KiRi 리포트 2018.1.15.
이슈 분석

사이버위험에 대한 인식과 사이버보험

임준 연구위원

요약

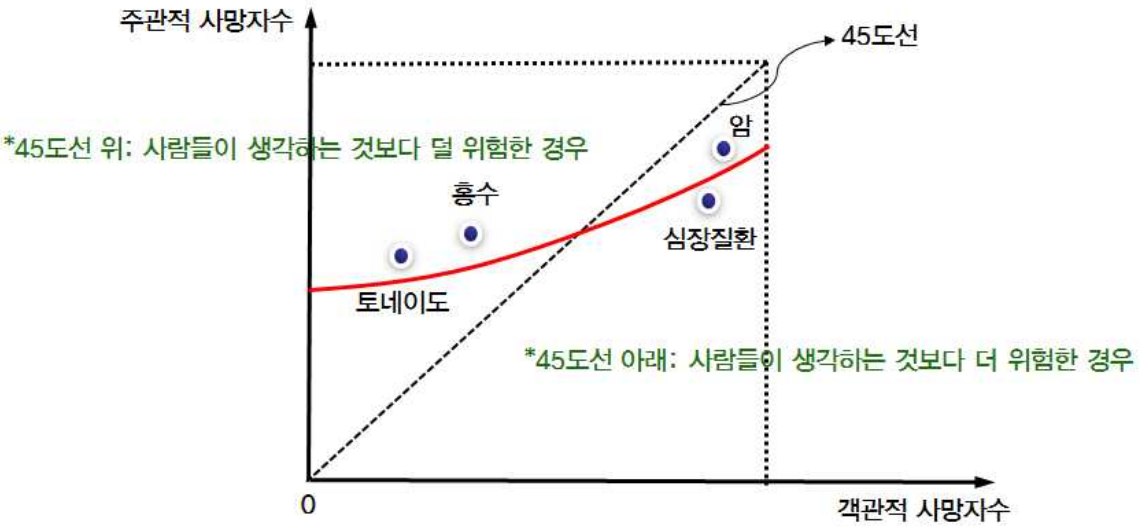
Smidt and Botzen(2017)은 네덜란드 기업을 대상으로 사이버위험의 인식에 대한 서베이 조사를 실시하였음. 조사 결과에 의하면, 대부분 자신의 조직이 사이버공격의 대상 가운데 하나이겠지만 우선적인 공격 대상은 아니라고 생각하는 'not-in-my-organization' 경향이 존재하였음. 그리고 사이버공격의 발생빈도와 관련해서는 과대평가하는 경향이 존재한 반면, 피해규모와 관련해서는 과소평가하는 경향이 존재하였음. 조사대상 기업 가운데 소수만이 사이버보험에 가입하고 있었는데, 저자들은 낮은 사이버보험 가입률이 피해규모에 대한 과소평가와 관련성이 있을 것으로 보았음. 국내에서도 사이버보험 활성화와 관련하여 사이버위험의 주관적 인식에 대한 연구와 잘못된 위험인식을 바로 잡을 수 있는 방안에 대한 연구가 필요하다고 여겨짐

위험에 대해 적절한 준비를 하기 위해서는 위험에 대한 정확한 인지가 선행되어야 하는데, 일반적으로 실제 위험(actual risk)과 개인이 인식하는 위험(perceived risk) 간에 차이가 존재함

- 아래 〈그림 1〉의 실선은 약 40여 개 위험의[1] 객관적 사망자 수와 주관적 사망자 수 간의 관계를 나타내는데, 발생빈도가 낮은 위험의 경우에는 위험이 과대평가되는 경향이 존재하는 반면, 발생빈도가 높은 위험의 경우에는 위험이 과소평가되는 경향이 존재함[2]
  - 예를 들어, 토네이도와 홍수의 경우에는 실제 사망자 수보다 개인들이 인식하고 있는 사망자 수가 더 많아 위험을 과대평가하는 경향이 있음
  - 반면, 암이나 심장질환 등의 경우에는 실제 사망자 수보다 개인들이 인식하고 있는 사망자 수가 더 적어 위험을 과소평가하는 경향이 있음

