
PROBABILITY
WEIGHT
LOW
HIGH

리스크의 계량화

사이버리스크 관리를 위해 금융업에서 배울 점은 무엇인가?

저자 JR Reagan, Ash Raghavan, Adam Thomas
일러스트레이션 Lucy Rose

금융업계가 자신들이 판매하는 금융상품의 리스크를 정교한 방식으로 관리한다는 사실은 익히 알려져 있다. 산업의 특성으로 인해 이는 불가피한 일이다: 양식 있는 고객이라면 대규모 손실을 방어할 준비가 돼있지 않은 금융기관을 통해 투자하지 않기 때문이다. 이런 방법들 중 가장 널리 알려진 것은 "대단히 복잡한 수학 모델을 사용해 다양한 포트폴리오들의 리스크를 측정하는 모델"을 사용하는 방법이다.[1] 이들 모델을 사용하면 회사는 리스크의 정도를 금액으로 측정할 수 있다. 즉 포트폴리오 관리자는 자신의 투자가 발생시키는 리스크를 효과적으로 계량화할 수 있다.

오늘날, 많은 조직들이 새로운 리스크의 영역—사이버리스크 관리—으로 진입하고 있는데, 이 영역은 금융산업에서의 재무리스크 관리와 비슷한 특성이 많다. 이 두 분야 간의 비교가 처음에는 생경하게 느껴질 수 있지만, 실제로 한 분야에서의 경험이 다른 분야에도 값진 교훈이 될 수 있는 많은 유사점이 있다. 이들 유사점은 다음과 같다.

- **복잡성:** 수년 간 금융업계는 복잡한 금융상품을 이용해 왔는데, 이들 상품에는 서로 이질적인 요소들의 상호작용에 의해 발생하는 리스크가 존재한다. 오늘날의 사이버보안의 관점에서 보자면, 복잡한 컴퓨터 시스템 아키텍처의 사용, 클라우드 컴퓨팅의 도입, 개인 장비를 사용하는(Bring-Your-Own-Device, BYOD) IT 모델, 모바일 통신, 그리고 기타 다양한 디지털 기술의 발전으로 인해 기업들은 더 많은 리스크를 발생시키고 있다. 고도로 복잡한 금융상품에서처럼 리스크 요소들 간의 복잡한 상호작용으로 인해 관련 리스크를 파악하고 평가하기가 어려워지고 있다. 리스크 모델과 기타 정량적인 지표들, 정성적인 자료 출처들이 위험을 미리 경고해 주지만, 현대 금융산업 및 사이버리스크 분야의 경영진이 이들 경보를 항상 확실히 이해할 수 있는 것은 아니다.

- **리스크 관리 모델의 사용:** 금융기관들은 다양한 리스크 모델을 사용하고 있으며, 이 중 오랜 기간을 거쳐 자리를 잡은 모델도 있고 비교적 최근에 개발된 모델도 있다. 오늘날 사이버리스크를 측정하기 위해 계량모델을 적용하려는 일부 선도적인 리스크 관리자들은 금융기관과 동일한 유형의 모델들을 사용한다. 여기서 문제는 최고경영진이나 이사회가 이들 모델의 복잡성과 한계를 간과할 수 있다는 점이다. 이들 모델의 결과물이 단순한 경우가 많은데, 즉 헤아리기 쉬운 숫자 하나로 된 결과값만을 도출하곤 한다. 이로 인해 모델의 입력값이나 분석 과정의 복잡성이 드러나지 않을 수 있다. 따라서 경영진은 특정한 환경 하에서 모델의 유효성을 주의 깊게 따져보지 않고, 모델이 우수하며 완전하다고 생각하는 우를 범할 수 있다.

- **시스템 리스크의 가능성:** 금융산업은 한 금융회사의 붕괴가 그 회사의 경계를 넘어 전체 산업 그리고 궁극적으로 국가 경제의 다른 부문에까지 영향을 미칠 수 있다는 점을 꾸준히 인지해 왔다. 마찬가지로 오늘날 사이버리스크는 기업, 정부, 사회를 포함한 전체 생태계를 위협할 가능성이 있다.

물론, 공공부문의 관리자들 및 많은 민간 산업부문의 경영자들이 사이버리스크에 대해 잘 인식하고 있다. 전 세계의 사이버보안 관련 지출이 증가하고 있는데, 지출 규모가 2015년 754억 달러에서 2020년까지 1,700억 달러로 늘어날 전망이다.[2] 그러나 많은 사람들이 이들 리스크의 범위를 결정하고, 어떻게 적절히 리스크와 보상간의 균형을 유지할 것인지에 대해 고심 중이다.

사이버리스크를 계량화하고 사이버보안에 대한 투자수익을 계산하려는 이러한 욕구가, 사이버리스크에도 숫자를 적용하려는 노력의 정도를 금융회사가 재무리스크의 계량화를 중시하는 것과 맞먹는 정도로 강화하고 있다. 투자사, 은행, 보험사의 경영진은 자신들이 때로는 상당한 리스크를 감내하며, 그 리스크를 측정하고 의사결정에 참고하기 위해 리스크 모델로부터 산출된 숫자를 이용하길 원한다는 점을 이해하고 있다. 그러나, 때로는 손에 닿을 듯한 커다란 이익의 가능성 때문에 경영진이 그 모델의 산출값을 무시하거나, 적어도 그 숫자가 진정으로 의미하는 바를 완전히 이해하지 못하고 당연시하는 경우도 있다.[3]

이와 유사하게, 오늘날의 경영진은 신기술의 활용과 투자를 통해 얻을 수 있는 막대한 수익을 요구하는 거센 목소리에 직면하고 있다. 또한 경영진은 복잡한 정보시스템과 네트워크를 지속적으로 확장함으로써 리스크를 크게 증가시키고 있다는 점도 인지하고 있다. 그 결과 사이버리스크를 측정하고 사이버리스크 전략 및 보안 프로그램의 개발과 실행을 지원하는 리스크 모델의 개발에 관심을 보이고 있다.

