Deloitte.

글로벌 사이버 서베이

: 사이버보안 리질리언스를 통한 가치 제고

Deloitte Global

Nov, 2024

Leader’s Message

서영수 파트너
Cyber 리더 |
Cyber Risk & Compliance

이제 기업 리더들은 사이버 보안이 단순한 IT 문제가 아니라,

조직 전체의 모든 기능과 수준에 통합되어야 하는 비즈니스 필수 과제임을 이해해야 합니다.

사이버 보안과 맞닿는 비즈니스 모든 영역에서

협업, 정보 공유, 의사 결정이 더욱 원활해질 수 있도록 지원하여,

조직의 중요한 자산과 명성을 더욱 잘 보호하고,

점점 더 디지털화되는 세상에서 전반적인 회복력을 강화해야 할 것입니다.

이번 서베이가 사이버 보안 전략 수립에 임하는 이들에게 좋은 인사이트가 되기를 바랍니다.

목차

사이버 전략의 새로운 시대가 열린다

사이버의 미래는 끊임없이 진화하고 있다. 전 세계 기업은 지속적인 비즈니스 복잡성과 변화, 새롭게 등장하는 수많은 위협과 위험에 대응하며 사이버 역량을 발전시키고 있다.

한 가지 변함없는 사실은 사이버와 비즈니스 가치가 서로 깊이 얽혀 있다는 점이다.

사이버 보안은 모든 업계의 기업이 원하는 성과 창출에 핵심적인 요인이 되었다.

딜로이트의 글로벌 사이버 서베이 2024~2025 (제4판)에서는 사이버 보안과 비즈니스 영향 사이의 강력한 연관성을 중점적으로 다룬다.

이 서베이는 **전 세계 다양한 업계의 약 1,200명의 리더에게 사이버 위협 및 보안, 기업 활동 및 미래에 대한 견해**를 조사했다.

설문 조사에는 기업의 최고 경영진은 물론 IT, 보안, 리스크, 비즈니스를 담당하는 고위 리더가 포함되었다.

서베이 방법론

조사 목적 및 개요

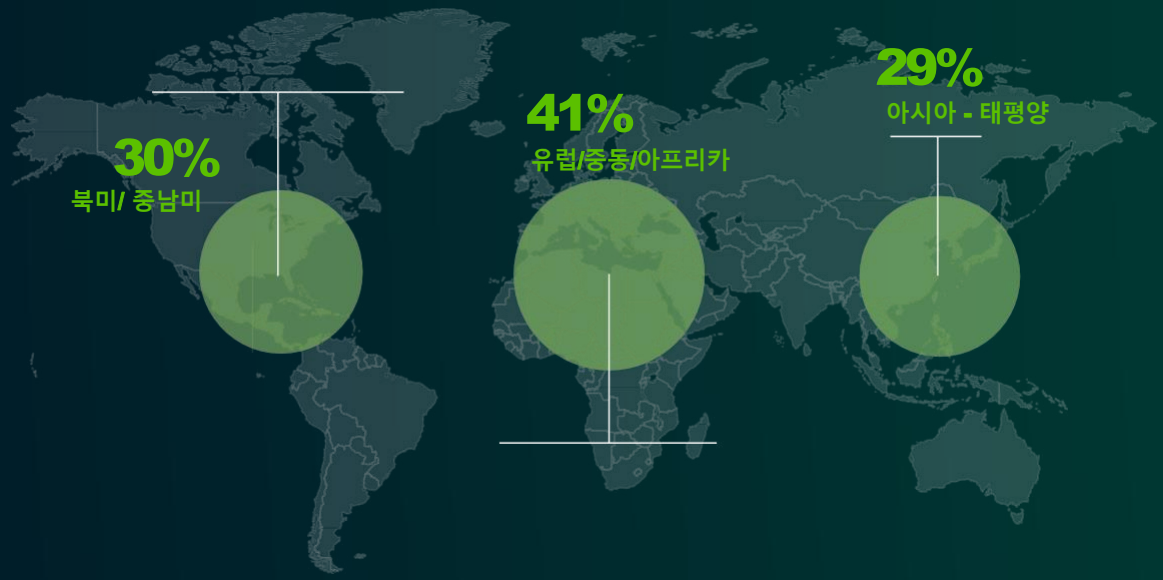
- 글로벌 비즈니스 및 기술 환경의 복잡성을 파악
- 사이버 보안의 중요성을 인식하고 있지만 그 가치를 활용하는 데 어려움을 겪고 있는 기업 리더들을 위한 설문 항목 설계

