의한 전 세계 연간 최대 손해액은 자연재해에 의한 손해액의 5배 규모이며, 전산 시스템과 휴대용 전자기기 보급 확대로 손해액은 매년 빠르게 증가하고 있음.

- McAfee(2013)에 따르면 전 세계에서 사이버 범죄에 의하여 매년 발생하는 비용은 3,000억에서 1조 달러 규모이며 매년 손해액수가 빠르게 증가하고 있음.[1)]

■ 사이버 배상책임보험(cyber liability insurance, 이하 CLI)은 e-business, 인터넷 네트워크 및 정보 자산 등 사이버 리스크와 관련하여 계약자와 제3자의 리스크를 담보하는 보험임.

- CLI는 정보자산의 유실 · 훼손 · 유출에 의한 소득 손실 또는 운영비용 증가, 시스템 · 정보 복구 중 발생한 비용 및 사업 중단 비용, 사이버 갈취[2)], 명성 손상 비용, 법적 대응 비용 등의 계약 당사자 리스크를 담보함.
- CLI가 담보하는 제3자 리스크는 고객정보 유실 · 훼손 · 유출에 대한 배상 · 보상 비용[3)], 금융정보 유출에 의한 피해 보상 비용, 조사 비용, 정보 유출 통지비용, 정보 유출 대중매체 공지 비용, 제3자 정보의 손실, 벌금 및 과징금 비용, 소송 비용, 카드 재발급 비용 등임.[4)]
- 일반적으로 배상책임보험은 제3자에 대한 손해배상을 담보하는 보험이나 외국에서는 CLI가 제3자 리스크와 당사자 리스크를 모두 담보하는 보험으로 정의됨.

■ 뮌헨 재보험은 향후 7년간 CLI가 현재의 3배 이상 성장할 것으로 예상함.

- 뮌헨 재보험은 현재 2013년에 13억 달러 규모인 CLI 시장이 7년 안에 50억 달러 이상으로 성장할 것으로 예상
- CLI를 제공하는 손해보험회사는 2002년 4개에서 2013년 40여 개로 10배 증가하였음.[5)]

---

1) http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf
Biener, Eling, Wirfs(2014), Insurability of Cyber Risk: An Empirical Analysis, IIS 50th Annual Seminar.
2) 미국에서는 해커가 기업으로부터 빼낸 정보를 담보로 금전을 요구하는 사고가 발생하고 있음.
3) 배상은 법적 책임이고 보상은 법적 책임은 없으나 도의적으로 책임을 지는 경우임.
4) 일부 CLI는 시스템 정지 및 오작동으로 인한 상해를 담보로 하고 있음.
5) Asia Cyber Liability Insurance Conference, http://www.asiainsurancereview.com/aircyber

■ 외국 보험회사들은 CLI와 함께 사이버 리스크 관리 컨설팅을 제공하여 사업 영역을 확장하고 이를 신성장동력으로 활용하고 있으나 국내 보험회사들의 CLI 관련 보험 실적은 미미한 편임.[6)]

- 외국 손해보험회사들은 사이버 리스크 관리 컨설팅과 CLI를 함께 판매하여 사업 영역을 확대하고 매출을 증대시키고 있음.
- 현재 국내에 출시된 CLI에는 개인정보 유출 관련 전자금융거래 배상책임보험, 공인전자문서 보관소 배상책임보험, 집적정보통신시설 사업자 배상책임보험, 개인정보 유출 배상책임보험, e-Biz 배상책임보험 등이 있으며, 시장규모는 연간 241억 원 정도임.

■ 본고는 사이버 리스크 현황 및 국내외 CLI 시장과 상품 비교를 통해 국내 손해보험회사에 주는 시사점을 제시함.

2. 세계 사이버 리스크 현황

■ 2014년 글로벌 비즈니스 리스크 Top 10에 의하면 사이버 범죄 · IT 시스템 고장 · 산업 스파이 활동 등에 의하여 발생하는 사이버 상의 손해가 새로운 리스크로 부상함.[7)]

- 알리안츠의 조사에 따르면 사이버 범죄, IT 시스템 고장, 해킹 등에 의한 피해는 전체 경영 리스크의 12%를 차지하였으며 매년 빠르게 증가하는 추세를 보이고 있음.[8)]

■ 세계적으로 매년 수천만에서 수억 건의 정보 유출이 이루어지고 있으며 정보 유출 건수와 유출된 정보 수는 급증하는 추세를 보임.[9)]

