8 WEF, 경제적 복원력의 필수 조건으로 사이버보안 전략 제안

세계경제포럼(WEF)은 사이버보안을 경제적 복원력의 필수 요소로 다룰 것을 강조하고 조직 리더가 추진해갈 전략 방향과 실행과제를 제안하는 보고서*를 발표('26.10)

* Cybersecurity's Strategic Inflection Point: A Senior Leadership Agenda for 2027

○ **(개요)** 조직들이 여전히 사이버보안 전략적 투자가 아닌 기술 비용으로 인식하고 있음을 지적하면서, 조직 리더를 위한 전략 방향과 '27년의 실행과제를 제안

- 결제·생산·공공 서비스·공급망을 지탱하고 경제성장의 기반 인프라를 뒷받침하는 디지털 시스템에 장애가 발생하면 그 영향은 개별 조직을 넘어 국가·산업 전반의 경제적 충격으로 확산될 수 있다고 강조

  ※ 일례로, '24년 2월 미국 의료 행정 서비스 업체 체인지 헬스케어(Change Healthcare)를 대상으로 한 랜섬웨어 공격은 미국 의료 시스템 전반에 광범위한 차질을 빚었고, 그 결과 모기업인 유나이티드헬스 그룹(UnitedHealth Group)은 '24년 한 해 동안 약 31억 달러 규모의 비용 발생 및 사업 운영 차질을 감수

- 그러나 아직도 다수의 조직에서 사이버보안은 기술적 비용으로만 취급되는 경우가 많아 그 경제적 중요성이 사이버보안 관련 투자·측정·거버넌스에 충분히 반영되지 못하고 있다고 지적

- WEF 글로벌 미래 사이버보안 위원회*는 설문조사, 사례 분석, 전문가 인터뷰 등을 실시·종합해 이러한 문제를 파악하고, 의사결정자를 위한 과제를 제안

  * Global Future Council on Cybersecurity: WEF 사이버보안 센터에서 사이버 복원력을 높이고 혁신적인 사이버보안 전략을 발굴하기 위해 운영하는 국제 전문가 싱크탱크 커뮤니티

○ **(사이버보안 인식)** 민간·공공 부문 경영진·관리자에 대한 설문조사 결과는 사이버보안의 경제적 중요성이 의사결정 과정에 적절히 반영되지 못하고 있음을 시사

※ 설문조사는 '26년 4월 실시되어 110건의 응답을 받았는데, 응답자의 60%가 라틴아메리카·카리브 지역에 소재해 결과의 일반화에는 주의가 필요

- 응답자의 42%는 사이버보안이 경제적 산출물, 시장, 공급망에 측정 가능한 영향을 미친다는 점을 인지하고 있었으나, 사이버보안을 '경제 안정화 장치'로 인식하고 있다고 답한 응답자는 9%에 불과

- 또한 응답자의 절반 이상은 사이버보안에 투자하게 된 계기로 '위기 사건 발생'을 꼽았고, '입증된 투자 성과'를 지목한 응답 비율은 8%

○ **(전략 방향)** 최고 의사결정자가 추진해야 할 전략 방향으로 ▲의사결정자 공통의 언어 정립 ▲'생산적 자본'으로 사이버보안 인식 ▲사이버보안 역량 및 경제효과 측정·평가 지표 마련 ▲지속가능한 재원 조달을 제시

〈 전략 방향 4가지 〉

구분	주요 내용
공통 언어 정립	• 주요 의사결정자들을 위해 사이버 위험에 대한 공통의 언어를 정립 – '사이버 리스크'는 위협과 취약성으로 인한 손실·중단 가능성, '사이버 복원력'은 중단을 예상하고 견디며 적응·복구하는 역량으로 구분 • 이러한 공통 언어는 특히 위기 상황에서 중요하게 작용
'생산적 자본'으로서의 사이버보안	• 사이버보안에 대한 투자를 단순히 피해를 방지하기 위한 수단이 아니라, 사업 성과와 혁신을 뒷받침하는 '생산적 자본'으로 간주 – 사이버보안 투자는 재무·운영 상 위험 노출을 줄이고, 비즈니스 생태계 전반의 신뢰를 강화하며, 디지털 전환을 촉진하고, 거버넌스 및 조직 문화를 개선함으로써 여러 측정 가능한 가치들을 창출
사이버보안 역량 및 경제 효과 측정·평가	• 사이버 사고의 경제적 파급효과와 복구 역량을 기관·국가·산업 간 비교 가능한 형태로 측정해 의사결정에 활용 • 특히 ▲서비스 연속성 ▲복구 역량의 신뢰성 ▲의존성 집중도 ▲극단적 손실 위험 노출도 ▲사이버보안 투자를 통해 보존한 경제적 가치 ▲사이버보안 태세가 자본비용에 미치는 영향의 6가지 지표를 사용 – 이들 지표는 사이버 복원력을 평가하고 경제적 의사결정에 사이버 보안 태세를 반영할 수 있는 비교 가능한 기준을 제공
지속가능한 재원 조달	• 자원이 부족한 국가·조직의 보안 취약성이 디지털 생태계 전체의 위험으로 번질 수 있으므로 보안 역량과 핵심 인프라에 대한 장기 지원체계를 마련 – 개인 기부, 기업 기부, 다자간 기금, 공동 기금 메커니즘이 공통의 원칙 아래 연계하는 체계로서 '지속가능 사이버보안 금융 메커니즘(Sustainable Cybersecurity Finance Mechanism)'을 구축하는 것이 바람직

○ **('27년 실행과제)** 전략 방향이 지금부터 실제 조직의 의사결정 및 운영에 반영될 수 있도록 기업·정부·금융기관 지도부가 추진해야 할 5가지 조치를 제안

- **(공통 언어 채택)** 사이버 복원력 논의를 기술 용어에서 벗어나 경제적 영향과 책임 등에 대한 언어로 전환하고, 이사회 보고 등에서 위험에 처한 대상, 영향받는 서비스, 복구 시간, 경제적 노출 규모, 책임 주체 등을 명확히 제시
- **(보고 개선)** 이사회·공공 부문 보고에 사이버 투자의 경제적 가치와 복구 역량을 나타내는 지표들을 포함해 투자 판단과 감독의 근거를 강화
- **(금융 관련 의사결정에 반영)** 사이버보안 태세를 자본 배분과 금융 조건에 반영해 보안 투자의 경제적 유인을 강화
- **(지속가능한 재원 확보)** 취약 국가·조직·소기업의 사이버 대비 태세를 민간·시민사회의 복원력 강화 관점에서 접근해 지속가능한 재원 조달 경로를 마련
- **(복원력 상설 의제화)** 주요 기관 경제·금융안정 논의에서 사이버 복원력을 상설 의제로 삼아 대형 사고 이후에만 관심을 기울이는 대응 방식에서 탈피

출처 : 세계경제포럼(WEF) (2026.10.6.)
https://reports.weforum.org/docs/WEF_Cybersecuritys_Strategic_Inflection_Point_2026.pdf