Deloitte.

Together makes progress

글로벌 사이버의 미래 서베이 2026 (5th Edition)

사이버 보안의 5가지 패러독스

[서베이 개요]

딜로이트 **‘글로벌 사이버의 미래 서베이 2026’**은 **전 세계 43개국, 5개 산업군 및 23개 세부 산업에 속한 비즈니스·기술 리더 1,058명을 대상으로 수행된 설문조사** 결과를 기반으로 한다. 또한 사이버 보안 및 디지털 리스크 분야에 대한 전문성을 보유한 **9명의 C-Level 경영진 인터뷰를 함께 반영**하여 글로벌 사이버 보안 환경 변화와 기업 대응 방향을 종합적으로 분석하였다.

본 보고서는 기업들의 사이버 보안 역량 수준을 ‘사이버 보안 신뢰도 및 실행 지수(Cybersecurity Confidence and Action Index)’를 기준으로 평가하였으며, 응답 기업을 크게 세 그룹으로 분류하였다.

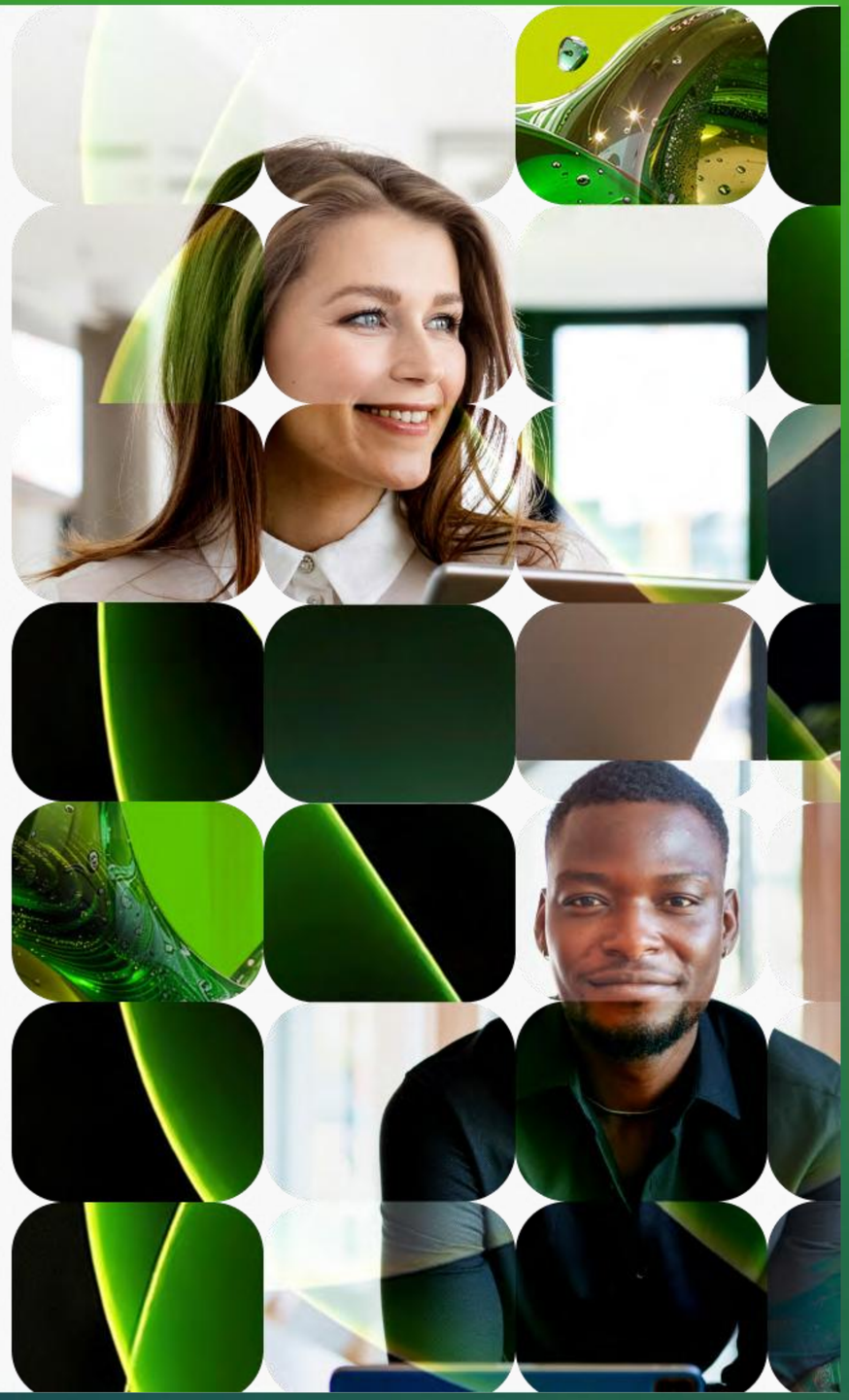
가장 높은 수준의 신뢰도와 실행 역량을 보유한 ▲‘Frontrunner’, 중간 수준의 대응 역량을 보이는 ▲‘Follower’, 그리고 상대적으로 낮은 수준의 준비도와 실행력을 나타낸 ▲‘Foundation Builder’이다.

평가 항목에는 사이버 보안 투자 효과 측정을 위한 리스크 정량화 도구 활용, 디지털 공급망 전반의 제3자 리스크 관리 수준, 연례 업데이트 및 테스트가 이루어지는 침해사고 대응 체계 구축 여부, 산업별 보안 표준 및 규제와의 정합성 확보 등 핵심 사이버 보안 실행 영역이 포함되었다. 특히 본 지수는 기업이 15개 주요 사이버 보안 활동을 어느 수준까지 실행하고 있는지, 그리고 8개 핵심 사이버 보안 전략에 대해 어느 정도의 신뢰도를 보유하고 있는지를 종합적으로 반영하여 산출되었다.

[3개 그룹 구성 비율]

FRONTRUNNER	FOLLOWER	FOUNDATION BUILDER
17%	60%	24%

*반올림으로 인해 총합이 정확히 100%가 되지 않을 수 있음



PARADOX #1

높아진 사이버 보안 자신감, 그러나 준비 수준은 충분한가?

사이버 보안 리더들은 신뢰와 확신을 확보하는 데 상당한 진전을 이루어 왔다.

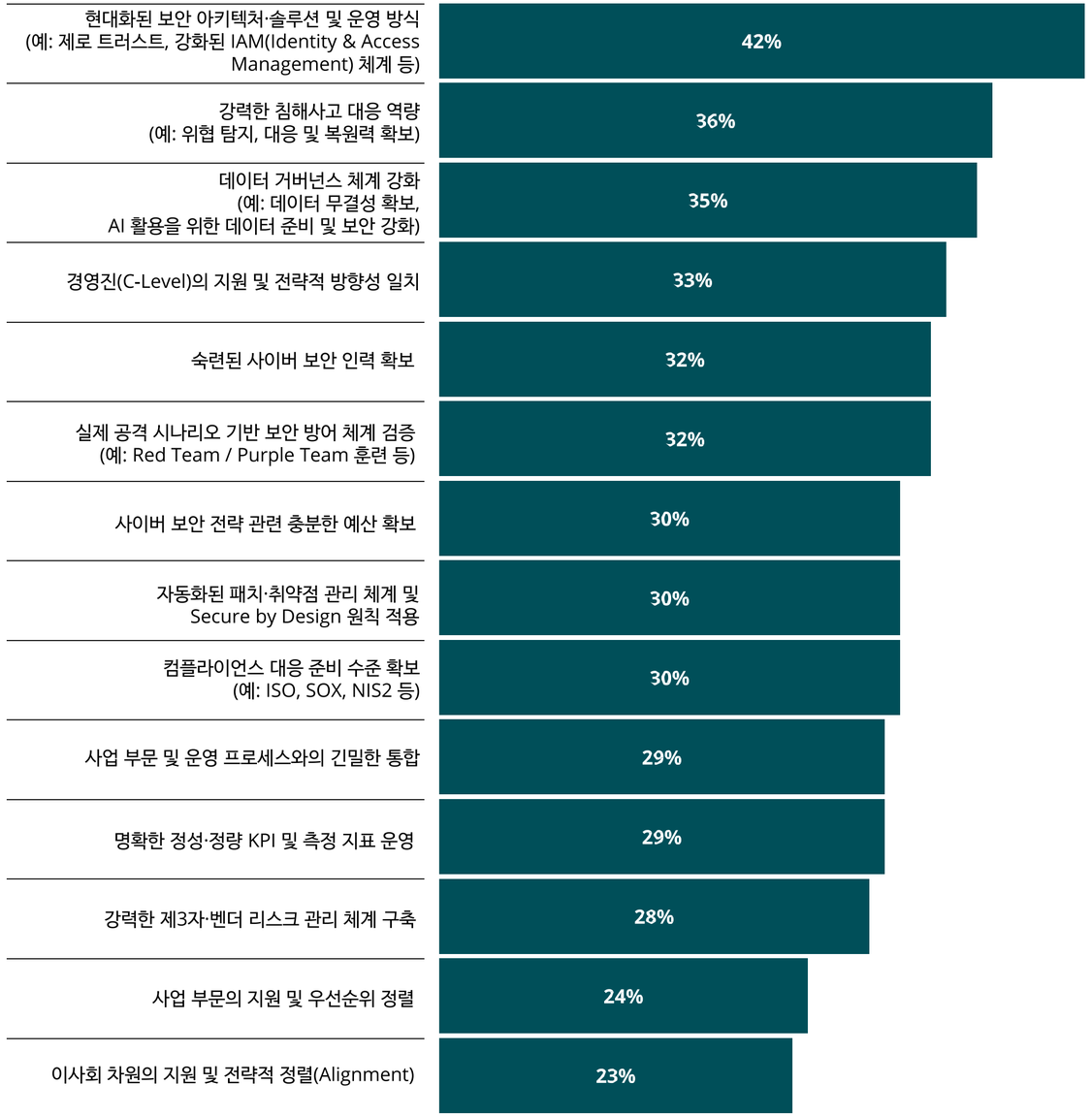
조사 응답자들은 최고정보보호책임자(CISO) 역할이 조직 내에 안정적으로 정착되고 있으며, 사이버 보안 전략 역시 조직 전반의 다양한 기능과 업무 영역에 통합되고 있다고 평가하였다.

C-Level 경영진 전반에서는 사이버 전략이 실질적인 비즈니스 가치 창출에 기여할 수 있다는 인식이 확대되고 있었으며, 기업들은 점차 사이버 보안을 긍정적인 사업 성과 창출 관점에서 접근하고 있는 것으로 나타났다. 전체 응답자의 85%는 자사의 사이버 보안 전략에 대해 '다소 자신 있음' 또는 '매우 자신 있음'이라고 응답했으며, 그 배경으로 현대화된 보안 아키텍처, 강력한 침해사고 대응 역량, 데이터 거버넌스 체계 등을 주요 요인으로 제시하였다.

아울러 응답자들은 C-Level 경영진의 높은 관심과 지원, 그리고 선제적 대응을 가능하게 하는 충분한 예산 확보 수준에 대해서도 긍정적으로 평가하였다. 이러한 변화는 사이버 보안이 단순 IT 운영 영역을 넘어 기업의 핵심 경영 활동과 통합되고 있다는 점에서도 확인된다.

응답자의 54%는 사이버 보안을 전사 비즈니스 및 기술 전략에 완전히 통합했거나, 미래 전략 수립 과정에 사이버 요구사항을 적극 반영하고 있다고 답했다. 이처럼 기업들의 자신감은 일정 수준 실질적인 역량 강화와 조직적 성숙도를 기반으로 형성되고 있다. 다만 한편으로는, **일부 기업들이 실제 준비 수준 이상으로 사이버 보안 역량을 과신하고 있는 것은 아닌지 점검이 필요한 시점**이기도 하다.

[조직의 사이버 보안에 대한 자신감 형성 주요 요인]



[표본 수: 1,058]

미래 사이버 위협에 대한 조직의 실질적 대응 준비 수준에는 여전히 우려가 존재한다.

