KiRi Weekly
2014.2.10 제270호

포커스

개인정보유출 등 사이버리스크 관리의 중요성과 대응방안

"보호자 없는 병원" 시행의 고려사항

2013년 4월~11월 자동차보험 손해율 분석과 시사점

글로벌 이슈

2013년 중국 보험산업 현황 및 2014년 전망

EU 솔벤시 II 시행 일정 확정

금융시장 주요지표

KiRi 보험연구원
Korea Insurance Research Institute

서울시 영등포구 여의도동 35-4 8층 보험연구원(문의 : 김세환 부장 / 02-3775-9051)

KiRi Weekly 2014.2.10

포커스

개인정보유출 등 사이버리스크 관리의 중요성과 대응방안

김진억 수석담당역, 전용식 연구위원

요약

최근 발생한 카드사 정보유출 사건은 사이버리스크 관리의 실패사례로 볼 수 있는데, 기업 · 금융회사의 산업간 연계성이 커지고 리스크 복잡성이 심화되면서 사이버리스크관리 실패의 영향은 더욱 커질 것으로 전망됨. 그러나 기업 · 금융회사들의 사이버리스크에 대한 인식 부족으로 사이버리스크관리 시스템 구축은 미미한 것으로 보임. 반면 미국, 영국에서는 사이버리스크를 담보하는 보험상품(Cyber Liability Policy)이 확산되고 있으며 세계경제포럼은 2014년 1월, 사이버리스크에 대한 민관 공동대응 방안을 제시하였음. 세계경제포럼의 제안은 사이버리스크 발생을 억제하기 위한 징벌적 규제 강화는 사회적 혼란을 확산시킬 수 있기 때문에 사이버리스크 관리를 위한 정부와 민간의 공동 노력이 필요하고 사이버리스크를 분산시킬 수 있는 시장메커니즘 구축으로 요약할 수 있음. 향후 발생할 수 있는 기업 · 금융회사의 복잡한 리스크를 헤지할 수 있는 보험산업의 역량제고가 필요함.

기업이나 금융회사의 사이버리스크관리(Cyber Risk Management)의 중요성이 커지고 있음.

- 사이버리스크(Cyber Risk)란 사이버범죄(Cyber Crime)나 사이버테러(Cyber Terrorism)로 인한 유 · 무형의 발생 가능한 손실로서, 기업이나 금융회사가 보유하고 있는 개인의 신원, 금융 및 보험정보 등 민감한 자료의 유출(Breach), 도난(Theft), 그리고 이와 유사한 행위로 인한 정보의 손실(loss) 등을 예로 들 수 있음.
  - 영국의 컨설팅회사 마쉬(Marsh)는 영국의 연간 사이버범죄로 인한 경제적 손실이 210억 파운드에 이를 것이라는 연구결과를 인용
- Allianz가 최근 발간한 기업 리스크 관련 보고서에서 사이버리스크(Cyber risk)가 기업이 관리해야할 중요한 리스크로 부각되고 있다고 평가함.[1)]

1) Allianz SE(2014. 1. 14), "Allianz Risk Barometer on Business Risks 2014".

- 독일에서 발생한 1천 6백만 건의 이메일주소 및 비밀번호 도난사건, 미국의 신용카드 정보 4천만 건 도난 사건과 우리나라에서 발생한 1억 건의 신용카드 정보유출 사건 발생으로 사이버리스크에 대한 우려가 현실화됨.
- 사이버리스크에 대한 우려는 지역별로 아메리카(8위), 유럽(9위)보다 아시아 태평양 지역(6위)에서 가장 상승정도가 컸으며, 이는 아시아 태평양 지역에서 2014년 가장 주목받는 리스크가 될 것으로 평가됨.

