pwc

2026 Global Digital Trust Insights

불확실성 시대의 사이버 보안

November 2025

Table of contents

본 보고서는 PwC의 '2026 Global Digital Trust Insights'를 기반으로 작성되었습니다.
원문은 2025년 5월부터 7월까지 72개국 3,887명의 비즈니스 및 기술 임원을 대상으로 진행한 서베이 결과입니다.

들어가며

60%

글로벌 정세 변화에 따라 사이버 보안에 투자를 늘렸다고 응답한 기업의 비율

6%

모든 데이터 리스크 대응 조치를 마쳤다고 응답한 기업의 비율

새로운 국면에 들어선 사이버 위협, 시험대에 오른 사이버 보안 전략

기업은 지금 탈세계화 시대의 새로운 현실에 직면하고 있습니다. 기술의 급격한 발전에 따라 세계 질서가 빠르게 변화하여 동맹의 균열, 약화된 국제기구의 영향력, 관세 충격, 교란된 공급망 등의 불확실성이 커지면서, 사이버 위협 또한 국가 차원의 공격으로 진화하고 있습니다.

PwC는 본 서베이를 통해 불확실한 시대에 리더들이 어떻게 대응하고 있고, 어떤 부분에서 부족하며, 어떤 방식으로 개선할 수 있을지를 제시합니다. 다음은 본 서베이에서 도출된 주요 내용입니다.

- **글로벌 정세 변화에 따른 전략의 변화**
  기업과 리더의 60%가 사이버 리스크 대응을 3대 전략 우선순위로 하여 투자를 증대했다고 응답했습니다.
- **아직 부족한 사이버 공격 회복력**
  기업의 6%만이 모든 대응 조치를 마쳤다고 응답했으며, 절반 가량은 주요 취약점에 대한 사이버 공격에 '어느 정도 대응만 가능하다'고 평가했습니다.
- **예방에 집중하지 않는 투자**
  기업의 24%만이 예방 중심으로 사이버 보안에 투자하며, 기업의 대부분(67%)은 예방과 사후 대응에 비슷한 예산을 투자한다고 밝혔습니다.
- **AI 에이전트의 활용**
  향후 12개월간 클라우드 보안, 데이터 보호, 사이버 방어 및 보안 운영에 AI 에이전트를 적극적으로 도입할 계획입니다.
- **양자 컴퓨터에 대한 대비 미흡**
  양자 컴퓨팅은 아직 준비도가 부족한 5대 위협에 속하나, 예산에서 이를 우선순위로 두는 기업은 10% 미만이며, 모든 양자 내성 조치를 도입 완료한 기업은 3%에 불과합니다.
- **사이버 인력 부족**
  기업의 과반수(53%)가 AI와 머신러닝 툴로써 사이버 인력의 격차를 줄이려고 하며, 매니지드 서비스의 필요성이 증가하고 있습니다.

01

새로운 사이버 위협의 등장

60%

글로벌 정세 변화에 따라 사이버 리스크 대응에 투자를 늘렸다고 응답한 기업의 비율

Only 6%

지정학적 상황을 고려할 때, 조사된 모든 영역에서 사이버 공격 대응 역량이 '매우 뛰어나다'고 답한 기업의 비율

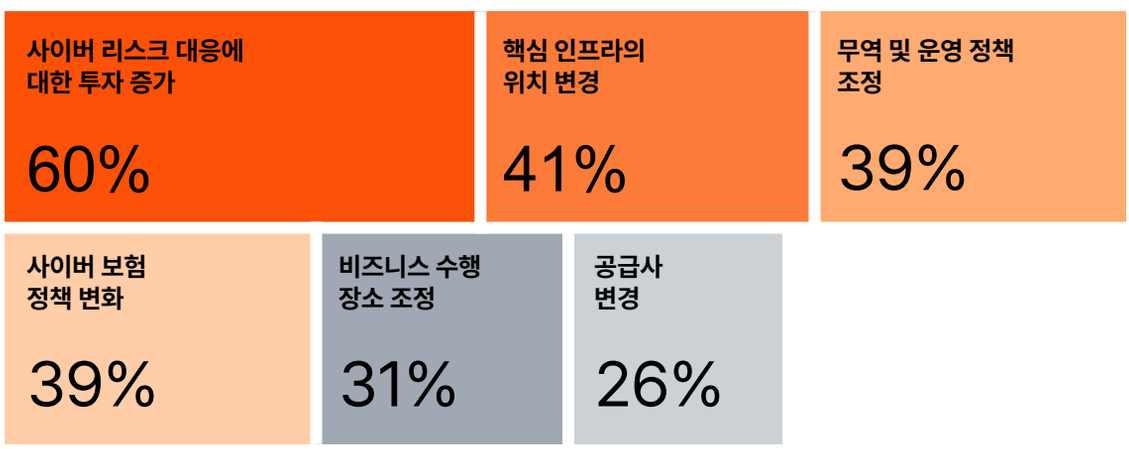
Top 2

기업이 가장 취약한 사이버 위협은 클라우드와 커넥티드 제품 공격

오늘날의 사이버 위협은 파괴적인 기술 발전만큼이나 글로벌 정세 변화에 의해 형성되고 있습니다. 동맹의 붕괴, 무역 분쟁, 국제 기구의 약화 등 불안정한 추세들은 이 새로운 전략적 경쟁의 시대에서 위협 환경 뿐만 아니라 전통적인 비즈니스 방식까지도 변화시키고 있습니다. 이러한 상황에 대응하기 위해 비즈니스 및 기술 리더의 60%는 사이버 보안에 대한 투자를 향후 1년간 상위 세 가지 우선순위 중 하나로 삼고 있습니다. 또한, 핵심 인프라의 위치 변경(41%), 무역 및 운영 정책 조정(39%), 사이버 보험 정책 변화(39%) 등을 함께 우선순위에 두고 있습니다. 지속적인 혼란이 이제는 일상이 된 상황에서, 사이버는 회복탄력성을 위한 핵심 수단으로 자리잡고 있습니다.

현재 글로벌 정세 변화에 따른 사이버 전략의 변화 (상위 3대 변화로 선택한 비율 %)

Q. 향후 12개월 동안, 지정학적 상황에 대응하기 위해 귀사의 사이버 전략에서 변화가 예상되는 영역은 무엇입니까?



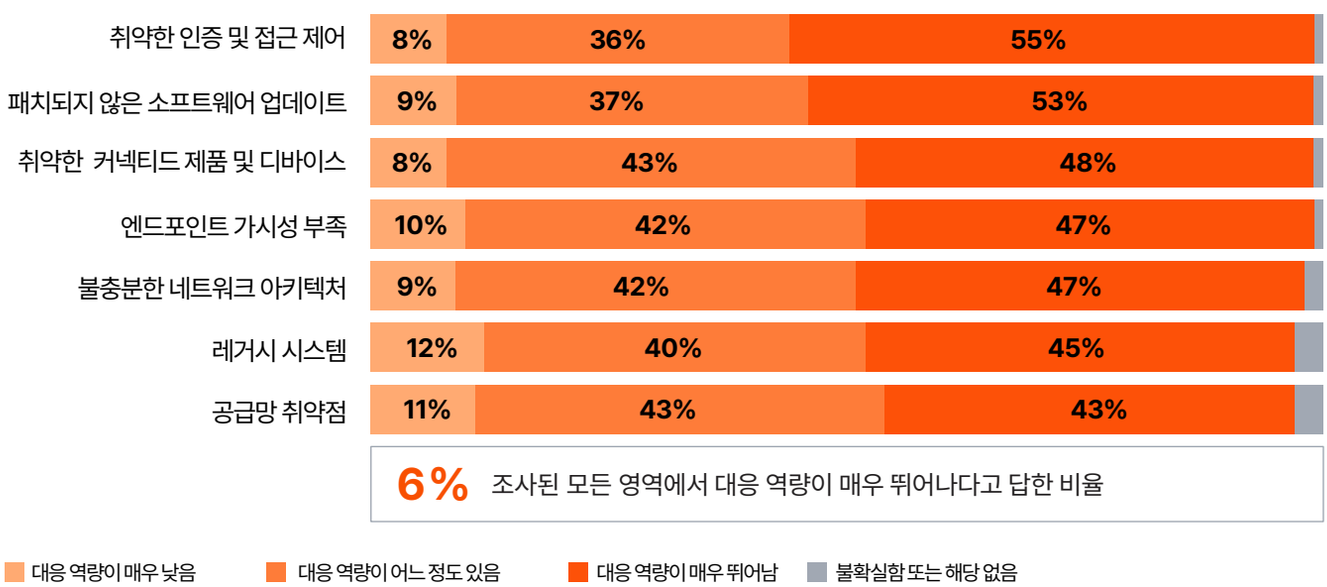
출처: PwC

안전하다고 느끼는 것 vs 실제로 안전한 것

현재의 환경 속에서 사이버 대비 태세에 대한 자신감은 엇갈리고 있습니다. 응답자의 약 절반은 자사 조직이 특정 취약점을 노린 사이버 공격을 견뎌낼 수 있는 '매우 높은 역량'을 갖추고 있다고 답했지만, 나머지 절반은 그렇지 않다고 응답했습니다. 더 나아가 모든 취약 영역에 대해 '매우 높은 역량'을 보유하고 있다고 답한 비율은 단 6%에 불과합니다. 레거시 시스템과 공급망 노출은 여전히 가장 취약한 부분으로, 중요 인프라를 교란하려는 국가 지원 공격자의 빈번한 표적이 되고 있습니다.