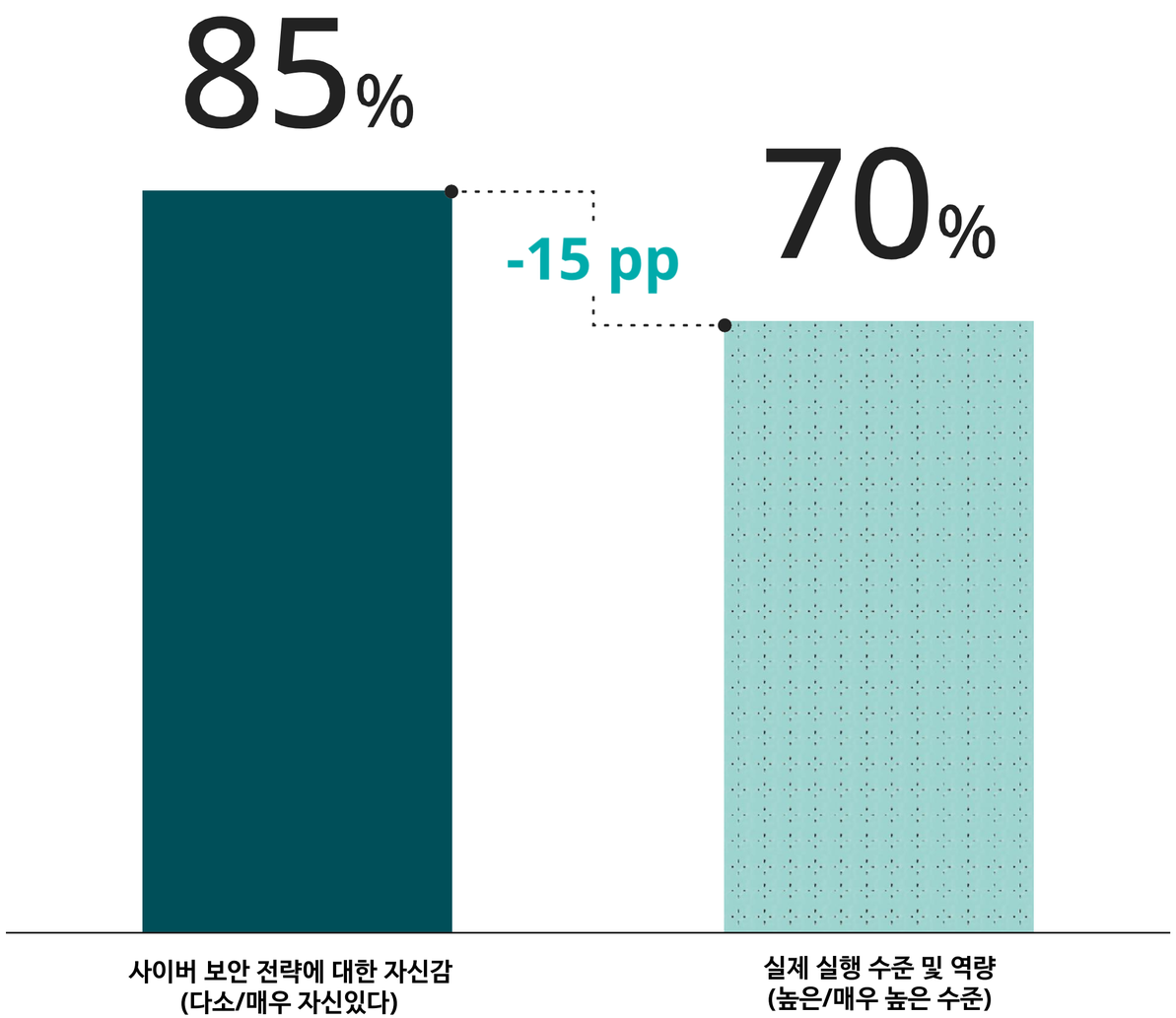
응답 기업들의 사이버 보안 준비 수준(Cyber Readiness)을 측정하기 위해, 본 조사에서는 다양한 사이버 보안 실행 항목을 제시하고 각 활동이 조직 내에서 어느 수준까지 구현되고 있는지를 평가하였다. 그 결과, 응답자의 70%는 주요 사이버 보안 활동을 '매우 높은 수준' 또는 '높은 수준'으로 운영하고 있다고 답해 전반적으로 높은 준비 수준을 나타냈다.

그러나 이러한 결과를 사이버 보안 전략에 대한 신뢰 수준과 비교해 보면 유의미한 격차가 확인된다. 응답자들은 평균적으로 **실제 준비 수준보다 약 15%p 더 높은 자신감을 보이고 있었으며, 이는 기업들의 인식과 실제 실행 역량 사이에 일정 수준의 차이가 존재할 가능성을 시사**한다.

한 글로벌 헬스케어 기업의 CISO는 이에 대해 다음과 같이 설명하였다.

"우리는 필요한 수준의 투자와 경영진의 지원을 받고 있으며, 적절한 도구와 프로세스도 갖추고 있다. 그러나 규모가 큰 조직일수록 위협 환경과 리스크를 이해하는 것과, 실제로 모든 통제 체계가 완벽하게 작동해 중대한 사고 가능성을 완전히 차단하고 있다고 확신하는 것은 전혀 다른 문제이다."

[기업의 자신감 VS 실행 역량 사이의 갭]



[표본 수: 1,058]

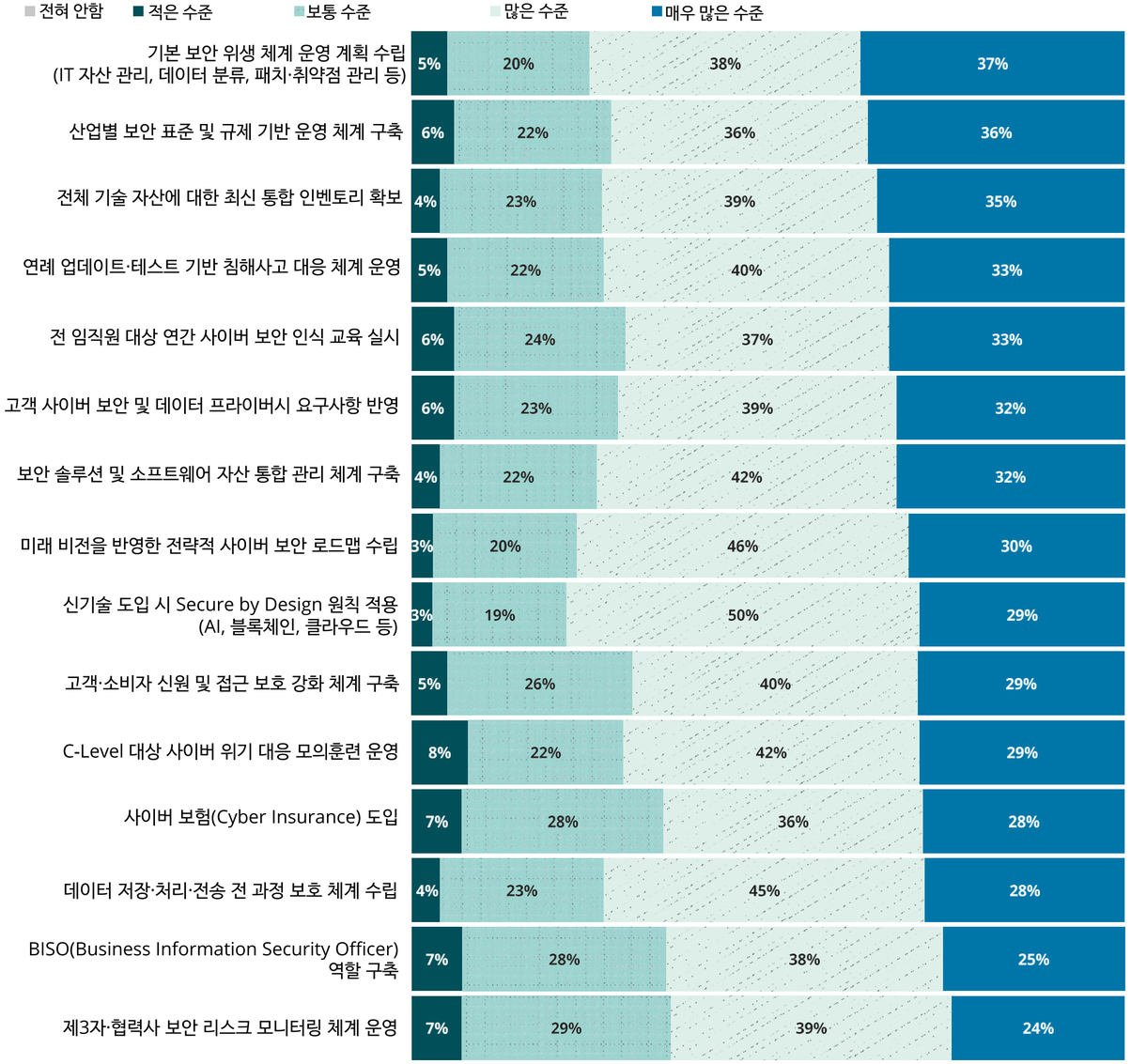
응답자들은 이사회 차원의 지원과 필요한 예산을 확보하고 있으며, 지금까지 조직이 이뤄낸 성과에 대해서도 자신감을 보이고 있다. 그렇다면 미래의 위협과 과제에 대비하는 과정에서 왜 더 높은 수준의 사이버 보안 준비도(Cyber Readiness)를 나타내지 못하고 있는 것일까? 이번 조사에서는 특히 **네 가지 주요 결과**가 그 이유를 보여준다.

우선, 비즈니스와의 연계 부족 문제가 지적되었다. 많은 응답자들은 **자사 조직이 아직 BISO(Business Information Security Office, 비즈니스 정보 보안 기능을 하는 부서) 역할을 구축하지 못했다고 답했다**.

BISO는 성숙한 사이버 보안 전략의 핵심 요소로 점점 더 중요하게 인식되고 있다. 그러나 해당 역할을 '높은 수준' 또는 '매우 높은 수준'으로 도입했다고 응답한 비율은 **63%에 불과**했으며, 이는 많은 조직들이 비즈니스 영역과 사이버 보안·리스크·복원력 운영을 연결하는 메커니즘을 아직 충분히 갖추지 못하고 있음을 시사한다.

또한 제3자(Third-party) 사이버 리스크 관리 역량 역시 충분히 활용되지 못하고 있는 것으로 나타났다. 응답자들은 점점 더 많은 기술 벤더에 의존하고 있다고 답했지만, 조직의 보안 상태(Security Posture)를 모니터링하고 추적하기 위한 제3자 사이버 리스크 관리 역량을 어느 정도 도입했는지에 대한 질문에서는 다른 사이버 보안 활동 대비 가장 낮은 수준의 평가가 나타났다. 실제로 해당 역량을 '높은 수준' 또는 '매우 높은 수준'으로 구현했다고 응답한 비율은 **65%에 불과**했다. 이는 충분히 완화되지 않은 잠재적 리스크가 존재할 가능성을 보여준다.

[사이버 보안 관련 경영 활동의 실행 정도]



[표본 수: 1,058]

**** 반올림 기준 적용에 따라 총합이 100%와 일치하지 않을 수 있음(이하 자료 동일).**

응답자들에게 사이버 이슈에 민첩하게 대응하는 데 가장 큰 제약 요인을 질문한 결과, **숙련된 사이버 보안 인력 부족 문제가 최상위 수준으로 지목**되었다. 전체 15개 과제 가운데 가장 높은 비중의 응답자들이 이를 핵심 제약 요인으로 선택했으며, 실제로 10%의 응답자는 이를 가장 큰 제한 요소로 꼽았다. 이는 사이버 보안 준비도를 확보하는 데 있어 전문 인력과 역량 확보가 얼마나 중요한 요소인지를 보여준다.

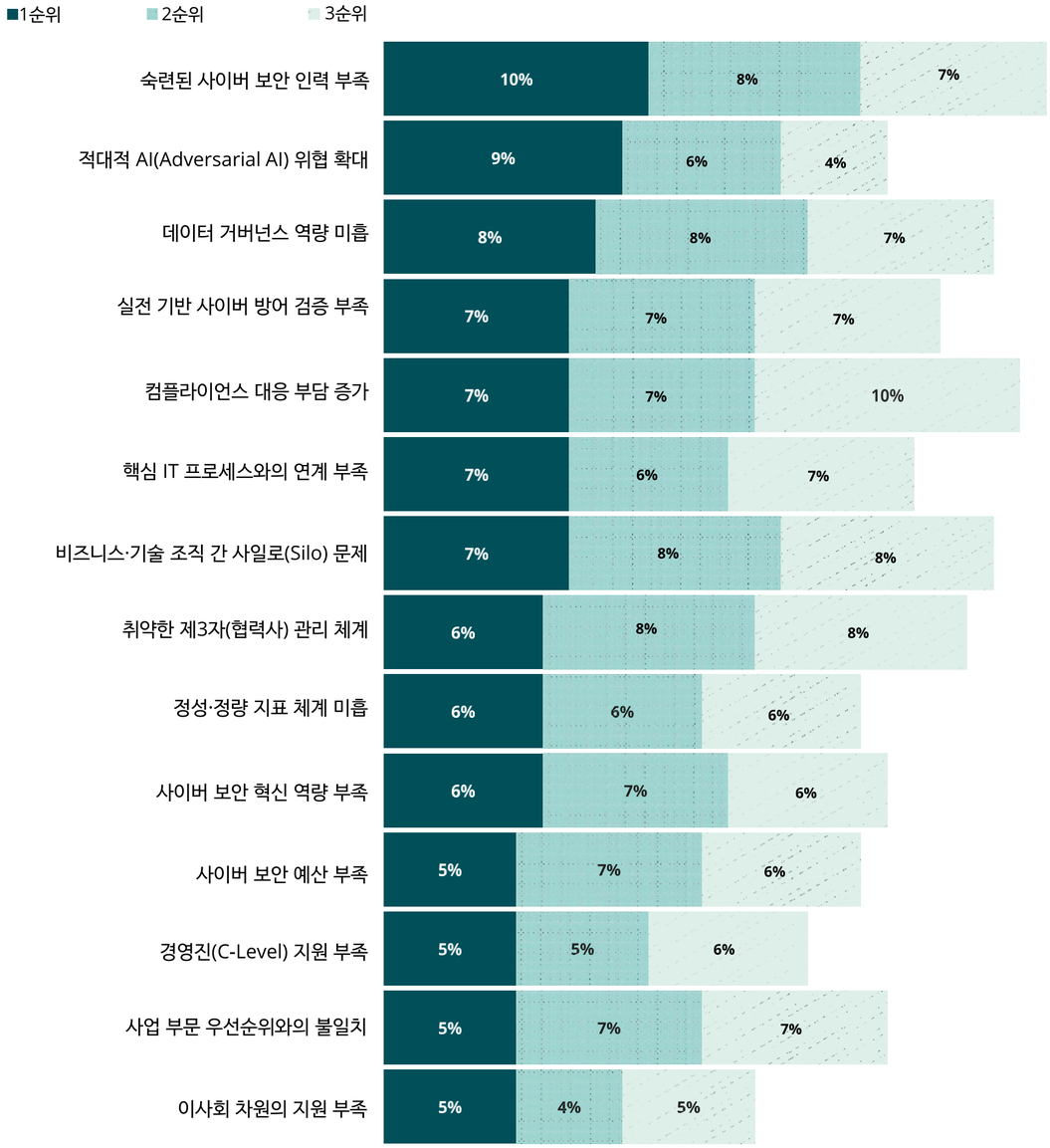
한편, 빠르게 진화하는 **위협 환경** 역시 기업들의 부담을 가중시키고 있다. 특히 **적대적 AI(Adversarial AI)**는 공격자가 AI 시스템의 취약점을 노리거나, 고도화된 AI 기술을 활용해 공격을 수행하는 방식을 의미한다. 응답자들은 이러한 적대적 AI를 사이버 대응 민첩성을 저해하는 두 번째 주요 요인으로 평가했으며, 이는 기업들이 급변하는 기술 환경과 AI가 초래할 수 있는 예측 불가능한 신규 위협에 얼마나 효과적으로 적응할 수 있을지에 대해 상당히 우려하고 있음을 시사한다.