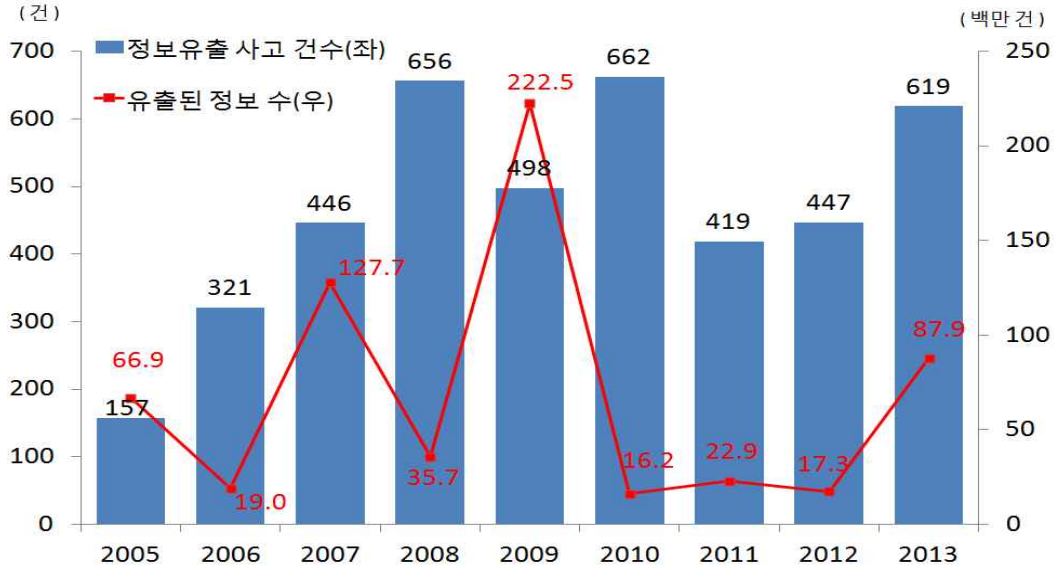
- 2013년에 정보 유출 사고 건수와 유출된 정보의 수는 각각 619건과 8,790만 건으로서 2012년도에 비해 각각 38%, 408% 증가하였음.

---

6) http://www.thebell.co.kr/front/news_print_free.asp?key=20140217010002603000158 4
7) Allianz Risk Barometer survey.
8) Allianz Global Corporate & Speciality 보고서.
9) http://www.datalossdb.org 참조.

- 정보 유출의 평균비용은 188달러이고 병원의 정보 유출은 사생활 침해의 위험이 있어 다른 자료유출에 비해 비용이 큼.

〈그림 1〉 정보 유출 건수와 정보 유출에 따른 비용



주: 2013년 자료는 2014년 1월 1일 자료로서 2014년 1월에 공개된 3천만 건의 유출된 정보 수를 포함, 왼쪽 축은 사고 건수, 오른쪽 축은 사고에 따른 정보 유출 건수.
자료: Identify Theft Resource Center.

정보는 다양한 피해 대상과 경로를 통해 유출된 것으로 나타남.

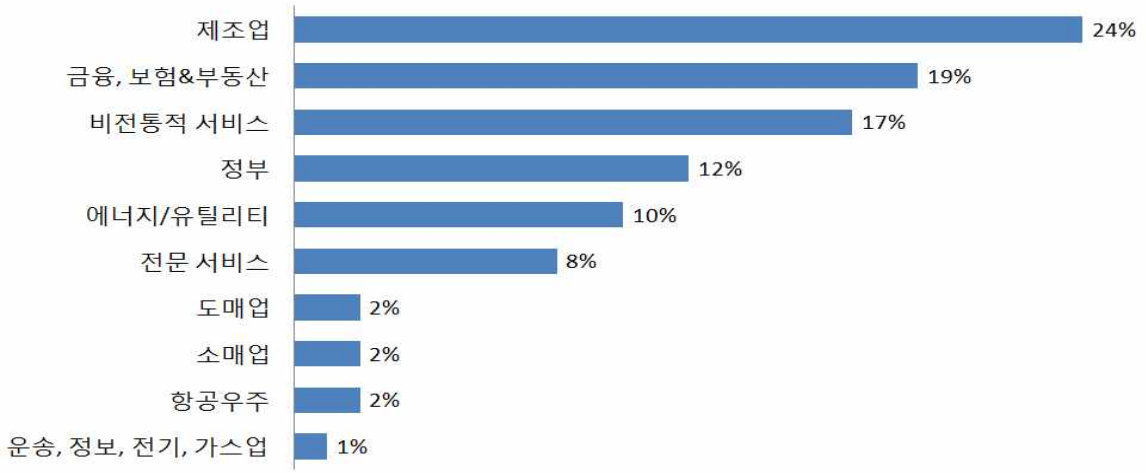
- 과거에는 금융기관, 정부 그리고 일반 대기업 등 개인정보를 다수 취급하는 기관 · 기업이 공격 대상이었으나 최근 들어 항공우주, 전기, 가스 등의 피해가 증가하는 추세를 보이고 있음.
  - 제조업(24%), 금융기관(19%), 비전통적 서비스(17%) 그리고 정부(12%)가 50% 이상을 차지
- 과거 해커들은 대기업을 타깃으로 하는 경우가 많았으나 최근 들어 중소기업을 타깃으로 한 해킹이 증가하는 추세를 보이고 있음.
- 해킹에 의한 정보 유출이 50% 이상을 차지하고, 웹, 이메일, 바이러스, 스키밍[10] 등에 의한 새로운 형태의 정보 유출도 꾸준히 발생하고 있음.