그렇다면, 어떠한 유형의 모델이 사용되고 있으며, 이는

어떤 맥락에서 사용되고 있는가? 이들 모델에 너무 의존하거나 다른 사이버리스크의 지표를 무시해서 경영진이 부지불식 간에 사이버 사고의 대재앙에 처할 위험은 없는가?

분명, 리스크 모델은 리스크 요소를 규정하고 이해하기 위해 중요한 틀이다. 하지만 경영진과 CISO(정보보안 최고책임자)는 사이버리스크를 계량화할 때 금융기관의 리스크 관리 경험을 이해하여 이득을 볼 수 있다. 조직은 오로지 리스크 모델에만 의존하는 것을 경계해야 하며, 대신 이 모델에 대한 강력한 통제절차를 마련해야 한다. 강력한 절차가 없다면, 경영진은 자신들의 사이버리스크에 대한 준비태세를 과신하거나 조기경보 신호를 감지하지 못해 잠재적인 재무적, 영업적, 평판적인 손실을 볼 수도 있다.

돌발 변수(블랙스완 이벤트)의 리스크

다양한 유형의 리스크들이 재무적 투자의 가치와 성과에 영향을 미칠 수 있는데, 이는 일반적으로 신용, 유동성, 시장, 운영리스크로 분류된다. 밸류 앳 리스크(Value at risk) 혹은 바(VaR)로 불리는 지표는 금융기관에서 사용하는 모델 중 가장 유명한 것으로 투자 포트폴리오의 시장리스크를 측정하는 데 수십 년 간 사용되어 왔다. VaR는 "한 회사 또는 투자 포트폴리오 내에서 특정 기간 동안 발생할 수 있는 재무리스크의 수준을 측정하고 계량화하는 통계적 기법"이다.[4]

가장 일반적인 유형을 들자면, VaR는 "정상적인" 시장상황 하에서 단기간의 포트폴리오 리스크를 측정한다. 예를 들어 한 투자관리자가 관리하는 포트폴리오의 1주일 VaR가 1억 달러로 산출되었다면 이는 다음 1주일 동안 그 포트폴리오에서 발생하는 손실이 1억 달러보다 작을 확률이 99%라는 것을 의미한다.[5] 그러나, 일반적으로 VaR는 1%의 확률로 발생하는 1억 달러 이상의 손실이 얼마나 클지 그 규모를 알려주지 못한다. 따라서 VaR는 연쇄적인 주택 담보의 압류나 서브프라임 모기지 손실과 같이 발생 가능성은 매우 낮으나 영향력은 엄청난 "돌발 변수(블랙스완 이벤트)"를 측정할 수 없다는 한계를 지닌다.[6]

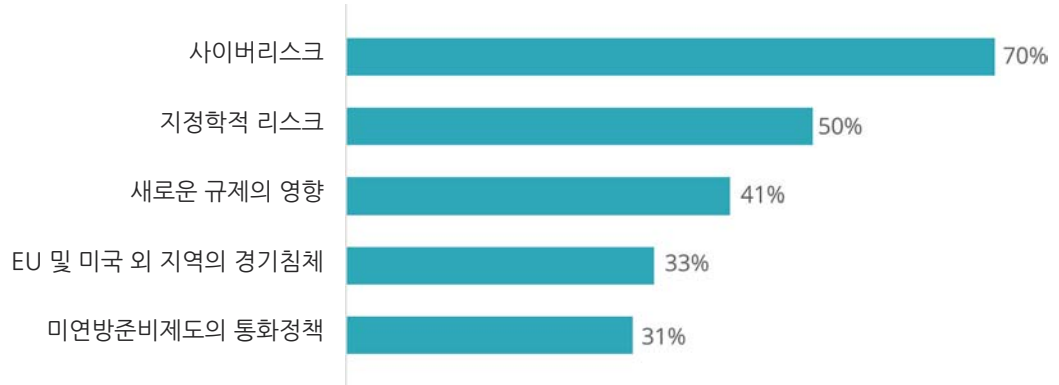
핵심 요약 VaR와 같은 리스크 모델은 광범위한 입력값을 통합하고 의사결정자의 추론에 참조할 지표를 제공하는 중요한 기능을 수행한다. 그러나 입력값의 품질에 따라 결과의 품질이 좌우되고, 모든 리스크를 계량화할 수 없는 선천적 한계를 지닌다.

사이버리스크에 대한 우려 증가와 사이버리스크 계량화의 추진

이쯤에서 사이버 돌발 변수(블랙스완 이벤트)에 대한 공공 및 민간 부문의 우려와 사이버리스크의 계량화에서 새롭게 떠오르는 "사이버 VaR" 모델의 역할을 이해하는 것이 중요하다.

