한국 사이버 보험 생태계 구축을 위한 실천적 로드맵:
(Unlocking the Potential! - A Roadmap for a Pragmatic Cyber Insurance Ecosystem in Korea)

최 용 민 (Yong-Min Choi)

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

Contents

EXECUTIVE SUMMARY

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

- 한국의 사이버 보험 시장은 수요자의 무관심, 공급자의 리스크 평가/ 인수 역량 부족, 인프라 미비라는 **'악순환의 고리'**에 빠져 성장이 정체되어 있음
- 미국·일본·호주 등 글로벌 시장은 **규제 강화라는 정부 정책의 주도**하에 기술 기반의 '능동형(Active)' 보험 도입과 같은 **민영 주체의 다양한 노력**이 함께해 **사이버 복원력 (Cyber Resilience)**을 강화하는 추세임

  (미국과 한국의 거버넌스 차이 - 미국은 사이버 리스크를 국가 안보 및 경제 복원력(Resilience)의 핵심으로 보고 정부가 시장의 메커니즘을 설계하는 반면, 한국은 제도적 강제성이나 인센티브 설계 없이 민간의 자율에만 의존하고 있는 실정임)
- 국내 사이버 보험시장에서 과거 10년 간의 과제가 2026년 오늘날까지 반복되고 있는 이 현실이야말로 우리 시장이 처한 가장 큰 리스크임. 이제는 **'무엇을 해야 하는가(What to do)'**가 아니라, **'어떻게 실행할 것인가(How to execute)'**로 우리의 패러다임을 전환해야 할 때임
- 사이버 보험시장의 활성화는 어느 한 주체의 노력만으로는 불가능함. **정부의 제도적 마중물**, **감독당국의 투명한 데이터 공유**, **보험사의 고객 중심의 혁신성 있는 서비스 통합**, 그리고 **기업의 인식 전환**이라는 네 개의 톱니바퀴가 동시에 맞물려 돌아가야 가능하다고 봄
- 정부 주도하에 각 역할 주체가 함께 하는 로드맵 추진을 제안함. 본 로드맵 추진을 통해 디지털 전환 시대의 **'데이터 리더십 확보'**, '**표준화 모델 수립**', **'의무보험 확대'**를 축으로, 단순한 손해 보상을 넘어 사고 예방과 복구 지원이 결합된 **실천적 사이버 보험 생태계**를 조성하는 것을 목표로 함

Recap: 주요 과거 발표주제

유사한 주제의 반복이 주는 시사점!

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

초기 형성기 (2016~2018): "제도 도입과 보험가입 의무화를 논의하던 시기"

- "사이버 리스크와 보험의 역할: 글로벌 동향과 시사점" (2016, 보험연구원 조찬회)
- "개인정보보호 배상책임보험 의무가입 제도 도입을 위한 정책 공청회" (2016, 방송통신위원회/행정자치부)
- "개인정보보호 배상책임보험 의무가입 제도 도입 방안" (2016, 보험연구원)
- "사이버 리스크 관리 실태 및 보험산업의 대응 과제" (2017, 금융감독원 금융경영브리프)
- "사이버 리스크와 보험 산업의 대응 과제" (2017, 금융감독원 포럼)
- "4차 산업혁명과 사이버 보험 활성화를 위한 법적 쟁점" (2018, 한국보험법학회 정기학술대회)
- "4차 산업혁명 시대, 사이버 보험 활성화를 위한 법적 과제" (2018, 국회 세미나)
- "국내 사이버보험 시장의 현황과 **활성화** 저해 요인 분석" (2018, 보험연구원 세미나)

확장 시도기? (2019~2022): "데이터 부족 호소와 사이버 보험 활성화 전략 얘기가 반복된 시기"

- "개인정보 손해배상책임 보장제도 시행에 따른 보험업계 대응 방안" (2019, 보험개발원 설명회)
- "사이버 보험 활성화를 위한 사이버 사고 데이터 공유 플랫폼 구축 방안" (2019, 한국화재보험협회 위험관리 포럼)
- "비대면 사회 확산에 따른 사이버 리스크의 재무적 전가 방안" (2020, 보험연구원 웹 세미나)
- "국내 중소기업의 사이버 보험 가입 실태와 정책적 지원 필요성" (2021, 중소기업 연구원/보안학회 합동 세미나)
- "랜섬웨어 공격 급증에 따른 사이버 보험의 역할과 한계" (2021, 보험정보학회)
- "국내 사이버보험 시장의 현주소와 발전 방향" (2022, 금융위원회 주관 회의)

최근의 새로운 위협 대응기 (2023~2025): "신기술(AI) 등장과 인식 제고를 재강조하는 단계"

- "디지털 전환 시대, 사이버 보험 시장 활성화를 위한 정책 제언" (2022, 금융위원회 주관 사이버보험 포럼)
- "국가 핵심기반시설 사이버 보안 강화를 위한 보험 연계 방안" (2023, 한국인터넷진흥원(KISA) 주관 세미나)
- "생성형 AI 시대, 새로운 사이버 리스크와 보험의 대응" (2023, 사이버보안 포럼)
- "생성형 AI 기술 악용에 따른 사이버 리스크의 새로운 국면과 보험의 한계" (2024, 사이버 보안 컨퍼런스)
- "기업의 사이버 복원력(Cyber Resilience) 확보를 위한 민관 합동 보험 모델" (2024, 보험연구원/보안업계 공동 포럼)
- "디지털 전환 시대, 사이버 보험 가입 확대를 위한 인센티브 구조 설계" (2025 세미나)

