



중소기업 사이버보험 시장 활성화 방안

임준 연구위원

중소기업은 사이버위험관리 역량 측면에서 대기업과 상당한 차이가 있기 때문에 사이버보험 시장 활성화 전략 수립 시 대기업과는 차별적인 접근이 필요함. 첫째, 중소기업의 사이버위험 및 사이버보험에 대한 낮은 이해도 제고를 위해 보험산업 차원에서 사이버보안 가이드라인, 사이버보험 상품 소개, 사이버 사고 발생 시 대처 요령 등을 담은 홍보책자를 발간하여 배포함. 둘째, 중소기업 시장의 경우에는 보험회사의 역할이 단순히 사이버보험만 판매하는데 그치지 않고 사이버위험관리 자문도 함께 제공함. 셋째, 현재 시행되고 있는 중소기업 대상 사이버보안 바우처 지원을 확대하는 방안을 검토함

- 중소기업은 사이버위험관리 역량 측면에서 대기업과 상당한 차이가 있기 때문에 사이버보험 시장 활성화 전략 수립에 있어서 대기업과는 차별적인 접근법이 필요함¹⁾

- 본고에서는 해외사례를 참고하여 중소기업 사이버보험 시장 활성화 방안을 제시하고자 함

- 먼저, 대기업과 중소기업의 사이버위험 준비도(Cyber Risk Readiness)를 살펴보면, <표 1>에서 보듯이 대기업과 중소기업 간에 상당한 차이를 보임

- 대기업의 경우에는 사이버위험 관련 내부조직의 구축이나 외부기관과의 파트너십 등에 있어서 중간 이상의 준비도를 보이고 있음
 - 사이버위험 관련 교육이나 문화 측면은 대기업의 경우도 아직 준비도가 높지 않음
- 반면, 중소기업은 거의 모든 영역에서 매우 낮은 수준의 준비도를 보이고 있음
 - 사이버위험 및 사이버보험에 대한 이해도가 낮고, 내부적으로 사이버위험관리 조직을 별도로 조직하기 어려울 뿐만 아니라 외부 컨설팅 업체와의 파트너십도 약한 편임

1) Michael Siegel, Nadya Bartol, Juan Jose Carrascosa Pulido, Stuart Mandick, Michael Coden, Mohammad Jalali, and Michael Bernaski(2018), "Cyber Insurance as a Risk Mitigation Strategy", The Geneva Association

〈표 1〉 기업규모별 사이버위험 준비도

구분	대기업	중소기업
사이버위험 교육(예: 사이버위험 이해 및 대비 계획 수립)	●	○
사이버위험 관련 기업문화	●	○
사이버위험 관련 내부조직(예: Chief Risk Officer)	●	○
IT 시스템 관련 외부 파트너	●	●
사이버위험 컨설팅 파트너	●	○
사이버보험	●	○

주: ●는 준비도가 매우 높음을, ●는 준비도가 중간 정도임을, 그리고 ○는 준비도가 매우 낮음을 의미함

자료: Michael Siegel et al.(2018), "Cyber Insurance as a Risk Mitigation Strategy", The Geneva Association

■ 국내외 실증 자료를 통해 중소기업의 사이버위험 및 사이버보험에 대한 인식 수준을 좀 더 자세히 살펴보면, 우선 호주 사례²⁾ 경우 중소기업이 자신들의 위험관리 능력을 과신하는 경향이 있었음

- 조사 대상 기업 가운데 약 87%가 사이버 사고 발생 시 대처 능력이 있다고 답하였으나, 약 67%의 기업이 자신이 어떤 사이버위험에 직면하고 있는지 잘 모르고 있어서, 주관적인 인식과 객관적인 위험관리 능력 사이에 괴리가 존재하였음
- 사이버보험의 경우에도 조사 대상 기업 가운데 약 62%의 기업이 보험에 가입하지 않았으며, 약 59%의 기업이 보험상품에 대해 잘 모르고 있었음

■ 국내 중소기업을 대상으로 사이버보험에 대한 인식 수준을 조사한 설문 결과³⁾ 의하면, 조사 대상 기업 가운데 약 68%의 기업이 사이버보험에 대해 잘 모른다고 답변하였음

- 단지 약 28%의 기업만이 사이버보험에 대해 잘 알고 있다고 답변하였음

■ 중소기업의 사이버위험 및 사이버보험에 대한 낮은 인식 수준을 제고하기 위해, 주요국에서는 보험협회 중심으로 홍보책자(Brochure)를 제작해서 배포하고 있음

- 프랑스 보험협회는 중소기업과 영세업체를 대상으로 사이버보안 가이드라인, 사이버보험 상품, 사이버 피해 사고 발생 시 대처 방안 등의 내용을 담은 소책자⁴⁾를 발간하였음

2) Chubb(2019), "Too Small To Fail?: Australia SME Cyber Preparedness Report"

3) 한국침해사고대응팀협의회(2017), 『지능정보사회 대비 사이버보험 활성화 방안 연구』, 방송통신정책연구 17-방통-24, 과학기술정보통신부·정보통신기술진흥센터

4) Fédération Française de l'Assurance, "Anticiper et Minimiser l'Impact d'un Cyber Risque sur Votre

