데이터 유출과 최적 규제 정책: 처벌의 균형을 묻다

쿠팡의 데이터 유출 사건을 둘러싼 논쟁이 확산되고 있다. 유출이 발생했다는 사실 자체는 다툼의 대상이 아니다. 논쟁의 핵심은 그 유출에 대한 한국 규제 당국과 국회의 대응이 적절했는가에 있다. 최근 미국 하원 법사위원회의 중간 보고서는 이 대응이 한쪽으로 치우친 것이었다고 주장한다. 이 글의 목적은 그 주장이 맞는지, 혹은 쿠팡 측 주장이 맞는지를 판정하는 데 있지 않다. 오히려 이런 문제 제기가 나왔다는 사실을 계기로, 데이터 유출에 대한 최적 규제, 즉 억제(deterrence) 정책을 어떻게 설계해야 하는지를 짚어보는 것이 더 유용하다.

어떤 기업도 사이버 공격으로부터 완전히 자유로울 수 없다. 충분한 보안 투자를 한 기업조차 침해를 겪을 수 있다는 점에서, 논의의 무게는 유출 발생 여부가 아니라 그 심각성과 사후 대응, 그리고 그에 대한 규제 당국의 대응 수준에 실려야 한다. 이를 판단하려면 먼저 데이터 유출이 실제로 어떤 성격의 피해를 낳는지 살펴보고, 이어 최적 억제의 경제학이 제재 설계에 어떤 함의를 갖는지 검토할 필요가 있다. 학계의 연구는 이 문제에 대해 보다 신중하고 정교한 접근을 요구한다.

무엇보다 모든 데이터 유출이 동일한 피해를 낳는 것은 아니다. 피해의 크기는 단순한 유출 건수가 아니라, 정보의 성격과 침해 지속 기간, 실제 유출 및 악용 여부, 그리고 기업의 대응 속도에 의해 좌우된다. 금융정보나 주민등록번호, 의료기록, 인증정보와 같이 직접적인 사기나 신원 도용으로 이어질 수 있는 데이터는 큰 피해를 유발한다. 반면 이름과 이메일 주소 수준의 정보는 피싱 위험과 신뢰 저하를 초래할 수 있지만, 측정 가능한 경제적 피해는 상대적으로 제한적인 경우가 많다.

피해의 성격뿐 아니라 기업의 사후 대응 역시 중요한 변수다. 침해를 신속히 탐지하고, 당국과 협력하며, 이용자에게 지체 없이 알리고, 실질적인 보완 조치를 취한 기업은 장기적 평판 손상이 상대적으로 작다는 연구가 다수 존재한다. 시장 또한 이를 구분해 평가한다. 합리적 보안 수준을 유지했음에도 고도화된 공격을 받은 경우와, 내부 통제 실패나 구조적 관리 부실이 드러난 경우를 시장은 다르게 본다.

이러한 구분이 시사하는 바는 분명하다. 사이버 보안은 위험을 제거하는 문제가 아니라 관리하는 문제이며, 어떤 기업도 침해로부터 완전히 자유로울 수 없다. 따라서

규제의 핵심은 침해 발생 여부 자체가 아니라, 사전에 합리적 예방 조치를 했는지, 사후 대응이 적절했는지를 평가하는 데 있어야 한다.

경제학의 최적 억제 이론 역시 같은 결론에 도달한다. 제재의 목적은 처벌의 극대화가 아니라 사회적으로 효율적인 예방과 행동을 유도하는 데 있다. 다시 말해 기업이 자신의 행위로 발생할 수 있는 사회적 비용을 내부화하도록 하되, 투자와 혁신, 그리고 기업의 존속 가능성을 훼손하지 않는 균형이 필요하다.

문제는 제재가 이 균형을 넘어설 때 발생한다. 제재 수준이 기업의 감당 능력을 위협할 정도에 이르면, 경영진은 침해 사실을 투명하게 공개하기보다 은폐하려는 유인을 갖게 된다. 기업은 실질적 보안 투자보다 규제 회피에 더 많은 자원을 투입하게 되고, 투자자는 높은 정책 리스크를 이유로 디지털 산업 투자를 기피할 수 있다. 무엇보다 기업이 무너질 경우, 피해 보상과 향후 보안 개선에 투입될 자원 자체가 줄어드는 역설이 발생한다. 즉 과도한 제재는 억제를 강화하기보다는 오히려 약화시키는 결과를 낳을 수 있다.

이 때문에 학계는 억제(deterrence)와 파괴(destruction)를 구분해야 한다고 강조한다. 효과적인 제재는 기업의 행태를 교정해야지, 사회적으로 가치 있는 기업을 시장에서 배제하는 결과로 이어져서는 안 된다. 모든 대규모 유출을 곧바로 과실의 증거로 간주하는 접근은 보안 강화를 유도하기보다 기업의 규모 확장 자체를 위축시키는 방향으로 작용할 수 있다.