왜 실행이 되지 않았는가 돌이켜 보면 >>

Korean Cyber Insurance Market: Status & Structural Gaps

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

"Vicious Cycle" of Stagnant Growth

표준화 부재 및 시장 불확실성

표준화된 약관이나 보장 범위가 없어 기업들이 상품을 비교·판단하기 어렵고 **가입 장벽**이 높음

정보 비대칭 및 데이터 부족

신뢰할 수 있는 **사고 데이터와 보험금 청구 통계**가 절대적으로 부족하여 정밀한 보험료 산정이 어려움

높은 비용 구조와 저조한 수요

리스크 평가의 불확실성으로 보험료는 높게 책정되는 반면, 기업들은 사이버 리스크를 과소평가하여 **가입 유인이 낮음**

시스템 위험(Systemic Risk)* 가능성

클라우드 마비 등 단일 사고가 대규모 연쇄 손해로 이어질 가능성이 커지며 **보험사의 인수 역량을 제한**함

* 시스템 리스크(Systemic Risk)는 특정 보험사의 부실이나 위험 요소가 금융 시스템 전체로 확산되어 실물 경제에 심각한 부정적 영향을 미칠 수 있는 위험을 의미

시장 실패 (Market Failure) 구간에 놓여 있는 건 아닌가? >>

시장 실패 구간에서 벗어나 시장 기제 복구를 위해선

자율에 맡겨진 시장 동력 상실 -> 정부의 "시스템 설계" 필요

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

정보 비대칭성

"리스크 산정의 불투명성"

취약점을 숨기는 기업(도덕적 해이), 위험 측정 데이터가 부재한 보험사 -> 고위험, 고보험료

역선택

"보안투자와 보험의 단절"

높은 보안수준이 보험료 할인으로 이어지는 계량화된 공식 지표 부재

부정적 외부효과

"법적 강제성의 모호함"

종합 사이버 리스크(조업 중단, 복구 비용 등)를 보장하는 보험은 여전히 자율에 맡겨져 있어, 경영진의 우선순위에서 밀리고 있음

정부/ 감독기관

- **데이터 표준화/ 공유**
- **강제성 및 인센티브**
- **국가 안전망 구축**

"멈춰버린 시장 기제 (Market Mechanism), 이제 **정부가 '시스템 설계자(System Architect)'로서 주도적으로 개입할 때!"**

Not What but HOW!! >>

‘무엇’을 해야 하는 가에서 ‘어떻게’ 실행할 것인가로 전환해야

정부 주도하에 사이버 리스크 복원력을 위한 생태계 구축 필요

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

AS-IS

시장 정체

정부 역할 주도하에 민간의 협업을 통한 생태계 조성이 해결의 핵심

TO-BE

사이버 리스크 복원력 생태계 구축

파편화된 접근?

정부(규제), 보험사(상품), 보안업체(기술)가 각자의 영역에서만 목소리를 냈을 뿐, 이를 통합할 주체가 없었음

인센티브 설계 실패?

기업들에게 '의무'만 강요하고, 가입했을 때 얻는 '실질적 이득(세제 혜택, 보안 등급 상향 등)' 제공 등의 유인책이 부족했음

데이터의 폐쇄성?

사고 통계가 공공과 민간 사이에서 선순환되지 못하고 단절됨

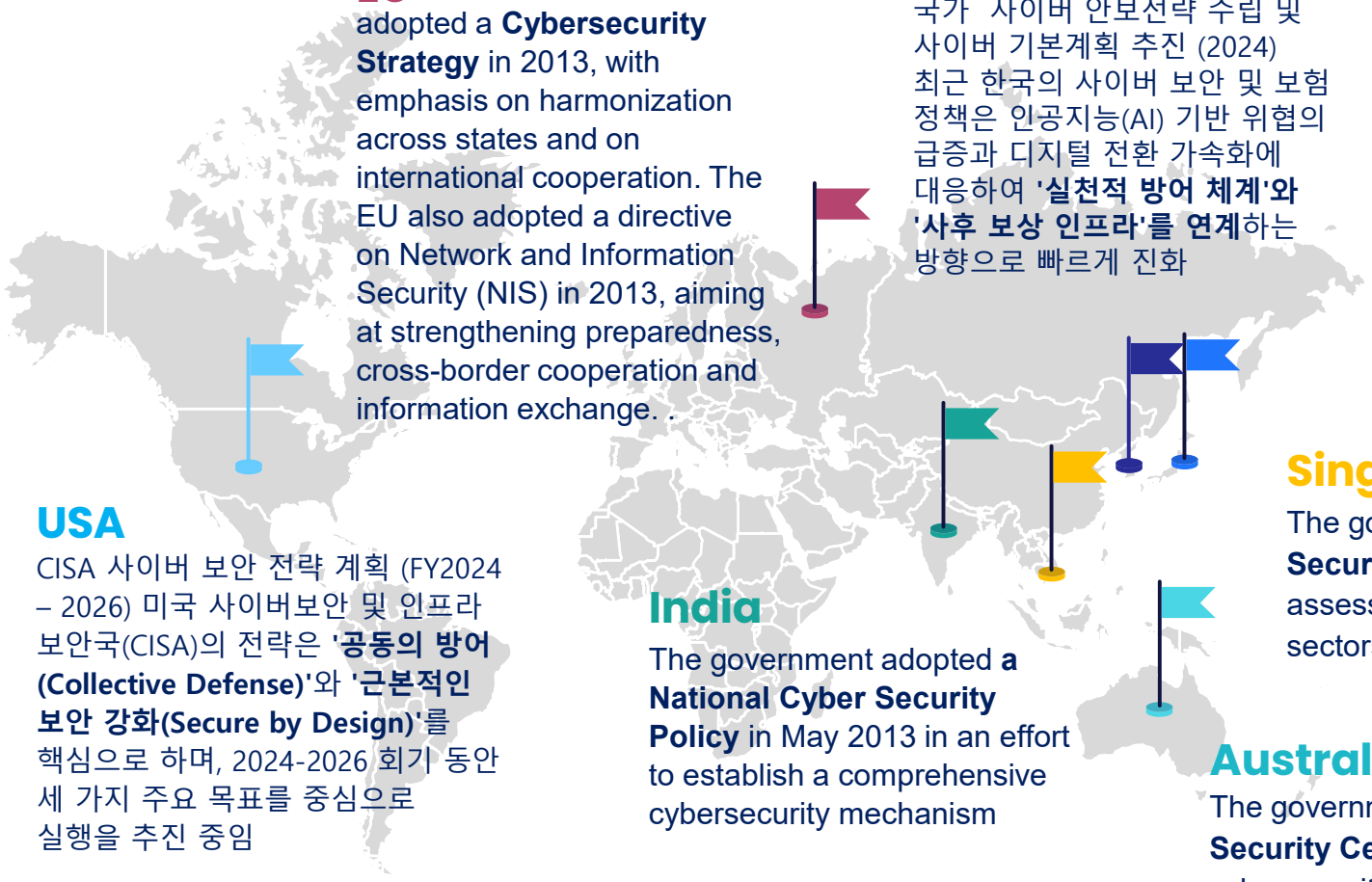
생태계?
생물과 환경이 그물망처럼 촘촘하게 연결되어 **에너지를 주고받는 "시스템"** 그 자체.