조사 대상

- 최고 경영진과 직속 부하 직원을 포함하여 이사급 이상 사이버 관련 의사 결정자 약 1,200명을 대상으로 설문조사 및 인터뷰 진행

- 43개 국가, 6개 산업군에서 수집된 데이터를 반영하며, 직원 수가 1,000명 이상, 연매출 5억 달러 이상인 기업으로 설문조사 대상 한정

조사 대상 기업 본사 위치 분포

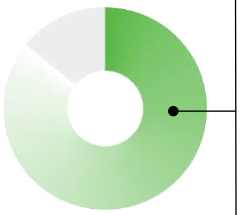


핵심 인사이트

사이버 보안은 비즈니스 가치 창출을 위한 전략적 필수 요소이며 그 중요성은 더욱 강화되고 있다.

오늘날 서로 깊이 연결된 디지털 환경에서 사이버 보안의 근본적인 중요성은 부정할 수 없다.

조직들은 비즈니스의 가치를 높이기 위해 잠재적인 사이버 위협에 대비할 수 있는 다양한 활동과 전략적 수단을 충분히 갖춰야 한다.



86%

응답자 86%가 사이버 보안을 강화하기 위해 중간 ~ 높은 수준의 특정 조치를 시행하고 있는 것으로 나타났다.

대다수 설문조사 응답자는 사이버 보안 조치의 필요성을 진지하게 받아들이고 있으며, 86%가 사이버 보안을 강화하기 위해 중간 수준 ~ 높은 수준의 특정 조치를 시행하고 있는 것으로 나타났다.

이는 조직이 사이버 보안 프로그램의 중요성을 크게 이해하고 있음을 시사한다. 또한, 조직들이 계속 증가하는 사이버 보안 활동에 발맞추어 나가고 있음을 보여준다.

설문조사 응답자는 사이버 보안을 관리하기 위해 위험 완화, 사이버 보안 통제 강화, 사고 대응 개선, 직원 인식 제고, 전략적 사이버 보안 계획 채택 등 다양한 활동에 집중하고 있었다.

