【 주간 포커스 】

금융회사의 디지털 리스크 관리

변혜원 연구위원

현대캐피탈의 정보유출과 농협의 전산망 장애 사건은 국내 금융회사의 디지털 리스크 관리에 대한 문제점을 부각시켰다. 아울러 기술정보 발달로 디지털 리스크에 대한 노출이 확대될 것으로 예측된다. 따라서 금융회사들은 디지털 리스크 관련 내부통제 강화, 정보기술 분야 관리 강화, 배상책임보험을 통한 리스크전가 방법을 활용할 필요가 있으며 이를 위해 개인정보보호 관련 제도의 개선 또한 필요할 것으로 판단된다.

□ 최근 현대캐피탈 해킹사건과 농협 전산망 장애 등 정보기술(IT)보안 관련 사건이 발생하면서 국내 금융회사의 디지털 리스크 관리 문제점이 드러나고 있음.

o 현대캐피탈 해킹사건은 사건 초기 42만명의 이름, 주민등록번호, 휴대전화번호가 유출된 것으로 알려졌으나 최근 추가로 132만명의 개인정보가 유출된 사실이 밝혀짐.

o 농협의 경우 지난 4월 12일 공격명령 프로그램 실행으로 인한 전산망 장애가 발생하였으며 4월 30일이 되어서야 전체 시스템을 복구

- 사건 기간 동안의 수수료 면제, 카드대금 결제 연기 등에 따른 피해액은 100억원 수준으로 추계됨.

o 이 밖에도 리딩투자증권 서버와 한국전자금융 홈페이지가 해킹되면서 개인정보가 유출되는 사건도 발생

o 금융위원회와 금융감독원은 40개 금융회사를 대상으로 정보기술 보안 실태 현장점검을 실시[1].

□ 디지털 리스크란 전자상거래 또는 정보기술을 매개로 하여 이루어지는 일반 영업이나 운영에서 발생할 수 있는 위험을 포괄하며 정보기술의 발달로 이러한 위험에 대한 노출은 더욱 확대될 것으로 예상됨.

1) 금융위원회, 「금융회사 IT 보안 강화 TF 추진계획」 2011.4.15.

o 디지털 리스크에는 자연재해로 인한 데이터 센터나 통신시설의 시스템 장애, 온라인 뱅킹 정보 강탈행위(사이버 범죄), 기업 또는 특정단체가 정보망을 통해 지적재산을 훔치는 행위 등이 포함됨.
- 이 밖에도 국가의 컴퓨터 기반시설에 침투하거나 혼란시키는 사이버 전쟁, 사이버 테러리즘 등도 이에 속함.

o 이러한 디지털 리스크는 기업의 운용 리스크(operational risk), 재무 리스크(financial risk), 지적재산 관련 리스크, 법률 및 규제 관련 리스크, 평판 리스크 등을 야기할 수 있음.

o 향후 디지털 정보량의 비약적 성장과 정보 활용 패턴의 변화, 클라우드 컴퓨팅[2] 등 컴퓨터를 이용한 사업이 증가하면서 디지털 리스크에 대한 노출은 확대될 것으로 예측되고 있음[3].

□ **현대캐피탈과 농협을 포함한 국내 금융회사들은 리스크위원회의 전문성 문제, 아웃소싱에 지나치게 의존한 정보기술 부문 등 디지털 리스크 관리에 문제를 갖고 있는 것으로 진단됨.**

o 금융회사 리스크관리위원회의 전문성 문제와 함께 독립성이 떨어져 사실상 그 역할을 하지 못하고 있어 리스크 가버넌스에 문제가 있음.
- 아울러 농협의 경우 전문성이 부족한 준법감시인이 내부통제 책임을 맡아 온 것으로 밝혀짐.