생태계의 특징?
구성 유기체간의 **상호 작용**과 **복원력**

정부 역할의 중요성 >>

주요국의 정부 주도 대응 전략

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions



EU

adopted a **Cybersecurity Strategy** in 2013, with emphasis on harmonization across states and on international cooperation. The EU also adopted a directive on Network and Information Security (NIS) in 2013, aiming at strengthening preparedness, cross-border cooperation and information exchange. .

Korea

국가 사이버 안보전략 수립 및 사이버 기본계획 추진 (2024)
최근 한국의 사이버 보안 및 보험 정책은 인공지능(AI) 기반 위협의 급증과 디지털 전환 가속화에 대응하여 **'실천적 방어 체계'와 '사후 보상 인프라'를 연계**하는 방향으로 빠르게 진화

Japan

Japan has established a comprehensive cybersecurity policy, most recently enhanced by an updated **Cybersecurity Strategy** in 2013, which seeks to strengthen **private public information sharing; introduce business continuity exercises; establish a platform for evaluation and authentication of systems** used by critical infrastructure; and enhance international cooperation.

USA

CISA 사이버 보안 전략 계획 (FY2024 – 2026) 미국 사이버보안 및 인프라 보안국(CISA)의 전략은 **'공동의 방어 (Collective Defense)'**와 **'근본적인 보안 강화(Secure by Design)'**를 핵심으로 하며, 2024-2026 회기 동안 세 가지 주요 목표를 중심으로 실행을 추진 중임

India

The government adopted **a National Cyber Security Policy** in May 2013 in an effort to establish a comprehensive cybersecurity mechanism

Singapore

The government has introduced the **National Cyber Security Masterplan** 2018, with expected assessments of cybersecurity preparedness of critical sectors and the national infrastructure more broadly

Australia

The government has established **Australian Cyber Security Centre (ACSC)** to 'bring under one roof' the cybersecurity capabilities of various government agencies

(Source: IMF Report)

한국의 정책 방향과 해외 주요국 전략과의 결정적 차이? >>

한국의 정부 주도 대응 전략 – 왜 실행력이 떨어지는가?

해외 주요국 전략과의 결정적 차이

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

	미국 / EU		한국
법적강제력	미국의 사이버보안 행정명령(EO 14028)이나 EU의 사이버 복원력 법 (CRA)은 미준수 시 **공공 조달 배제**나 **과징금**을 부과	VS.	**가이드라인과 권고 위주의 전략**에 그쳐 기업 입장에서는 "지켜야 하겠지만, 안 지켜도 당장 큰일 나지 않는" 지침으로 인식되어 실행 동력이 미약한 상황
보안의 '비즈니스화' 고리	보안 수준이 낮다고 평가되면 보험 가입이 거절되거나 상장 조건에 결격 사유가 되는 등 **'시장 기제'**가 작동함	VS.	**보안 투자를 순수 비용**으로만 보며, 보험 가입이나 보안 인증이 실제 기업 가치 상승이나 비용 절감 (보험료 할인 등)으로 이어지는 연결고리가 보이지 않는 상황
보험의 연계 기능	단순히 보험을 드는 것이 아니라, Zero Trust 등 **가이드라인 준수 여부를 보험료율과 직접 연동**하듯 정책이 기업의 '체질 개선'을 강제하는 동력으로 작동	VS.	현재 의무 보험은 사고 발생 시 **'배상'에 초점**이 맞춰져 있음. 보험 가입이 보안 투자의 끝이 아니라 시작이 되려면, 보안 사고 예방 활동(Hygiene)을 보험료 산정의 표준 지표**로** 강제하는 실행력이 더 구체화되어야 함
민간의 지위	민간 (빅테크 등)을 정부와 대등한 **'공동 방어자'**	VS.	민간은 여전히 정부의 관리·감독 대상이자 사고 시 보고 의무를 가진 **'수동적 주체'**

실행력 강화를 위한 개선 방안? >>

정부의 사이버 리스크 거버넌스 패러다임 전환 필요

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

거버넌스 패러다임 비교: 미국 vs. 한국

'보안 투자가 기업의 재무적 가치와 직결되는 시장 메커니즘'을 어떻게 제도화할 것인가가 거버넌스 혁신의 핵심이며 정부의 역할!!