사이버 공격에 대한 방어력

Q. 귀사는 아래의 취약점을 노린 대규모 사이버 위협에 대한 대응 역량은 어느 정도입니까?



출처: PwC

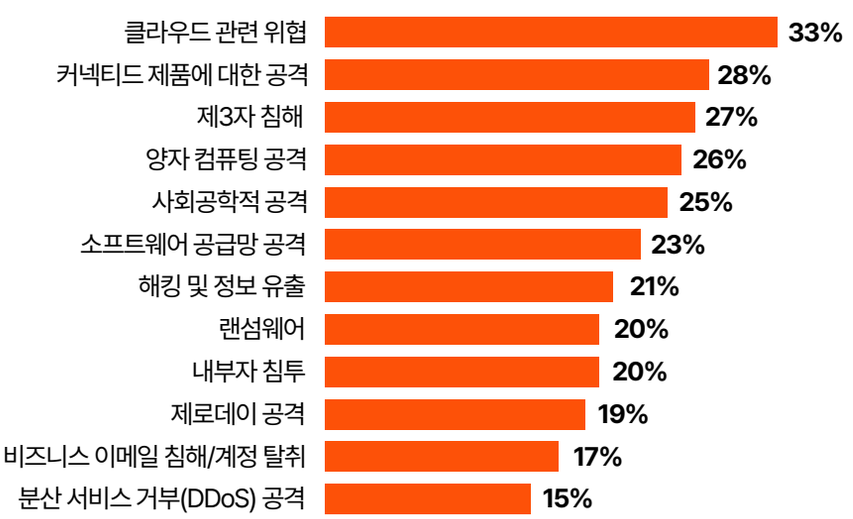
지속되는 격차, 높아지는 리스크

앞서 언급한 취약점 외에도, 경영진은 특정 유형의 위협에 대한 대응 수준을 우려하고 있습니다. 클라우드와 커넥티드 제품에 대한 공격은 여전히 주요 우려 사항으로, 지난해와 마찬가지로 약 3분의 1의 리더가 이를 가장 대응하기 어려운 세 가지 사이버 위협 중 하나로 꼽았습니다.

이러한 리스크가 새로운 것은 아니지만, AI를 활용한 공격이 한계를 확장함에 따라 거버넌스, 통제, 가시성 등 기본적인 부분에서의 격차를 해소하지 못하는 문제가 지속적으로 드러나고 있습니다. 기술과 생태계의 복잡성이 증가함에 따라 많은 조직이 이를 따라가는 데 어려움을 겪고 있으며, 특히 제3자 및 공급망 의존 관계에서 그 어려움이 두드러집니다.

가장 대응하기 어려운 사이버 위협 (상위 3대 위협으로 선정한 비율 %)

Q. 향후 12개월 동안 다음 중 어떤 사이버 위협이 가장 대응 준비가 부족하다고 느낍니까?



출처: PwC

혹독한 교훈

경영진의 4분의 1 이상은 지난 3년간 발생한 가장 큰 데이터 유출 사고로 인해 최소 100만 달러 이상의 손실을 입었다고 말했습니다. 가장 큰 노출 리스크를 가진 조직은 연 매출 50억 달러 이상인 대기업(41%), 미국 기반 기업(37%), 그리고 기술·미디어·통신 기업(33%)입니다. 이들은 규모와 운영의 복잡성으로 인해 고비용 사고가 발생할 가능성이 높습니다.

복구의 어려움을 겪은 후, 대규모 공격을 경험한 조직은 값비싼 교훈을 실질적인 행동으로 전환하고 있습니다. 이들은 사이버 예산을 늘리는 비율이 88%로, 전체 평균 78%인 다른 조직에 비해 높습니다. 또한 핵심 기술 인력 부족을 보완하기 위해 매니지드 서비스를 도입하는 비율(48%)도 전체 평균(39%) 대비 높습니다.

더불어 사이버 보험 정책을 변경하는 기업의 비율도 49%로, 전체 평균(39%) 대비 높습니다. 이는 상승하는 보험료와 보험사의 강화된 요구 사항에 대응하기 위한 조치로 보입니다. 아울러 많은 기업이 조직 전반에 데이터 최소화 정책을 더욱 적극적으로 도입하고 있습니다.

02

사이버 전략과 운영

Only 24%

사후 대응 보다 사전 예방 중심으로 사이버 보안에 투자하는 기업의 비율

78%

향후 1년간 사이버 예산이 증가할 것이라 답한 기업의 비율

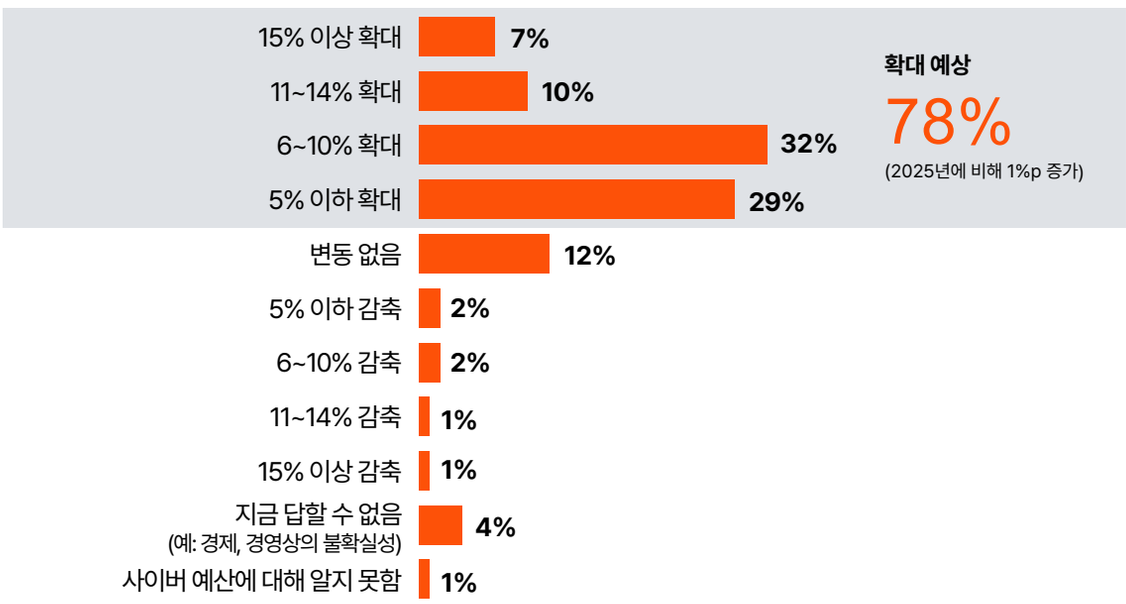
Only 16%

사이버 리스크의 재무적 영향을 상당한 수준으로 측정하는 기업의 비율

응답자의 약 78%가 향후 1년간 사이버 보안 예산이 증가할 것이라고 답했습니다. 그러나 이는 지난해 77%와 거의 변함없는 수준입니다. 응답자들은 현재의 글로벌 정세 급변에 대응하기 위해 사이버 보안 투자를 확대하고 있다고 말하지만, 이러한 증가는 다른 지출 우선순위의 희생을 대가로 이루어지고 있을 가능성이 있습니다.

2026년 사이버 예산의 변화

Q. 2026년에 귀사의 사이버 예산 편성은 어떻게 변화할 예정입니까?



출처: PwC

사전 예방 vs 사후 대응

사이버 보안의 핵심은 사전 예방입니다. 이는 위기가 발생하기 전에 모니터링, 평가, 테스트, 통제, 교육 등 선제적 조치에 계획적으로 투자하는 것을 의미합니다. 반면, 사후 대응 중심 접근 방식(예: 사고 대응, 고객 관리, 복구, 소송, 벌금 등)에 의존하는 것은 훨씬 더 비용이 많이 들고, 위험하며, 지속 가능하지 않습니다.

전체 조직의 약 67%는 선제적, 사후적 비용 비율이 대체로 비슷하다고 답했습니다. 즉, 두 영역에 거의 동일하게 지출하거나 어느 한 영역에 약간 더 많이 지출하고 있다는 의미입니다. 반면, 단 24%의 조직만이 선제적 조치에 훨씬 더 많이 투자하고 있습니다. 또한 이러한 수치에는 실제 대응 비용이 과소평가되고 있을 가능성이 높습니다. 선제적 지출은 보안 리더의 예산에 포함되어 있어 쉽게 추적할 수 있지만, 사후 대응 비용은 법무, 커뮤니케이션, 운영, IT, 마케팅, 대외 관계 등 여러 부서에 분산되어 있고, 기회 손실이나 평판 손상과 같이 정량화하기 어려운 비용도 포함되기 때문입니다.