사이버 리스크는 정확한 정보 유출 위치 및 피해액을 파악하는 것이 힘든 경우가 많음.

10) 스키밍(skimming)이란 카드 소지자의 동의 없이 카드상의 정보를 몰래 전자적으로 복사하는 행위임.

- 전통적인 사이버 리스크는 일반대중을 목표로, 한 번 발생함으로써 그 발생을 쉽게 인식할 수 있었음.
- 최근 들어 사이버 리스크 관련 기술이 발달함에 따라 해킹, 바이러스, 직원의 고의 및 실수, 회사 파일 및 노트북의 분실 등 새롭고 다양한 방법에 의한 정보 유출이 발생함.
- 또한 다국적 기업 등에 의해 정보가 세계 각국에 산재하여 있어 어느 곳에서 정보가 유출됐는지 정확히 파악하기 어려운 경우가 많음.
- 사이버 리스크는 눈에 보이지 않는 손실이 대부분이므로 정확한 손실 금액을 산정하기 어려운 경우가 자주 발생함.

〈그림 2〉 정보 유출 대상(2013년)



자료: Symantec: Internet Security Report 2013.

〈표 1〉 정보 유출 경로 유형

(단위: %)

구분	비중	구분	비중
해킹	57	컴퓨터 도난	2
사기	9	이메일	2
컴퓨터 도난	5	바이러스	1
웹	5	드라이브 도난	1
폐기문서	3	드라이브 분실	1
서류 도난	3	스키밍	1
재래식 우편제도	2	문서 분실	2

자료: GUY CARPENTER.

■ 오늘날 기업환경의 특성상 사이버 리스크가 발생하기 쉽고, 한번 정보 유출이 되면 해당 기업에 심각한 타격을 주는 것으로 나타남.

- 기업들의 정보 · 기술에 대한 관심 및 상호 연결성이 증가하고 있으며, 기업들이 보유한 정보의 양도 방대해지고 있음.
- 따라서 양질의 개인정보를 가진 금융기관, 보험회사, 보건기관, 정부기관 그리고 대학 등의 교육기관이 주요 공격대상이 되어 개인정보 유출의 영향이 심각함.
- 정보 유출 후 기업은 중요 데이터 손실, 시장점유율 하락, 순이익 감소 그리고 온라인 기업의 경우 서비스 정지 시 고객 이탈 등 영업에 부정적인 영향을 받음.
  - 정보 유출 후 소비자의 71%는 해당 기업을 떠나는 것으로 나타남.

■ 보험회사의 입장에서 볼 때 사이버 리스크의 특징은 다음과 같이 요약될 수 있음.

- 사이버 리스크는 발생 빈도는 낮으나 발생 시 피해 규모가 큼.
- 사이버 상의 해킹 사고는 새로운 해킹 기술에 의하여 발생하는 경우가 많고 이전에 발생한 유례가 없는 형태의 사고 발생이 빈번하여 이러한 리스크를 평가하는 것이 어려움.
- 사이버 사고 관련 소송은 내용이 전문적이고 복잡하여 소송을 수행하고 관련 비용을 추정하는 것이 어려움.
- 사이버 리스크는 전산 시스템 보안 수준과 관리 인력의 교육 및 운영 체계 등에 의하여 발생하므로 보험계약자 간 사이버 리스크 관리 수준에 큰 편차가 존재함.