	미국 – 주도적 시장 설계	한국 – 제도적 공백과 자율의 역설
구매력을 통한 시장 선도	미국 정부는 세계 최대의 IT 구매자임. **관련 행정명령(EO 14028)**을 통해 정부에 납품하기 위한 필요 기준을 명시하는데 이는 규제가 아니라 **'거래 조건'**이 되며, 기업은 정부라는 **큰 시장을 잃지 않기 위해 스스로 보안 투자**를 강화하고 있음	**공급망 통제력 부족** 미국처럼 강력한 구매력을 바탕으로 표준을 강제하기 보다는, **가이드라인 배포 수준**에 머물러 있어 민간 공급망 전체의 보안 수준을 상향 평준화 하는 데 한계가 있음
소프트웨어 투명성 제고 (SBOM)	식품의 영양성분표처럼 SW 구성 요소를 공개하도록 강제함. 이는 구매자가 제품의 위험도를 판단할 수 있게 하여, **'보안이 우수한 제품이 시장에서 더 비싸게 팔리거나 선택 받는'** 환경을 조성	**민간 자율의 한계** 자율성을 강조하지만, 실제로는 사고 발생 시 '과징금' 위주의 사후 처벌에 치중하고 있는 상황에서 시장 구성원들이 보안을 내재화할 수 있는 **경제적 유인 체계**가 설계되지 않고 있음
사이버 보험 시장과의 연계	정부는 **리스크 평가 표준을 제공하고, 보험사는 이를 바탕으로 기업의 보안 수준에 따라 보험료를 차등 산정**함. 보안 수준이 낮으면 금융 비용 (보험료)이 상승하는 상황으로, 기업이 경제적 이득을 취하기 위해서 보안을 강화할 수 밖에 없는 구조	**'비용'으로 인식되는 보안** 보안 투자가 비즈니스의 경쟁력이나 자산 가치 상승으로 이어지는 기전이 부족한 실정임. 인센티브(세제 혜택 등)나 강제적 페널티가 약하다 보니, 경영진에게 **보안은 '사고만 안 나면 되는 매몰 비용'으로 인식**되고 있음

'사이버 안보 기본법' 제정 하에 역할 재조명 >>

사이버 보험 생태계 구축 - 5대 핵심 과제

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

역할 주체자별 세부과제

	데이터 리더십 확보	리스크 평가 표준화	리스크 통제	시장 확대	사이버 복원력 증대
정부/감독기관 (역할 조율)	리스크 평가 계량화 기반 '참조요율' 구축	한국형 사이버 보안 표준 모델 수립	시스템 리스크 관리 및 재보험 전략 수립 -> 정부 협력 '국가 사이버 재난 보험 체계' 도입	공시 의무 강화 및 수요 창출을 위한 의무 보험 제도 단계적 확대	사이버 복원력 (Resilience) 중심의 서비스 확장 -> 보험의 역할을 '손해 보상'에서 '사고 복구 지원'으로 확대
보험사 및 파트너 (보상을 넘어선 '토탈 케어 서비스' 제공자)	제조업(OT 보안), 금융업, 서비스업 등 각 산업군이 직면한 고유의 위험 (생산라인 중단, 데이터 유실 등)과 재무적 상황 (기업의 규모별) 에 맞춤형으로 대응할 수 있는 상품 라인 구축				포렌식, 로펌, PR 업체 등이 포함된 디지털 긴급 대응팀 파트너십 구축
기업(가입주체) " 인식의 전환: 비용에서 투자로 "	사이버 보안은 단순히 IT 부서가 안고 있는 업무 과제가 아닌, 기업의 지속 가능성(ESG)과 직결된 경영상의 과제로 인식하고 사이버 보험 가입을 '리스크 전가(Risk Transfer)'의 핵심 수단으로 채택 보험사가 요구하는 사이버 보안 수준에 부응하는 과정 자체가 기업 자체의 보안 역량을 강화하는 프로세스로 활용할 수 있는 선순환 구조 수립				

추진 로드맵 일정 >>

참고: 추진 로드맵

단계별 세부 일정 (제안)

1단계 (~ 6개월)

Planning / Execution

- 시장 조사 및 현재 상태 분석
- 기업 인식제고 캠페인 파일럿 프로그램
- 사이버 안보 기본법 시행
- 기타 정책 도입을 위한 입법 연구 및 협의 (국회, 협회, 보험개발원, 금감원 등 중심으로 협의체 구성)

2단계 (7~12개월)

Execution

- 의무보험 및 인센티브 프로그램 시행
- 산업별 맞춤형 사이버 보험 상품 (리스크 경감 플랜) 론칭
- 기업 대상 사이버 보안 교육 및 훈련 프로그램 시행

3단계 (13~24개월)