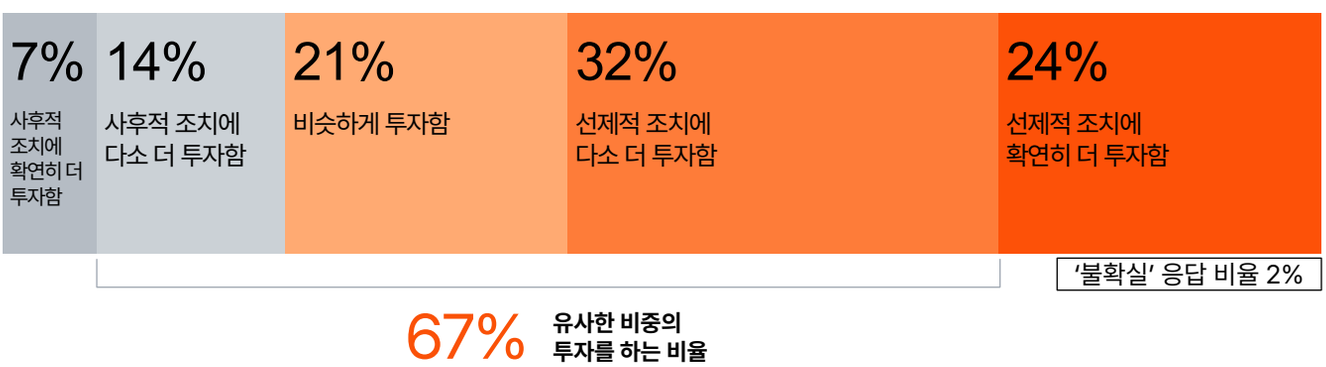
그러나 선제적 조치에 투자한다고 해서 반드시 효과적인 대처가 이루어지는 것은 아닙니다. 투자가 잘못된 리스크에 집중되어 있거나, 새로운 환경 변화에 신속히 적응하지 못한다면, 실질적인 대비 효과는 낮습니다. 진정한 준비태세는 리스크와 위협 환경을 깊이 이해하고, 이를 토대로 사이버 전략, 인력 구성, 프로세스, 시스템 등을 결정하는 데서 비롯됩니다.

선제적 vs 사후적 조치에 대한 투자

Q. 귀사는 선제적 조치와 사후적 조치 중 어느 쪽에 더 많은 예산을 투자합니까?

사후적 조치:
사고 대응, 고객 관리, 정상화, 복구, 소송, 벌금 등

선제적 조치:
모니터링, 평가, 테스트, 사전 통제, 교육, 거버넌스 등



출처: PwC

투자 우선순위와 대비 수준의 연계

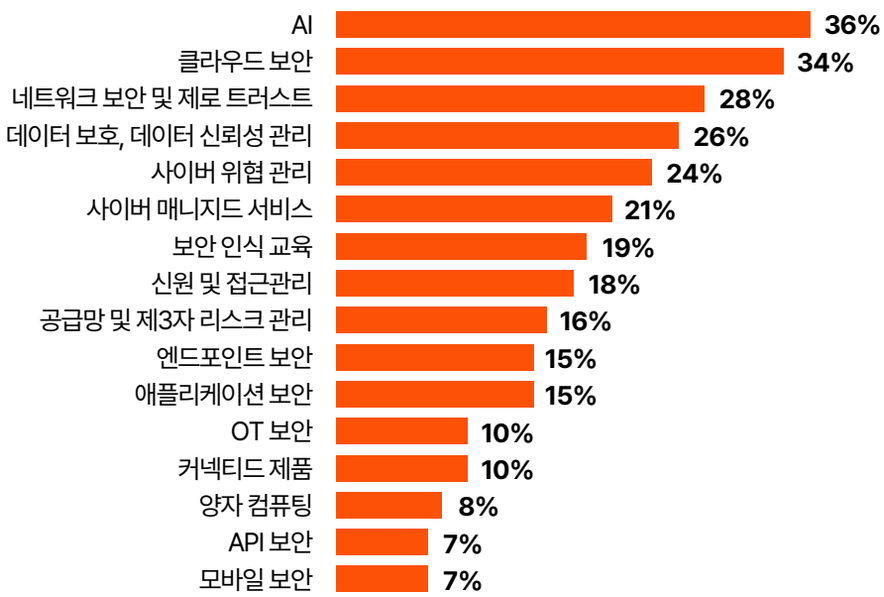
내년의 사이버 보안 예산에서 AI와 클라우드 보안이 가장 높은 우선순위를 차지하고 있습니다. 앞서 언급했듯이, 클라우드는 리더들이 가장 대응 준비가 부족하다고 느끼는 위협으로 꼽히고 있습니다. 따라서 위험과 대비의 격차가 인식되고 있으며, 그에 따라 자금이 집중되고 있습니다.

그러나 전체적인 설계는 완전하지 않습니다. 조직들이 대비가 가장 부족하다고 느끼는 두 번째 영역은 커넥티드 제품에 대한 공격이지만, 이 분야에 예산을 배정하는 조직은 훨씬 적습니다. 이러한 불일치는 일부 위협이 여전히 인식의 사각지대에 머물러 있음을 보여줍니다.

또한 사이버 매니지드 서비스도 많은 조직에서 주요 투자 우선순위로 꼽히고 있습니다. 특히 고성장 기업의 30%는 이를 상위 3대 투자 우선순위로 선정했습니다. 이는 외부 전문성을 적극 활용하여 사이버 대비의 핵심 격차를 해소하려는 전략적 움직임을 반영합니다.

기업들이 우선적으로 사이버 예산을 투자하는 영역 (상위 3대 우선순위로 선택한 비율 %)

Q. 향후 12개월 동안, 귀사는 다음 중 어느 영역에 사이버 예산을 우선적으로 투자할 계획입니까?



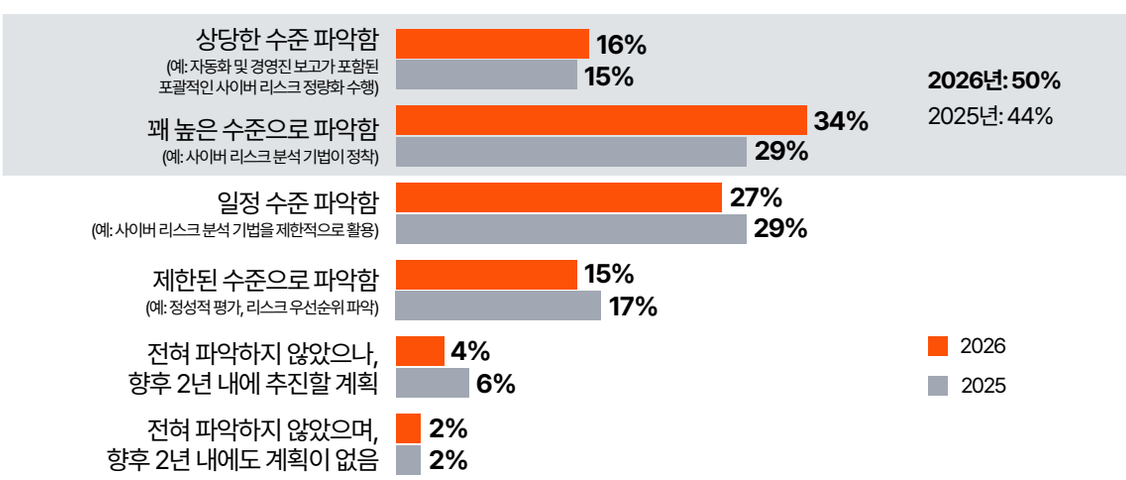
출처: PwC

사이버 보안 리스크 비용

점점 더 많은 기업이 자신의 사이버 리스크를 수치화하고 있습니다. 현재 절반의 조직이 사이버 리스크 정량화를 통해 재무적 영향을 상당 부분 측정하고 있다고 보고했으며, 이는 전년의 44%에서 증가한 수치입니다. 그러나 자세히 살펴보면, 이러한 정량화를 '상당한 수준'으로 수행하는 조직은 16%에 불과합니다. 경영진은 조직이 직면한 위협을 평가하고, 가장 적절한 대응 방안을 결정하기 위해 신뢰할 수 있고 실행 가능한 사이버 리스크 보고 인사이트를 필요로 합니다.