미국 하원 보고서가 제기한 문제의식도 바로 이 지점과 맞닿아 있다. 해당 보고서는 일부 제재가 기업의 존속 자체를 위협할 수준일 수 있다고 지적하며, 이를 과도하거나 차별적 대응일 가능성으로 해석한다. 다만 이러한 주장 역시 어디까지나 보고서의 시각이며, 별도의 엄밀한 사실 검증이 필요한 사안이라는 점을 분명히 해둘 필요가 있다.

그럼에도 이번 논쟁이 던지는 함의는 개별 기업의 사례를 넘어선다. 대규모 데이터 유출은 여론의 분노와 정치적 압력을 동반하고, 강한 처벌 요구로 이어지기 쉽다. 입법자나 규제 당국이 특정 사건에 대해 한쪽으로 치우친 발언을 내놓는 경우가 실제로 존재한다면, 이는 여론의 압력이 제재 수준 결정에 얼마나 강하게 작용하는지를 보여주는

사례로 볼 수 있다. 경제학 연구는 일관되게 분노에 기반한 규제의 위험성을 경고해 왔다. 여론의 압력에 따라 제재 수준을 결정하는 방식은 단기적으로는 정치적으로 매력적일 수 있으나, 장기적으로는 오히려 억제 효과를 떨어뜨릴 위험이 크다.

결국 필요한 것은 처벌의 일률적 강화가 아니라 정교한 조정이다. 기업이 보안 의무를 의도적으로 무시하거나, 침해를 은폐하거나, 반복된 경고를 무시하거나, 기본적 보호 조치를 이행하지 않은 경우에는 강한 제재가 정당하다. 반대로 신속한 통제와 투명한 공개, 적극적 협력과 실질적 개선이 이루어진 경우에는 제재 역시 그에 맞게 완화되어야 한다. 이러한 차등적 접근이야말로 억제의 본래 목적에 부합한다.

만약 모든 유출 사건에 대해 기업 존속을 위협하는 수준의 제재를 일괄적으로 가한다면, 기업은 정보 공유와 투명한 공개보다 법적 위험 최소화에 집중하게 된다. 이는 결과적으로 사회 전체의 학습과 대응 능력을 약화시키는 역효과로 이어진다.

데이터 유출에 대한 정책은 피해의 실질적 규모, 예방 가능성이 있었던 과실 여부, 조직의 유인 구조, 그리고 사후 대응을 종합적으로 고려해야 한다. 규제의 목적은 과거 행위에 대한 응징이 아니라 미래 피해의 감소, 즉 효과적인 억제에 있다.

장기적으로 성공적인 규제는 가장 강한 처벌을 부과하는 규제가 아니라, 가장 바람직한 행동을 이끌어내는 규제다. 필요 수준을 넘어선 제재는 투자와 혁신, 시장 안정성을 훼손하고, 결국 억제라는 본래 목표와 반대로 사회 전체의 보안을 약화시킬 수 있다.

Data breaches and optimal regulatory policy

A dispute over the data breach at the center of Coupang's clash with South Korean regulators has been escalating. The fact that a breach occurred is not in dispute. The real question at issue is whether the response by Korean regulators and lawmakers has been proportionate. A recent interim report by U.S. House Judiciary Committee staff argues that this response has been one-sided. Given that such concerns have been raised, a more important issue may be how optimal regulatory policy, that is, deterrence policy, should be designed in response to data breaches.

That question is not whether any given company will experience a data breach. Every company is a potential target, and even firms with substantial security investments cannot fully insulate themselves from attack. The weight of the analysis should instead fall on how severe a given breach turns out to be, how firms respond afterward, and how regulators calibrate their response. Answering that question requires first understanding what the empirical literature tells us about how breaches actually cause harm, and then asking what the economics of optimal deterrence implies about the appropriate design of sanctions. The academic literature paints a more nuanced picture than the public debate might suggest.

Not all data breaches are equally harmful. Research consistently finds that breach severity depends less on the number of records exposed than on the nature of the compromised information, the duration of unauthorized access, whether the data were actually exfiltrated or misused, and whether firms acted promptly once the incident was discovered.

Financial credentials, government identifiers, medical records, and authentication credentials typically generate the largest downstream harms because they facilitate fraud or identity theft. By contrast, breaches involving names and email addresses alone often generate substantially lower measurable consumer losses, although they may still increase phishing risks and reduce trust.

Firm behavior after a breach compounds or mitigates these underlying harms. Firms that discover intrusions quickly, cooperate with investigators, notify affected customers promptly, and implement credible remediation generally suffer smaller long-run reputational losses than firms that conceal breaches or delay disclosure. Indeed, many studies find that markets distinguish between firms that experience sophisticated attacks despite reasonable security precautions and firms whose breaches reveal systematic governance failures.