Innovation

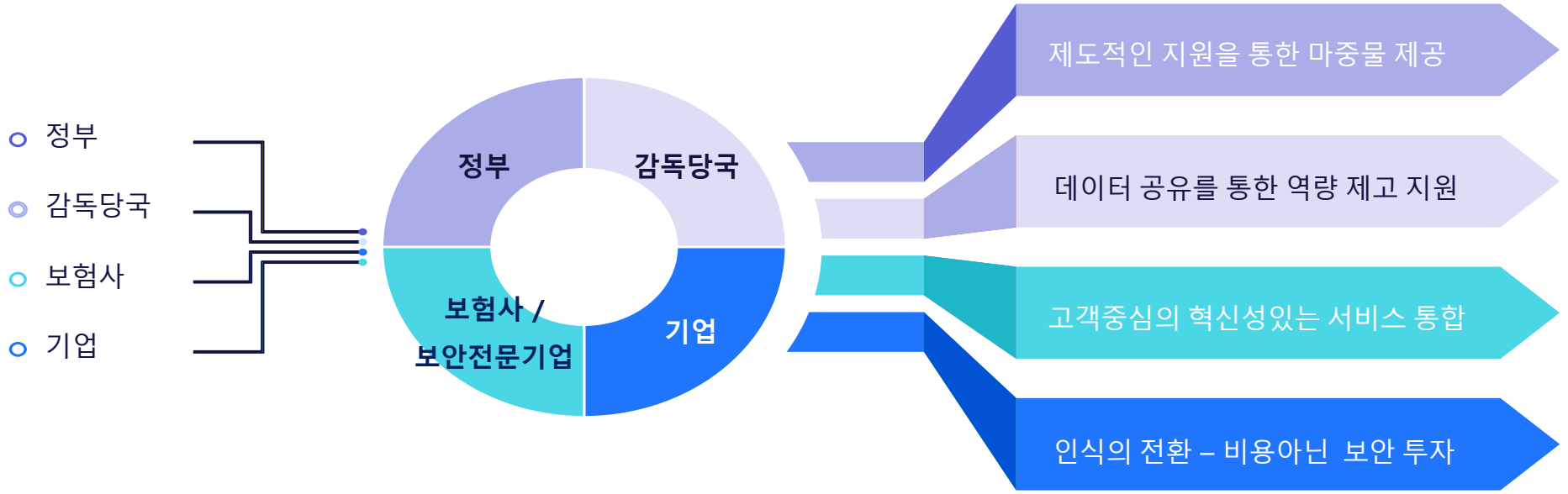
- 초기 프로그램 평가 및 최적화 방안 수립
- 인식개선 캠페인 지속 및 교육 프로그램 범위 확장
- 성공 사례 기반의 정책 고도화 및 추가 인센티브 발굴

Wrap-up:

"사이버 보험 생태계의 성패는 정부와 감독당국의 강력한 거버넌스를 중심으로 보험사, 보안 기업, 기업이 얼마나 유기적으로 연결되느냐에 달려 있음.

정부가 먼저 신뢰의 토대를 닦고 방향을 제시하는 중심축 역할을 수행할 때, 각 역할 주체의 실천력은 상호 보완적인 톱니바퀴처럼 맞물려 돌아갈 수 있음.

이러한 거버넌스 주도의 융합 체계하에 서로 유기적으로 연결된 생태계를 통해, 한국 사이버 보험 시장이 글로벌 표준과 함께 하는 새로운 전기가 마련되기를 희망함."



Thank you for your interest and attention!!

APPENDIX: 사이버 안보 기본법 핵심 내용

1 국가 사이버안보 컨트롤타워 명문화

- **내용:** 대통령 직속 또는 국가안보실 중심의 **'국가 사이버 안보위원회'** 설치를 명문화
- **목적:** 국정원(공공), 과기부(민간), 국방부(군), 경찰(수사)로 흩어진 지휘 체계를 하나로 묶어 사고 발생 시 즉각적인 통합 대응이 가능하도록 함

2 민관 합동 대응체계(통합대응센터) 구축

- **내용:** 국가 차원의 위협 인텔리전스를 실시간으로 통합 분석하는 **'국가 사이버 안보협력센터'**의 법적 근거를 마련
- **목적:** 미국 CISA의 JCDC처럼 민간 전문가와 정부 요원이 한 공간에서 협력할 수 있는 제도적 기반을 제공

3 민간 협력 시 '법적 면책권' 부여 (핵심 과제)

- **내용:** 민간 기업이 정부에 위협 정보를 공유하거나 공동 조사에 참여하는 경우, **영업비밀 누설 책임이나 개인정보 보호법 위반 등에 대한 면책** 조항을 명시
- **목적:** 기업들이 "정보를 줬다가 오히려 규제를 받거나 소송을 당할 수 있다"는 우려를 해소하여 자발적 참여를 유도

4 국가 핵심인프라 및 공급망 보안 강화

- **내용:** 에너지, 금융, 통신 등 국가 필수 서비스와 이를 지탱하는 SW 공급망에 대한 보안 점검 및 관리 의무를 강화
- **목적:** 민간 영역의 사고가 국가 안보 위기로 전이되는 것을 차단하기 위한 '최소한의 안전 기준'을 법제화

5 능동적 방어 (Active Defense)의 법적 근거

- **내용:** 위협 배후를 추적하고 공격 인프라를 무력화하는 등 능동적인 대응 활동에 대한 수행 주체와 범위를 규정
- **목적:** '방어' 위주의 수동적 대응에서 벗어나 국가 차원의 억지력을 확보하기 위한 행동의 정당성을 부여