전 세계의 공무원들은 전 세계적인 위협을 가하는 사이버

그림 1. 국제 금융시스템에 대한 5대 리스크



출처: 디포지터리 트러스트 & 클리어링 코퍼레이션(The Depository Trust & Clearing Corporation), 시스템적 리스크 지표 설문조사, 2015.12.01

그래픽: Deloitte University Press | DUPress.com

리스크에 대해 점점 더 우려하고 있고, 일부는 시스템적인 재앙으로 확대될 수 있는 사이버 사건의 가능성에 대해 경고하고 있다. 일례로, 국제증권감독기구(International Organization of Securities Commissions)의 전 이사회 의장인 그렉 메드크래프트(Greg Medcraft)는 "다음 번의 큰 금융 위기—혹은 돌발 변수(블랙스완 이벤트)—는 사이버 공간에서 기인할 것이며, 금융계에 대한 일련의 공격 후에 발생할 것"이라고 말했다.[7]

기업의 리스크관리자들 또한 사이버 돌발 변수(블랙스완 이벤트)를 걱정하고 있다. 미국 증권예탁결제원(Depository Trust & Clearing Corporation)의 2015년 연구에 따르면, 설문조사에 참여한 금융기관 리스크관리자의 61%가 국제 금융시스템에 큰 영향을 미칠 사건이 발생할 가능성이 최근 6개월 간 증가해 왔다고 답변했다. 2015년 1분기에 실시한 지난 조사에서와 동일하게 사이버리스크는 전 세계적인 관심사항 1위의 자리를 유지했는데, 응답자의 70%가 사이버리스크를 5대 리스크 중 하나로 꼽았다(그림 1). 응답자들은 공격의 빈도와 이에 대한 대응 능력이 가장 걱정되는 점이라고 답변했다.[8]

분명, 사이버위협은 금융업계와 국제 금융시스템에만 국한된 문제는 아니다. 다른 분야에서도 사이버 돌발 변수(블랙스완 이벤트)가 발생할 가능성은 엄연한 현실이다:

- **공공 산업.** 2015년 12월 발생한 사이버 공격으로 우크라이나의 전력망이 부분적으로 마비되자, 오바마 행정부는 미국의 전력회사, 수도 공급회사, 교통 운송망에 대해 유사한 공격에 주의하도록 경보를 발령했다.[9]
- **의료산업.** 북미 지역에서 2015년과 2016년에 지속된 의료시설 및 병원에 대한 사이버 공격 이후, 미국의 국토안보부(US Department of Homeland Security)는 캐나다 사이버 사고대응 센터(Canadian Cyber Incident Response Centre)와 함께 의료기관에 대해 "민감 혹은 독점 정보의 일시적 혹은 영구적 손실, 일상 업무의 중단, 재무적 손실"과 평판의 손상을 초래할 수 있는 랜섬웨어 및 기타 변종에 대한 경보를 발령했다.[10]
- **석유 및 가스.** 2015년 말 가스, 에너지, 유틸리티 산업의 IT 전문가를 대상으로 한 설문조사에서 응답자의

3/4이 성공적인 사이버 공격이 증가하고 있음을 경험했으며, 다수의 응답자(68%)가 성공적 사이버 공격의 비율이 지난 달에만 20% 증가했다고 답했다.[11]

- **정부.** 2014-2015년에 발생한 미 인사국(US Office of Personnel Management)의 대량 정보유출 사건으로 인해 직원 및 계약상대방 신원조회 데이터베이스의 2,150만 명의 사회보장번호를 포함한 민감 정보가 도난 당했다.[12]

체계화된 사이버위협이 증가하는 트렌드에 대응하기 위해 정부 및 이해관계자들은 대국적인 견지에서 어떤 행동을 취하고 있는가?

주요 추진계획 중 하나는 스위스 다보스에서 매년 개최되는 세계경제포럼(World Economic Forum)이 2011년 발표한 다자간 "사이버 탄력성 강화를 위한 협력(Partnering for Cyber Resilience)"이다. 100명 이상의 전문가, 사업가, 정책입안자들이 참여한 이 프로젝트의 목표는 "사람, 프로세스, 인프라에 대한 디지털 연결의 증가에서 발생하는 글로벌한 시스템 리스크에 대처하자"는 것이다.[13]

우선은 사이버 탄력성에 대한 최고경영진들의 인식 강화에 초점을 맞춘 이후, 회원들은 2014년과 2015년에 "다양한 산업과 영역에 걸쳐 공유된 사이버 탄력성 보증 벤치마크(Cyber resilience assurance benchmark)"의 필요성에 관심을 돌렸다.[14] 성공적인 리스크 계량 모델을 만들기 위해, 그들은 자신의 조직에서 사용되고 있는 다양한 유형의 모델을 목록화하는 데서부터 시작했다. 몬테카를로 시뮬레이션 방법론이 주로 사용되었으나 다음과 같은 다른 모델의 요소들 또한 중요하게 여겨졌다.

- 행동 모델링(Behavioral modeling)
- 파라메트릭 모델링(Parametric modeling)
- 베이스라인 보호(Baseline protection)
- 델파이 기법(Delphi method)
- 인증(Certifications)

이러한 연구 끝에 "금융산업에서 널리 쓰이고 있는 VaR의 개념에 기반한" 사이버 VaR의 틀을 마련하게 되었다.[15] 사이버 VaR 모델은 확률적인 방법을 사용해 조직이 특정 기간 동안 사이버 공격으로 인해 입을 수 있는 손실을 추정한다. 다시 말해, "성공적인 사이버 공격이 있을 때, 회사는 일정 기간 동안 95%의 정확성으로 X 달러를 초과하는 손실을 입지 않을 것"을 의미한다.[16]