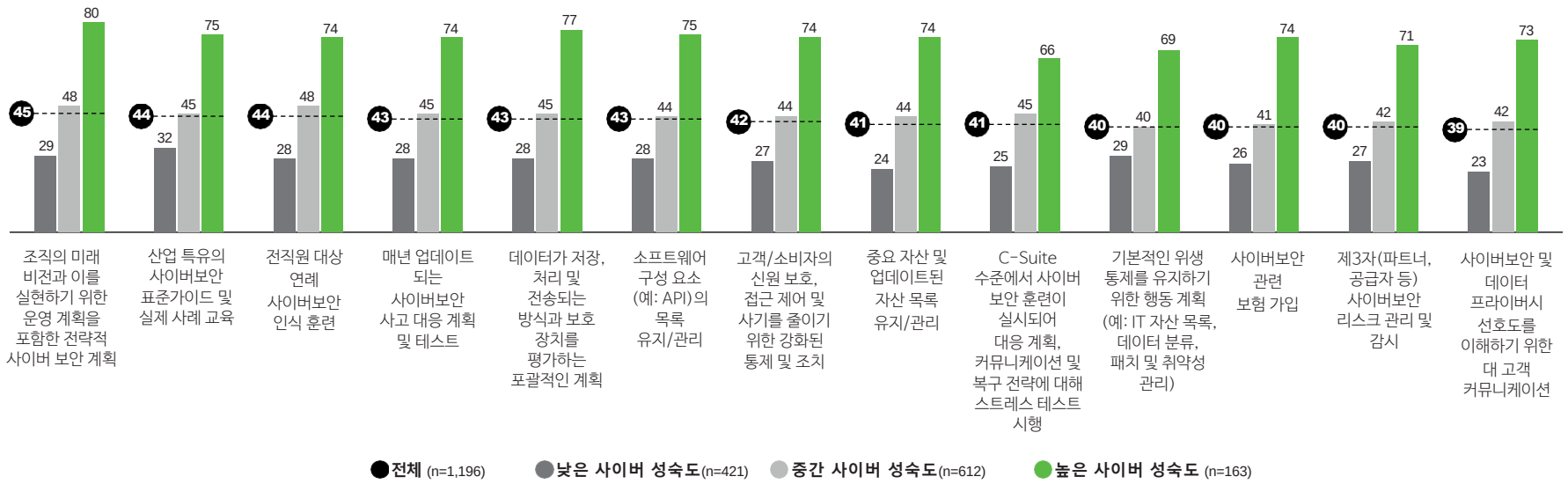
사이버 성숙도의 관점에서 살펴보면, 사이버 성숙도가 높은 조직들이 그렇지 않은 조직들에 비해 이러한 조치를 더 많이 수행하고 있는 것으로 나타났다.

사이버 보안의 기본 원칙을 올바르게 설정하고 이를 지속적으로 발전시키는 것이 핵심입니다. 기본적인 통제, 자산 관리, 취약성 관리와 같은 것들 말이죠. 이런 부분에서는 거의 무의식적으로 뛰어난 역량을 발휘해야 합니다. 그것들이 그냥 자연스럽게 이루어져야 합니다.