APPENDIX: 2025-2026년 주요 정책 동향

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

1. 사이버 보험 의무화 및 실효성 강화

- 개인정보보호법 기반 의무 가입: 2024년 3월부터 시행된 개정『개인정보보호법』에 따라 일정 규모 이상의 개인정보 처리자는 손해배상책임보험 가입 의무화. 2025년 이후에는 보험 가입 여부 및 보상 한도의 적절성을 점검하는 사후 감독 강화
- 의무화 대상 확대 논의: 금융, 의료, 통신 등 국가 핵심 인프라 산업뿐만 아니라, 사고 발생 시 파급력이 큰 주요 IT 서비스 공급망 전반으로 의무 가입 대상을 확대해야 한다는 목소리가 커지고 있으며, 이를 위한 최저 보험가입금액 재검토 등이 활발히 논의 중

2. AI 기반 지능형 보안 정책 추진

- AI 위협 대응 체계 고도화: 과학기술정보통신부와 한국인터넷진흥원(KISA)은 2025년 사이버 침해 사고가 전년 대비 약 26% 급증함에 따라, 2026년을 'AI 기반 사이버 공격 대응의 원년'으로 삼고 선제적 대응 체계를 강화하고 있음
- 보안 실태 평가 지표 개정: 2026년도 사이버 보안 실태 평가는 인공지능 서비스 보안과 클라우드 취약점 관리 비중을 대폭 확대하여, 기업들이 실제 위협에 부합하는 보안 전략을 수립하도록 유도하고 있음

3. 민관 협력 기반의 '리스크 데이터 생태계' 조성

- 사이버 위협 정보 공유 플랫폼: 미국 CISA의 JCDC 모델을 벤치마킹하여, 정부(KISA), 기업, 보안 업체, 보험사가 실시간 위협 정보를 공유하고 익명화된 사고 데이터를 보험 상품 개발에 활용하는 데이터 풀링(Pooling) 체계 구축이 추진되고 있음
- 인센티브 구조 설계: 보험 가입 기업에 대해 법인세 공제, 세금 감면뿐만 아니라 사이버 사고 발생 시 과징금을 감경해 주는 등 보안 투자가 실질적인 재무적 이득으로 이어지도록 하는 정책적 유인책을 검토

4. 상위법 체계 및 거버넌스 정립

- 사이버 안보 기본법 추진: 부처별로 산재한 사이버 대응 체계를 하나로 묶기 위해 대통령 직속 또는 국가안보실 중심의 컨트롤타워를 명문화하는『사이버 안보기본법』제정 논의 지속
- 공급망 보안 가이드라인: 소프트웨어 구성 요소를 명시하는 SBOM(SW 성분표) 도입 권고 등을 통해, 제품의 보안 수준이 시장에서 가치로 인정받는 환경 조성을 목표로 하고 있음

전반적으로 정부는 단순 가이드를 넘어 '의무화 확대'와 '데이터 기반 요율 산출 지원'을 통해 2026년까지 국내 사이버 보안 시장 규모를 4조 원 이상으로 확대하고자 총력을 기울이고 있음

APPENDIX: 주체별 세부 추진 과제

정부 / 감독기관 (규제 및 인프라 지원)

- **핵심산업 의무화 입법** - 금융, 의료, 통신 등 핵심 인프라 산업부터 가입 의무화 후 점진적 확대
- **인센티브 제공:** 보험 가입 기업에 대한 세금 감면, 법인세 공제, 보안 사고 발생 시 과징금 감경 혜택 제공
- **민관 합동 데이터 풀링(Pooling):** 보험개발원, KISA, 금융보안원이 협력, 익명화된 사이버 사고 및 보험금 지급 데이터를 통합 관리
- **누적 위험 모니터링:** 특정 클라우드(CSP)나 소프트웨어 공급망에 집중된 위험을 시뮬레이션하고 보험사의 인수한도 설정 가이드 마련
- **국가 재보험:** 보험사가 단독으로 감당하기 어려운 거대 사이버 사고에 대해 정부가 일부 책임을 분담하는 국가 사이버 재보험 도입

기업 (리스크 관리 및 인식 제고)

- **제로 트러스트 도입:** '절대 신뢰하지 않고 항상 검증한다'는 원칙하에 보안 아키텍처를 현대화
- **보안 투자 및 교육 확대:** 사이버 보험을 단순 비용이 아닌 '비즈니스 연속성'을 위한 투자로 인식, 임직원 대상 모의 훈련 정례화
- **사고 데이터 공유 참여:** 익명화된 사고 데이터를 공유하여 산업 전체의 방어력을 높이는 데 기여

보험사/ 보안전문기업 (상품 내실화 및 서비스 확대)

- **AI 기반 리스크 평가:** AI 기반 기업별 보안 점수(Risk Index)를 바탕으로 적정 보험료 산출 역량 제고
- **사고 대응 패키지 개발:** 보안 점검, 포렌식, 로펌 연계 등 사고 복구 전 과정을 지원하는 '토탈 케어' 서비스 제공
- **SME 특화 상품 출시:** 중소기업의 부담을 경감하는 저가형 상품과 단체형 보험상품 개발
- **글로벌 재보험 협력 강화**: 코리안리 및 글로벌 재보험사와의 파트너십을 통해 선진 리스크 분산 기법 도입
- **24/7 헬프데스크 운영:** 사고 발생 즉시 전문가 지원을 받을 수 있는 전용 채널을 운영하여 피해 확산 최소화