〈표 1〉 2014년 기업리스크 인식 변화

구분	2014년 순위		2013년 순위	응답비율	% 변동	순위변동
1	영업중단(BI), 공급사슬	43%	1	46%	−3%	—
2	자연재해	33%	2	44%	−11%	—
3	화재, 폭발	24%	3	31%	−7%	—
4	입법 및 규제 변화	21%	4	17%	+4%	—
5	시장침체 또는 축소	19%	8	12%	+7%	↗(3)
6	평판, 브랜드가치 손실	15%	10	10%	+5%	↗(4)
7	경쟁심화	14%	5	17%	−3%	↘(2)
8	사이버범죄, IT실패	12%	15	6%	+6%	↗(7)
9	도난, 사기, 부패	10%	11	9%	+1%	↗(2)
10	품질결함, 순차결함	10%	6	13%	−3%	↘(4)
11	시장변동	8%	7	13%	−5%	↘(4)
12	긴축프로그램	7%	18	4%	+3%	↗(6)
13	상품가격상승	7%	14	7%	–	↗(1)
14	기술혁신	7%	13	8%	−1%	↘(1)
15	신용이용가능성	6%	12	9%	−3%	↘(3)
16	인재부족, 노령인력	6%	16	6%	–	—
17	공해	5%	20	3%	+2%	↗(3)
18	정치적/사회적 격변, 전쟁	4%	17	5%	−1%	↘(1)
19	정전(power blackouts)	3%	21	3%	–	↗(2)
20	건강 이슈, 유행병	3%	19	3%	–	↘(1)
21	유로존 붕괴	3%	9	12%	+9%	↘(12)
22	테러리즘	3%	24	2%	+1%	↗(2)
23	환경변화	3%	22	2%	+1%	↘(1)
24	인플레이션	2%	23	2%	–	↘(1)
25	보호주의	1%	25	1%	–	—
26	디플레이션	1%	26	0%	+1%	—

주: 수치는 총 응답자(557)중 응답비율임.

■ 기업과 금융회사가 직면하는 리스크가 복잡해지고 상호연관성이 증가하고 있어 사이버리스크 관리에 실패했을 경우, 상당한 사회적 손실을 피할 수 없으나 사이버리스크 관리는 점점 어려워지고 있는 것으로 평가됨.

- 최근 경제 · 사회적으로 큰 혼란을 일으켰던 신용카드회사의 대규모 정보유출과 뒤이은 고객의 혼란, 정책 및 감독당국의 혼란스러운 대응 조치는 사이버리스크, 규제리스크, 영업중단리스크, 평판리스크가 상호 연관되어 리스크가 복잡해지는 현상을 극명하게 보여줌.
- 기업이나 금융회사의 사이버리스크 피해에 대한 인식은 확산되고 있으나 사이버리스크의 특성을 파악하는 데는 시간이 더 필요한 것으로 보이고 규제환경은 개인정보보호 실패에 따른 징벌 강화 추세가 확산되고 있어 기업의 리스크관리 어려움이 가중되고 있음.
- 반면 미국의 전미보험감독자협의회(NAIC)는 사이버리스크 배상보험(Cyber Liability Policies)이 점차 확산되고 있다고 보도한 바 있어, 사이버리스크를 시장에 분산할 수 있는 메커니즘이 구축되고 있음을 보여줌.[2)]

2014년 1월 세계경제포럼(World Economic Forum)은 사이버리스크관리 역량 제고를 위한 로드맵을 발표[3)]하였는데, 사이버리스크를 효과적으로 관리하고 경제적 이익 모색 방안을 제시하고 있음.[4)]

- 기술혁신과 이를 통한 경제적 이익 창출을 위해서는 사이버리스크관리를 위한 민간 · 공공부문의 주요 기관이 협력할 수 있는 환경 조성이 필요함을 강조함.
  - 2020년까지 사이버범죄의 증가속도와 이에 대한 민간 및 공공부문의 대응속도에 따라 경제적 손실이 달라질 수 있는데, 최악의 경우 3.06조 달러에 이를 것으로 전망하였음.[5)]
- 사이버리스크관리 시스템 구축을 위한 각 기관, 부문별 대응 방안을 제시함(〈표 2〉참조).
  - 악의적인 사이버공격과 범죄를 저지하기 위해서 기업과 금융회사는 감사와 준법관리 위주로 구성된 리스크 관리시스템을 개선해야 함.
  - 최고경영자는 사이버리스크관리 프로그램을 전사적 리스크관리 시스템과 통합해야 하며, 기업 및 금융회사의 구성원 모두의 일상 업무가 사이버리스크와 관련이 있음을 주지시켜야 함.
  - 사이버리스크의 실체와 특성에 대한 이해가 부족한 상태에서의 과도한 규제와 법률제정은 사이버범죄 및 테러 발생 시 사회적 혼란을 가중시킬 우려가 있어, 민간과 정부가 참여하는 협의체를 통해 사이버리스크관리 관련 정책과 보험상품 개발 등 시장메커니즘을 조성해야 함.
  - 사이버공격의 위협을 줄이기 위해서는 정책당국과 기업 및 금융산업간 정보공유 협력과 노력이 긴요함.