3. 국내외 CLI 시장 비교

〈규모 비교〉

■ 2013년 해외 CLI 시장의 보험료는 약 13억 달러 정도이며 40개의 보험회사에서 CLI를 판매하고 있음.

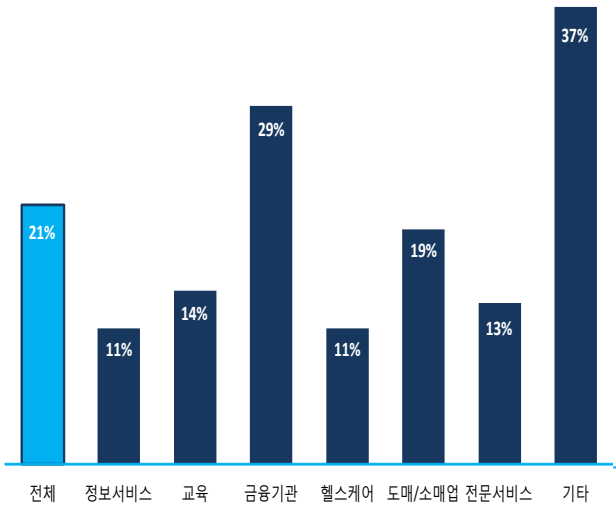
- 미국의 경우 2013년 현재 CLI가 손해보험시장의 약 2% 정도를 차지함.
  - 2013년 미국 손해보험산업의 총보험료는 7,260억[11] 달러임.

- CLI의 전형적인 담보액은 5백만 달러에서 2천5백만 달러임.
- 시장에서 상위 6개사(A사~H사)가 시장의 50%를 차지함.

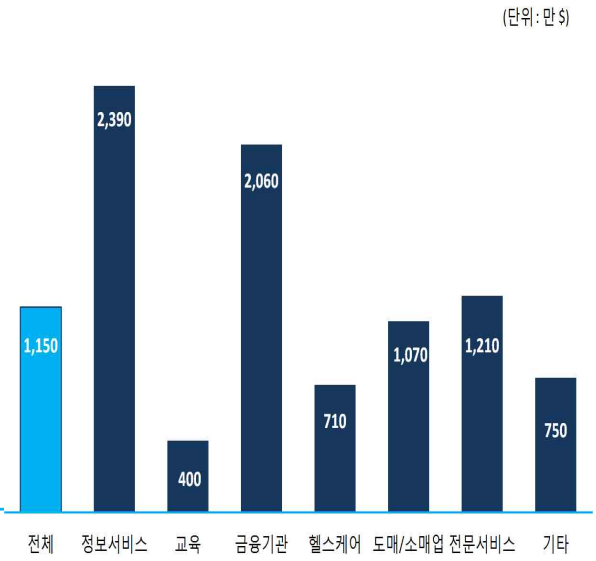
산업 전체에서 CLI 보험가입이 2012년 대비 2013년에 21% 증가하였으며, 2013년도 전체 산업이 구매한 CLI의 평균한도는 1,150만 달러임.

- 산업전반에서 전년도 대비 보험가입이 증가하였으며, 특히 금융기관의 증가가 두드러짐.
- 산업별 구매한도 평균은 정보서비스가 2,390만 달러로 가장 높았고, 금융기관이 2,060만 달러로 그 뒤를 이음.

〈그림 3〉 전년도 대비 산업별 보험구매 증가율(2013년)



〈그림 4〉 산업별 평균 구매 한도(2013년)



자료: GUY CARPENTER.

국내 CLI는 대부분 의무보험으로 전체 산업에서 차지하는 수준은 미미

- FY2010년 기준 CLI 보험료는 78.8억 원으로 손해보험 전체 보험료 51.4조 원의 0.015% 수준에 불과함.
  - 의무보험인 전자금융거래 배상책임보험 54.4억 원, 공인전자문서보관소 배상책임보험 1.8억 원이며, 임의보험인 개인정보 유출배상책임 4.3억 원, e-Biz 배상책임보험은 8.3억 원임.[12]

11) Swiss re, sigma(2014. 3).
12) 보험개발원(2012. 12), 『개인정보 유출 배상책임보험의 활성화 방안』, CEO Report.

