

대규모 개인정보 유출 사고와 보험산업의 대응 과제

요약

2025년 11월에 발생한 쿠팡의 대규모 개인정보 유출 사고는 독점적 지위에 있는 빅테크·디지털 플랫폼 기업의 사이버 보안 실패가 금융·실물·사회 시스템 전체에 광범위한 충격을 줄 수 있음을 보여준 시스템적 사이버 사고임. 증가하는 사이버 공격과 시스템적 피해에 대응하여 글로벌 사이버보험 시장은 미국을 중심으로 성장해왔으나, 국내 사이버보험 시장의 성장은 더딘 상황임. 시스템적 사이버 리스크 사고에 효과적으로 대응하기 위해서는 기업, 보험산업, 정부의 공동 노력이 요구됨

1. 대규모 개인정보 유출 사고 요약

- 쿠팡은 2025년 11월 대규모 개인정보 유출 사고를 겪었으며, 피해 영향 범위와 공시 방식에 대한 논란이 제기됨
 - 쿠팡은 사실상 쿠팡 이용자의 전체 규모 수준인 3,370만 건의 계정 정보가 무단 접근에 노출된 사실을 뒤늦게 확인·공지함
 - 유출된 정보는 이름, 연락처, 주소, 구매 내역 등 소비자의 일상과 직접 연결되는 항목이 다수 포함되어 있음
 - 2차 피해 우려로 인해 고객 이탈 상황이 발생하면서 쿠팡으로의 매출 의존성이 높은 소상공인들의 피해가 발생하고 있으며, 이는 국가 경제 측면에서도 부담으로 작용할 수 있음
- 쿠팡의 개인정보 유출 사고는 독점(또는 과점)적 지위에 있는 기업의 사이버 보안 실패가 2차·3차 피해를 유발할 수 있는 새로운 형태의 시스템적 사이버 리스크라고 볼 수 있음
 - 소위 빅테크·플랫폼 집중 시장 구조에서 독점적 지위에 있는 기업이 사이버 보안에 실패하여 사실상 대다수 국민의 개인정보가 유출되는 사고는 특정 기업 또는 산업을 넘어서 금융·실물·사회 시스템 전체에 광범위한 충격을 줄 수 있다는 점에서 시스템적 특성을 가지고 있음

2. 사이버보험 시장 확대 필요성 대두

- 증가하는 사이버 공격과 시스템적 피해에 대응하여 글로벌 사이버보험 시장은 미국을 중심으로 빠르게 성장해왔음
 - 팬데믹 이전 사이버보험 시장은 가입자가 증가 대비 보험 청구가 많지 않아 수익성이 매우 높은 시장으로 알려졌으나 최근 위험 노출이 급격히 증가하고 가입자 수와 청구 건수가 모두 크게 증가하면서 수익성이 다소 악화되고 효율도 빠르게 증가하는 추세임
 - 특히, 시스템적 사이버 리스크 노출 증가는 시장 내 위험인지(Risk awareness)를 제고하면서 공급과 수요를 증가시키는 효과를 가져왔지만, 누적위험(Accumulation risk)과 국가지원 사이버공격(State-backed cyberattacks)에 대한 공급 측면에서의 우려 또한 크게 증가시킴
 - 이를 극복하기 위한 방안으로 보험시장 확대 정책지원 및 민관협력 프로그램(Public-Private Partnership)의 필요성에 대한 목소리가 글로벌시장 전반에서 커지고 있는 상황임
- 국내 사이버보험 시장은 여전히 성장세가 더딘 상황이며, 특히 사이버보험 가입 대상인 기업의 정보보안 인식과 정책은 사이버보험 시장의 수요를 억제하는 요인으로 작동하고 있음
 - 기업의 경영진이 사이버 보안의 중요성을 정확히 인식하고 이와 관련한 거버넌스를 보다 체계화할 필요가 있음
 - 당국에서도 기업의 내부통제 시스템에 사이버 리스크 관리체계 수립 및 시행 여부를 감독하고 보안 투자에 관한 공시기준을 마련하여 산업 전반의 사이버 보안수준을 상향시키는 제도가 필요함
- 또한, 개인정보 유출로 인해 발생하는 배상책임액이 크지 않아 기업 입장에서 사이버보험을 가입할 유인이 높지 않음
 - 올해부터 적용된 개인정보보호법의 과징금 기준이 매출액 3%로 상향되었으나, 피해 고객에 대한 실질적 보상으로서 배상책임액은 여전히 매우 제한적이라는 점에서 민사 배상 리스크가 매우 낮고 이는 보험 가입 유인을 저해할 수 있음