이 외에도 사회공학 공격(Social Engineering), 딥페이크(Deepfake), 합성 신원(Synthetic Identity), 허위정보(Misinformation), 데이터 오염(Data Poisoning) 등이 대표적인 사례로 언급되었다.

한 글로벌 의료기술 기업의 글로벌 보안 담당 부사장은 이러한 위협의 진화 양상을 다음과 같이 설명하였다.

“일부 AI 시스템은 탐지된 이후에도 스스로 형태를 변화시키며 악성코드처럼 대응 체계를 회피할 수 있다. 이후 또 다른 형태의 악성코드로 변형되기도 한다. 이는 결국 대규모 자동화 공격으로 이어질 수 있다. 따라서 이에 대응하기 위해서는 방어 역시 자동화되어야 한다. 만약 공격자들이 에이전틱 AI 기반 공격 군집(Attack Swarm)을 활용한다면, 방어 측 역시 공격 패턴을 학습할 수 있는 고도화된 AI 기반 방어 체계를 갖춰야 한다.”

[사이버 보안에 제약이 되는 요인]



[표본 수: 1,058]

패러독스 분석 및 해결 전략

사이버 보안에 대한 높은 자신감과 실제 준비 수준 간의 격차는, 전략과 비전을 실제 실행으로 연결하는 과정에서 가장 잘 드러난다. 기업들은 지난 수년간 사이버 보안 이니셔티브를 위한 경영진 차원의 지원과 예산 확보에 성공해 왔으며, 사업 부문과 함께 전략 수준의 사이버 계획을 수립·추진해 왔다. 그러나 아직까지 사이버 보안 원칙, 프로세스, 기술을 **조직 전반의 운영 수준까지 깊이 확산시키지는 못한 것으로 나타났다**.

즉, 기업들은 사이버 이슈를 조직 차원에서 추진할 수 있다는 자신감은 가지고 있지만, 실제 준비도를 확보하기 위해 필요한 실행 메커니즘은 아직 충분히 구축하지 못한 상황이다. 그렇다면 전략 수준의 성과를 현업 실행 수준으로 연결하기 위해 리더들은 어떤 다음 단계를 준비해야 할까? 이번 조사 결과와 심층 인터뷰, 특히 높은 자신감과 준비 수준을 동시에 보유한 기업들의 사례는 몇 가지 핵심 방향을 제시한다.

우선 BISO(Business Information Security Officer) 역할 도입을 고려할 필요가 있다. BISO는 사이버 보안 조직과 비즈니스 조직을 연결하는 핵심 가교 역할을 수행할 수 있으며, 사이버 전략을 실제 사업 실행으로 연결하려는 기업에게 매우 중요한 기능으로 평가된다. 실제로 많은 기업들은 제품(Product), DevOps, 아키텍처 조직과 긴밀하게 연계하기 위해 보안 아키텍트 및 BISO 역할을 조직 내에 배치하고 있다고 응답했다.

또한 외부 전문 파트너(Third Party)의 전략적 역량 활용 역시 중요하게 제시되었다. 많은 기업들은 자체적으로 수행하기 어려운 반복적·시간집약적 업무를 자동화하거나 운영하기 위해 외부 파트너를 활용하고 있으며, 이러한 관계는 점차 단순 운영 지원을 넘어 전략적 협업 관계로 발전할 수 있다.

즉, 제3자 파트너는 강력한 사이버 보안 체계를 구성하는 핵심 요소로 자리잡고 있다. 한편 신규 위협 대응에서는 우려와 실제 리스크 사이의 균형 있는 접근이 필요하다는 점도 강조되었다. 조사에서는 적대적 AI(Adversarial AI)에 대한 우려 수준이 매우 높게 나타났지만, 현재 시점에서의 실질적 리스크 대비 우려가 과도한 측면도 존재하는 것으로 분석되었다.

인터뷰에 참여한 응답자들 역시 적대적 AI의 불확실성과 예측 어려움에 대한 부담을 언급했다. 기업들은 이미 '알려진 위험(known unknowns)'에 대해서는 대응 경험을 축적해 왔지만, '알려지지 않은 위험(unknown knowns)'에 대해서는 상대적으로 더 큰 불안감을 느끼고 있다는 것이다.

현재 시점에서는 생성형 AI 환경에서 발생할 수 있는 데이터 유출, 민감정보 오남용과 같이 보다 현실적이고 즉각적인 리스크 대응이 더욱 중요할 수 있다. 따라서 기업들은 적대적 AI에 대한 과도한 불안에 집중하기보다, 실제 투자 필요 수준을 냉정하게 판단하면서 보다 시급한 과제들에 대한 대응 역량을 지속적으로 강화할 필요가 있다.

"우리는 필요한 수준의 투자와 경영진의 지원을 받고 있으며, 적절한 도구와 프로세스도 갖추고 있다. 그러나 규모가 큰 조직일수록 위협 환경과 리스크를 이해하는 것과, 실제로 모든 통제 체계가 완벽하게 작동해 중대한 사고 가능성을 완전히 차단하고 있다고 확신하는 것은 전혀 다른 문제이다."

— 글로벌 헬스케어 기업 CISO

PARADOX #2

경영진은 사이버 보안을 핵심 전략으로 인식하고 있지만, 조직 전반의 영향력은 아직 제한적이다.

최고경영진 차원의 공감대와 지원은 이미 확보되었다.

사이버 보안은 이제 기업 최고경영진 차원의 핵심 우선순위로 자리잡고 있다. 특히 'Frontrunners' 그룹은 CISO가 CEO, C-Level 경영진, 이사회와 매우 긴밀한 관계를 구축하고 있다는 점에서 차별화된다(90% 이상).

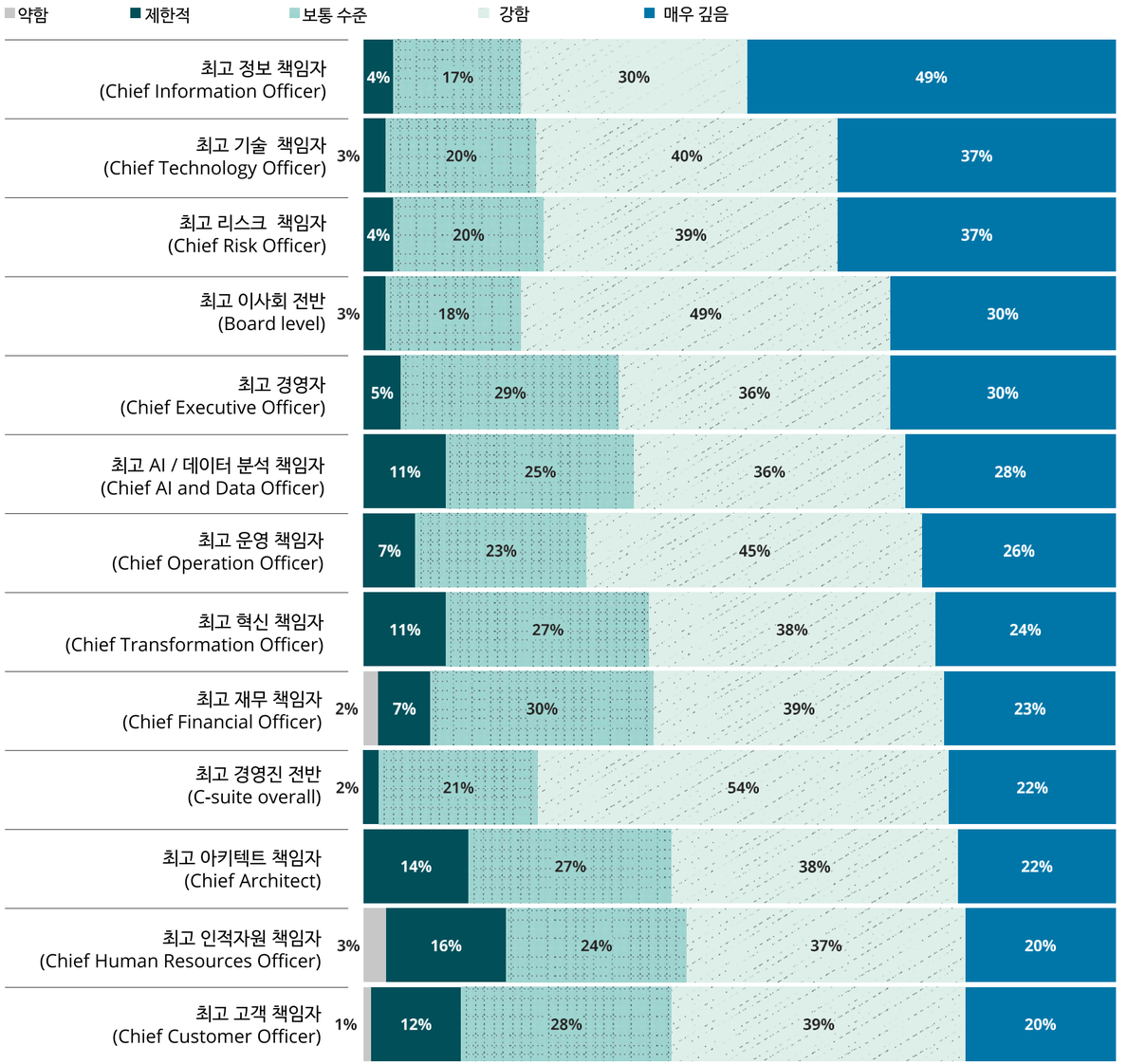
반면 'Followers' 그룹의 CISO는 이사회 및 CIO와의 관계가 상대적으로 강한 수준(각 80%)으로 나타났으며, 'Foundation Builders' 그룹에서는 CIO와의 관계가 가장 높은 수준(72%)을 보였다.

응답자의 66%는 자사 CISO가 CEO와 강력한 협력 관계를 구축하고 있다고 답했으며, 76%는 C-Level 경영진 전반과의 관계 역시 긴밀하다고 응답했다. 이는 미래 사이버 위협 대응 준비 수준을 강화하는 핵심 기반 요소로 평가된다. 또한 상당수 CISO는 CEO(28%) 또는 CIO(33%)에게 직접 보고하는 구조를 갖추고 있어, 최고경영진과의 직접적인 의사결정 연결 체계를 확보하고 있는 것으로 나타났다.

아울러 응답자의 절반 이상(54%)은 사이버 보안을 전사 비즈니스 및 기술 전략에 완전히 통합했거나, 미래 전략 수립 과정에 사이버 요구사항을 적극 반영하고 있다고 답했다. 특히 'Frontrunners' 그룹은 핵심 IT 전략(61%)과 전사 비즈니스 전략(57%) 양측에서 사이버 보안이 공동 의사결정자(Co-owner) 또는 핵심 추진 역할을 수행하고 있다고 응답한 비율이 높게 나타났다. 이는 'Followers'(각 43%, 29%) 및 'Foundation Builders'(각 31%, 15%) 대비 현저히 높은 수준이다.

다만, 이러한 경영진 차원의 강력한 지원에도 불구하고, 많은 기업들은 사이버 보안 원칙과 요구사항을 **일상적인 운영 프로세스와 현업 의사결정 수준까지 확산시키는 데에는 여전히 어려움을 겪고 있는 것**으로 나타났다.

[CISO와 다른 최고경영진과의 관계 수준]



[표본 수: 1,039]

PARADOX #2

사이버 보안의 영향력은 아직 전략적 비전 단계에서 실행 단계로 확장되지 못하고 있다.

대부분의 기업에서 경영진 내부적으로는 사이버 보안에 대해 강한 공감대가 형성되어 있다. 그러나 많은 조직들에게 남아 있는 다음 과제는, **사이버 보안을 핵심 사업 부문과 기술 기능 전반에 구조적으로 통합**하는 것이다.