1) 그림에서는 편의상 홍수, 토네이도, 암, 심장질환 등의 4개 위험만 표시하였음. 이외에도 40여 개의 위험에 포함된 다른 예로는 자동차사고, 살인 등이 있음
2) Viscusi, W, et al.(2005), *Economics of Regulation and Antitrust*, The MIT Press

〈그림 1〉 객관적 사망자 수와 주관적 사망자 수



주: 객관적 사망자 수와 주관적 사망자 수는 1년 단위임
자료: Fischoff, B. et al.(1981), *Acceptable Risk*, Cambridge University Press; Viscusi, W, et al.(2005), *Economics of Regulation and Antitrust*, The MIT Press에서 재인용

■ 사이버위험의 경우에도 실제 위험과 주관적 위험 사이에는 차이가 존재할 것이라고 많은 사람들이 예상은 했지만 실증자료를 통해 보여준 경우는 거의 없었는데, 최근 주목할 만한 연구논문이 발표되었음

■ Smidt and Botzen(2017)은[3] 네덜란드의 일정규모 이상의 기업을 대상으로 사이버위험의 인식에 대한 서베이 조사를 2016년에 수행하였음

- 모두 1,891명에게 이메일을 통해 설문을 보냈으며, 그 가운데 172명이 응답하였음

■ 주요 연구결과 몇 가지를 소개하면, 첫째, 응답자 가운데 약 84%가 자신의 조직이 사이버공격의 대상이 될 가능성이 있다고 응답하였으나, 자신의 조직이 매력적인 공격 대상이라고 응답한 경우는 60.6%였음

- 대부분 자신의 조직이 사이버공격의 대상 가운데 하나이겠지만 우선적인 공격 대상은 아니라고 생

3) Smidt, G, and W.J. Wouter Botzen(2017), "Perceptions of Corporate Cyber Risks and Insurance Decision-Making", Working Paper # 2017-18, Risk Management and Decision Processes Center, The Wharton School, University of Pennsylvania

각하는 경향이 존재하였음[4]

둘째, 사이버공격의 발생 빈도와 관련해서는 과대평가하는 경향이 존재하였음

- 몇 년에 한 번 사이버공격이 발생할 것으로 예상하느냐는 질문에 응답자의 약 75%가 5년에 한 번에서부터 25년에 한 번 사이의 구간에 포함되었음
- Smidt and Botzen(2017)은 객관적 발생 빈도의 추정치로 샘플의 평균치인 약 18년에 한 번을 사용하여, 많은 응답자가 사이버공격의 발생 빈도를 과대평가하고 있다고 주장하였음
  - 그러나 샘플의 평균치를 객관적 발생 빈도의 추정치로 가정한 것에 대한 설득력 있는 논거를 제시하지 못하고 있어서 이 주장의 타당성은 다소 떨어짐

셋째, 피해규모와 관련해서는 과소평가하는 경향이 존재하였음

- 응답자의 약 67.2%가 피해규모가 100만 유로 이하일 것으로 응답하였는데, 저자들이 피해규모의 객관적 추정치를 얻기 위해 참조한 Ponemon(2016)의[5] 연구에 의하면, 평균 피해액 규모가 약 400만 유로 정도 되었음
- 조사대상 기업 가운데 약 18%만이 사이버보험에 가입하고 있었는데, 저자들은 낮은 사이버보험 가입률이 피해규모에 대한 과소평가와 관련성이 있을 것으로 보았음

국내에서도 사이버보험 활성화와 관련하여 사이버위험의 주관적 인식에 대한 연구와 잘못된 위험인식을 바로 잡을 수 있는 방안에 대한 연구가 필요하다고 여겨짐 KiRi

4) 이러한 경향을 'not-in-my-organization' effect라고 함
5) Ponemon Institute(2016), "2016 Cost of Data Breach Study", Ponemon Institute Research Report; 정보유출 경험이 있는 기업을 대상으로 피해규모 산정