2) NAIC(2014. 1. 21), "Cyber Risk".
3) WEF(2014. 1. 19), "Risk and Responsibility in a Hyperconnected World".
4) 전세계 민간 및 공공부문 대표들이 제시한 사이버리스크관리에 필요한 방안들임.
5) MGI disruptive technologies, social economy & Internet Matters reports, UNCTAD 직접투자, IMF global GDP, McKinsey Economic Platform, 산업별 인터뷰.

〈표 2〉 사이버리스크관리를 위한 부문별 역할

구분	행동분야		점검 권고사항
1	기업 및 금융기관의 대응 (Institutional readiness)	· 관리방식	· 사이버리스크 관리를 전사적 위험관리 프로세스에 통합 · 최고경영진이 직접 실무와 정책을 주도
		· 프로그램/네트워크 개발	· 정보자산의 중요도에 따른 차별적인 보호 · 정보보호기능의 확장 통합 · 사이버범죄, 테러에 대한 능동적 방어 기능 실시 · 임직원의 정보 자산 가치에 대한 이해도 제고
2	정부/국제 정책 (Public/international policy)	· 국가사이버전략	· 모든 정책 분야의 전략, 규정과 통합될 수 있는 포괄적이고 투명한 사이버 전략 수립 · 전략은 민간부문, 경제 및 안보 이슈를 통합해야 함
		· 사법전략	· 기관의 사이버범죄 조사와 기소 기능 마련, 법체계 수립 필요
		· 정책	· 규제 및 정책, 시장메커니즘 개발을 위한 민간과 공공부문간의 협의체 구축 및 활성화
		· 외교	· 국가적 차원의 사이버원칙 수립 · 지역, 정부, 그리고 국가적 차원의 사이버보안 전문인력 발굴 · 행정기관간의 공식/비공식적 의사소통채널 구축 · 사이버보안 담당 국가 기관간의 상호 운용체계를 구축 · 사이버범죄 기소와 관련한 국가 정책과 국제적 정책의 조화
		· 공동노력	· 사이버리스크 관련 기술 교육 투자 · 사이버리스크 관련 연구 및 조사에 대한 자금지원 · 기업과 정부간 제한된 정보공유에 대해 안식처 역할제공
3	지역사회 (Community)	· 연구	· 사이버리스크에 대한 교육과 인식 제고 · 사이버보안의 기업과 거시경제적 영향에 대한 연구 촉진
		· 자원공유	· 기술개발을 위한 정부, 대학 및 민간부문 간 파트너쉽 조성
		· 정보공유	· 정보공유를 위한 상호운영가능을 구축 · 사이버사건정보 공유를 위한 공동프로토콜 제공
4	금융 및 IT 시스템 (Systemic)	· 리스크시장	· 사이버리스크 보험시장 확대
		· 내재화된 보안	· 안전한 인터넷을 만들 수 있는 방법 연구 및 개발 · 사이버리스크의 영향을 계량화할 수 있는 방법론 개발

자료: 세계경제포럼(2014).

■ 전 세계적으로 확산되고 있는 사이버리스크에 대한 인식제고와 대응방안 모색은 사이버범죄를 방지하고 발생했을 경우, 이에 대한 성숙한 대응이 중요함을 시사하고 있음.

- 국가단위의 사이버범죄 관리 강화를 위해 정부, 공공기관, 민간기관 모두 각각의 입장에서 사이버리스크가 파생할 수 있는 상호연관성을 이해하고 성숙하고 바람직한 대응 및 극복 방안이 무엇인지 차분히 점검하고 대응하여야 함.
- 미국, 영국 등에서 확산되고 있는 사이버배상책임보험(Cyber Liability Policy)은 사이버리스크를 시장에 분산하는 역할을 할 것으로 보이는데, 이와 같은 혁신적인 보험상품을 개발할 수 있는 여건 조성이 시급함. KiRi