APPENDIX: KISA 사이버 위협 동향 보고서

개선방안

현재 자료는 사고의 빈도(Frequency)는 보여주지만, **얼마나 큰 경제적 피해 (Severity)가** 있었는지는 파악하기 어려움

- **사고당 평균 손실액 부재:**
  서버 해킹 504건 중 실제 보상금이 나갈 만한 규모의 사고가 몇 건 인지, 평균 복구 비용은 얼마인지 알 수 없음
- **노출 지수(Exposure) 부족:**
  전체 기업의 숫자 대비 사고가 발생했던 비율을 알아야 '사고 발생 확률'을 계산하는데, 전체 모수 데이터가 없는 상황임
- **보안 수준별 차등 데이터 미흡:**
  백업 여부 정도는 나오지만, MFA(다요소 인증)나 EDR 도입 여부에 따른 사고율 차이 같은 구체적인 상관관계가 없는 점도 아쉬움

필요 통계 항목	리스크 모델링 활용 방안
사고 유형별 평균 복구 비용	사고당 예상 손실액(Severity) 산정 및 보상 한도 설정
비즈니스 중단 시간(Downtime)	기업휴지손해(BI) 담보의 적정 보험료율 산출
유출된 레코드당 단가	개인정보 유출 배상책임 리스크 측정
업종별/매출 규모별 사고율	타겟 업종별 기본 요율(Base Rate) 차등화
보안 컨트롤(MFA, ISMS 등) 효과	보안 우수 기업에 대한 할인율(Discount) 근거 마련
랜섬웨어 지급건수 비율 및 금액	랜섬웨어 보장담보의 손해율 예측

개선 방안

- **손실 데이터 표준화:**
  침해사고 신고 시 '피해 규모(추정치)'를 표준화된 항목으로 수집, 익명화된 통계로 제공
- **보험-보안 데이터 결합:**
  KISA의 침해사고 데이터와 보험사의 보험금 데이터를 결합한 **'사이버 리스크 데이터베이스'** 구축 필요
- **시나리오 기반 리스크 평가:**
  보고서에 나온 '공급망 공격'이나 '가상자산 탈취' 사례를 바탕으로, 대규모 연쇄 사고 발생 시의 **누적 리스크(Accumulation Risk)** 분석 모델이 포함되어야 함

Unlocking the Potential! - A Roadmap for a Pragmatic Cyber Insurance Ecosystem in Korea

최 용 민 (Yong-Min Choi)

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

Contents

EXECUTIVE SUMMARY

- The Korean cyber insurance market is currently trapped in a **vicious cycle** caused by low consumer interest, a lack of underwriting expertise and risk assessment capabilities among insurers, and insufficient infrastructure. This has led to a prolonged period of stagnant growth
- In contrast, global markets such as the US, Japan, and Australia are enhancing **Cyber Resilience** through government-led regulatory strengthening and private-sector adoption of "Active" technology-based insurance
- The biggest risk facing the Korean market today is that the same challenges identified a decade ago remain unresolved in 2026. We must now shift our paradigm from identifying **"What to do"** to executing **"How to do it.“**
- The revitalization of cyber insurance cannot be achieved by a single entity. It requires the **synchronized efforts of four key stakeholders:** 1) Government: establishing institutional catalysts, 2) Regulators: ensuring transparent data sharing, 3) Insurers: integrating innovative, customer-centric services, 4) Corporates: shifting internal perceptions of cyber risk
- Here, I propose a government-led **Strategic Roadmap** focused on three pillars: **Data Leadership** in the digital era, the establishment of **Standardized Models**, and the **Expansion of Mandatory Insurance**. The goal is to build a practical cyber insurance ecosystem that moves beyond simple loss compensation to integrate proactive accident prevention and recovery support

Recap: Key Past Presentation Topics

Implications of Recurring Challenges!

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

Early Formation Phase (2016–2018):
"Focus on regulatory frameworks and mandatory insurance discussions."

- "사이버 리스크와 보험의 역할: 글로벌 동향과 시사점" (2016, 보험연구원 조찬회)
- "개인정보보호 배상책임보험 의무가입 제도 도입을 위한 정책 공청회" (2016, 방송통신위원회/행정자치부)
- "개인정보보호 배상책임보험 의무가입 제도 도입 방안" (2016, 보험연구원)
- "사이버 리스크 관리 실태 및 보험산업의 대응 과제" (2017, 금융감독원 금융경영브리프)
- "사이버 리스크와 보험 산업의 대응 과제" (2017, 금융감독원 포럼)
- "4차 산업혁명과 사이버 보험 활성화를 위한 법적 쟁점" (2018, 한국보험법학회 정기학술대회)
- "4차 산업혁명 시대, 사이버 보험 활성화를 위한 법적 과제" (2018, 국회 세미나)
- "국내 사이버보험 시장의 현황과 **활성화** 저해 요인 분석" (2018, 보험연구원 세미나)

Expansion Attempt Phase (2019–2022):
"A period marked by recurring calls for more data and strategies to revitalize the market."

- "개인정보 손해배상책임 보장제도 시행에 따른 보험업계 대응 방안" (2019, 보험개발원 설명회)
- "사이버 보험 활성화를 위한 사이버 사고 데이터 공유 플랫폼 구축 방안" (2019, 한국화재보험협회 위험관리 포럼)
- "비대면 사회 확산에 따른 사이버 리스크의 재무적 전가 방안" (2020, 보험연구원 웹 세미나)
- "국내 중소기업의 사이버 보험 가입 실태와 정책적 지원 필요성" (2021, 중소기업 연구원/보안학회 합동 세미나)
- "랜섬웨어 공격 급증에 따른 사이버 보험의 역할과 한계" (2021, 보험정보학회)
- "국내 사이버보험 시장의 현주소와 발전 방향" (2022, 금융위원회 주관 회의)

New Threat Response Phase (2023–2025):
"Addressing emerging technologies (AI) and re-emphasizing the need for heightened risk awareness."