사이버 보안 리스크의 금전적 비용

Q. 귀사는 사이버 리스크의 잠재적, 재무적 영향에 대해 어느 정도 파악하고 있습니까?



출처: PwC

03

AI와 사이버 보안

#1

보안 리더들의 사이버 투자 최우선순위는 AI

#1

보안 리더들이 가장 중요시하는 AI 보안 역량은 위협 감지

Top 3

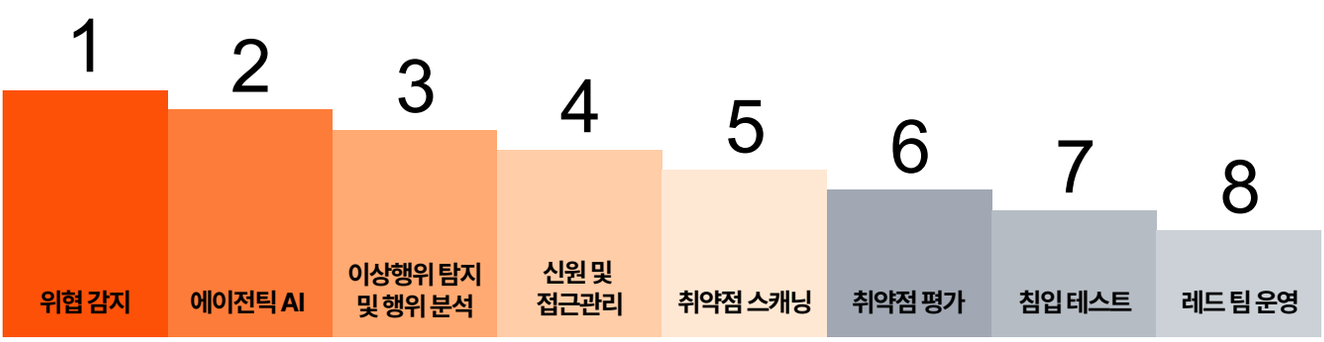
에이전틱 AI 활용이 우선시되는 상위 3대 영역은 클라우드 보안, 데이터 보호, 사이버 방어

AI가 사이버 보안 역량을 변화시킬 잠재력은 명확하며 그 범위 또한 매우 광범위합니다. 이러한 이유로, AI는 여러 조사 항목에서 가장 높은 우선순위를 차지했습니다. AI를 활용한 핵심 사이버 보안 기능 강화는 사이버 예산 배분, 사이버 매니지드 서비스 활용, 인력 격차 해소 측면에서 모두 최우선 과제로 꼽히고 있습니다.

향후 12개월 동안 보안 리더들은 AI 기반 보안 역량을 강화하기 위해 위협 감지를 가장 중요한 우선순위로 선정했습니다. 이와 함께, 에이전틱 솔루션, 이벤트 탐지 및 행동 분석, 신원 및 접근관리(IAM), 취약점 스캐닝 및 평가 등의 역량도 강화하고 있습니다.

AI 보안 역량 중 우선순위가 높은 에이전틱 AI (우선순위 높은 순)

Q. 향후 12개월 동안 귀사는 다음 중 어떤 AI 보안 역량 강화를 우선시할 것입니까?



출처: PwC

사이버 보안을 변화시키는 AI 에이전트

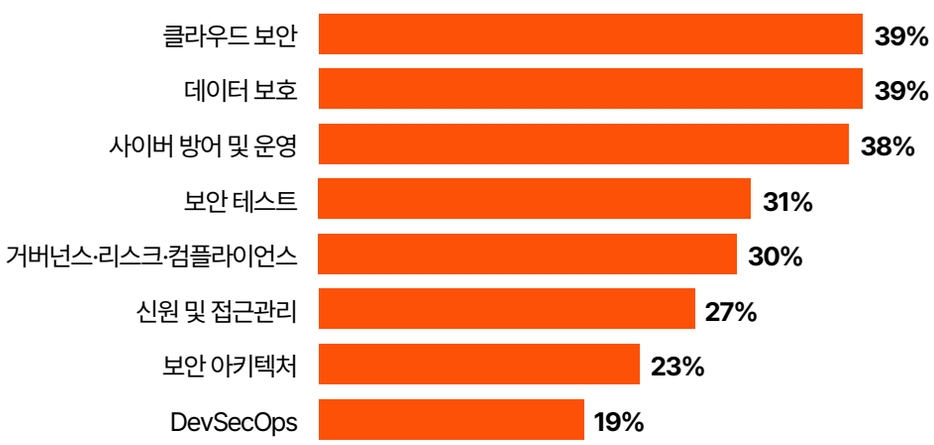
기업들은 이제 AI 에이전트, 즉 제한된 인간 개입으로도 목표 지향적 업무를 수행할 수 있는 자율 시스템이 사이버 보안 프로그램을 혁신할 수 있는 막대한 잠재력을 지니고 있음을 인식하고 있습니다. 이제 AI는 단순히 분석을 제공하는 도구가 아닙니다. 독립적으로 행동하고, 인간과 협력하며, 심지어 보안 대응을 스스로 시작할 수 있는 디지털 어시스턴트로 진화하고 있습니다. 이러한 변화는 효율성과 생산성 향상을 동시에 이끌어내고 있습니다.

이러한 이유로 보안 리더들은 향후 12개월 동안 조직이 우선적으로 강화해야 할 AI 보안 역량 중 하나로 AI 에이전트를 꼽고 있습니다.

향후 1년간 에이전트 솔루션이 가장 중점적으로 적용될 보안 우선순위 영역은 클라우드 보안, 데이터 보호, 그리고 사이버 방어 및 운영입니다. 이 밖에도 보안 테스트, 거버넌스·리스크·컴플라이언스(GRC), 신원 및 접근관리가 주요 우선순위 영역으로 꼽히고 있습니다.

효율성, 생산성을 증대하는 AI 에이전트 (상위 3대 우선순위로 선택한 비율 %)

Q. 향후 12개월 동안 귀사는 효율성, 생산성 향상을 위해 AI 에이전트를 어느 영역에 우선 적용할 계획입니까?



출처: PwC

AI 데이터 리스크 관리

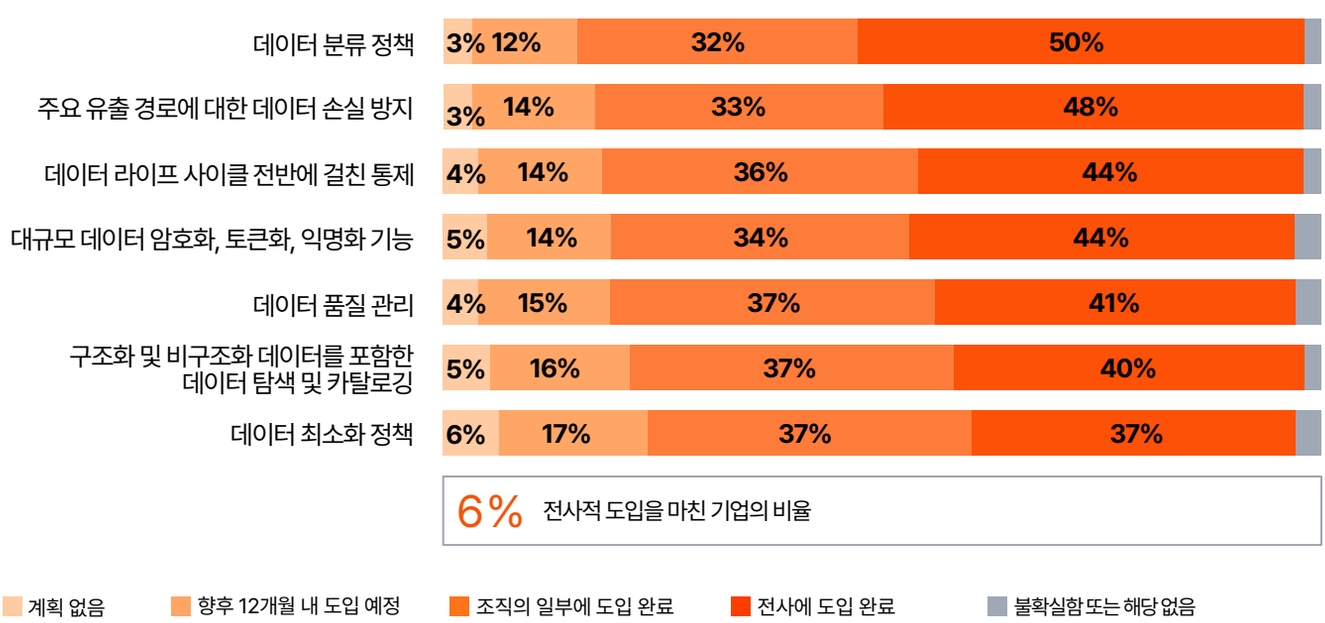
AI를 성공적으로 활용하기 위해서는 강력한 데이터 리스크 관리가 필수적입니다. AI 솔루션이 효과적으로 작동하려면 고품질로 정제된 데이터에 대한 접근해야 하며, 해당 데이터가 적절한 맥락에서 안전하게 사용되도록 하는 전사적 수준의 거버넌스와 보안 체계가 뒷받침되어야 합니다.