- 영국의 보험협회도 중소기업을 위하여 사이버보험 상품의 주요 보장 담보와 보장 대상에서 제외되는 담보를 정리한 소책자를⁵⁾ 발간하였음
- 일부 국가에서는 보험협회 산하의 위험관리 전문기관의 업무 영역을 사이버위험까지 확대하여, 사이버 보안 표준화 및 중소기업의 사이버위험관리 능력 제고를 위해 노력하고 있음
 - 예를 들어, 독일의 경우에는 보험협회 산하 위험관리 전문기관인 VDS(Vertrauen Durch Sicherheit)가 중소기업을 위한 사이버 보안 가이드라인 및 표준을 제정하였음⁶⁾
 - VDS의 위험관리 업무 영역은 화재뿐만 아니라 환경 및 사이버위험 등을 포괄하고 있음
 - 프랑스의 경우에도 보험회사들이 설립한 위험관리 전문기관인 CNPP(Centre National de Prévention et de Protection)가 2018년에 사이버위험을 담당하는 부서를 신설하였음⁷⁾
- 한편, 스코틀랜드의 경우에는 중소기업의 사이버보안 능력 제고를 위해 바우처(Voucher) 제도인 “Cyber Essentials Voucher Scheme”을 시행하고 있음
 - 종업원 규모가 250명 이하인 중소기업의 경우, 정부로부터 1,000파운드 한도 내에서 사이버 보안 인증 획득에 필요한 비용을 지원 받을 수 있음
- 해외 사례를 참고하여, 국내 중소기업 사이버보험 시장 활성화 방안을 몇 가지 제시하면, 우선 중소기업의 사이버 위험 및 사이버보험에 대한 인식 제고를 위한 홍보책자를 발간할 필요가 있음
 - 홍보책자에 담을 내용으로는 사이버 보안 가이드라인, 사이버보험 상품 소개, 사이버 사고 발생 시 대처 요령 등을 우선적으로 생각해볼 수 있음
 - 사이버보험 상품 소개의 경우에는 주로 보장하는 담보와 보장 대상에서 제외되는 담보 등을 정리해서 책자에 담음
- 둘째, 중소기업 시장의 경우에는 보험회사의 역할이 단순히 사이버보험만 판매하는데 그치지 않고 사이버위험관리 자문도 함께 제공할 필요가 있음⁸⁾
 - 국내의 경우에는 보험회사 자체적으로 사이버위험 컨설팅 능력을 보유하고 있지 않기 때문에 보안업체와

Entreprise: TPE, PME, vous êtes Concernées”

5) Association of British Insurers, “Making Sense of Cyber Insurance: A Guide for SMEs”

6) Vertrauen Durch Sicherheit, “VDS Certification for Your Information Security: Cyber-Security for Small and Medium Sized Enterprises(SMEs)”

7) CNPP 홈페이지

8) 전게서 Michael Siegel et al.(2018)

협력을 해야 하는데, 컨설팅 비용 문제로 인해 협력이 용이하지 않은 상황임

- 보험회사는 매출에 연동하여 컨설팅 대가를 지불하기 원하는 반면, 보안업체의 경우에는 매출과 상관없이 고정액을 요구하기 때문임
- 사이버보험 시장이 성숙하여 가입자가 많은 경우에는 충분한 매출이 발생하기 때문에 보안 컨설팅에 필요한 자원 마련이 용이하나, 가입자가 적은 시장 초기에는 자원 마련에 어려움이 있음
- 따라서 사이버보험 시장 초기에는 보험회사들이 협력하여 사이버위험관리 전문기관을 만들어 활용하는 방안에 대해 검토할 필요가 있음
- 독일과 프랑스 사례를 참고할 때, 새로운 기관을 신설하기보다는 기존의 화재위험관리를 다루던 조직의 기능을 사이버위험으로 확대하는 방안을 생각해볼 수 있음

■ 셋째, 현재 시행되고 있는 중소기업 대상 사이버보안 바우처 제도를 확대하는 방안에 대해 검토할 필요가 있음

- 정부는 2018년 5월부터 신청 기업에 대해 취약점 분석 및 종합 대책 제시 후 보안 솔루션 구매 시 300만 원까지 바우처의 형태로 지원하는 정책을 시행하고 있음⁹⁾
 - 그러나 아직은 예산상의 이유로 지원 대상 기업의 범위가 제한적임
- 정보통신망법 개정을 통해 정보통신서비스사업자도 사이버보험 의무가입 대상에 포함되었는데, 일부 중소기업의 경우에는 비용측면에서 부담이 될 수 있음
 - 중소기업의 비용 부담을 완화해주는 방법에는 두 가지가 있는데, 하나는 보험료를 직접적으로 낮추어주는 것이고, 다른 하나는 바우처 지원을 통해 사이버위험관리 능력을 제고함으로써 간접적으로 보험료를 낮추어 주는 것임
 - 보험제도의 건전성 유지 측면에서 볼 때 후자의 방법이 더 바람직할 수 있음 [kiri](#)

9) ZDNet Korea(2018. 9. 3), “지역 사이버 안전망 사각, 클라우드 보안으로 메운다”