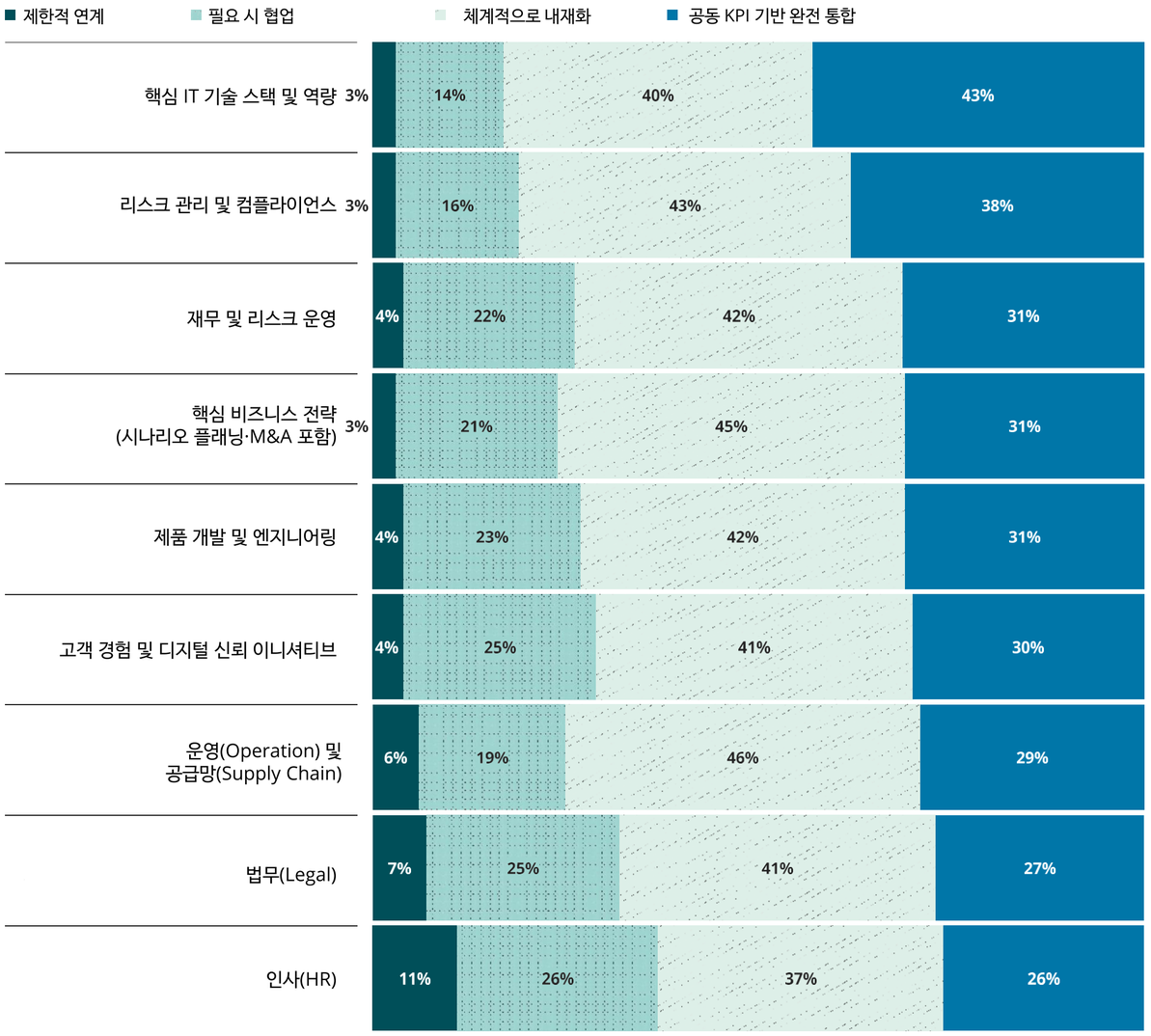
특히 사업 부문 단위에서의 실행력은 사이버 전략이 실제 성과로 이어지는 데 있어 핵심 요소로 평가된다. 조사 결과에 따르면, 9개 주요 영역 가운데 사이버 보안은 핵심 IT 및 리스크 관리 관련 전략과 프로세스에서 가장 큰 영향력을 미치는 것으로 나타났다. 두 영역 모두에서 응답자의 80% 이상은 비즈니스와 사이버 보안 간 강력한 협업 체계를 구축하고 있다고 답했다. 반면, 사이버 보안은 전사 비즈니스 전략 및 기타 기능 영역에서는 상대적으로 그 영향력이 제한적인 것으로 나타났다.

한편 'Frontrunners' 그룹의 다수는 사이버 보안을 전사 전략 전반에 완전히 통합하고 있다고 응답했으며, 특히 전사 리스크 관리(ERM) 전략 영역에서는 비즈니스 전략과 사이버 보안을 연결하는 핵심 메커니즘을 거의 모두 갖추고 있는 것으로 나타났다(96%).

한 금융서비스 기업의 그룹 CISO는 이러한 변화 방향에 대해 다음과 같이 설명하였다.

"CISO의 목표는 기존의 전술적·기술적 역할에서 벗어나, 새로운 접근 방식을 통해 비즈니스와 더욱 긴밀하게 연계되는 방향으로 전환하는 것이다. 특히 비즈니스 수익 가치사슬(Value Chain) 관점에서 위협 모델링과 리스크 평가를 수행할 수 있어야 하며, 이것이야말로 경영진이 실제로 중요하게 생각하는 부분이다."

[사이버 보안이 다른 비즈니스 영역과 연계된 정도]



[표본 수: 1,058]

사이버 보안은 아직 **기술 기반 제품 개발 영역에까지 충분한 영향력을 발휘하지 못하고 있는 것**으로 나타났다. DevSecOps는 비교적 높은 수준의 성숙도를 달성했으며, 응답자의 78%는 자사 사이버 보안 리더가 DevSecOps 운영 체계에 공식적으로 통합되어 있다고 답했다. 그러나 실제로 공동 KPI와 책임 체계를 기반으로 한 '실질적 공동 운영(Joint Ownership)'이 이루어지고 있다고 평가한 비율은 40%에 불과했다.

이러한 결과는 사이버 보안 조직이 CTO, Chief Architect 등 조직의 핵심 기술 통제 메커니즘을 담당하는 리더들에게 아직 충분한 영향력을 미치지 못하고 있기 때문으로 해석된다. 이들은 제품 엔지니어링, 애플리케이션 설계, 보안 기능의 구조적 통합을 이끄는 핵심 역할을 담당하고 있으며, 전략적으로 매우 중요한 협업 대상이다.

현재 대부분의 CISO는 이러한 영향력 부족 문제를 해결할 수 있는 보고 체계와 조직 관계를 충분히 확보하지 못한 상황이다. 실제로 응답 결과를 보면, CTO와 깊고 신뢰 기반의 관계를 구축하고 있다고 답한 CISO는 37%에 불과했다. CTO는 기술 개발과 실행을 주도하는 핵심 파트너임에도 불구하고 협업 수준은 제한적이다.

마찬가지로 조직의 미래 기술 구조를 설계하는 Chief Architect와 깊은 신뢰 관계를 형성하고 있다고 응답한 비율 역시 22%에 그쳤다. 이러한 결과는 앞서 제시된 '사이버 자신감과 실행 준비도 간 격차', 즉 전략과 실행 사이의 간극이 여전히 존재하고 있음을 다시 한번 보여준다.

"CISO의 역할은 단순히 전술적·기술적 대응에 머무르는 것이 아니라, 새로운 접근 방식을 통해 비즈니스와 더욱 긴밀하게 연결되는 방향으로 전환되어야 한다. 특히 비즈니스 수익 가치사슬 관점에서 위협 모델링과 리스크 평가를 수행할 수 있어야 하며, 이것이야말로 경영진이 실제로 중요하게 여기는 부분이다."

— 금융서비스 기업 그룹 CISO

패러독스 분석 및 해결 전략

모든 의사결정에 사이버보안 고려
대부분의 기업들은 이미 일정 수준의 사이버 보안 기반 체계를 갖추고 있다. 예를 들어 DevSecOps 원칙과 프로세스는 광범위하게 도입되고 있다. 그러나 사이버 보안이 기술 아키텍처에 실질적으로 내재화되기 위해서는, 엔지니어링 조직과 보안 조직 간 공동 책임(Co-ownership)과 공동 성과지표(Shared KPI)를 기반으로 시스템이 설계되어야 한다.
이는 초기 설계 단계부터 보안 원칙을 반영하는 ‘Secure by Design’ 접근 방식의 핵심 개념이기도 하다.

이러한 구현은 단순히 강력한 보안 체계를 구축하거나 형식적 체크리스트를 충족하는 수준만으로는 충분하지 않다.
보안 원칙이 내재화된 엔터프라이즈 아키텍처를 구현하기 위해서는 조직 전체가 단순히 프로세스를 따르는 사고방식에서 벗어나, 민첩성과 회복탄력성 확보 같은 '공동의 성과'를 지향하는 방식으로 전환해야 한다. 이를 위해서는 사이버 보안이 조직 전반의 프로세스 초기 단계부터 반드시 참여해야 한다.

CISO와 Chief Architect 간 전략적 협력 강화 필요
현재 많은 조직에서 CISO는 제품 엔지니어링, 애플리케이션 설계, 기술 기능 전반에 사이버 보안 원칙을 내재화할 수 있을 만큼 Chief Architect와 충분한 전략적 관계를 구축하지 못하고 있는 것으로 나타났다. 그러나 이러한 관계는 자연스럽게 강화되지 않으며, CISO는 핵심 이해관계자인 Chief Architect와 보다 긴밀한 협업 체계를 구축하기 위한 명확한 계획을 마련할 필요가 있다. 이를 통해 미래에 개발되는 기술과 솔루션에 보안 체계가 설계 단계부터 직접 반영될 수 있어야 한다.

한 글로벌 헬스케어 기업의 CISO는 다음과 같이 설명하였다.

“과거에는 중앙집중형 엔터프라이즈 아키텍처 조직이 존재했지만, 이후 CTO 조직 아래로 분산되면서 추진 동력이 약화되었다. 이에 우리 팀은 아키텍처 보안 검토 위원회(Security Review Board)를 구축했고, 이를 기술 조직이 자유롭게 자문을 받을 수 있는 공간으로 운영하기 시작했다.”

조직 핵심 우선순위와 책임 리더 간 연계 강화
현재 조직의 핵심 우선순위는 무엇이며, 이를 주도하는 책임 리더는 누구인가? 이러한 질문에 대한 답은 CISO를 비롯한 사이버 보안 리더들이 앞으로 어떤 조직 및 리더와 가장 긴밀한 관계를 구축해야 하는지를 보여주는 실질적인 방향성이 될 수 있다. 예를 들어 조직이 고객 중심(Customer-focused) 전략을 강화하고 있다면, 사이버 보안 책임자 역시 고객 데이터, 고객 경험(Customer Experience), 프라이버시 등 핵심 논의 과정에 반드시 참여해야 한다. 이러한 비즈니스 핵심 영역과의 연결은 사이버 보안의 영향력을 단순 전략 수준을 넘어 실제 사업 운영 영역까지 확장시키는 중요한 기반이 될 수 있다.

실제 조사 결과에서도 이러한 효과는 뚜렷하게 나타난다. 'Frontrunners' 그룹의 CISO 중 61%는 IT 운영 표준 수립 과정에서 공동 의사결정(Co-ownership) 역할을 수행하고 있었으며, 솔루션 설계 및 위협 모델링에 대한 자문 지원 영역에서도 선도적인 수준을 보였다. 실제로 Frontrunner 그룹 CISO의 52%는 이러한 핵심 기술·비즈니스 이니셔티브에 직접 참여하고 있는 것으로 나타났다.

소프트 스킬 역량 강화 필요
CISO를 비롯한 사이버 보안 리더들은 일반적으로 뛰어난 기술적·전략적 역량을 기반으로 현재 위치에 오르게 된다. 그러나 조직 내 다른 부문과 효과적으로 협업하고 영향력을 확대하는 능력은, 과거 역할에서는 상대적으로 덜 중요했던 이른바 '소프트 스킬(Soft Skills)'에 크게 좌우된다.

즉, 경청과 커뮤니케이션 역량을 갖추고 있는지, 다양한 조직 및 리더들과 공감대를 형성할 수 있는지가 점점 더 중요해지고 있다. 이러한 역량은 사이버 보안을 단순한 규제나 장애 요소가 아니라, 비즈니스 성장을 지원하는 핵심 동력(Business Enabler)으로 조직 구성원들에게 설득하는 데 직접적인 영향을 미친다.

"과거에는 최고기술책임자(CTO) 산하에 중앙집중형 엔터프라이즈 아키텍처 조직이 있었지만, 이후 조직이 분산되면서 추진 동력이 약화되었다. 이에 우리 팀은 아키텍처 보안 검토 위원회(Security Review Board)를 구축했고, 이를 기술 조직이 자유롭게 자문과 지원을 받을 수 있는 공간으로 운영하기 시작했다."

— 글로벌 헬스케어 기업 CISO

PARADOX #3

“벤더는 더 줄여야 한다.”
VS
“오히려 더 늘려야 한다.”

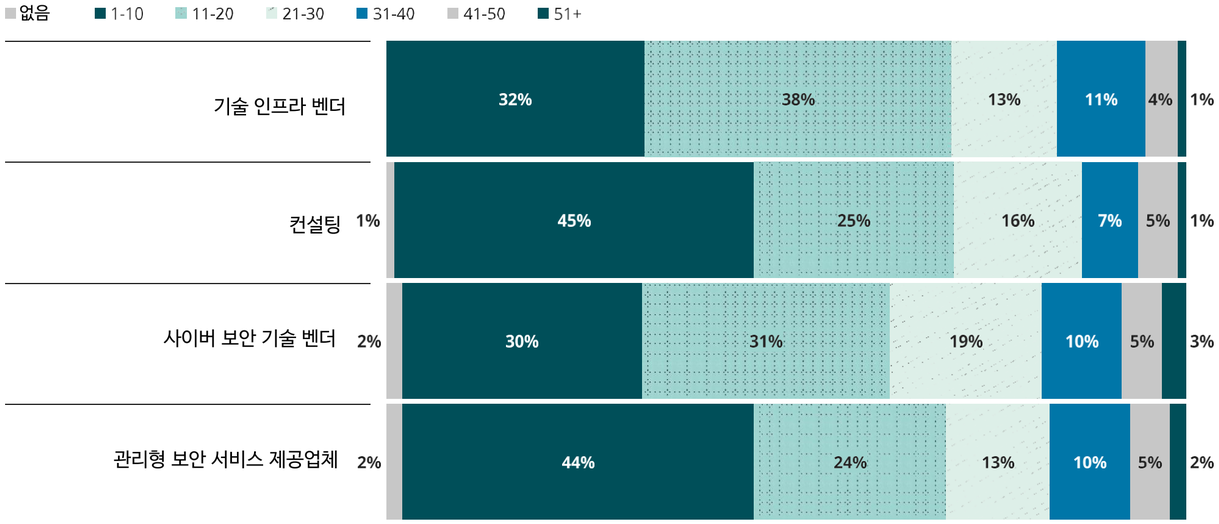
과도한 벤더 숫자

끊임없이 변화하는 위협 환경과 빠르게 진화하는 보안 솔루션·기술 역량으로 인해, 사이버 보안 조직은 점점 더 많은 벤더와 협력 관계를 구축하고 있다. 이러한 흐름은 당분간 지속될 것으로 전망된다. 실제로 응답자들은 이미 관리 부담이 상당한 수준으로 다수의 벤더와 협업하고 있다고 답했으며, 향후 3~5년 내 그 수는 더욱 증가할 것으로 예상하고 있다.