기업이 이러한 과제를 잘 수행하고 있는지 조사한 결과, 조직의 절반 정도만이 데이터 분류 정책을 전사에 도입하였으며(50%), 주요 데이터 유출 경로에 대한 데이터 손실 방지(DLP) 조치를 전사에 도입한 비율은 48%에 불과했습니다. 그 밖의 데이터 리스크 관리 조치들은 이보다 더 낮은 수준으로 나타났습니다. 더 나아가, 모든 주요 데이터 리스크 조치를 전사적으로 도입한 조직은 단 6%에 그쳤습니다.

이는 조직이 AI 솔루션에서 데이터의 잠재력을 완전히 활용하기까지 여전히 많은 과제가 남아 있음을 보여줍니다. 투명하고, 책임 있으며, 안전한 데이터 관리 관행을 통해 디지털 신뢰(Digital Trust)를 구축하는 것이 AI 기반 혁신과 성장을 실현하기 위한 열쇠입니다.

데이터 리스크 대응을 위한 조치의 실행 현황

Q. 귀사는 전사적 데이터 리스크 관리를 위해 다음의 조치를 어느 정도 도입했거나 도입을 계획하고 있습니까?



출처: PwC

04

양자 컴퓨팅에 대한 대비

Top 4

기업들이 가장 대비가 부족한 상위 4대 위협에 양자 컴퓨팅이 포함

49%

양자 내성 보안 조치를 고려하거나 도입하지 않은 기업의 비율

Only 8%

양자 컴퓨팅에 대한 대응을 최우선 예산 3대 순위에 포함한 리더의 비율

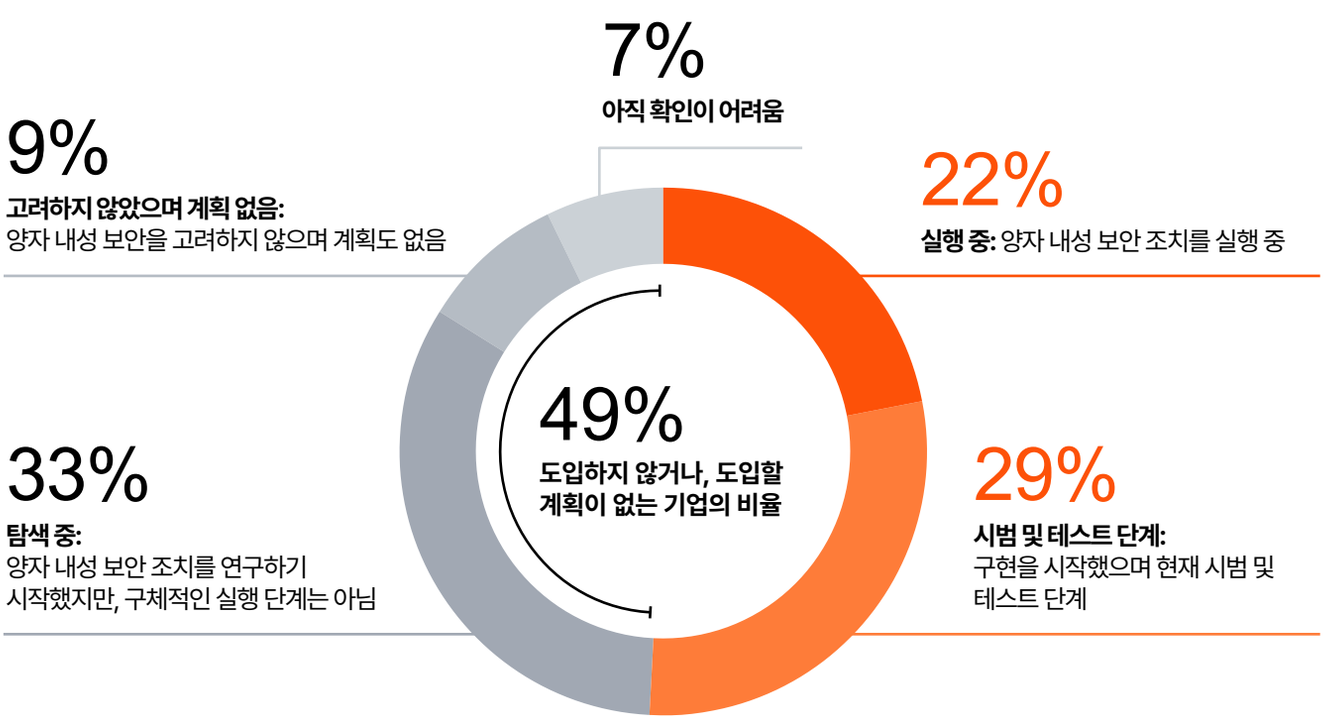
양자 컴퓨팅의 카운트다운이 이미 시작되었습니다. 이제 더 이상 이론적 단계에 머물지 않고, 연구실을 넘어 금융 모델링, 물류 최적화와 같은 복잡한 문제 해결에 실제로 활용되기 시작했습니다. 또한 수십 년간 유지되어 온 사이버 보안의 전제와 가정들을 근본적으로 뒤흔들고 있습니다.

양자 기술은 당장 사이버 위협으로 작용하지는 않지만, '포스트 양자 암호화(Post-Quantum Cryptography, PQC)'로의 전환을 늦추는 조직은 민감한 데이터, 인증 서비스, 암호화 시스템을 위험에 노출시킬 가능성이 있습니다. 양자 내성 보안(Quantum-resistant Security)을 구현하는 데에는 수년에 걸친 준비와 전환 과정이 필요하므로, 지금의 선제적 조치가 미래의 위협으로부터 조직을 보호하는 핵심이 됩니다.

현재 일부 기업들은 초기 단계를 진행 중이며, 29%가 시범 도입 및 테스트 단계에 있습니다. 그러나 22%만이 실제 구현 단계로 진입했으며, 49%는 양자 내성 보안 조치를 고려하거나 시작조차 하지 않은 상태입니다. 그렇다면 이들은 왜 뒤처지고 있을까? 대부분의 경우, 포스트 양자 리스크(Post-Quantum Risk)에 대한 이해 부족, 내부 자원의 한계, 그리고 다른 우선순위에의 투자가 주요 원인으로 나타났습니다.

양자 내성 보안의 준비도

Q. 귀사는 양자 내성 보안 도입에 있어 어느 정도 단계에 와있습니까?



출처: PwC

양자 위협 인식에 비해 더딘 조치

양자 위협에 대한 인식은 점점 높아지고 있습니다. 현재 양자 컴퓨팅은 조직이 가장 대응 준비가 부족하다고 느끼는 4대 위협 중 하나로 꼽히며, 이는 전년도 대비 여러 단계 상승한 결과입니다.

이러한 인식이 실제 행동으로 이어지고 있는지 조사 결과, 전체의 약 3분의 1만이 하나 이상의 양자 내성 보안 조치를 도입했으며, 모든 7개 조치를 도입 완료한 조직은 단 3%에 불과했습니다. 그럼에도 불구하고, 향후 1년간 보안 예산의 상위 3대 우선순위에 양자 대비를 포함한 보안 리더는 단 8%에 그쳤습니다.

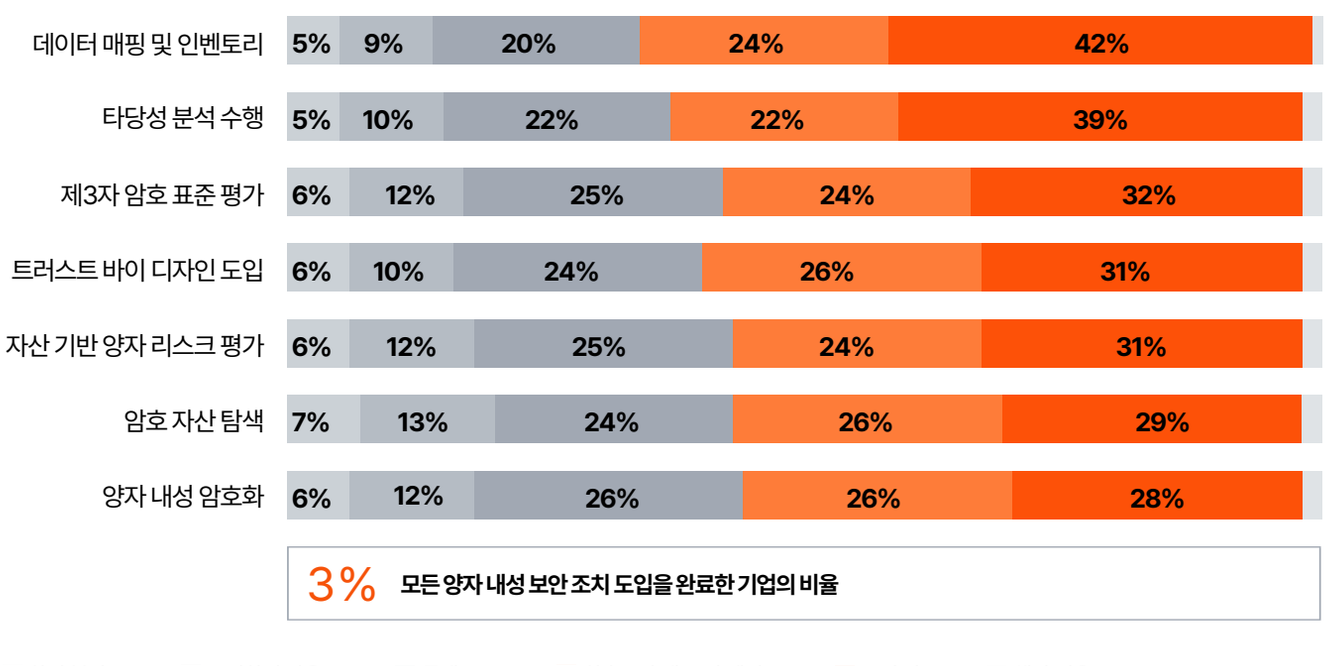
매출 50억 달러 이상의 대기업들은 상대적으로 준비가 잘 되어 있는 편입니다. 이들은 데이터 인벤토리 구축을 통한 '선수집, 후해독(HNDL, Harvest Now, Decrypt Later)[1]' 리스크 완화, 암호 자산 탐색을 통한 취약한 암호 시스템 식별, 양자 내성 암호화 테스트 및 구현, 타당성 분석과 양자 리스크 평가 수행 등을 포함한 조치를 취하였습니다. 또한 고성장 기업 역시 양자 기술이 초래할 사이버 위협을 인식하고 이에 맞추어 전략적으로 대비하고 있습니다.