This market behavior points to a broader lesson because cybersecurity is fundamentally a problem of risk management rather than risk elimination. No business is immune from attack. Even firms with substantial investments in security occasionally experience successful intrusions by sophisticated adversaries or trusted insiders. The relevant policy question is therefore not whether a breach occurred, but whether reasonable precautions were taken before the breach and reasonable responses followed afterward.

The economics of deterrence reaches a parallel conclusion from a different direction. The objective of sanctions is not to maximize punishment but to induce efficient precaution. Optimal

deterrence requires firms to internalize the expected social costs of their conduct while preserving incentives to invest, innovate, and remain solvent.

Excessive sanctions can undermine these objectives. If penalties approach or exceed a firm's financial capacity, several distortions emerge. Managers may underinvest in voluntary disclosure because admitting a breach could threaten corporate survival. Firms may devote excessive resources to avoiding regulatory attention rather than improving cybersecurity itself. Investors may become reluctant to finance innovative firms operating in high-risk digital sectors. Most importantly, sanctions that effectively bankrupt companies rarely improve compensation for consumers, since insolvent firms possess fewer resources to fund remediation or future security improvements.

The literature therefore distinguishes between deterrence and destruction. Efficient penalties should encourage better behavior without eliminating socially valuable firms. A regulatory system that treats every large breach as evidence of negligence risks creating incentives that discourage scale rather than encouraging better security.

The House Judiciary Committee report's concerns raise precisely these issues. Although not itself an empirical study, the report illustrates how concerns about deterrence versus over-deterrence have entered contemporary policy debates. It argues that some Korean legislators advocated exceptionally severe responses following the Coupang breach that, taken together, could threaten the company's continued operations. The report characterizes these proposals as disproportionate and potentially discriminatory toward an American-owned company, though this characterization remains the report's own view and would require independent factual verification.

Whether one accepts those allegations is ultimately an evidentiary question that this analysis does not attempt to resolve. Nevertheless, the debate highlights an important policy issue extending well beyond a single company. Legislators understandably respond to highly publicized breaches with demands for tougher penalties. Large breaches affect millions of consumers, generate public anger, and create political pressure for visible enforcement. If lawmakers or regulators do in fact make one-sided public statements about a particular case, this illustrates how strongly public pressure can shape sanction levels. Yet economic research consistently cautions against allowing public outrage to determine sanction levels.

The alternative to outrage-driven punishment is calibration. Optimal enforcement requires calibration rather than escalation. Penalties should increase when firms knowingly disregard security obligations, conceal breaches, ignore repeated warnings, or fail to implement widely accepted safeguards. Enhanced sanctions are also justified when executives intentionally mislead regulators or obstruct investigations. Conversely, punishment should be moderated when firms rapidly contain incidents, cooperate with authorities, and undertake remediation.

This calibration matters because incentives compound over time. If every disclosed breach trigger penalties approaching corporate insolvency, firms may rationally devote more effort to limiting legal exposure than to sharing information that helps regulators and other

organizations defend against future attacks. Society loses valuable learning opportunities precisely when collective knowledge is most needed.

Taken together, these two strands of research point in the same direction. The empirical literature on data breaches suggests that regulators should focus on actual harm, preventable negligence, organizational incentives, and post-breach conduct rather than adopting sanctions designed primarily to maximize punishment. Likewise, the economic literature on optimal deterrence reminds us that the objective of regulation is to reduce future harm, not merely to express public condemnation. In the long run, regulatory systems succeed not because they impose the largest penalties, but because they create the strongest incentives for better behavior.

Sanctions that exceed what is necessary for efficient deterrence impose costs that extend beyond the regulated firm. By increasing uncertainty for investors and threatening the viability of productive enterprises, excessive penalties can reduce innovation and discourage capital formation. The result is a society that is less secure rather than more secure, precisely the opposite of what deterrence-based regulation is meant to achieve.

Citations

Campbell K, Gordon LA, Loeb MP, Zhou L (2003) The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. J. Comput. Security 11(3):431–448.

Kamiya S, Kang J-K, Kim J, Milidonis A, Stulz RM (2021) Risk management, firm reputation, and the impact of successful cyberattacks on target firms. J. Financial Econom. 139(3):719–749.

Romanosky S (2016) Examining the costs and causes of cyber incidents. J. Cybersecurity 2(2):121–135.

Romanosky S, Hoffman D, Acquisti A (2014) Empirical analysis of data breach litigation. J. Empirical Legal Stud. 11(1):74–104.

Sokol, D. D., and T. Wang. 2023. A review of empirical literature in information security. Southern California Law Review 95 (Postscript): 95–109.