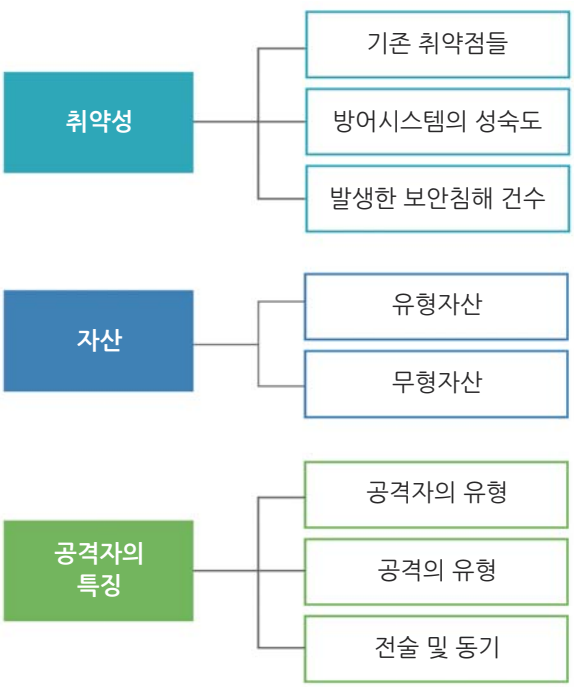
"사이버 탄력성 강화를 위한 협력" 추진계획은 재무적인 VaR 모델에 기반한 측정법을 개발하기로 한 결정에 대해 "금융산업은 과거 30년 간 정교한 계량 모델을 사용해 왔고, 정확하고 신뢰성 있는 리스크 계량 추정치를 만드는 데 있어 많은 경험을 쌓아왔다. 사이버 탄력성의 계량화에 있어, 관계자들이 사이버 위협 측정치에 대한 인식과 신뢰도를 높이기 위해 이러한 접근법들에서 교훈을 얻고 이를 적용해야 한다"고 설명했다.[17]

세계경제포럼의 관계자들은 하나의 특정한 사이버 VaR 모델을 개발하려 하지는 않았다. 대신, 사이버 VaR 프레임워크의 특정한 속성들을 제안해서, 각 산업 및 개별 기업들이 자신들의 필요에 맞춰 자체 모델에 반영하도록 했다. 이러한 방식으로 각 조직은 구성요소들의 적용가능성과 자신의 환경에 미치는 영향을 결정하기 위해 구성요소들을 평가할 수 있다. 사이버 VaR 프레임워크는 다음의 광범위한 구성요소들로 구성된다.(그림 2)

- 기존 자산과 시스템의 취약성과 방어 시스템의 성숙도
- 위협 대상이 되는 유무형의 자산
- 유형(예. 국가의 지원을 받는 전문가 vs 아마추어, 정교함의 수준), 전술 및 동기와 같은 공격자의 특징

확률 변수(공격의 빈도, 일반적인 보안 트렌드, 조직의 보안 시스템 성숙도와 같은 "확률에 따라 바뀔 수 있는" 변수)를 일부 포함하고 있는 사이버 VaR의 구성요소들이 확률적 모델에 입력된다. 이 모델은 일정 기간에 대해 하나 혹은 그 이상의 확률변수를 포함하고 있는 확률분포를 추정하기 위한 통계적 도구다. 구성요소들 간의 상관관계 분석은 리스크 익스포져를 추정하기 위한 다양한 모델에 사용될 수 있다.

그림 2. 사이버 VaR의 구성요소들



출처: 세계경제포럼, 사이버 탄력성 강화를 위한 협력: 사이버 위협의 계량화를 향해서(Partnering for cyber resilience: Towards the quantification of cyber threats), 2015년 1월

그래픽: Deloitte University Press | DUPress.com

리스크 계량 모델은 사이버리스크 관리가 한 단계 진화했음을 보여준다. 그러나, 사이버보안의 영역을 고려할 때, 리스크 모델—특히 VaR—의 일반적 활용은 다음의 중요한 질문을 제기한다. 사이버 VaR 모델이 이의 도입을 선택한 조직에게 근본적인 리스크를 일으킬 수 있을까?

핵심 요약 사이버위협이 극도로 복잡해지고 범위가 지속적으로 확대되면서, 금융기관들이 1990년대부터 2000년대 초반 사이에 급성장한 복잡한 파생금융상품에 내재된 시장리스크를 계량화할 방법을 찾았었던 것처럼, 조직들은 사이버리스크를 계량화하려는 계획을 추진하게 된다.

(사려 깊은) 리스크 모델 활용의 중요성

위에서 제기된 문제에 대한 답은 조직이 어떤 맥락에서 사이버 VaR를 채택했는지에 크게 달려 있다. 우리는 이제 VaR 모델을 활용하는 3가지 상이한 접근법이 어떻게 서로 다른 3가지 결과를 도출했는지를 살펴볼 것이다.

VaR 모델의 한계는 1990년대부터 익히 알려져 왔는데, 아마도 그 중 가장 유명한 것은 1998년도의 롱텀캐피털 매니지먼트(Long Term Capital Management, LTCM)의 붕괴일 것이다.