그러나 이러한 기업들은 여전히 소수에 불과합니다. 기술이 발전할수록, 양자 내성 암호화 기술을 신속히 취할 수 있는 역량이 기업 경쟁력을 좌우하는 핵심 요소가 될 것입니다.

1) 양자 시대를 앞두고 해커들이 주목하는 수법으로서, 암호화되어 지금은 풀 수 없는 데이터를 일단 수집하고, 향후에 고도화된 양자 컴퓨팅이 가능해지면 암호를 풀겠다는 의도

양자 내성 보안 조치 구현 현황

Q. 귀사는 다음의 양자 내성 보안 조치를 어느 정도 진행하였습니까?



출처: PwC

포스트 양자 암호화가 어려운 이유

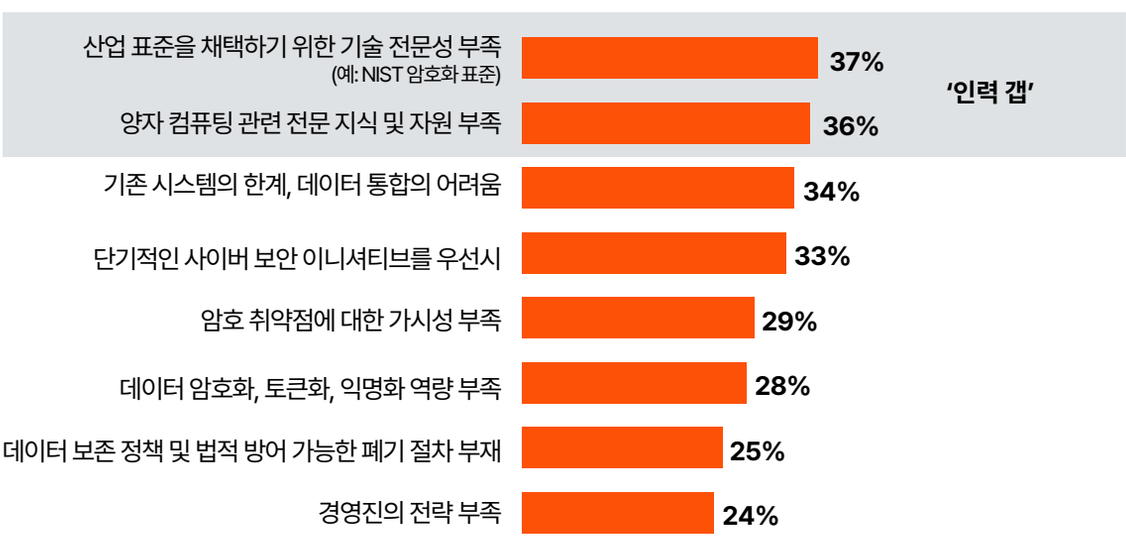
양자에 대한 대비는 단순한 기술 업그레이드가 아니라, 미래 지향적 보안 체계를 구축하기 위한 근본적이고 전략적인 변화입니다. 내부적인 저해요인으로는 기술 전문성의 격차, 조직 내 지식 및 이해 부족, 경직된 레거시 시스템 등이 있습니다.

조직이 양자 내성 암호로 전환하기 위해 암호화 인벤토리를 구축할 때는 기술 스택 전반에서 취약한 알고리즘을 식별해야 합니다. HNDL 리스크 때문에 공개 키 암호화가 취약하다는 점은 널리 알려져 있지만, 보안 리더들은 로그인 인증이나 전자 서명 같은 기능에서도 양자 컴퓨터 공격에 취약한 동일한 암호 알고리즘을 사용하고 있다는 사실을 인식해야 합니다.

이러한 과제들은 양자 대비를 우선순위에 두더라도, 암호 인벤토리를 구축하고 양자 내성 암호를 구현하는 데에는 시간이 필요하다는 사실을 명확히 보여줍니다. 그런데 그 시간은 충분하지 않습니다. 미국 국립표준기술연구소(NIST) 등 주요 암호화 표준 기관들은 공격자들이 양자 컴퓨팅 역량을 확보하기 전에 취약한 알고리즘을 폐기할 것을 권장하고 있습니다. 따라서 기업은 지식 격차를 해소하고, 자사 암호 의존도를 평가하며, 양자 대비 로드맵을 수립하는 것이 시급합니다.

포스트 양자 암호화 달성을 막는 주요 과제 (상위 3대 과제로 선택한 비율 %)

Q. 향후 12개월간 귀사가 포스트 양자 암호화를 달성하는 데 있어 가장 큰 내부 과제는 무엇입니까?



출처: PwC

05

매니지드 서비스의 필요성

Top 2

사이버 보안을 위한 AI 도입 시 두 가지 큰 걸림돌은 지식과 기술의 부족

53%

향후 12개월 동안 사이버 인력 격차 해소를 위한 3대 우선순위로 AI 및 머신러닝 툴을 꼽은 기업의 비율

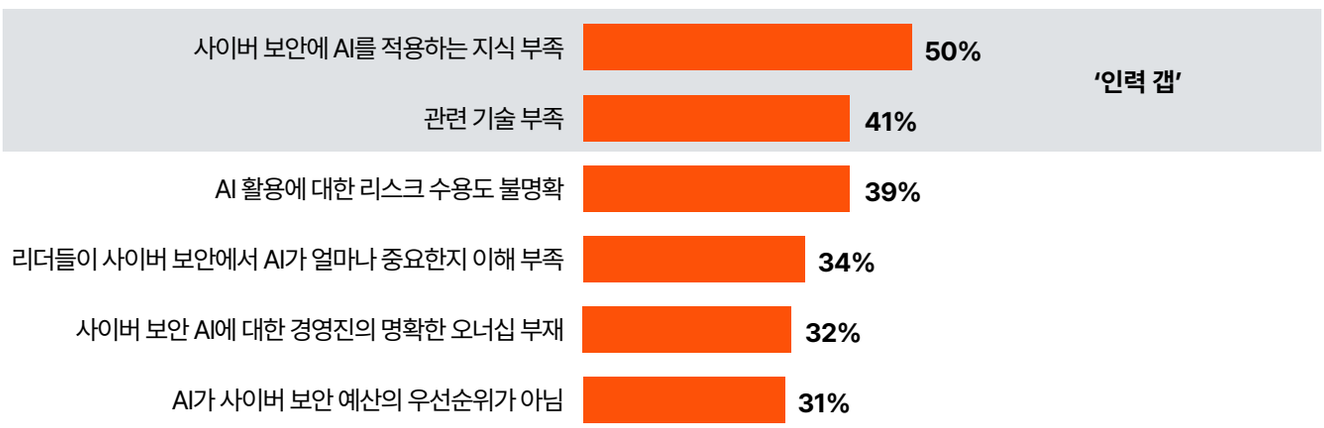
Only 48%

대규모 공격을 경험한 후 인력 격차 해소를 위해 매니지드 서비스를 우선시하는 기업의 비율

사이버 보안 인력 부족은 여전히 발전의 걸림돌이 되고 있습니다. 지난 1년 동안 사이버 보안을 위한 AI 도입의 가장 큰 장벽은 지식과 기술의 부족이었습니다. 이로 인해 많은 조직들이 역량 확장 방식을 재고하고 있으며, 대부분은 AI 툴(53%), 보안 자동화 도구(48%), 사이버 툴 통합(47%), 기존 인력의 재교육 또는 역량 강화(47%) 등을 모색하고 있습니다. 특히 대규모 공격을 경험한 조직(48%)은 매니지드 서비스를 우선순위로 두고 있습니다.