3. 향후과제

- 대규모 개인정보 유출 사고, 국가 기반시설로의 사이버공격, 랜섬웨어에 의한 전신망 마비 등 시스템적 사이버 리스크 사건에 효과적으로 대응하기 위해서는 기업, 보험시장, 정부의 공동 노력이 요구됨

- 보험회사는 종합적 사이버 리스크 관리 서비스 공급자로서의 정체성을 확립하고, 사고 예방과 손해사정 역량을 포함한 공급 능력을 강화할 필요가 있음
 - 사이버 리스크는 네트워크 특성상 피해 규모가 시간이 지나면서 확장될 수 있을 뿐만 아니라 2·3차 피해를 유발함으로써 잠재적 확산성이 높다는 특징이 있음
 - 이러한 특성은 기존 보험시장에서 담보하는 위험과 차이가 있으며, 리스크 사건 발생 시 결과의 불확실성이 크다는 점을 시사함
 - 따라서, 보험회사는 단순히 사고 발생 시 보상을 제공하는 역할을 넘어, 정보보안 및 업데이트 역량 제고를 위한 전문가를 적극 채용하거나 사이버 보안 업체와의 협력을 통한 리스크 관리 컨소시엄을 구축하여 사고 예방 가능성을 높이고 사고 발생 시 피해 범위를 억제할 수 있는 리스크 사전관리 서비스 능력을 확보해야 함
 - 또한, 개인정보 유출 신고 의무제도 대응 및 대민 관계 관리를 위하여 공격 발생 여부 탐지, 피해 범위의 신속한 파악 등 사이버 손해사정 역량이 필수적임

- 사이버보험 시장에서 수요(기업) 및 공급(보험회사)의 균형을 이루고 안정적인 성장 토대를 마련하기 위해서는 공공부문에서의 적극적인 정책 수립 및 지원이 필요함
 - 기업의 개인정보 보호에 대한 안일한 인식을 개선하기 위해 제재 수준을 강화할 필요가 있음
 - 과징금 확대와 더불어 피해 고객에 대한 배상책임 규모를 대폭 확대하여, 사이버 리스크 관리 실패가 기업의 재정건전성 및 가치에 심각한 손상을 초래할 수 있다는 경각심을 높여야 함
 - 또한, 국가지원 사이버 공격(혹은 사이버 테러리즘)이 보험의 면책 사항임을 감안했을 때 국가 재보험 제도 또는 공사협력 보험 프로그램 구축이 필요할 수 있음
 - 미국 재무부는 기존 테러위험 보험 프로그램(Terrorism Risk Insurance Program; TRIP)에 사이버 배상책임을 보장하는 사이버보험을 포함하며, 영국 정부 또한 보험회사로부터 테러위험을 수재하는 기존 재보험 프로그램(Pool Re)에 사이버 테러로 인한 기업의 재물 손해 및 영업중단 피해로 보장을 확대함 (송윤아·홍보배(2021), 『주요국 정부의 사이버보험 시장 참여 배경 및 동향』, 이슈보고서, 보험연구원 참조)
 - 금융당국 입장에서는 사이버 리스크를 시스템적 리스크로 규정하고, 이에 관한 스트레스 테스트 모델을 구축함으로써 금융 및 보험회사뿐만 아니라 빅테크 및 대형 디지털 플랫폼 사업자로의 시스템적 사이버 사고로 인해 유발할 수 있는 금융 피해를 추정하도록 적용할 필요가 있음

포항공과대학교 산업경영공학과 정광민 교수
kwjung@postech.ac.kr

Large-Scale Personal Data Breaches and Challenges for the Insurance Industry

ABSTRACT

The large-scale personal data breach at Coupang in November 2025 was a cyber incident that underscored how cybersecurity failures at Big Tech and digital platform companies with dominant market power can disrupt financial markets, the real economy, and broader social systems. Although the global cyber insurance market—driven largely by the United States—has expanded in response to the rise in cyberattacks and systemic losses, growth in Korea’s cyber insurance market has been comparatively slow. Effective management of systemic cyber risk will therefore require coordinated efforts from firms, the insurance industry, and the government.

1. Summary of the Large-Scale Personal Data Breach Incident

In November 2025, Coupang suffered a major personal data breach that exposed roughly 33.7 million user accounts—essentially its entire customer base—to unauthorized access. The compromised information included names, contact details, addresses, and purchase histories, many of which relate directly to consumers’ daily routines. Fears of secondary misuse led to a notable decline in number of customers, creating losses for small businesses that rely heavily on Coupang as a sales channel. This situation also poses potential risks for the broader national economy.