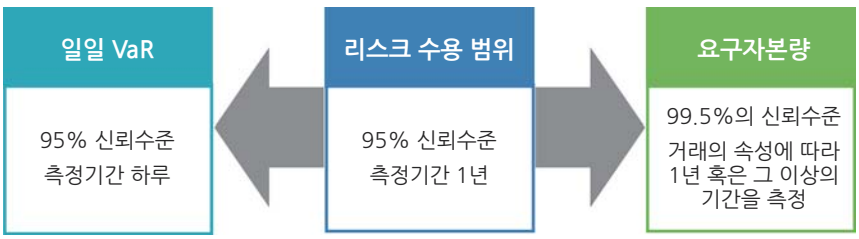
> LTCM의 붕괴로 인해, VaR 모델의 한계와 미래 예측에 있어 역사적 확률 사용의 부적절함이 드러났다. 러시아는 (해외 채무보다는) 국내 채무 상환에 실패했는데, 이는 전례가 없는 일이라 LTCM의 VaR 모델은 이 사건의 발생 확률을 0으로 추정했고 손실을 정확히 계산하지 못했다. 그 결과, LTCM은 유동성 위기에 빠졌고 최종적으로 은행 및 금융기관들이 구성한 민간 협력단의 구제금융을 받게 되었다.[18]

그림 3. 대표적인 리스크관리 통합 체계

리스크 수용 범위(Risk appetite): 리스크에 대한 접근법의 핵심

리스크 수용 범위란 기업이 1년 동안 시장, 사건, 거래상대방 신용리스크로부터 발생하는 "감내할 수 있는 손실" 총량을 의미한다. 이는 95% 신뢰수준에서 정의되고 측정된다.

신뢰수준 및 측정기간



그래픽: Deloitte University Press | DUPress.com

바로 이렇게 잘 알려진 VaR의 한계에도 불구하고, 이 모델은 금융업계에서 여전히 인기가 있고 널리 사용되고 있다. VaR를 변형시킨 서로 다른 모델들을 기업들이 사용하고 있지만, 일반적으로 기업의 공식적인 리스크 측정법은 그림 3에서 볼 수 있듯 95% 신뢰수준의 일일 VaR다.

VaR 값에 대한 자유방임주의적 태도가 가져오는 결과는, 이사회의 지지하에 공격적인 투자를 실행해 온 X기업이라는 한 회사의 경험을 통해 볼 수 있다. 리스크관리부서에서 발송한 이메일을 보면 이 회사의 최고경영진은 리스크관리자를 무시하고 리스크 한도와 관련된 정책들을 따르지 않았음을 알 수 있다. 게다가, 경영진들은 이사회에 보고하지 않고 일부 위험한 자기자본 투자를 스트레스테스트에서 누락했으며, 유동성이 떨어지는 대규모 투자의 증가에서 발생할 수 있는 치명적 손실의 규모를 분석하는 정기적이고 시스템화된 수단을 갖추지 못했다. 결국, X기업은 천문학적인 손실을 입고 파산해 버렸다.

X기업이 파산한 이후 수년간의 교훈은 기업의 거버넌스(Governance)와 리스크관리에 대한 다양한 접근법의 가치를 일깨워준다. 이는 Y기업이라고 하는 또 다른 대형 금융기관의 이야기를 통해 살펴볼 수 있다.

이 이야기는 손익 수치를 살펴보던 Y기업의 경영진들이 모기지 사업부가 10일 연속 손실을 기록했음을 발견하면서 시작된다. 이러한 추세를 면밀히 살펴본 경영진과 리스크관리자는 왜 이런 일이 발생하고 있는지 더 깊이 파헤쳐 보기로 했다. 그들은 데이터를 철저히 조사했고, 함께 회사의 트레이딩 포지션을 조사해 보기로 결정한다.

강력한 재무적 거버넌스 체계가 갖춰져 있던 Y기업은 다양한 정량적 리스크 측정 모델을 사용했으나 그 중 어떤 것도 손익계산서보다 더 큰 중요성을 갖지 않게 했다. 경영진은 어떤 한 가지 계산값이나 입력치에만 전적으로 의존하지 않도록 주의를 기울였다. 모든 가용한 증거를 정기적으로 저울질하고, 전문가적인 판단을 활용해 Y기업의 경영진은 모기지담보증권(Mortgage backed security) 포지션을 줄이고 위험을 헷지(Hedge)해야 한다는 사실을 깨달음으로써 재난을 피해갈 수 있었다.

LTCM과 X기업, Y기업의 사례를 어떻게 사이버리스크 계량화와 연관 지을 수 있을까? 한 보고서는 이사회의 사이

"사이버 탄력성 강화를 위한 협력"의 결과물 중 하나는 참여자들이 "실시간에 가까운 정보 공유로 데이터 가용성 문제를 해결하고 통계적 모델을 구축하는 데 충분한 데이터를 제공하는" 접근법을 고안하기 위해 협력하는 것이다.

버리스크 감독 부족을 지적하면서, 이사회가 예산, 평가, 정책, 역할과 책임, 보안침해, 정보기술 리스크 등 보안 관련 이슈에 대해서 충분한 주의를 기울이고 있지 않다고 결론지었다.[19]

한 글로벌 대형 은행의 집행위원회 위원인 호세 마뉴엘 곤잘레스-파라모(José Manuel González-Páramo)는 리스크 모델에 과도하게 의존하는 행태에 대한 우려를 해결할 리스크 체계가 필요함을 논하면서, "역사적으로 모델과 외부 의견을 과도하게 의존하고 기계적으로 사용해 왔다……이들 모델, 측정값, 의견들은 여전히 유효한 도구이지만 올바른 방식으로 사용되어야 하며, 다른 도구, 더 일반적으로 말해, 전문가의 판단에 의해 보완되어야 한다"고 말했다.[20]

이러한 맥락에서 보면 사이버리스크를 측정하기 위해 사이버 VaR나 다른 모델들을 효과적으로 사용하려면 금융기관들이 종종 직면하는 것과 유사한 도전과제들을 다뤄야 하는 데 그 중에는 데이터의 품질과 같은 해묵은 문제도 있다. 대다수의 사이버 사고들이 알려지지 않기 때문에, 공격 빈도와 같이 사이버리스크 모델에 사용되는 일부 기본 데이터는 구하기 어려울 수 있다.[21] 게다가, 사이버 공격의 확률을 모델화하는 데 필요한 광범위한 데이터 집합은 아직도 개발단계에 있다. "사이버 탄력성 강화를 위한 협력"의 결과물 중 하나는 참여자들이 "실시간에 가까운 정보 공유로 데이터 가용성 문제를 해결하고 통계적 모델을 구축하는 데 충분한 데이터를 제공하는"[22] 접근법을 고안하기 위해 협력하는 것이다. 이러한 사업은, 그들 자신의 내부 데이터를 더 잘 이해하고 특성화하려는 개별 기업의 노력—예를 들어, 기업 자산과 회사의 매출 및 이익간의 관계 계량화—과 함께 사이버 VaR 및 기타 사이버 리스크 계량 모델의 효과를 높이기 위해 필수적이다.