기술 인프라 영역에서는 가장 높은 비중의 응답자(38%)가 11~20개의 벤더와 협력하고 있다고 답했으며, 29%는 21개 이상의 벤더를 운영 중인 것으로 나타났다. 인터뷰 결과에 따르면 많은 기업들은 **플랫폼 중심 운영 체계로 전환하기 위해 벤더 수를 줄이고 싶어 하지만, 현재 기술이 미래 요구사항까지 충분히 충족하지 못할 경우 추가 벤더 도입이 불가피할 수 있다는 인식도 존재**했다.
일부 기업들에게는 다수의 벤더를 유지하는 것 자체가 전략적 선택이기도 하다. 특정 벤더에 대한 집중도를 낮춰 '벤더 집중 리스크(Vendor Concentration Risk)'를 회피하기 위한 목적이다.

반면, 통합 효율성과 운영 복잡성 감소를 위해 벤더 수를 줄이려는 기업들조차도 지나친 통합은 새로운 단일 장애 지점(Single Point of Failure)을 만들 수 있다는 점을 우려하고 있다.

[사이버 보안 관련 파트너 숫자]



[표본 수: 1,058]

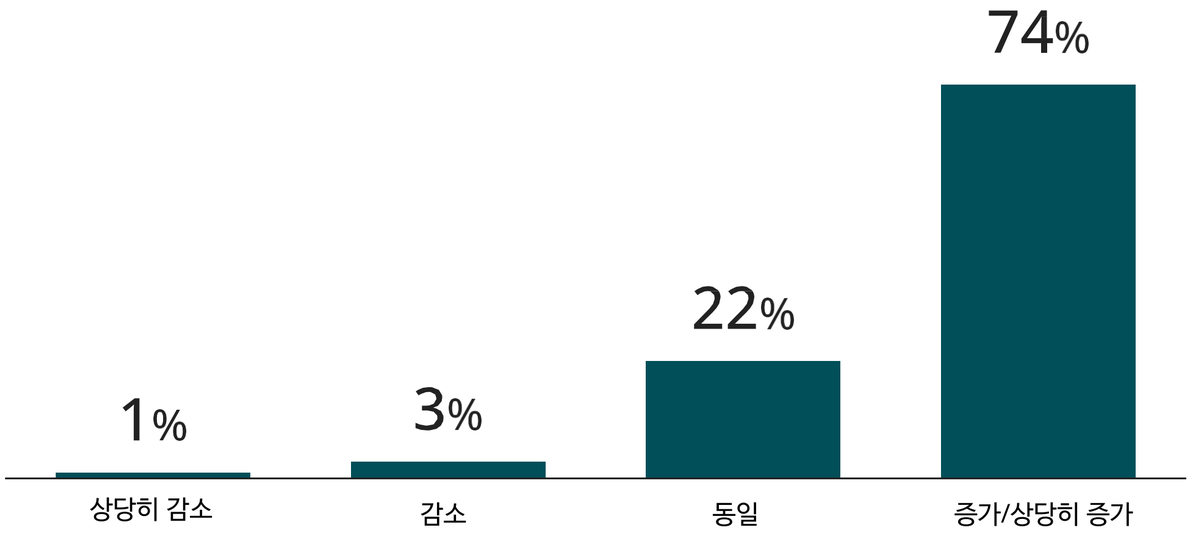
확대되는 벤더 포트폴리오
이미 상당수의 벤더를 운영하고 있음에도 불구하고, 응답자들은 지난 1년 동안 벤더 수가 증가하거나 크게 증가했다고 답했으며, 향후 1~5년 이내에 더 많은 벤더에 의존하게 될 것으로 전망하고 있다. 실제로 응답자의 74%는 자사가 협력하는 사이버 보안 파트너 수가 지난 1년간 증가 또는 크게 증가했다고 응답했다.

한 금융서비스 기업의 CISO는 이에 대해 다음과 같이 설명하였다.

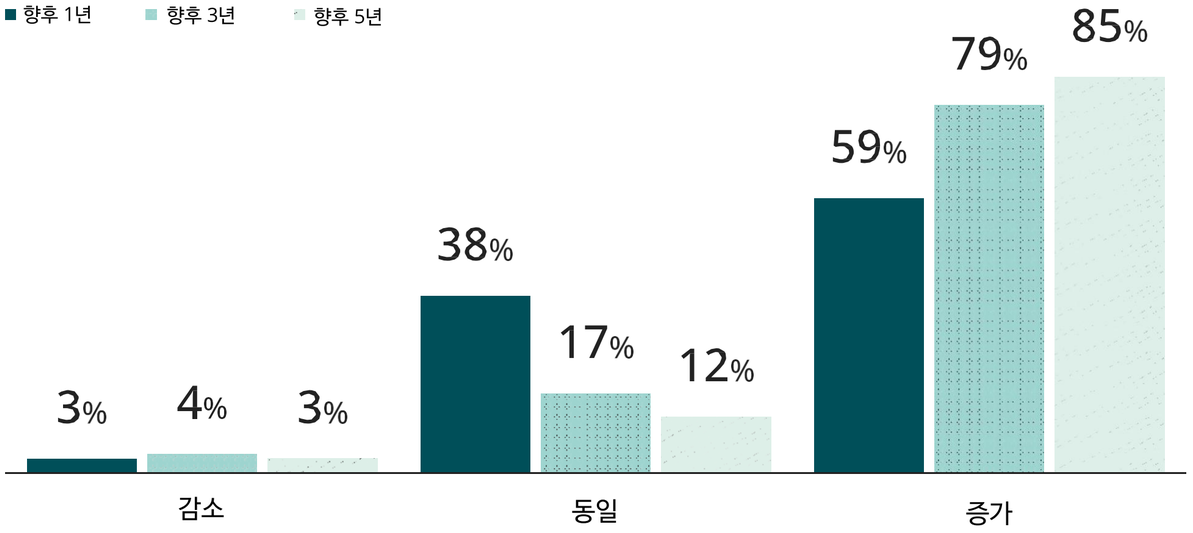
“우리는 새로운 사이버 보안 솔루션 제공업체들을 추가로 도입했으며, IT 조직 역시 인프라 운영 관리를 위해 더 많은 파트너와 협력하고 있다. CIO 조직도 마찬가지로 애플리케이션 운영을 위해 추가 솔루션과 외부 파트너를 확대하고 있다.”

향후 전망 역시 비슷한 흐름을 보였다. 향후 1년 동안 사이버 보안 파트너 수가 현재 수준에서 유지될 것이라고 답한 비율은 38%에 불과했으며, 대부분의 응답자들은 앞으로 벤더 수가 지속적으로 증가할 것으로 예상했다. 실제로 응답자의 79%는 향후 3년 내 벤더 수가 증가하거나 크게 증가할 것으로 전망했으며, 5년 기준으로는 그 비율이 85%까지 확대되었다.

[사이버 보안 관련 파트너사 증감(전년 대비)]



[사이버 보안 관련 파트너사 증감 예상 (향후 1~5년)]



[표본 수: 1,058]

무엇이 이러한 벤더 증가를 이끌고 있는가?

AI 확산으로 신규 벤더 수요 증가
이미 많은 벤더와 협업하고 있음에도 불구하고, 기업들은 새로운 기술 역량 확보와 신흥 리스크 대응을 위해 신규 전략 파트너를 지속적으로 도입하고 있다. 특히 AI는 지난 1년간 사이버 역량 고도화를 이끈 핵심 요인으로 작용하였다. 응답자의 약 75%는 실시간 위협 분석과 디지털 인프라 모니터링을 위한 고급 추론 기능을 기존 사이버 프로그램에 반영하기 위해 시스템을 업데이트했다고 답했다. 또한 76%의 응답자는 AI 기능을 서비스에 적용한 사이버보안 벤더와 협업하고 있다고 밝혔다.

사이버 보안은 아직 기술 스택에 충분히 통합되지 못함
현재 사이버보안 기능이 기술 스택 전반에 고도로 통합되어 있다고 보는 응답자는 약 30% 수준에 그쳤다. 이는 중복된 아키텍처 구조가 존재할 가능성을 시사하며, 보다 간결한 엔터프라이즈 아키텍처를 기반으로 벤더 통합 및 효율화(vendor rationalization & consolidation)를 추진할 여지가 있음을 의미한다.

“우리는 회사에 사이버보안 솔루션을 제공하는 새로운 외부 파트너들을 추가했고, IT 부문 역시 인프라 서비스 운영을 위해 더 많은 파트너를 도입했다. CIO 조직도 마찬가지다. 애플리케이션 팀을 위해 더 많은 솔루션과 외부 업체를 추가하고 있다.”

— 금융서비스 기업 Group CISO

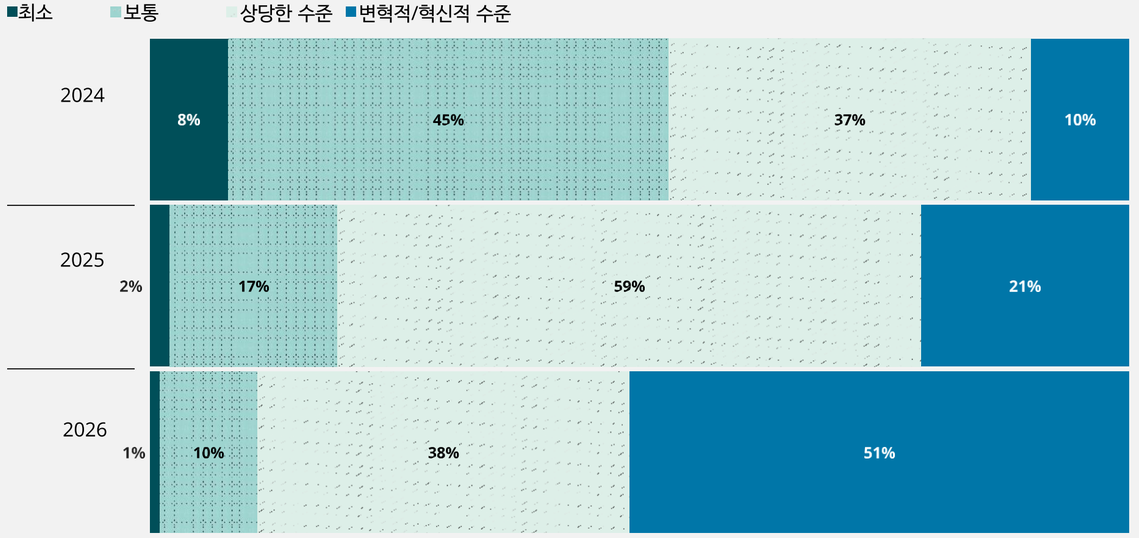
응답자들은 통합형 사이버보안 플랫폼 (integrated cyber platform)으로의 전환이 2024년 대비 2026년에 약 5배 증가했다고 보고했다.

이전 조사(2024년)에서는 응답자의 단 10%만이 자사 조직이 통합형 사이버보안 플랫폼(integrated cyber platform)으로의 전환을 혁신적(transformational) 수준으로 추진하고 있다고 답했다. 그러나 2025년에는 이 비율이 21%로 두 배 이상 증가했으며, **2026년에는 응답자의 51%가 이러한 통합 플랫폼이 혁신적 변화를 가져올 것으로 예상**하고 있다. 이는 통합 플랫폼 중심으로 시장의 흐름이 빠르게 이동하고 있음을 보여준다.

그렇다면 왜 통합형 사이버 플랫폼으로의 전환 속도가 빨라지고 있는 것일까?
전통적인 요인으로는 운영 복잡성 감소와 총소유비용(TCO) 절감이 있다.
일부 기업들은 여러 개의 전문 솔루션(best-in-class niche providers)을 개별적으로 운영하는 대신, '충분히 우수한(good-enough)' 단일 플랫폼으로 통합하는 방식을 선호하고 있다.

여기에 AI 역시 중요한 촉진 요인으로 작용하고 있다. 사이버 및 기술 리더들은 AI가 효과적으로 작동하기 위해서는 일관되고 표준화된(normalized) 데이터가 필요하다는 점을 인식하고 있으며, 플랫폼은 이러한 데이터를 제공하는 데 유리한 구조를 갖고 있다.
특히 에이전틱 AI(agentic AI) 전략을 추진하는 기업들에게 통합 플랫폼은 에이전트 기반 워크플로우 구축에 필요한 표준화된 데이터 모델을 제공할 수 있다는 점에서 핵심 기반으로 주목받고 있다.

[통합형 사이버보안 플랫폼으로의 전환을 추진하는 정도]



[표본 수: 1,043]

패러독스 분석 및 해결 전략

벤더 확산은 불가피한가?
현재로서는 그렇게 보일 수 있다. 위협 환경이 계속 변화하고 있으며, 이에 대응하기 위한 새로운 도구와 기술 역량이 끊임없이 요구되고 있기 때문이다. 충분한 예산과 경영진의 지원을 확보한 기업들은 새로운 보안 벤더를 지속적으로 추가하며 대응 역량을 확대하고 있다. 이러한 상황에서 플랫폼 기반 접근 방식의 매력은 더욱 커지고 있다. 통합 플랫폼은 운영 부담(overhead)이 상대적으로 낮고, 전문 벤더들이 제공하던 다양한 기능을 상당 부분 포함할 수 있으며, 여러 기술을 더 낮은 총소유비용(TCO)으로 통합할 수 있기 때문이다.