Coupang's data breach represents a new type of systemic cyber risk in which cybersecurity failures at firms with significant market power (whether monopolistic or oligopolistic) can trigger widespread second- and third-order effects. In highly concentrated digital platform markets, a breach at a major Big Tech firm can expose the personal information of a large share of the population. Because such incidents can disrupt not only individual companies or sectors but also financial markets, the real economy, and society as a whole, they exhibit clearly systemic characteristics.

2. Emerging Need for the Cyber Insurance Market

Increasing cyberattacks and rising systemic losses have driven rapid growth in the global cyber insurance market, particularly in the United States. Before the pandemic, the market was widely viewed as highly profitable because claim frequencies were relatively low compared with the growth in policyholders. In recent years, however, exposure to cyber risks has grown markedly, accompanied by a substantial rise in both policyholders and claims. These trends have eroded profitability and led to rapid increases in premium rates. Although rising exposure to systemic cyber risk has increased market awareness and encouraged growth on both the supply and demand of the cyber insurance market, concerns among insurers have intensified due to accumulation risk and state-backed cyberattacks. In response, many countries are calling for policy measures to expand cyber insurance capacity and for stronger public-private partnership programs to manage large-scale cyber incidents.

In Korea, the cyber insurance market continues to grow slowly. Low levels of cybersecurity awareness and weak internal policies among firms—who form the primary customer base for cyber insurance—remain major obstacles to market development. Corporate management must first recognize the seriousness of cyber threats and establish more structured governance around cybersecurity. Regulators,

in turn, should supervise whether firms have appropriate cyber-risk management systems in place and introduce disclosure standards for security investments to raise cybersecurity across industries.

From firms' perspective, the relatively small scale of compensation typically paid to customers after data breaches also reduces the incentive to purchase cyber insurance. Although the maximum administrative fine under the Personal Information Protection Act was raised to 3% of annual revenue this year, actual civil liability paid to affected individuals remains limited. As a result, civil compensation risk remains low, weakening the motivation for firms to seek insurance coverage.

3. Future Directions

To effectively respond to large-scale personal data breaches, cyberattacks targeting national infrastructure, ransomware-induced system paralysis, and other forms of systemic cyber risk, coordinated efforts by firms, the insurance market, and the government are essential. Insurers, in particular, must strengthen their identity as comprehensive cyber-risk management providers and enhance their capabilities—not only in underwriting but also in loss prevention and cyber claims assessment. Because cyber risks can spread across networks and generate secondary and tertiary losses, the scale of damage can grow over time—unlike risks typically covered in traditional insurance. This means that the consequences of a cyber incident are far more uncertain and potentially much larger.

Accordingly, insurers must move beyond the traditional role of simply providing compensation after an incident. They should build proactive risk-management capacity—for example, by hiring cybersecurity specialists, partnering with cybersecurity firms, or establishing risk-management consortia. Such efforts can improve clients' security posture, reduce the likelihood of incidents, and limit the scale of damage when breaches occur. In addition, robust cyber-claims assessment

capabilities—such as the ability to detect attacks quickly, assess the scope of damage, and support firms in meeting breach-notification requirements—are now indispensable.

Active policy support from the public sector is also required to balance supply and demand in the cyber insurance market and to establish the foundations for stable long-term growth. First, alongside higher administrative fines, the scale of civil liability for affected customers must be expanded substantially. Stronger financial consequences will make it clear to firms that failures in cyber-risk management can seriously undermine their financial soundness and corporate value. In short, stronger penalties are needed to correct the prevailing complacency toward personal data protection.

In addition, given that state-backed cyberattacks (or cyber terrorism) are typically excluded from insurance coverage, there may be a need for a national reinsurance mechanism or a public-private insurance program. The U.S. Treasury has incorporated cyber liability coverage into the existing Terrorism Risk Insurance Program (TRIP), and the U.K. government has expanded its public reinsurance scheme (Pool Re) to include property damage and business interruption losses arising from cyber terrorism. (See Song Yoon-ah and Hong Bo-bae, 2021, Government Participation in Cyber Insurance Markets in Major Countries, KIRI Issue Report.)

Lastly, financial regulators should formally classify cyber risk as a systemic risk and develop stress-testing models that require not only financial institutions and insurers—but also Big Tech companies and major digital platforms—to assess potential financial losses stemming from a systemic cyber incident.

Kwangmin Jung, Ph.D.,
Department of Industrial and Management Engineering, POSTECH
kwjung@postech.ac.kr