그 외의 도전과제들은 조직의 속성에 보다 가까운 문제인데, 운영 상의 단절 지속, 의사소통의 부족, 부적절한 거버넌스 등이 있다. 이 중 부적절한 거버넌스는 리스크 모델에 대한 과도한 의존과 더불어 보안에 대한 근거 없는 자신감을 키우는 아마도 가장 큰 잠재요인이다.

핵심 결론 사이버리스크의 증가는 조직들이 리스크 모델 사용을 고려하도록 강제하고 있다. VaR와 같은 리스크 모델이 제공할 수 있는 가치 있는 정보는 기타 입력값들과 함께 고려되어야 한다. 사이버리스크 관리 활동을 주의 깊게 구조화하고 관리하기 위해 조직은 특정 변수가 과도한 영향력을 가지지 않게 막아야 한다.

사이버리스크 관리에서 모델 사용의 관리

"사이버 탄력성 강화를 위한 협력"에서 강조한 사이버 VaR 모델의 바람직한 속성은 이 모델이 경영진과 의사결정자를 위한 효과적인 리스크 측정 도구로서 사용될 수 있다는 것이다. 이러한 역할을 충족하기 위해 중요한 점 하나는 기업의 기존 전사적 리스크관리 체계에서 제공하는 관점을 통해 이 모델을 바라봐야 한다는 점이다. COSO(Committee of Sponsoring Organizations of the Treadway Commis-

sion)에서 개발한 내부통제 통합 체계(Internal Control Integrated Framework)나 전사적 리스크관리 통합 체계(Enterprise Risk Management Integrated Framework) 등이 그러한 체계다.[23] 상위 수준에서의 내부통제 구성요소들은 일반적으로 아래와 같다.

- 이사회에 의해 감독되는 통제 환경
- 운영, 보고, 컴플라이언스 목표 및 이들에 대한 사이버리스크의 잠재적 영향을 고려한 리스크 평가
- 조직의 리스크 한도(Risk tolerance) 내에서 특히 사이버리스크 관리를 목표로 한 통제 활동
- 일반적인 사이버리스크와 특정 사이버리스크 사건과 관련된 정보 및 커뮤니케이션 관리
- 사이버리스크를 다루는 내부통제의 효과성을 평가하는 모니터링 활동[24]

이러한 관점을 통해 사이버 VaR를 바라봄으로써 이사회와 고위경영진은 확고한 태도로 사업 목표, 중요 정보 시스템에 대한 정의, 관련된 사이버리스크에 대한 리스크 수용 범위를 효과적으로 소통할 수 있다. 그 결과, 이사회와 고위경영진의 지도는 엄정한 사이버리스크 분석에 대한 전사적 기조를 설정하고 기대수준을 확립시킨다.

"사이버 탄력성 강화를 위한 협력"은 사이버 VaR를 폭넓은 전사적 리스크관리 체계에 포함시킴으로써 "고위경영진의 지속적이고 사전적인 참여"[25]가 이뤄져 기업의 사이버보안 프로그램이 강화될 수 있다고 주장한다. 아일랜드 중앙은행의 금융규제 담당 부총재인 시릴 루(Cyril Roux)는 2015년 한 연설에서 사이버보안과 관련해 금융회사들에 대한 중앙은행의 기대를 약술하면서 경영진의 참여

가 중요함을 강조했다. 시릴 루가 설명한 아래의 주제들은 사이버 침입을 탐지, 예방, 복구하는 능력을 강화하고자 하는 모든 산업의 기업들에게 도움되는 가이드를 제시한다.

- **이사회는 주요 리스크에 대해 잘 이해하고 있어야 한다.** 이는 이사회 임원들이 보안 전략에 대해 최고 경영진에게 효과적으로 이의를 제기하는 데 도움을 줄 것이다.
- **리스크 평가와 침입 테스트를 수행하라.** 조직들은 주기적으로 사이버보안 리스크 평가를 수행해야 한다.
- **공격 성공에 대비하라.** 조직들은 분산 아키텍처, 다중 방어망, 고객에 대한 영향을 완화하기 위한 준비를 통해 탄력성을 갖춰야 한다.
- **아웃소싱 리스크를 관리하라.** 조직들은 현재 및 장래의 외부 서비스 제공자에 대한 사이버보안 실사를 수행해야 하며 아웃소싱 계약 내에 사이버보안 및 데이터보호 조항을 포함시켜야 한다.

- **정보를 수집하고 주요 선례를 따르라.** 조직들은 영업의 규모와 속성에 맞게 자신들의 사이버보안 리스크 관리 체계에 산업 표준을 적용해야 하며 산업 내 정보 공유 모임에 참여해야 한다.

- **직원을 교육하라.** 조직들은 전 직원을 대상으로 한 주기적인 보안 인식 교육을 통해 "인적 요소"를 관리해야 한다.