벤더의 실제 가치와 잠재력을 재평가
오늘날 벤더는 사이버 전략의 핵심 구성 요소이다. 그러나 기업은 각 벤더가 현재 어떤 가치를 제공하고 있는지, 어디에서 기능 중복이 발생하는지, 혹은 추가적인 전략적 가치를 창출할 수 있는지를 명확히 이해하고 있는가? 이를 파악하기 위해서는 전략적·의도적·리스크 기반의 체계적인 벤더 평가 체계가 필요하다. 그렇지 않으면 벤더 포트폴리오의 실제 효율성과 기여도를 정확히 판단하기 어렵다.

엔터프라이즈 아키텍처 관점에서 핵심 벤더와 중복 영역 식별
기업들은 그동안 사업 부문과 지역별로 발생하는 즉각적인 리스크에 대응하기 위해 새로운 벤더를 추가해 왔다. 그러나 이러한 방식은 장기적으로 중복 투자를 초래할 수 있다. AI 관련 솔루션 확산 역시 대표적인 사례이다. 기업은 엔터프라이즈 아키텍처 팀과 긴밀히 협력하여 어떤 벤더가 미션 크리티컬한지, 어떤 영역에서 통합·효율화(consolidation)가 가능한지를 식별해야 한다. 또한 중복 기능을 제거하고, 효율화 및 통합 기회를 지속적으로 검토할 필요가 있다.

플랫폼의 비용·효율성 이점 그 너머의 가치 모색
플랫폼 확산은 단순히 비용 절감과 운영 효율성 때문만이 아니다. AI 활용 확대, 데이터 전환(data transformation), 에이전틱 워크플로우(agentic workflow) 재설계 등 다양한 요인이 플랫폼 중심 전략을 가속화하고 있다. 특히 에이전틱 AI에 대한 관심이 급증하는 상황에서 플랫폼은 표준화된 데이터, 통제 체계, 통합 기능을 제공할 수 있으며, 동시에 벤더 통합 및 최적화 전략을 지원하는 핵심 기반으로 자리잡고 있다.

PARADOX #4

사이버 침해는 지속적으로,
꾸준하게 발생하고 있다.
다만, 그로 인한 비즈니스 영향은
일정 수준 내에서 통제되고 있다.

사이버 침해는 이제 피할 수 없는 '상시 리스크'가 되었다.

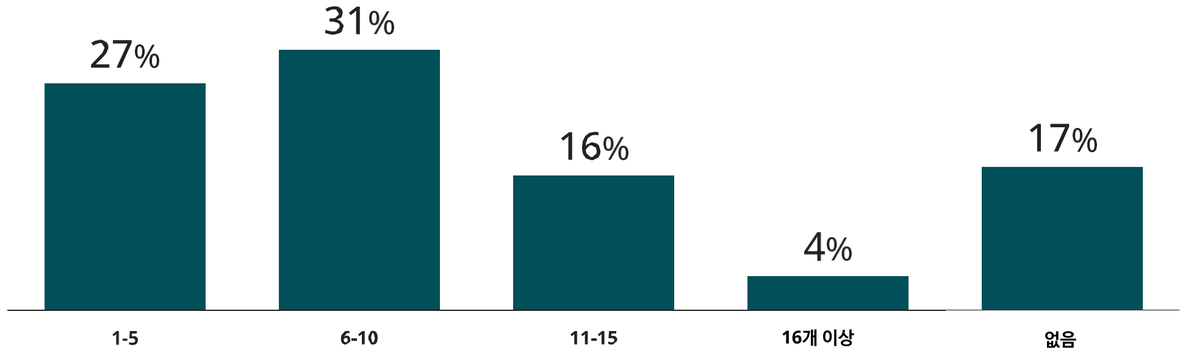
사이버 침해는 여전히 빈번하게 발생
응답자들은 여전히 높은 수준의 사이버 침해 사고를 경험하고 있다고 보고했다. 2025년에는 응답 기업의 78%가 최소 한 건 이상의 침해 사고를 공개적으로 보고했으며, 이는 2024년의 91% 대비 감소한 수치이다. 또한 2025년에는 약 3분의 1이 6~10건의 침해를 경험했다고 답했는데, 이는 2024년의 40%보다는 낮아진 수준이다. 전년 대비 사고 건수는 감소했지만, 여전히 높은 수준의 침해가 지속되고 있다는 점은 변하지 않았다.

익숙한 위협은 계속되고, AI 오남용이 새로운 리스크로 부상
응답자들이 가장 우려하는 위협 행위자는 사이버 범죄 조직(30%)이었으며, 그 뒤를 사이버 테러리스트(15%)와 핵티비스트(hacktivists, 10%)가 이었다. 공격 방식 역시 기존과 유사했다. 랜섬웨어(20%), 악성코드(malware, 15%), 데이터 유출(data exfiltration, 14%)이 여전히 주요 위협으로 지목되었다. 다만 올해 조사에서는 새로운 변화가 확인되었다. 바로 AI 오남용(misuse of AI)이 새로운 주요 위협 요인으로 부상하며 네 번째로 높은 우려 요소에 올랐다는 점이다.

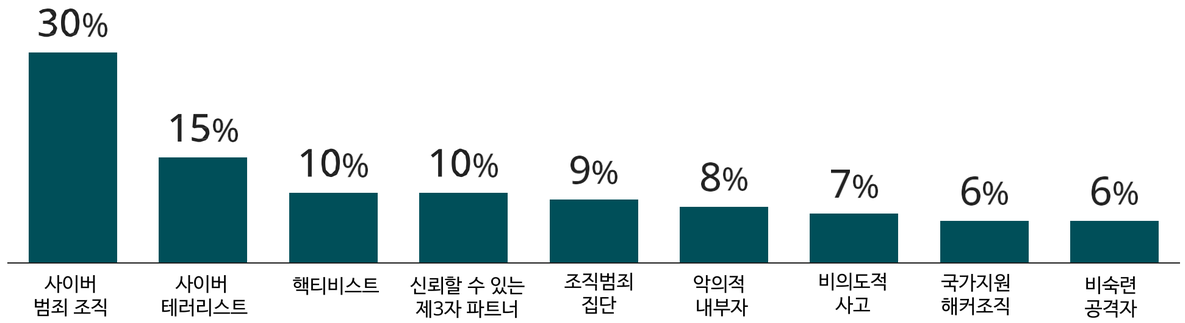
"시스템, 애플리케이션, 환경이 침해되는 일은 앞으로도 계속 발생할 것이다. 모든 침해를 완벽하게 막으려 한다면 기업은 정상적으로 비즈니스를 수행하기 어려워진다. 중요한 것은 시스템이 침해되었을 때 가능한 한 빠르게 탐지하고, 즉시 격리·제거하여 더 큰 피해로 확산되지 않도록 만드는 것이다."

— 헬스케어 기업 Global CIO

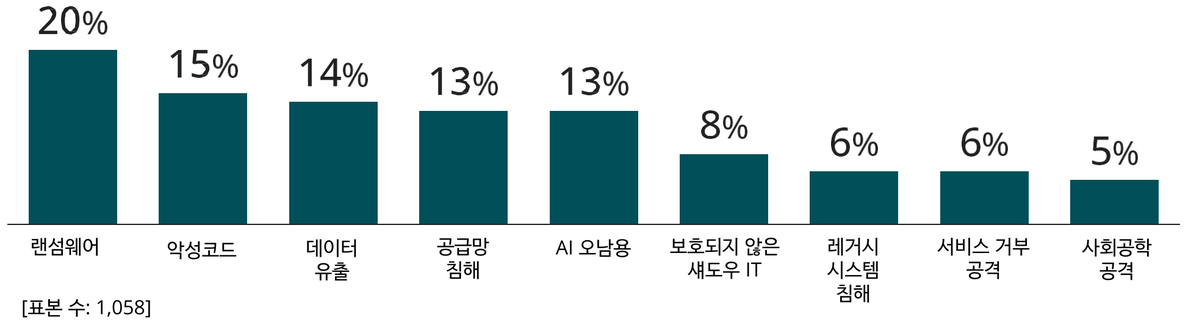
[공식적으로 보고된 침해 사건 건수(전년 기준)]



[가장 우려되는 사이버 침해 행위자]



[가장 우려되는 사이버 보안 침해 방식]



[표본 수: 1,058]

PARADOX #4

기업들은 지금까지 사이버 침해의 영향을 비교적 효과적으로 최소화해 왔다.

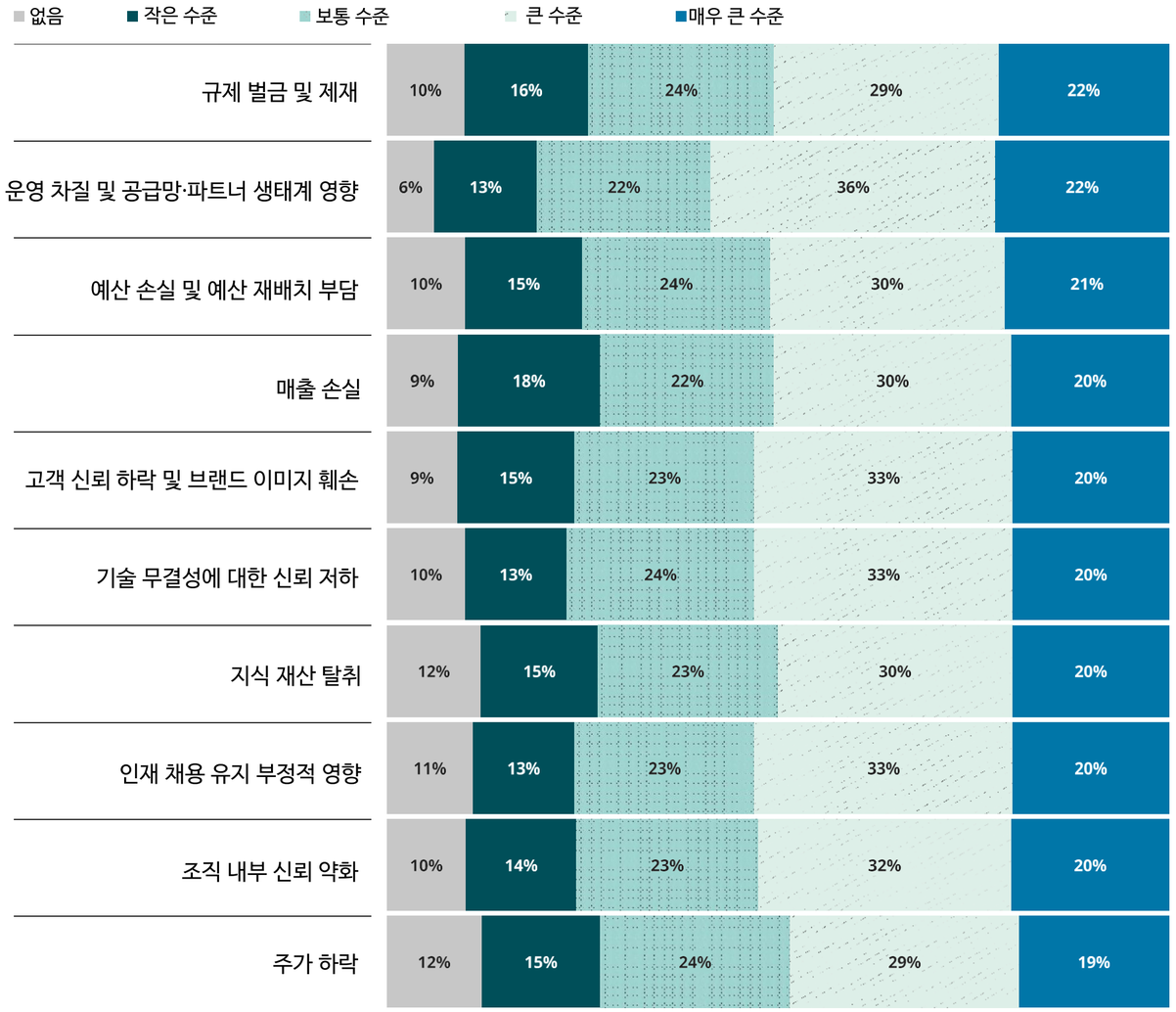
사이버 침해 사고가 상당한 수준으로 발생하고 있음에도 불구하고, 평균적으로 응답자의 52%는 사이버보안 사고로 인한 부정적 영향이 자사에 '큰 수준 또는 매우 큰 수준(large/very large extent)'으로 영향을 미쳤다고 답했다. 이는 전년도 64% 대비 감소한 수치이다.

물론 이것이 사이버 사고의 영향을 과소평가할 수 있다는 의미는 아니다. 가장 큰 영향은 운영 차질(operational disruption)로 나타났다. 응답자의 58%는 사이버 사고로 인해 공급망과 파트너 생태계 전반에서 심각한 운영 중단을 경험했다고 답했다. 다만, 이 역시 전년도 66% 대비 감소한 수치로, 기업들이 사고의 부정적 영향을 관리하는 역량을 점차 강화하고 있음을 시사한다.

특히 Frontrunner 기업들은 이러한 특징이 더욱 두드러졌다. 이들은 성숙한 위협 인텔리전스 체계를 바탕으로 오히려 더 많은 침해 사고를 탐지·보고할 가능성이 높다. 실제로 지난 1년간 11건 이상의 사이버 침해를 경험했다고 답한 비율은 Frontrunner가 26%로, Followers(19%)와 Foundation Builders(20%)보다 높았다.

그럼에도 불구하고 Frontrunner들은 더 많은 사고를 보고하면서도, 사고로 인한 부정적 영향 수준은 Followers와 유사한 수준으로 유지하고 있었다. 이는 단순히 침해를 막는 것보다, **침해 이후 영향을 빠르게 통제하고 복원하는 역량이 점점 더 중요해지고 있음**을 보여준다.