- 2013년 53개의 금융회사가 납부한 전자금융거래 배상책임 보험료는 약 43억 원 수준임.

● 김소연 외(2014)[13]는 CLI 시장의 실적이 부진한 이유를 다음과 같이 진단하였음.

- 약관에 다양한 면책사유 포함, 법원의 친기업적 판결로 인한 손해 발생 사례 부족, 낮은 위자료 판결 액수 그리고 담보하는 리스크의 다양성 부족

〈표 2〉 금융회사별 개인정보 유출 배상책임보험 납입 현황

(단위: 억 원)

구분	은행* (9개사)	생명보험 (12개사)	손해보험 (15개사)	여신전문회사 (4개사)	증권사* (13개사)	합계
총납입액	12.39	5.72	9.99	2.19	12.61	42.90

주: 연간보험료 납입 현황으로 2013년에 납부한 보험료를 기준으로 하여 작성.
* 증권사의 경우 특약에 따른 보험료 상승분 계산이 시간상 어려운 회사 5개에 대해서는 전체보험료를 포함하여 계산함.
자료: 금융회사별 개인정보 유출 배상책임보험 납입 현황.[14]

〈표 3〉 금융회사 개인정보 유출 배상책임보험 가입 현황

구분	조사대상 수	가입 수	미가입 수
은행	17	9	8
생명보험	25	12	13
손해보험	15	15	0
여신전문회사	58	4	4
증권사	13	13	0
합계	78	53	25

자료: 금융회사별 개인정보 유출 배상책임보험 납입 현황.

〈담보 비교〉

■ 미국의 CLI는 손해배상금 및 소송관련 비용을 기본으로 컴퓨터 관련 직접적인 손해에 대해 다양한 담보를 제공하고 있으며, 외주업체 직원 제3자의 과실, 고의적인 유출까지도 담보하는 상품이 존재함.

● 우리나라의 개인정보 유출관련 보험은 제3자 보호를 위한 손해배상을 주 담보로 제공함(〈표 4〉와 〈표 5〉 참조).

13) 김소연 · 차윤주 · 김창기 · 최양호(2014), 『국내 사이버 위험과 사이버 보험에 관한 연구』, 보험학회 하계 학술대회.
14) http://kanggijung.com/bbs/board.php?bo_table=ok_05&wr_id=1061&page=2

〈표 4〉 한국, 미국, 일본 CLI의 담보 비교

국가별 CLI의 담보 내용			
특약의 내용	미국	일본	한국
데이터 재건, 대체 비용	O	O	O
개인정보 유출로 인한 손해배상 비용	O	O	O
네트워크 안전 확보 실패로 인한 손해배상 비용	O	O	O
도난당한 정보가 공적으로 노출되었을 때 손해배상 비용	O	O	O
해킹, 바이러스 관련 손해배상 비용	O	O	O
사이버 범죄 유죄 판결 시의 위자료 비용	O	O	O
기술적인 오류나 부주의로 일어난 손해배상 비용	O	O	O
도난당한 정보의 사용과 관련된 협박처리 비용	O		
정보 유출 시 그 정보의 소유자에게 고지하라는 법률 비용	O		
서비스 중단으로 인한 외부비용과 수입 감소분	O	O	
적절한 서비스를 제공했음에도 불구하고 생긴 외부 비용과 수입 감소분	O	O	
정보도난, 유출에 대한 위기관리 비용	O	O	
정보도난 처리 비용	O	O	
벌금	O		
기업평판 관련 비용	O		
사이버 공공기물 파손 시 처리 비용	O	O	
네트워크 파괴 및 침입 시 대처 비용	O	O	
유럽의 개인정보보호법과 관련된 비용	O		
포괄적인 접근에 대한 보호 비용(오프라인 매개체 포함)	O	O	
사이버 테러리즘에 대한 보상	O	O	
내부 직원에 의한 데이터 유출		O	
개인정보 위탁처의 사업자의 누설로 인한 피해보상 시 구상권[1] 불행사		O	
피보험자의 부주의, 실수로 인해 생긴 데이터 손실 보상		O	
클라우드 컴퓨팅 이용 기업을 대상으로 일반 사이버보험 보장 제공		O	

주: 1) 구상권: 보험회사가 보험계약자에게 발생한 손해배상책임을 보험금으로 대납하고 보험사고에 책임이 있는 제3자에게 보상을 청구할 수 있는 권리.

자료: 김소연 외(2014) 참조.