o 현대캐피탈의 경우 삭제하지 않았던 퇴직자의 ID 및 비밀번호를 통해 해킹이 이루어진 것으로 밝혀졌으며, 농협의 경우도 시스템 계정 비밀번호를 장기간 바꾸지 않거나 지나치게 단순한 번호를 사용

o 국내 금융기관들의 정보기술 분야는 대부분 아웃소싱의 형태로 관리되고 있으며 이들에 대한 적절한 리스크 관리가 이루어지지 않고 있음.

o 현재 국내에는 전자금융거래배상책임보험, 개인정보유출배상책임보험, e-biz배상책임보험 등 금융회사의 디지털 리스크 전가 상품이 있으나 담 낮거나 가입률이 매우 저조

□ **현재 국내 금융회사의 디지털 리스크 관련 보험상품 가입률이 저조한 원인은 배상금 지급사례가 드물다는 점과 배상을 받기 위해 피해여부를 소비자가 입증해야한다는 점에서 찾을 수 있음.**

2) 클라우드 컴퓨팅이란 인터넷 상의 서버에 데이터나 프로그램을 두고 필요에 따라 사용하는 웹기반 소프트웨어 서비스를 의미함.
3) Lloyd's(2010) "Managing Digital Risk," Lloyd's 360 Risk Insight.

o 전자금융거래법(제9조제4항)은 금융회사 또는 전자금융업자가 배상책임보험 또는 공제에 가입하거나 이에 준비금을 적립하도록 의무화되어 있으나 대비수준은 제한적

- 전자금융거래배상책임보험의 보험가입금액은 1~20억원 수준[4]이며 금융회사 대부분이 최저금액인 10억원 수준의 준비금을 적립하고 있음[5].

o 기존 판례 중 국내 기업이 개인정보 유출사고를 이유로 배상금을 지급한 사례는 드묾.

- 옥션의 2008년 회원정보 해킹건, 다음의 메일 서비스 장애에 의한 전자메일 유출건, GS칼텍스 고객 정보 유출건 등에 대해서 법원은 배상책임이 없다는 판결을 내림.
- 예외적으로 엔씨소프트의 게임이용자 개인정보 유출건에 대해서는 32명에게 1인당 10만원을 배상하도록 판결함.

o 배상책임보험은 피해자의 보험금 직접청구권이 인정되고 있으나 보험금을 받기 위해서는 가해자의 귀책사유와 손해와의 인과관계를 입증해야 함.

o 그러나 최근 제정된 「개인정보보호법」에서는 정보주체에게 정보유출사실을 통보하도록 되어 있어 배상청구가 용이해질 전망임[6].

□ 금융회사들은 고객의 개인정보와 거래정보가 유출되지 않도록 전사적 리스크 관리 체계를 재구축할 필요[7]

o 실무대책팀을 구성하여 디지털 리스크에 대한 노출에 대해 상시 점검하고 정기적으로 해당 위원회에 보고하도록 해야 함.

o 리스크 관리자는 정보기술 관리 및 전략, 주요 기술 변화에 더 깊이 관여해야 할 것임.

o 디지털 리스크 관리 전략의 하나로서 컴퓨터 관련 보험상품(cyber-insurance) 등과 같은 리스크 전가 상품을 고려해야 할 필요 KiRi

4) 은행권역의 보험가입금액은 10억원에서 20억원으로 차등화, 증권회사는 5억원, 보험 및 기타 금융기관은 1억원임(산업연구실, 「개인정보 유출리스크 증대에 따른 안전망 구축 필요성」, 보험연구원 주간이슈, 2010.12.13.).
5) 현대캐피탈도 10억원의 준비금만을 적립하였으며 배상책임보험에는 가입하지 않았음.
6) 「개인정보 보호법」 제34조(개인정보 유출 통지 등), 법률 제10465호, 2011. 3.29 제정, 2011.9.30 시행.
7) Lloyd's(2010)는 디지털리스크 관리에 대한 대응방안을 리스크 가버넌스, 리스크 완화, 리스크 전가 등의 측면에서 제시하고 있음.