[사이버 보안 침해로 받은 피해의 종류와 정도]



[표본 수: 823]

패러독스 분석 및 해결 전략

침해 사고 증가에 대한 과도한 해석 지양
침해 사고 보고 건수 증가는 오히려 탐지·대응 체계가 제대로 작동하고 있다는 신호일 수 있다. 중요한 것은 단순 건수가 아니라, 무엇이 탐지되었고 얼마나 빠르게 대응했으며 실제 비즈니스 영향이 어느 수준이었는지에 대한 인사이트다. 낮은 영향도의 사고를 빠르게 탐지하는 사례가 늘어난 것이라면, 이는 사이버 대응 성숙도가 향상되고 있다는 긍정적 신호일 수 있다. 반대로 반복적인 공격 경로, 장시간 잠복, 운영 차질과 연결된다면 보다 근본적 대응이 필요하다. 맥락 없이 숫자만 볼 경우 불필요한 통제를 강화하거나, 반대로 실제 위험을 과소평가할 위험이 존재한다.

침해 사고가 없다는 결과도 면밀히 검토할 필요
침해 사고가 보고되지 않는 것은 긍정적 결과일 수도 있지만, 반대로 탐지 역량 부족의 신호일 수도 있다. 충분한 모니터링 및 분석 체계가 부재할 경우 악성 행위나 잠복형 공격을 인지하지 못할 가능성이 존재한다. 따라서 “사고가 없는 것” 자체보다, 실제로 탐지·분석·대응 체계가 제대로 작동하고 있는지를 검증하는 것이 중요하다.

복원력(Resilience) 확보를 위한 시나리오 기반 대응 강화
응답자의 67%는 사이버 전략과 비즈니스 전략을 연결하기 위해 시나리오 플래닝을 선제적으로 추진하고 있었다. 이는 조직의 복원력을 강화하는 핵심 요소 중 하나이다. 또한 이러한 과정은 사이버 조직이 매출 보호, 운영 안정성 확보, 서비스 중단 방지 등 어떤 방식으로 비즈니스 가치에 기여하는지를 명확히 보여준다. 시나리오 기반 대응 체계는 빠르게 변화하는 위협 환경에 맞춰 지속적으로 고도화되어야 한다.

PARADOX #5

사이버 예산은 매년 안정적으로 유지되고 있으나,
사이버 위협 환경은 극도로 불안정하게 급변하고 있다.

지속적이고 안정적인 투자

투자 필요성에 대한 명확한 비즈니스 근거를 제시할 수 있는 조직일수록 필요한 예산을 확보할 가능성이 높다. 한 헬스케어 기업의 글로벌 CIO는 “충분히 검토된 타당한 근거와 명확한 비즈니스 케이스가 있다면, 대부분 예산 승인을 받을 수 있다”고 설명했다.

사이버보안 예산은 향후 1년간 점진적으로 증가할 것으로 전망되며, 주요 투자 영역 간 예산 배분 구조는 큰 변화 없이 비교적 안정적으로 유지될 것으로 보인다.
특히 선도 기업(Frontrunners)은 사이버 투자 성과에 대해 경쟁사 대비 훨씬 높은 기대감을 보이고 있으며, 다음 영역에서 가시적 비즈니스 효과를 예상하고 있다.

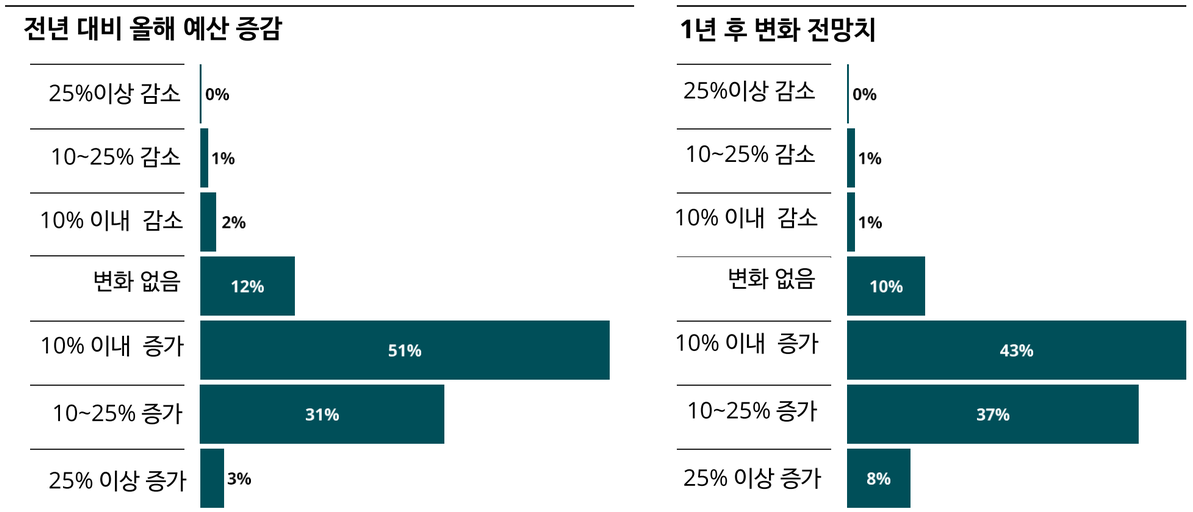
- 운영 효율성·민첩성·전략 실행력 강화
- 신뢰·복원력·안정성 제고
- 고객 가치 향상

선도 기업의 90% 이상은 각 영역에서 실질적 성과를 기대하고 있는 것으로 나타났다.
전체 **응답자의 85%는 전년 대비 사이버보안 예산을 확대했다고 답했으며, 88%는 향후 12개월 내 추가 증액을 계획하고 있다고 응답**했다. 일부 기업은 공격적인 투자 확대도 예상하고 있다. 응답자의 8%는 향후 1년 내 사이버 관련 지출이 25% 이상 증가할 것으로 전망했으며, 3분의 1 이상은 현재 전체 사이버 예산 대비 10~25% 수준의 추가 확대를 예상했다.

한편 향후 12~24개월 동안 예산 재원 구조 자체는 비교적 안정적으로 유지될 것으로 예상되며, 기업들은 **IT·비즈니스·전사 리스크 관리 조직 전반에 걸쳐** 사이버 투자 재원을 지속적으로 배분할 것으로 보인다.

IT	비즈니스	전사 리스크 관리
43%	30%	26%

[조직의 사이버 보안 관련 예산 편성]



[표본 수: 1,058]

대부분의 기업들은 이미 **다년(多年) 단위의 사이버 투자 계획을 운영하고 있는 것으로** 나타났다. 조사 대상 중 단년도 예산 체계만 운영한다고 답한 비율은 7%에 불과했다.

한 헬스케어 기업의 글로벌 CIO는 “프로그램 자체는 보통 2~3년 단위로 운영되지만, 실제 예산은 여전히 매년 승인받는 구조”라고 설명했다. 즉, 장기 전략과 투자 방향은 존재하지만, 예산 집행은 연 단위 관리 체계에 따라 운영되고 있다는 의미이다.
다년 투자 계획 중 가장 큰 비중은 현재 예산 사이클 이후 1~2년 범위에 집중되어 있다.

•현재 사이클 이후 1년 연장 투자: 전체 사이버 예산의 35%
•현재 사이클 이후 2년 연장 투자: 전체 사이버 예산의 26%
•향후 4~5년 장기 투자: 전체 사이버 예산의 19%

한편, 사이버 투자 우선순위와 지출 구조는 단기간 내 큰 변화 없이 유지될 것으로 전망된다. 응답자들은 내년에도 현재와 거의 동일한 예산 배분 구조가 유지될 것이라고 답했으며, 가장 높은 투자 비중은 위협 탐지 및 대응(20%) 분야에 집중될 것으로 나타났다.
그 뒤를 이은 주요 투자 영역은 다음 순으로 나타났다.

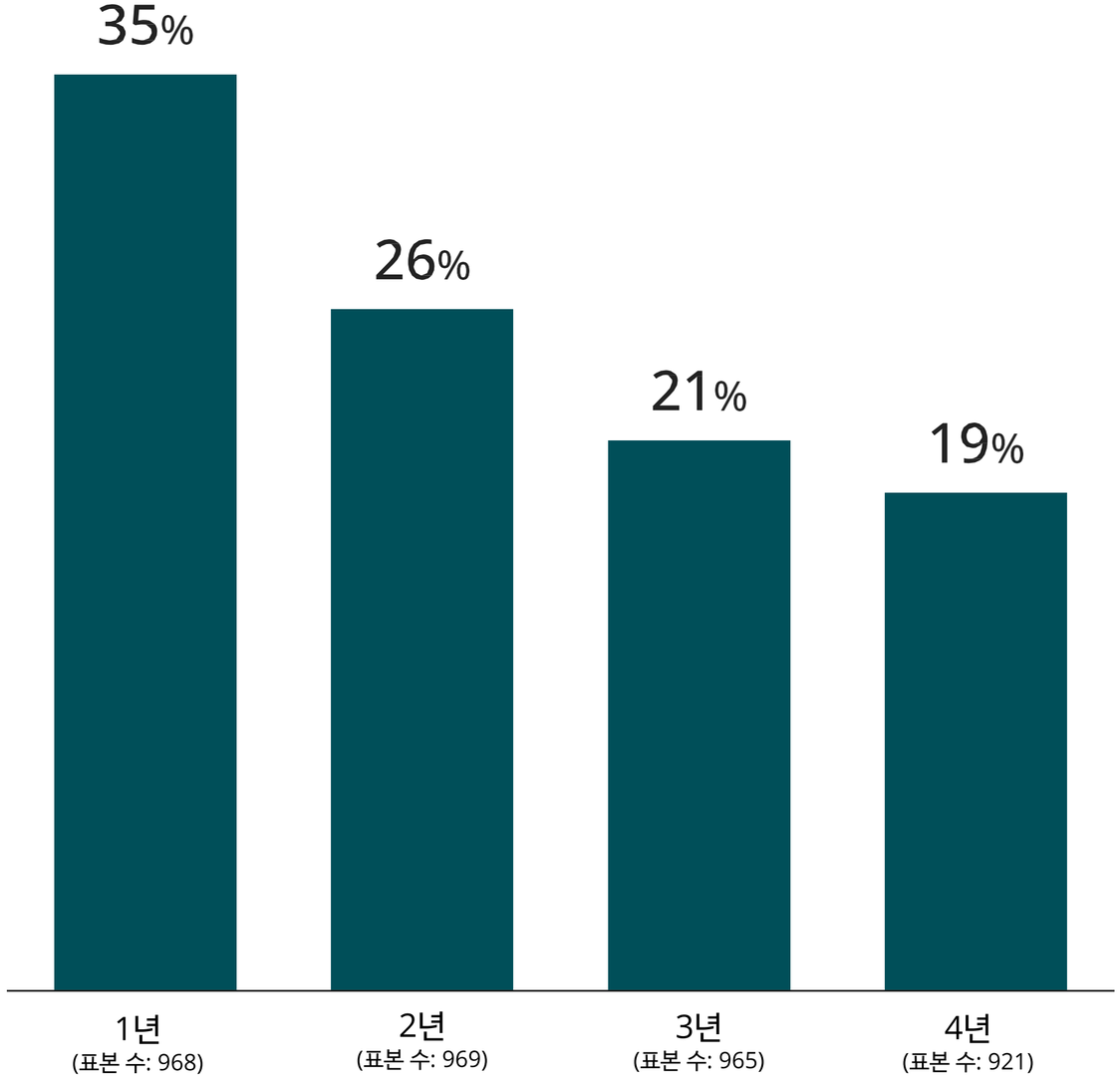
- 인프라 보안
- 데이터·ID·애플리케이션 보안
- 전략·거버넌스·컴플라이언스

즉, 기업들은 새로운 영역으로 급격히 이동하기보다는, 핵심 보안 체계를 지속적으로 강화하는 방향으로 안정적 투자를 이어가고 있는 것으로 해석된다.

“명확하고 충분히 검토된 비즈니스 타당성이 있다면, 대부분 예산 승인을 받을 수 있다.”