〈표 5〉 한국과 미국의 CLI 비교

<table>
<tr><th>구분</th><th colspan="3">국내 개인정보 유출관련 배상책임보험</th><th colspan="2">미국 CLI</th></tr>
<tr><td>대상</td><td colspan="3">– 금융기관 및 전자금융업자, 공인전자문서보관소, 온라인 쇼핑몰 등 고객정보를 다루는 업종 및 인터넷 개발업자</td><td colspan="2">– 컴퓨터 관련 직접적인 손해를 입을 수 있는 금융, 제조, 통신, 기술 등 다양한 기업</td></tr>
<tr><td rowspan="3">보상하는 손해</td><td rowspan="2">개인정보 유출</td><td>기본담보</td><td>– 제3자 보호를 위한 손해배상
– 법률 비용</td><td colspan="2" rowspan="3">– 보안 또는 개인정보 침해에 대한 손해배상
– 법률비용
– 정보 유출통지 비용 및 신용모니터링 비용 등과 같은 개인정보 침해 관련 비용
– 전자적으로 저장된 기업 자산의 복원, 업데이트, 교체와 관련된 비용
– 사업 중단 및 보안 또는 개인정보 침해와 관련된 추가 비용
– 웹사이트, 소셜 미디어 또는 인쇄 매체를 통한 타인의 명예훼손, 비방, 저작권 침해 등 평판 손상에 대한 손해배상
– 사이버 테러 연관 비용
– 결제오류, 응급의료치료를 위한 규제 준수 연관 비용
– 해킹, 바이러스 등 사이버 공격에 의한 사고뿐만 아니라 내부직원 또는 제3자의 과실, 태만, 고의적인 정보 유출로 인한 손해배상
– 기업 평판 회복 비용 등</td></tr>
<tr><td>선택담보</td><td>– 위기관리 컨설팅 회사가 제공하는 위기관리 서비스에 의해 발생한 비용
– 피보험자가 개인정보유출로 인한 위기 영향을 관리 및 최소화하려는 목적으로 부담한 비용
– 신용정보 누출로 인한 제3자의 경제적 손해배상
– 파견근로자가 파견지에서 행한 행위로 인한 배상청구 담보 등</td></tr>
<tr><td colspan="2">e – Biz</td><td>– 사이버 위험을 전문적으로 담보하여 인터넷 및 네트워크 활동으로 기인한 제3자 보호를 위한 손해배상
– 법률 비용</td></tr>
<tr><td rowspan="2">보상하지 않는 손해</td><td>개인정보 유출</td><td colspan="2">– 피보험자 보험자의 임원 또는 임원이었던 사람의 고의 또는 범죄행위에 기인한 손해배상청구
– 개인정보 이외의 정보누출로 기인한 손해배상청구</td><td rowspan="2">서비스 제공</td><td rowspan="2">– 사이버 리스크 관리차원에서 손실예방서비스 및 보안·정보 침해 후 이를 해결하기 위한 서비스 제공</td></tr>
<tr><td>e – Biz</td><td colspan="2">– 고의에 기인한 손해배상청구
– 예방조치를 하지 않은 바이러스 유포에 의한 손해배상청구</td></tr>
</table>

자료: 배병환 외 1인(2013. 7), 『국내 정보보호 보험시장 활성화 방안에 관한 정책제언』, Internet & Security, 수정 인용; NAIC, Cyber Risk, 2014. 1. 21.

〈제도 비교〉

■ 정보보호법의 역사는 25년이 되었지만, 정보보호법을 제정하고 개인정보유출통지를 의무화하는 것은 각국의 상황에 따라 다른 것으로 나타남.