- "디지털 전환 시대, 사이버 보험 시장 활성화를 위한 정책 제언" (2022, 금융위원회 주관 사이버보험 포럼)
- "국가 핵심기반시설 사이버 보안 강화를 위한 보험 연계 방안" (2023, 한국인터넷진흥원(KISA) 주관 세미나)
- "생성형 AI 시대, 새로운 사이버 리스크와 보험의 대응" (2023, 사이버보안 포럼)
- "생성형 AI 기술 악용에 따른 사이버 리스크의 새로운 국면과 보험의 한계" (2024, 사이버 보안 컨퍼런스)
- "기업의 사이버 복원력(Cyber Resilience) 확보를 위한 민관 합동 보험 모델" (2024, 보험연구원/보안업계 공동 포럼)
- "디지털 전환 시대, 사이버 보험 가입 확대를 위한 인센티브 구조 설계" (2025 세미나)

Looking back: Why haven’t we moved forward? >>

Government-Led Cyber Strategy – Critical Gaps – Korea vs. Global Leaders

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

	USA / EU		KOREA
Legal Enforceability	미국의 사이버보안 행정명령(EO 14028)이나 EU의 사이버 복원력 법 (CRA)은 미준수 시 **공공 조달 배제**나 **과징금**을 부과	VS.	**가이드라인과 권고 위주의 전략**에 그쳐 기업 입장에서는 "지켜야 하겠지만, 안 지켜도 당장 큰일 나지 않는" 지침으로 인식되어 실행 동력이 미약한 상황
Security as a Biz Link	보안 수준이 낮다고 평가되면 보험 가입이 거절되거나 상장 조건에 결격 사유가 되는 등 **'시장 기제'**가 작동함	VS.	**보안 투자를 순수 비용**으로만 보며, 보험 가입이나 보안 인증이 실제 기업 가치 상승이나 비용 절감 (보험료 할인 등)으로 이어지는 연결고리가 보이지 않는 상황
Insurance linked risk mitigation	단순히 보험을 드는 것이 아니라, Zero Trust 등 **가이드라인 준수 여부를 보험료율과 직접 연동**하듯 정책이 기업의 '체질 개선'을 강제하는 동력으로 작동	VS.	현재 의무 보험은 사고 발생 시 **'배상'에 초점**이 맞춰져 있음. 보험 가입이 보안 투자의 끝이 아니라 시작이 되려면, 보안 사고 예방 활동(Hygiene)을 보험료 산정의 표준 지표**로** 강제하는 실행력이 더 구체화되어야 함
Status of Private Sector	민간 (빅테크 등)을 정부와 대등한 **'공동 방어자'**	VS.	민간은 여전히 정부의 관리·감독 대상이자 사고 시 보고 의무를 가진 **'수동적 주체'**

실행력 강화를 위한 개선 방안? >>

Need for a Paradigm Shift in Government Cyber Risk Governance

ProSyS Underwriting Solutions
Advanced Property Insurance Value Chain Process Solutions

Government Paradigm: USA vs. Korea

" The core of government's primary role is **institutionalizing a market mechanism** where security investment directly translates into **corporate financial value**."

	미국 – 주도적 시장 설계		한국 – 제도적 공백과 자율의 역설
구매력을 통한 시장 선도	미국 정부는 세계 최대의 IT 구매자임. **관련 행정명령(EO 14028)**을 통해 정부에 납품하기 위한 필요 기준을 명시하는데 이는 규제가 아니라 **'거래 조건'**이 되며, 기업은 정부라는 **큰 시장을 잃지 않기 위해 스스로 보안 투자**를 강화하고 있음	**공급망 통제력 부족**	미국처럼 강력한 구매력을 바탕으로 표준을 강제하기 보다는, **가이드라인 배포 수준**에 머물러 있어 민간 공급망 전체의 보안 수준을 상향 평준화 하는 데 한계가 있음
소프트웨어 투명성 제고 (SBOM)	식품의 영양성분표처럼 SW 구성 요소를 공개하도록 강제함. 이는 구매자가 제품의 위험도를 판단할 수 있게 하여, **'보안이 우수한 제품이 시장에서 더 비싸게 팔리거나 선택 받는'** 환경을 조성	**민간 자율의 한계**	자율성을 강조하지만, 실제로는 사고 발생 시 '과징금' 위주의 사후 처벌에 치중하고 있는 상황에서 시장 구성원들이 보안을 내재화할 수 있는 **경제적 유인 체계**가 설계되지 않고 있음
사이버 보험 시장과의 연계	정부는 **리스크 평가 표준을 제공하고, 보험사는 이를 바탕으로 기업의 보안 수준에 따라 보험료를 차등 산정**함. 보안 수준이 낮으면 금융 비용 (보험료)이 상승하는 상황으로, 기업이 경제적 이득을 취하기 위해서 보안을 강화할 수 밖에 없는 구조	**'비용'으로 인식되는 보안**	보안 투자가 비즈니스의 경쟁력이나 자산 가치 상승으로 이어지는 기전이 부족한 실정임. 인센티브(세제 혜택 등)나 강제적 페널티가 약하다 보니, 경영진에게 **보안은 '사고만 안 나면 되는 매몰 비용'으로 인식**되고 있음

'사이버 안보 기본법' 제정 하에 역할 재조명 >>