— 글로벌 CIO, 헬스케어 기업

[다년 투자 계획 중, 현재 사이클 이후 연장 투자 집행 예정 기간]



PARADOX #5

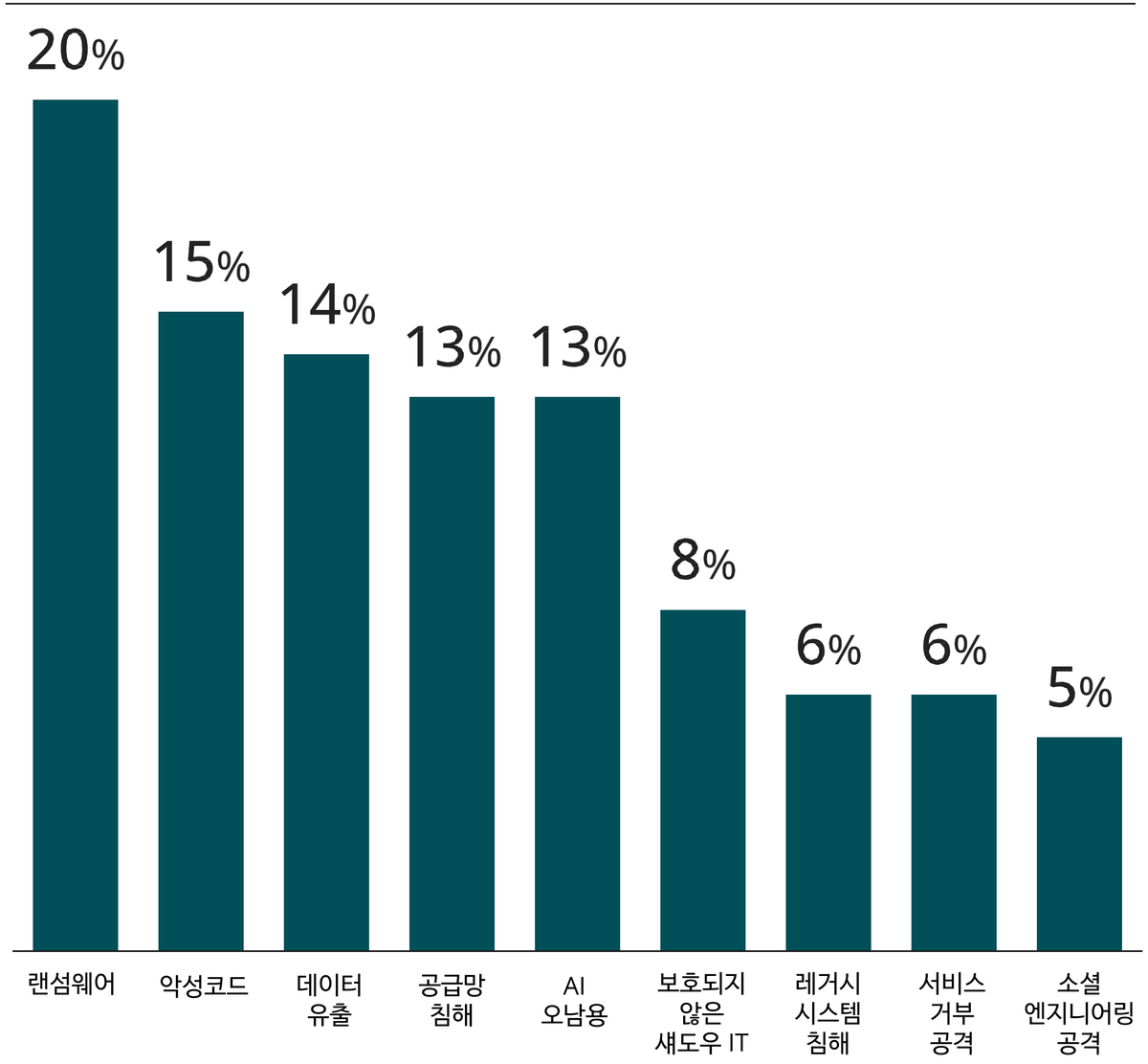
사이버 환경은 결코 안정적이거나 예측 가능하지 않다.

생성형 AI의 급속한 발전만 보더라도, 사이버 환경이 얼마나 빠르게 변화하고 있는지를 알 수 있다. 불과 2~3년 전만 해도 생성형 AI 역량에 대한 즉각적 투자 필요성을 본격적으로 논의하는 기업은 많지 않았으며, 실제 행동에 나선 사례는 더욱 드물었다. 그러나 현재는 응답자의 약 **72%가 기존 AI 체계 내 거의 10여 개에 달하는 사이버 이니셔티브에 새로운 생성형 추론(Generative Reasoning) 기반 접근 방식을 이미 적용**하고 있다고 답했다.

이는 사실상 대부분의 기업이 기존 정적(static) 예산 체계만으로는 예상하거나 준비하기 어려웠던 변화이다.위협 환경 역시 빠르게 변화하고 있다.
예를 들어 “AI 오남용(Misuse of AI)”은 불과 3년 전만 해도 주요 사이버 위협 목록에 포함되지 않았지만, 현재는 랜섬웨어·악성코드·데이터 유출과 함께 상위 5대 위협으로 부상했다.

그리고 이러한 위협은 기존 보안 방식만으로는 대응이 어렵다.
특히 비결정형(non-deterministic) AI 시스템은 프롬프트 해킹(prompt hacking)과 같은 새로운 공격에 노출될 수 있기 때문에, 기존 통제 체계와는 다른 수준의 정교한 가드레일(guardrail)이 요구된다. 이는 기업이 지금 당장 대응해야 하는 새로운 차원의 복잡성을 의미한다.

[가장 우려되는 사이버 보안 침해 유형]



[표본 수: 1,058]

PARADOX #5

패러독스 분석 및 해결 전략

조직이 예산 측면에서 예측 가능성과 안정성을 추구하는 것은 자연스러운 일이다.
특히 기술 발전 속도가 매우 빨라지면서 전체 IT 예산 구조 역시 크게 변화해야 한다는 점은 이미 널리 인식되고 있다. 그러나 사이버보안 투자는 일반적인 기술 투자와는 본질적으로 다르다. 사이버 리스크는 조직 운영과 비즈니스에 심각한 혼란을 초래할 수 있는 높은 파괴력을 갖고 있기 때문이다.

사이버 리더들은 AI를 활용해 보안 운영 효율성을 높이는 동시에, 진화하는 위협에 대응하기 위해 AI에 대한 투자를 더욱 확대해야 하는 상황에 놓여 있다.이에 따라 기업들은 다음과 같은 사항을 고려할 필요가 있다.

사이버 예산에 유연성 확보
예상치 못한 위협과 새로운 기술 등장에 대응할 수 있도록, 연간 사이버 예산의 일정 비율(예: 10~20%)을 별도 유연 투자 재원으로 확보할 필요가 있다. 이를 통해 신규 보안 역량 도입이나 긴급 대응 투자를 보다 민첩하게 수행할 수 있다.

다년 예산 체계 재검토
기존의 고정형 다년 예산 구조가 오히려 변화 대응을 제약할 수 있다.
이에 따라 롤링 포캐스트(Rolling Forecast, 일정한 기간마다 미래 전망치를 계속 업데이트하는 예측 방식)나 지속적 예산 운영(Continuous Budgeting) 방식과 같은 보다 유연한 접근법을 검토할 필요가 있다.

예산 관점 자체의 전환
재무 조직과 예산 의사결정자들은 사이버보안이 가진 특수성과 불확실성을 충분히 이해하지 못할 수 있다. 따라서 사이버 리더들은 경영진과 재무 조직을 대상으로 현재의 위협 환경과 리스크 구조를 지속적으로 설명하고, 새로운 예산 운영 방식에 대한 공감대를 형성해야 한다.

패러독스가 만들어내는 기회와 가능성

이번 조사에서 드러난 5개의 역설(paradox)은 새로운 기회를 의미한다.
이러한 역설을 해결할 수 있는 조직은 비전과 실행 사이의 격차를 줄이고, 보다 높은 수준의 사이버보안 경쟁력을 확보할 수 있다. 현재는 이러한 변화와 혁신을 추진하기 위한 핵심 조건들이 상당 부분 갖춰져 있는 상황이다.

경영진과 주요 의사결정자들은 조직 목표 달성을 위해 사이버보안이 얼마나 중요한지를 이미 인식하고 있으며, 이를 위한 충분한 투자와 지원 의지도 보이고 있다.
동시에 CISO와 사이버 리더들 역시 증가하는 위협에 대응하기 위해 전략, 프로세스, 운영 체계 전반을 지속적으로 고도화해 왔다.

이제 필요한 것은 이러한 요소들을 하나로 연결해, **보다 강력하고 조직 전반에 깊게 내재화된 통합형 사이버 문화와 실행 체계를 구축하는 것**이다. 즉, 미래의 **복합적 위협 환경에 대응할 수 있는 전사적 사이버 운영 메커니즘을 만드는 단계로 나아가야 한다는 의미**이다.
이를 위해서는 조직 내부의 변화 추진자(Change Agent)가 필요하다.
그리고 이 보고서를 읽고 있는 당신이 바로 그 역할을 맡아야 할 가능성이 높다.

이번 보고서에서 제시된 역설의 관점으로 조직을 다시 바라볼 필요가 있다. 어떤 역설이 현재 조직에 가장 크게 적용되는지 식별하고, 동료 리더들과 함께 그 문제를 해결해 나가야 한다.
이러한 과정이 결국 사이버 보안 전략을 성장의 핵심 축으로 전환시키는 출발점이 될 수 있다.

딜로이트 One Cyber & Resilience

디지털 전환이 지속적으로 진행되고 AI 활용이 증가하면서 사이버 공간에서의 위협은 더욱더 다양해지고 증가하고 있으며, 사이버 사고는 단순 기술적 사고가 아닌 사업 연속성을 크게 훼손하는 비즈니스 재난으로 인식되고 있습니다. 사이버 전략수립, 규제/법규 준수,위험 및 취약점 진단 및 개선, 정보보호 시스템 구축, 사고 대응, 비즈니스 연속성 확보 등 자문 서비스를 통해 기업의 리스크를 사전에 관리해야 합니다. **One Cyber & Resilience** 그룹은 사이버 상에서 발생하는 다양한 위험을 관리하고, 사업 연속성을 확보 하기 위한 종합적인 서비스를 제공합니다.

백철호 부대표
One Cyber & Resilience 리더

02 6676 2250
cbaek@deloitte.com

서영수 파트너
One Cyber & Resilience

02 6676 1929
youngseo@deloitte.com

유선희 파트너
One Cyber & Resilience

02 6676 2956
sunhyou@deloitte.com

문범석 파트너
One Cyber & Resilience

02 6676 3687
bsmoon@deloitte.com

이창성 파트너
One Cyber & Resilience

02 6099 4888
changsulee@deloitte.com

Deloitte Insights

세일즈&마케팅 대표
권지원 Partner
jekwon@deloitte.com

성장전략부문 부대표
서정욱 Partner
juseo@deloitte.com

딜로이트 인사이트 편집장
박경은 Director
kyungepark@deloitte.com

연구원
양원석 Manager
wonsukyang@deloitte.com

Contact us
krinsightsend@deloitte.com

Deloitte.

딜로이트 인사이트 카카오 채널 & 앱

전 세계 경제·산업·경영 트렌드와 인사이트를

실시간으로 확인하세요!

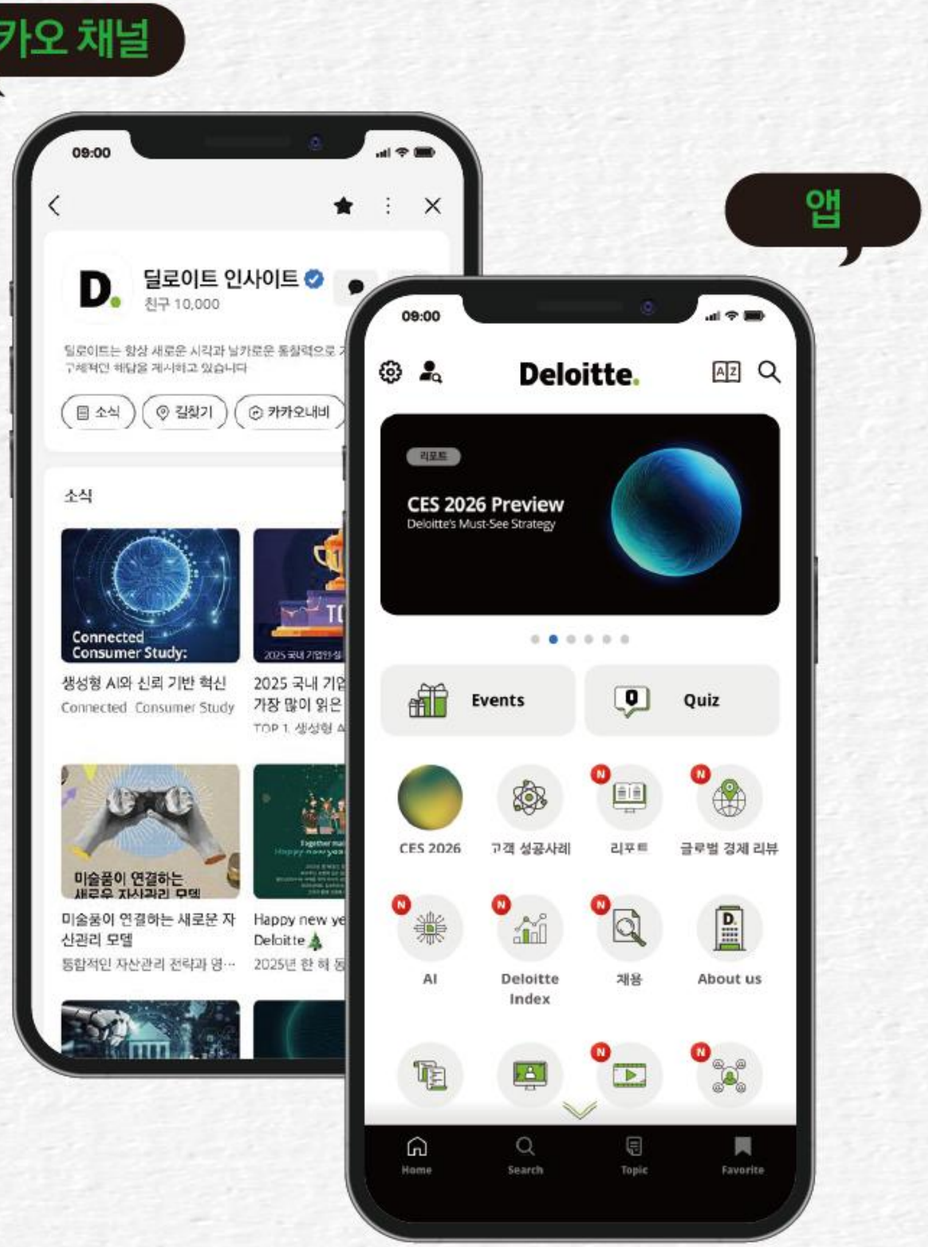
- AI 시대의 전략과 리스크, 산업별 핵심 이슈를 다룬 **분석 리포트**
- 소비심리지수·자동차 구매의향 등 실물경제의 향방을 보여주는 **Deloitte Index**
- 딜로이트 전문가의 인사이트와 글로벌 행사의 현장을 담은 **영상 콘텐츠**
- 글로벌 프로젝트에서 검증된 실행 인사이트를 담은 **고객 성공 사례**

카카오채널

앱

Download on the App Store

GET IT ON Google Play



앱스토어, 구글플레이/카카오톡에서 **'딜로이트 인사이트'** 를 검색해보세요.
더욱 다양한 소식을 만나보실 수 있습니다.

Deloitte.