● 미국의 47개 주(州)는 민간 또는 정부 기업이 개인정보유출이 되면 개인에게 통지해야 하는 법을 제정

– 연방정부는 은행, 신용조합, 보험, 건강정보를 취급하는 산업에 대해서 개인정보유출통지 요구

- 유럽은 정보보호지침(European Data Protection Directive)에 의해 국가마다 서로 다른 법이 시행되고 있으나, 대략 2016년에는 유럽연합 정보보호법에 의해 일원화될 것으로 기대됨.
  - 덴마크: 개인 또는 감독자에게 정보유출통지 의무가 없음.
  - 프랑스: 전자통신서비스 공급자에 한하여 개인정보유출통지 의무 존재
  - 독일: 정보의 종류 및 유출의 심각성 정도에 따라 개인정보유출을 통지해야 함.
  - 그리스: 전자통신서비스 공급자를 제외하고는 개인정보유출통지 의무가 없음.
  - 영국: 일반적으로 요구되지는 않으나, 금융서비스 및 공공기관은 정보유출통지가 요구되며, 공공전자통신서비스법이 존재
- 아시아도 일관된 법을 시행하지 않으며, 일부 국가에서는 정보보호법이 존재하지 않음.
  - 인도: 개인 및 감독자에게 정보유출을 통지할 필요 없음.
  - 일본: 법적인 의무 없으나 산업부분별 지침에 의해 요구될 수 있음.
  - 중국: 일반적인 정보보호법이 존재하지 않으나 일부산업은 감독당국에 정보유출을 알릴 의무가 존재함.

우리나라는 2011년 9월부터 개인정보보호법을 시행하여 개인정보유출사실 통지를 의무화하였으며, 최근 개인정보보호 정상화 대책 실행으로 사이버 리스크에 대한 기업들의 관심이 증가하고 있음.

- 개인정보보호법에 의해 개인정보 처리자는 개인정보가 유출되었음을 알게 되었을 때는 해당 정보주체에게 유출 항목, 시점과 그 경위 등을 지체 없이 통지해야 할 의무가 있음.
  - 동법의 적용 대상은 업무를 목적으로 개인정보파일을 운용하기 위하여 정보를 처리하는 공공기관, 법인, 단체 및 개인 등임.
- 국내법은 개인정보 유출 자체를 손해로 보지 않고 개인정보 유출로 인하여 손해가 발생하였다는 것을 피해자가 증명하여야 하고 대부분의 소송에서 대법원이 피해자의 위자료 청구를 기각하는 사례가 많아 개인정보 유출에 대하여 손해를 배상한 경우가 많지 않았음.
- 그러나 최근 들어 개인정보 유출 관련 집단 소송[15]과 징벌적 손해배상[16]을 도입하려는 움직임과 개인정보 유출 자체를 손해로 보아야 한다[17]는 여론이 조성되고 있어 사이버 리스크에 대한 기업들의 관심이 증가되고 있음.
  - 2014년 도입 예정인 “개인정보보호 정상화 대책”은 징벌적 · 법적 손해배상 강화, 범죄이익 몰

15) http://www.ytn.co.kr/_ln/0101_201401311059285507
16) http://biz.chosun.com/site/data/html_dir/2014/07/31/2014073102653.html
17) http://www.thebell.co.kr/front/news_print_free.asp?key=20140217010002603000158 4

수·추징, 주민등록번호 변경 허용 등의 내용을 포함하고 있음.

- 최근 서울 지방법원이 KT에 개인정보 유출에 대하여 손해배상 명령을 내린 것은 법원이 개인정보 유출에 대하여 강경한 입장을 보일 수 있다는 것을 보여줌.[18]
- 현재 이동통신사에만 적용되는 불법 텔레마케팅 신고제가 전 업종으로 확대될 것으로 예상되어 관련 과징금 부과 건수가 빠르게 증가할 것으로 보임.

4. 해외 보험회사의 CLI 운영 사례

〈알리안츠〉

■ 알리안츠는 CLI의 언더라이팅을 위하여 보험회사가 계약자의 사이버 리스크 관리 수준을 정확히 파악할 필요가 있다는 것에 착안하여 사이버 리스크 관리 컨설팅을 CLI와 함께 제공함.

● 알리안츠의 사이버 프로젝트는 아래와 같은 3개의 상품으로 구성됨.

- 표준: 다양한 담보를 포함하는 CLI
- 프리미엄: 표준 상품에 확장형 휴지보험[19]과 사이버 리스크 평가 컨설팅 제공
- 플러스: 외부 파트너가 참여하는 사이버 리스크 컨설팅과 맞춤형 사이버 리스크 관리 솔루션

〈그림 5〉 알리안츠의 사이버 리스크 평가 프로세스

자료: Allianz.

18) http://www.hankyung.com/news/app/newsview.php?aid=2014082281931
19) Business Interruption.

- 알리안츠 CLI의 담보는 다음과 같음.
  - 제3자 배상책임: 사생활 침해, 개인정보 침해, 네트워크 보안 문제에 따른 배상책임, 대중매체 비용, 정보유출 사실 통보 비용
  - 계약자: 휴지 보상, 복구 비용, 손해평가 비용, 해킹 손해 복구, 해커 협박 대응 비용
  - 규제관련 비용: 법률비용, 과징금 및 벌금

알리안츠는 표준화된 평가서를 이용하여 CLI 보험의 언더라이팅을 효율화함.