사이버 보안을 위한 AI 도입 시 걸림돌 (상위 3대 과제로 선택한 비율 %)

Q. 지난 12개월간 귀사가 사이버 보안을 위한 AI를 도입하는 과정에서 주요 걸림돌은 무엇입니까?



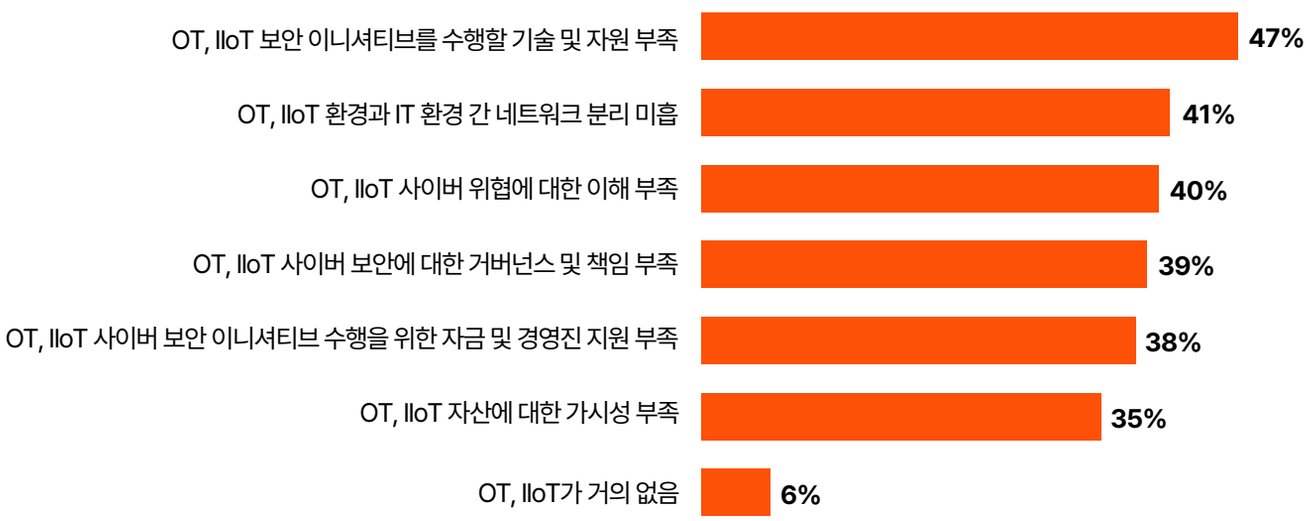
출처: PwC

OT 및 IIoT 보안 인력 부족

OT(Operational Technology)와 IIoT(Industrial IoT)은 오늘날 보안 환경에서 주요한 페인 포인트가 되고 있습니다. 경영진의 거의 절반(47%)은 자격을 갖춘 인력 부족을 상위 3대 과제로 꼽았으며, 39%는 거버넌스와 책임의 불명확성을 지적했습니다. 이러한 문제들은 많은 조직이 여전히 커넥티드 운영 시스템을 안정적으로 관리할 수 있는 구조와 전문성을 갖추지 못하고 있음을 보여줍니다.

OT 및 IIoT 보안의 주요 과제 (상위 3대 과제로 선택한 비율 %)

Q. 귀사가 OT 및 IIoT 보안에서 직면한 상위 3대 과제는 무엇입니까?



출처: PwC

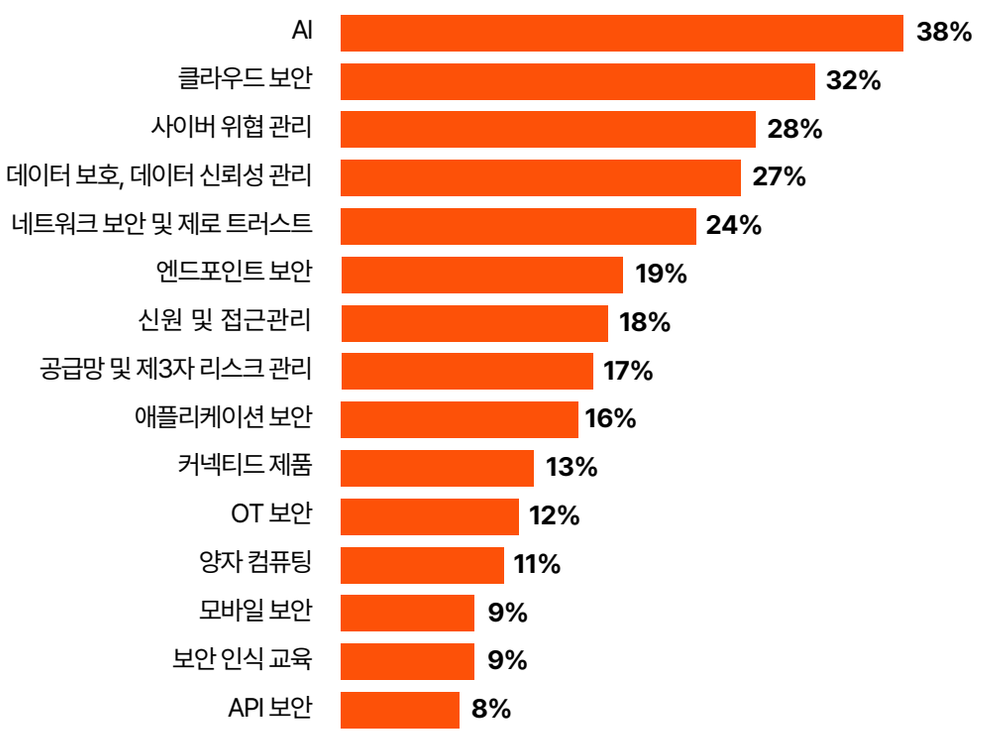
매니지드 서비스의 전략적 역할

AI와 클라우드는 가장 중요한 사이버 보안 투자 분야이자, 매니지드 서비스의 주요 활용 사례로 꼽히고 있습니다. 조직들은 단순히 역량을 외부에 위탁하기 위해서가 아니라, 핵심 시스템의 제공 방식을 현대화하기 위해 매니지드 서비스를 활용하고 있습니다.

매니지드 서비스는 단순히 기술 부족을 보완하는 것을 넘어, 속도, 확장성, 전문 지식을 동시에 제공하며, 날로 복잡해지는 위협 환경 속에서 조직이 혁신과 성장에 집중하면서 방어 체계를 현대화할 수 있는 수단을 제공합니다.

사이버 보안을 위한 매니지드 서비스의 우선순위 (상위 3대 우선순위로 선택한 비율 %)

Q. 향후 12개월 동안 귀사는 사이버 보안 프로그램의 어떤 영역에서 매니지드 서비스 활용을 우선시하고 있습니까?



출처: PwC

경영진의 Key Actions

불확실성을 돌파하는 리더십

올해 조사 결과에 따르면, 가장 미래지향적인 조직은 사이버 보안을 비즈니스 전략과 연계하고 사후 대응보다 사전 예방을 우선시하고 있습니다.

다수의 기업은 이미 주요 사이버 프레임워크에 부합하는 거버넌스 구조를 강화하고, 기업 전반에 걸쳐 사이버 리스크 통제를 내재화하며, 리스크 평가 및 보고를 우선시함으로써 사이버 리스크 관리의 기초를 다지고 있습니다.

그러나 미래에 대비하기 위해서는 기존 방식 이상의 노력이 필요합니다. 즉, 불확실성을 직면하고, 대담하지만 정보에 기반한 결정을 내리며, 전략에 민첩성을 더해야 합니다.

CISO와 CSO

복잡한 사이버 위협을 비즈니스 리스크로 인식하고, 사이버 보안이 조직 전체의 공동 책임임을 효과적으로 소통하는 역량이 중요합니다. 이러한 역량은 거버넌스, 회복력, 규제 준수, 대응 체계의 기반을 강화하는 데 도움이 됩니다. 앞으로는 시큐어 바이 디자인(Secure-by-design, 소프트웨어 개발 단계부터 보안 체계를 갖추는 것) 원칙을 발전시켜 새로운 유형의 리스크를 선제적으로 관리하고, 데이터 기반 의사결정을 통해 사이버 보안 투자의 우선순위를 명확히 제시해야 합니다.