- **강력한 IT 정책, 절차 및 기술적 통제를 갖추라.** 여기에는 사고 보고 및 대응 계획, 복구 및 업무 연속성 계획, 패치 관리, 직원 접근권한이 포함된다.

- **사이버 보험 가입을 검토하라.** 조직들은 부분적인 리스크 경감 전략으로써 사이버 보험의 사용 가능성을 평가하고 검토할 수 있다.[26]

위의 목록 중 첫 번째 주제는 매우 중요하다. 이사회와 고위 경영진은 모든 리스크 입력값을 중요하게 분석하고 평가하도록 서로에게 도전해야 한다. 이사회의 리스크 감독에 대한 주요 사항은 다음과 같다.

- 이사회와 고위 경영진 간의 커뮤니케이션

- 이사회, 하부 위원회, 자문역 내의 커뮤니케이션

- 필수 인원만 참여하는 명확한 리스크관리 프로세스를 통한 효율적 협업

- 발생 가능한 리스크 시나리오에 대해 리스크관리팀과 토론하고 분석하여 예상 못한 것을 예측하기[27]

이 네 가지 요소 중 마지막은 리스크관리팀이 다양한 리스크 시나리오를 검토할 때 이사회가 적극적으로 참여할 기회를 가져야 함을 지적한다. 이 접근법을 통해 이사회는 리스크관리팀이 리스크관리 프로세스 상에서 효과적인 행동을 취하고 있는지를 이해하고, 개선이 필요한 분야를 인식하게 한다.

어떤 이사회는 리스크관리에 대한 감독의 책임을 감사위원회에 부여하기도 한다. 또는 독자적인 사이버리스크 감독 위원회를 설립하여 사이버리스크 관리의 책임을 맡은 전사 임원들을 주기적으로 직접 참여시키는 것을 검토할 수도 있다.

사이버리스크에 대해 이사회와 고위 경영진을 교육하는 것은 사이버 위협에 대응하는 이사들의 역할을 강화시키는 데 있어 매우 중요하다. 전미 기업 이사 협회(National Association of Corporate Directors, NACD)[28]에서 발간한 "사이버리스크 감독 핸드북(The cyber-risk oversight handbook)"이나 뉴욕증권거래소 거버넌스 서비스(NYSE Governance Services)의 "사이버리스크 관리하기: 기업들은 자산을 안전하게 보호하고 있는가?(Managing cyber risk: Are companies safeguarding their assets?)"[29] 와 같은 자료들은 매우 유용하게 사용될 수 있다.

주요 시사점 이사회와 고위 경영진은 조직의 사이버보안 태세를 모니터링하고, 사이버보안 전략의 실행을 감독하며, 사이버보안 활동에 대한 투자자, 애널리스트, 규제당국의 질의에 답변을 준비할 책임이 있으며 이 책임은 더 커지고 있다. 사이버 VaR와 기타 리스크 입력값은 이러한 책임을 완수하는 데 있어 중요한 역할을 수행한다.

과거로부터 배우고 미래를 준비하라

경영진은 사이버리스크를 계량화하는 것이 사이버리스크의 잠재적인 결과를 이해하고 디지털 자산을 보호하기 위해 자원을 배분하는

데 있어 필수적이라는 사실을 점점 더 크게 인식하고 있다. 우리가 살펴본 것처럼 재무리스크를 다루건 사이버리스크를 다루건 간에 리스크 모델은 위협을 관리하는 데 중요한 역할을 수행한다. 모델은 데이터의 패턴 및 추세의 인식과 평가에 도움을 주며, 건전한 통제구조 프로세스, 가용한 리스크 데이터, 숙련된 사이버보안 및 분석 전문가와 함께 리스크 계량화 과정에서 중요한 요소다.

동시에, 다른 고려사항은 무시하거나 부차적인 것으로 여기며 모델에 과도하게 의지하는 것은 파멸적인 결과를 향해 한걸음을 내딛는 것과 마찬가지이다. 대신, 특정 사업의 본질과 조화를 이룬 제대로 정의된 사이버리스크 모델을 개발하는 것이 중요하다.[30] 기업들은 리스크 모델에서 산출된 결과물을 이해하기 쉬운 개념으로 해석하여 각 계층의 경영진과 이사회에서 솔직한 리스크 VS 보상에 관한 대화를 시작하는 데 사용할 수 있다. 그 개념은 이해관계자들이 사이버리스크와 관련된 위험과 잠재적 기회의 양면을 사업의 혁신과 성장이라는 맥락에서 이해할 수 있게 돕는다. 특정 모델에 입력할 수 있는 경험적 데이터가 부족하다는 점을 고려한다면, 이 개념을 전달할 때 모델의 정확성에 대한 그릇된 인식을 심어주지 않도록 하는 것이 중요하다.

사이버 위협 환경에 모델을 적용할 때, 모델의 역할과 중요성을 맥락 내에 유지함으로써 기업과 감독당국은 리스크 인텔리전스(Risk intelligence)를 강화하고, 투자자와 고객의 이익을 위해 관리를 개선할 수 있다. **DR**

JR 리건(JR Reagan)*은 딜로이트 투쉬 토마츠 유한회사의 글로벌 정보보안 최고 책임자이다.*

애쉬 라그하반(Ash Raghavan)*은 딜로이트 투쉬 LLP의 사이버리스크 서비스 사업부의 프린시펄이며 딜로이트 리스크 센터 오브 엑설런스의 글로벌 리더다.*