- 알리안츠는 1) 사이버 리스크 지속 경영, 2) 산업 표준 사이버 리스크 관리 시스템, 3) 관리 인력 평가, 4) 자료/보고체계/사이버 리스크 관리 방침, 5) 사이버 리스크 관리 소프트웨어, 6) 서버/저장소, 7) 네트워크, 8) 물리적 보호 체계의 8개 부분으로 나누어진 표준화된 평가서를 활용하여 계약자의 사이버 리스크를 평가하고 언더라이팅을 효율화하고 있음.

〈AIG〉

AIG는 사이버 리스크 관리 솔루션 CyberEdge를 이용하여 사이버 리스크 관리 서비스를 제공함.[20]

- CyberEdge의 기능은 다음과 같은 서비스를 제공하는 것임.
  - 계약자에 대한 사이버 리스크 노하우와 전문 지식
  - 솔루션을 통한 보험금 청구 및 정보 유출 사고 관련 자문
  - 과거 사이버 사고/범죄 사례, 사이버 리스크 관리를 위한 신기술, 해커와 핵티비스트 관련 정보, 관련 정부 발표 등의 정보
- CyberEdge 보험은 정보 유출로 인한 제3자 손해, 계약자에게 발생하는 손해, 휴업 손해, 사이버 갈취 손해, 명예 손실 및 저작권 침해 등을 담보함.
- CyberEdge 보험의 특징 중 하나는 사이버 사고에 의한 상해를 담보한다는 것임.[21]
- AIG는 RiskAnalytics, IBM 등의 기업들과 협력하여 리스크 관리 서비스를 제공

20) http://www.aig.com/CyberEdge_3171_417963.html, CyberEdge는 상품명으로도 사용됨.
21) http://www.ft.com/cms/s/0/07f85b78-cae5-11e3-9c6a-00144feabdc0.html#axzz3AAyAPgSH

〈그림 6〉 AIG의 CyberEdge 솔루션

5. 국내 보험회사의 대응 전략

■ 국내 보험회사는 장래에 시장 규모가 커질 것으로 예상되는 CLI 상품의 개발과 운영을 위하여 사이버 리스크 관련 전문 지식을 축적할 필요가 있음.

- 다양한 사이버 리스크를 가지고 있는 고객층을 확보하기 위해 다양한 담보를 포함한 CLI상품 개발
- 또한 손해보험회사는 CLI의 언더라이팅, 고객 지원 및 컨설팅, 손해배상 소송 지원 등을 위하여 다음과 같은 역량을 확보할 필요가 있음.
  - IT 시스템에 관한 전문 지식, 사이버 리스크 관련 손해배상 소송 수행 능력, 사이버 리스크 관리 체계에 대한 이해, 다양한 CLI 담보에 대한 평가 능력
- 특히 재보험회사들은 원수보험회사의 언더라이팅 역량을 기반으로 CLI의 재보험 수재 여부와 요율을 결정하므로 손해보험회사의 CLI 언더라이팅 능력은 CLI 보험의 재보험 요율에 영향을 미침.
  - 사이버 리스크는 대재해와 유사한 형태를 가지고 있어 재보험을 통한 리스크 전가가 CLI 보험 개발을 위하여 필수적임.

사이버 리스크 관리를 위한 리스크 평가 및 컨설팅 등 부수업무로 사업 영역 확대

- 외국의 유수 손해보험회사들은 CLI를 리스크 평가·관리 컨설팅, 관련 교육 등의 서비스와 함께 제공하는 전략을 통하여 사업 영역을 확장하고 매출을 증대시키고 있음.
- 국내 손해보험회사들도 이러한 사업 모델의 도입을 고려할 필요가 있음.

국내에 진출해 있는 외국 기업에 적극적인 CLI 마케팅 수행

- CLI의 특성상 국내에서 활동하는 외국 기업들은 소송에 대한 적절한 대비를 위하여 국내에서 CLI 상품을 구매해야하는 유인동기를 가지고 있으므로 손해보험회사들은 국내에 진출한 외국 기업들이 필요로 하는 CLI 상품을 개발하고 CLI 상품 판매를 촉진하는 전략을 고려할 필요가 있음.