현재 필요한 핵심 조치	미래를 위한 선제적 조치
글로벌 정세 변화에 대한 리스크 노출도를 정량화하고, 이를 핵심 인프라, 글로벌 운영, 산업별 교란 요인과 연계된 지표로 측정하여 C-레벨과 공유	C-레벨 및 이사회와 사이버 보안을 공동 책임으로 확립하고, 위협 인텔리전스 및 새로운 위협, 공격자 역량에 대한 요약 보고를 기반으로 거버넌스 논의를 정례화
고위험 지역, 사이버 위협 캠페인, 데이터 갈취 등의 최신 인텔리전스에 맞춰 동적 위협 모델링(Dynamic Threat Modelling) 구현	AI 에이전트 관리 및 거버넌스 체계를 운영화하고, 발견, 분류, 노출 매핑, 지속적 모니터링 및 적대적 시뮬레이션을 수행
AI 배포 전반에 책임 있는 AI 방법론을 내재화하고, AI 시스템(모델, 에이전트, 애플리케이션, 학습 데이터)을 민감도, 중요도, 노출 수준에 따라 분류	일회성 공급사 평가(Point-in-time Assessment)에서 지속적인 제3자 리스크 모니터링 체계로 전환
AI 보안을 강화하기 위해 기존 보안 통제를 AI 시스템으로 확장하고, AI 가드레일이나 LLM 게이트웨이 등 새로운 보안 역량이 필요한 부분의 격차를 식별	암호 기술에 의존하는 시스템을 식별하고, 필요한 경우 양자 내성 암호(PQC) 표준을 채택
AI나 양자 기술과 같은 신기술 리스크를 반영할 수 있도록 사이버 리스크 거버넌스 모델을 주기적으로 재검토 및 업데이트	기술과 인력을 보유하고 요구사항에 대응할 수 있는 매니지드 서비스를 활용할지를 ROI 기반으로 판단
제3자, 공급망, 레거시, 클라우드 기반 리스크 관리 성과를 추적할 수 있는 KPI를 설정하여 거버넌스를 강화	데이터를 평가하여 지금 즉시 양자 대비가 필요한 요소를 식별하고, 데이터 거버넌스 팀과 협력하여 양자 도입 계획을 수립
모의훈련 및 시뮬레이션을 수행하여 의사결정 과정, 보고 체계, 복구 절차를 검증	

CTO와 CIO

기술을 안전하게 확장하고, 인력 및 교육 격차를 선제적으로 해결하는 역할은 조직의 사이버 보안 태세를 강화하는 데 핵심적인 지원을 제공합니다. 앞으로도 보안 리더십과 긴밀히 협력하여 기술 도입 전반에 걸쳐 리스크 통제 및 거버넌스를 내재화해야 합니다. 또한 AI와 양자 컴퓨팅과 같은 신흥 기술을 보안 내재형으로 도입·통합하는 시범 프로젝트를 주도함으로써, 미래의 사이버 위협을 예측하고 완화하는 혁신을 추진해야 합니다.

현재 필요한 핵심 조치	미래를 위한 선제적 조치
AI 및 기타 신기술을 안전하게 확장하고, 예방 중심의 핵심 보안 조치에 예산을 배정 및 내재화	CISO 및 데이터 리더와 협력하여 AI 학습 데이터의 보안 및 AI 모델 입출력 거버넌스를 강화
CISO, CRO와 긴밀히 협력하여 기술 배포를 리스크 관리 및 규제 준수 요건과 연계	양자 기술 도입 및 시범 프로젝트를 보안 리더와 협력하여 조직 전반의 양자 내성 보안 전략과 연계
AI 보안 확보를 위해, 설계 단계부터 시큐어 바이 디자인 원칙에 맞춘 거버넌스 및 리스크 통제 체계를 적용	자동화 및 AI 기반 리스크 탐지·대응 도구를 적극 도입하여 운영 효율성과 회복력을 강화
제3자 플랫폼, API, 통합 시스템 전반에서 일관된 접근 및 정책 통제를 시행	커넥티드 제품의 전 생애 주기에 걸쳐 시큐어 바이 디자인 프레임워크를 적용
IIoT 및 OT 거버넌스를 아키텍처 전략에 통합하여 분산 환경 전반의 가시성과 통제력을 확보	

CRO

조직의 리스크를 식별하고, 사이버 보안과 연관되는 지점을 관리하는 역할은 조직 보호에 핵심입니다. 취약점에 맞게 통제 조치를 조정하고, 기존 리스크 관리 프레임워크가 최신 상태인지 지속적으로 검증해야 합니다. 또한 AI, 양자 기술, 정세 변화로 인한 영향을 통합한 적응형, 미래지향적 리스크 관리 전략을 구축하여, 조직의 민첩성과 회복력을 지원해야 합니다.

현재 필요한 핵심 조치	미래를 위한 선제적 조치
위협 시나리오를 리스크 등록부, 스트레스 테스트 주기에 포함하고, 지정학적 요인이 있는 위협을 우선순위로 설정	제3자 리스크 모델을 확장하여 공급사 환경의 양자 역량과 AI 오남용에 대한 회복력을 평가
위협 노출에 대응하기 위해 기존 통제 조치를 평가하고, 필요 시 완화 전략을 조정	AI를 활용해 사이버 리스크를 지속적으로 평가, 정량화, 보고할 수 있도록 체계를 고도화
AI 및 양자 관련 리스크를 맞춤형 비즈니스 영향 분석을 통해 정량화하고, 디지털 인력 자동화와 관련된 영역을 우선순위로 설정	지능통합형 리스크 프레임워크(IIRF) 를 개발하여 전략적 위협 인텔리전스를 기업 리스크 평가에 통합
사이버 위협 관리 체계를 규제 요구사항과 연계하여 준수 활동을 지원	예측형 위협 모델링 도구를 시범 운영하여 향후 12~36개월 내 발생 가능한 위협 및 그 비즈니스 영향 가능성을 정량화

CFO

전략적 이니셔티브와 기술 구현에서 선제적 사이버 보안 예산을 확보하고 관리하는 역할은 조직의 회복력 유지에 필수적입니다. 비효율을 식별하고, 효과적인 사이버 보안 프로젝트에 예산을 배정하는 노력을 해야 합니다. 앞으로는 미래 리스크에 대비하기 위해, 향후 예산 수요를 선제적으로 예측하고 ROI 중심의 투자 모델을 구축하여 조직이 보안 기술 및 인력에 현명하게 투자할 수 있도록 지원해야 합니다.

현재 필요한 핵심 조치	미래를 위한 선제적 조치
장기적 회복력, 경쟁 우위, 규제 대비성을 강화하는 전략적 투자를 지원	사이버 보안을 중요한 비즈니스 기능으로 격상하고, 투자 수준을 이사회 성과 목표와 연계
보안 사고에 대응하는 비용과 사전 방어 투자(매니지드 서비스, 보험, 규제 준수 등)의 장기 비용을 비교	제로데이 대응 역량 및 포스트 양자 보안 강화를 포함한 회복력 강화 예비 자금을 마련
사이버 보안 ROI 지표를 재정립하여, 사고 예방, 벌금 방지, 대응 시간 단축으로 인한 절감 효과를 포함	보안 매니지드 서비스에 대한 ROI 기반 비즈니스 케이스를 개발
CISO, CTO, CIO와 협력하여 보안 역량 개발 및 기술 교육에 대한 예산을 효과적으로 배분	툴 중복 및 비효율을 식별·감축하고, 가능한 경우 통합을 추진
운영비와 전략적 사이버 투자 간의 균형을 유지하는 지속 가능한 자금 조달 모델을 구축	

CEO

사이버 보안을 비즈니스의 핵심 우선순위로 유지하려는 지속적인 노력이 매우 중요합니다. 비즈니스 전략과 사이버 리스크 관리 전략을 연계하고, 이사회 및 C-레벨 간의 협력을 강화하는 역할을 지속해야 합니다. 앞으로는 산업 간 파트너십을 구축하고, 새로운 사이버 위협에 대응할 수 있는 투자를 주도하는 리더십이 요구됩니다.

현재 필요한 핵심 조치	미래를 위한 선제적 조치
워크숍 등을 통해 사이버 공격 대응 훈련을 필수로 진행하고, 업종별 위기 상황과 복합 위협을 가상 시나리오로 연습	포스트 양자 표준화, 공동 방어 태세, 위협 인텔리전스 공유를 위한 산업 간 협력체를 주도
사이버 회복력과 매출 창출을 연계하여, 디지털 플랫폼 보안, 고객 데이터 신뢰 확보, 해외 시장 확대를 지원	AI와 양자 등 신기술 투자를 초기부터 시큐어 바이 디자인 원칙에 따라 추진
AI 및 양자 프로젝트가 초기 단계부터 윤리와 보안 관점에서 기준을 갖추도록 책임 있는 혁신을 주도	양자 및 글로벌 정세 변화 리스크 전망을 전략 기획 업무와 이사회 리스크 헌장에 통합
사이버 보안 예산의 트레이드 오프가 리스크 허용 범위에 부합하는지 평가	정세 급변, 기술적 교란에 대비한 스트레스 테스트에 직접 참여
이사회부터 실무진까지 모든 수준에서 사이버 보안을 공동 책임으로 확립	
이사회에 사이버 프로그램의 우선순위를 정기적으로 보고하고, 이사회 구성원들과 지속 논의	

Contacts

문 홍 기 Partner

hong-ki.moon@pwc.com
02-709-0394

박 현 출 Partner

hyunchul.park@pwc.com
02-709-0412

이 성 호 Partner

sungho1.lee@pwc.com
02-3781-1773

김 태 형 Partner

taehyung2.kim@pwc.com
02-709-0583

S/N: 2511C-RP-130