아담 토마스(Adam Thomas)*는 딜로이트 투쉬 LLP의 사이버리스크 서비스 사업부의 프린시펄이며 사이버 보험이 전문 분야다.*

Endnotes

1. Joe Nocera, "Risk mismanagement," *New York Times Magazine*, January 2, 2009, http://www.nytimes.com/2009/01/04/magazine/04risk-t.html?_r=1.
2. Mike Billings, "The daily startup: Increased spending in cybersecurity drives funding surge," *Wall Street Journal*, February 17, 2016, http://blogs.wsj.com/venturecapital/2016/02/17/the-daily-startup-increased-spending-in-cybersecurity-drives-funding-surge/.
3. Research shows that risk tolerance changes with context. For example, stock market investors are more likely to be tolerant of larger risks when the market is high than when it is low. This may seem like common sense, but it helps to frame why some executives do not heed the risk models that they themselves implement. For more information, see Yao et al., "Changes in financial risk tolerance, 1983–2001," *Financial Services Review* 13, no. 4 (2004): pp. 249–266.
4. Investopedia, "Value at risk—VaR," http://www.investopedia.com/terms/v/var.asp#ixzz436g0659c, accessed May 6, 2016.
5. Nocera, "Risk mismanagement."
6. "Black swan" is a metaphor coined by risk analyst Nassim Nicholas Taleb to describe highly improbable events with outsized impact, in his book, *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets*, Incerto series, book one (New York: Random House Trade Paperbacks, 2005, 2nd edition).
7. Sam Fleming, "Market watchdog warns on danger of cyber attack," *Financial Times*, August 24, 2014, https://next.ft.com/content/82519604-2b8f-11e4-a03c-00144feabdc0.
8. Depository Trust & Clearing Corporation, "Over 60 percent of risk managers at financial services firms believe probability of a high-impact event has increased, according to new DTCC survey," December 1, 2015, http://www.dtcc.com/news/2015/december/01/financial-services-firms-believe-probability-of-a-high-impact-event-has-increased.
9. David Sanger, "Utilities cautioned about potential for a cyberattack after Ukraine's," *New York Times*, February 29, 2016, http://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyber-attack-after-ukraines.html?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=0.
10. US Computer Emergency Readiness Team, "Alert (TA16-091A) ransomware and recent variants," March 31, 2016, https://www.us-cert.gov/ncas/alerts/TA16-091A.
11. Barbara Vergetis Lundin, "Oblivious in energy: Cyber attacks more successful than ever," SmartGridNews.com, April 8, 2016, http://www.smartgridnews.com/story/oblivious-energy-cyber-attacks-more-successful-ever/2016-04-08.
12. US Office of Personnel Management, "Cybersecurity Resource Center: Cybersecurity incidents," https://www.opm.gov/cybersecurity/cybersecurity-incidents/, accessed April 8, 2016.
13. World Economic Forum, *Partnering for cyber resilience towards the quantification of cyber threats*, January 2015, http://www.weforum.org/reports/partnering-cyber-resilience-towards-quantification-cyber-threats.
14. Ibid.
15. Ibid, p. 12.
16. Ibid.
17. Ibid.
18. Amy Poster and Elizabeth Southworth, "Lessons not learned: The role of operational risk in rogue trading," *Risk Professional*, June 2012.
19. Jody Westby, "How boards and senior executives are managing cyber risks," Carnegie Mellon University CyLab, May 16, 2012, http://www.hsgac.senate.gov/download/carnegie-mellon-cylab-cybersecurity-report.
20. José Manuel González-Páramo, "Rethinking risk management: From lessons learned to taking action," Risk and Return South Africa Conference, March 4, 2011, https://www.ecb.europa.eu/press/key/date/2011/html/sp110304_1.en.html.
21. Center for Strategic and International Studies and McAfee, *Net losses: Estimating the global cost of cybercrime*, June 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.
22. World Economic Forum, *Partnering for cyber resilience*, p. 15.
23. COSO, "Guidance on internal control," http://www.coso.org/ic.htm, accessed May 6, 2016.
24. Mary Galligan and Kelly Rau, *COSO in the cyber age*, Committee of Sponsoring Organizations of the Treadway Commission and Deloitte, January 2015, p. 3, http://www.coso.org/documents/coso%20in%20the%20cyber%20age_full_r11.pdf.
25. World Economic Forum, *Partnering for cyber resilience*, p. 15.

26. Cyril Roux, "Cybersecurity and cyber risk," address to Society of Actuaries in Ireland Risk Management Conference, Dublin, September 30, 2015, http://www.bis.org/review/r151002d.htm.

27. David A. Katz, *Boards play a leading role in risk management oversight*, Harvard Law School Forum on Corporate Governance and Financial Regulation, October 8, 2009, https://corpgov.law.harvard.edu/2009/10/08/boards-play-a-leading-role-in-risk-management-oversight/.

28. National Association of Corporate Directors, *Cyber-risk oversight handbook*, June 10, 2014, https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=10688.

29. NYSE Governance Services, *Managing cyber risk: Are companies safeguarding their assets?*, https://www.nyse.com/publicdocs/nyse/listing/NYSE_Governance_Services_Managing_Cyber_Risk.pdf, accessed May 6, 2016.

30. One example of a tailored approach to quantifying cyber risk is provided in "The hidden costs of an IP breach" elsewhere in this issue of *Deloitte Review*, in which the authors demonstrate a scenario-based method for anticipating the impact of a particular type of cyberattack an organization could experience. See Emily Mossburg, J. Donald Fancher, and John Gelinne, "The hidden costs of an IP breach: Cyber theft and the loss of intellectual property," *Deloitte Review* 19, July 2016, http://dupress.com/articles/loss-of-intellectual-property-ip-breach.