- CISO, Life Sciences and Healthcare Organization

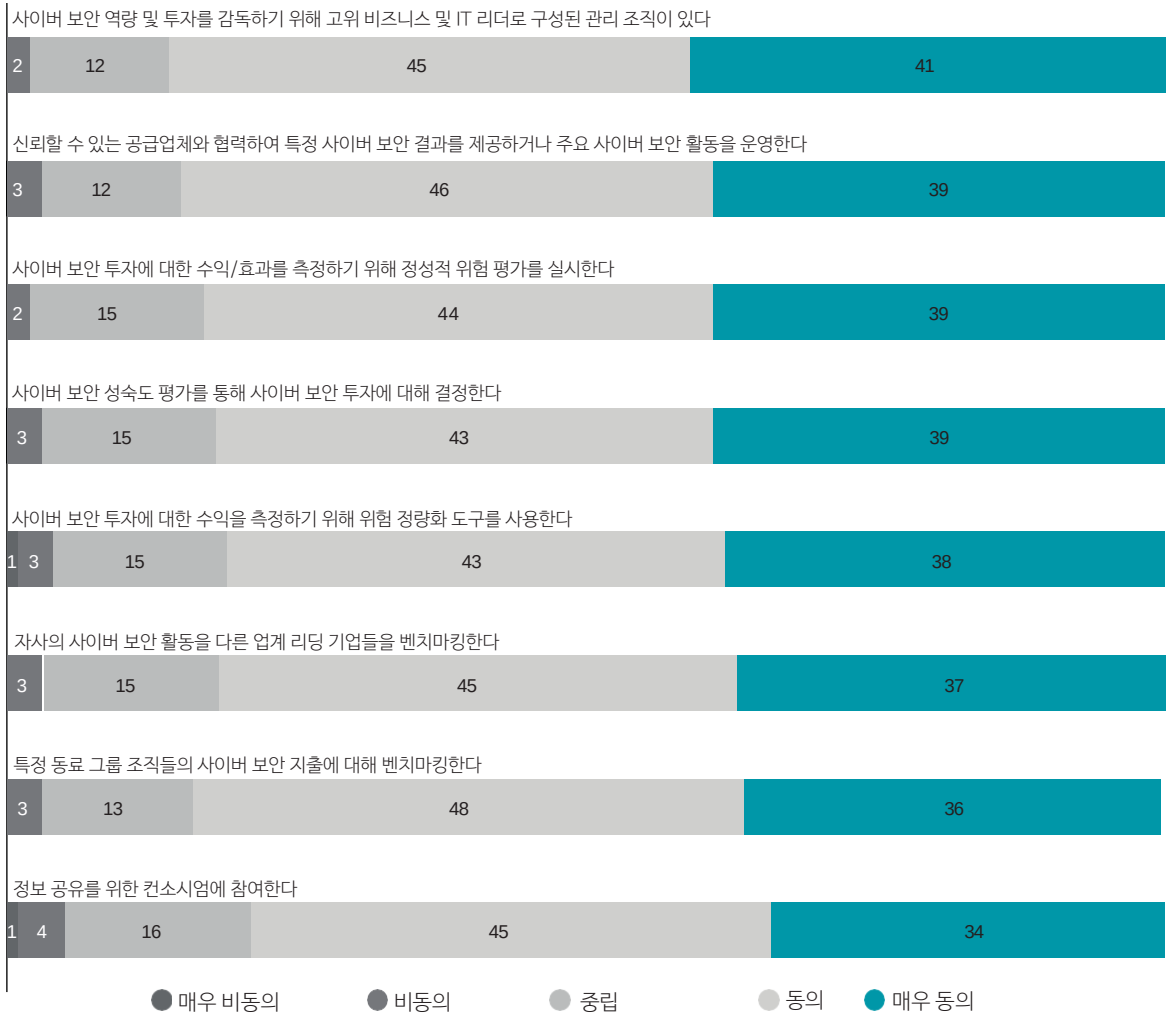
그림1: 사이버 성숙도가 높은 조직일수록 많은 사이버 보안 활동 수행

(단위: %)



(n=1,196)

그림2: 전략적 차원에서 사이버 보안 강화 조치/활동 수행 여부



(n=1,196)

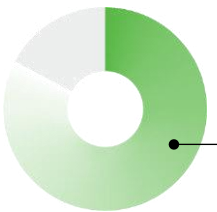
Note: 반올림으로 인해 총합이 100이 되지 않을 수 있음.

조직의 전략 차원에서 사이버 보안 강화 조치는 비즈니스 전반에 더 통합되고 있다.

대다수 조직들은 벤치마킹 및 측정, 신뢰할 수 있는 공급업체와의 협력, 정보 공유를 위한 컨소시엄 참여, 사이버 보안 역량 및 투자 감독을 위해, 고위 비즈니스 및 IT 리더로 구성된 관리 기관 설립 등 여러 전략적 사이버 보안 조치를 수행하고 있다.

조사에 응답한 83%는 이러한 조치가 전체 사이버 보안 전략의 필수 요소라고 일부 동의하거나 전적으로 동의했다.

이러한 동의 수준은 사이버 보안 전략이 비즈니스에 지속적으로 통합되고 있음을 시사한다.



83%

응답자의 83%는 이러한 조치가 전체 사이버 보안 전략의 필수 요소라고 동의했다.

조사에 응답한 전 세계 응답자의 **절반 이상(57%)이 향후 12~24개월 동안 사이버 보안 예산을 증액할 것으로** 응답했다.

또한, 응답자의 58%는 사이버 보안 지출을 디지털 전환 이니셔티브, IT 프로그램, 클라우드 투자와 같은 다른 프로그램 예산과 통합하기 시작할 것이라고 답했다.

이러한 투자와 예산 통합 수준은 사이버 보안 활동이 비즈니스 전반에 걸쳐 점점 더 긴밀하게 연결되어 있다는 점을 시사한다.

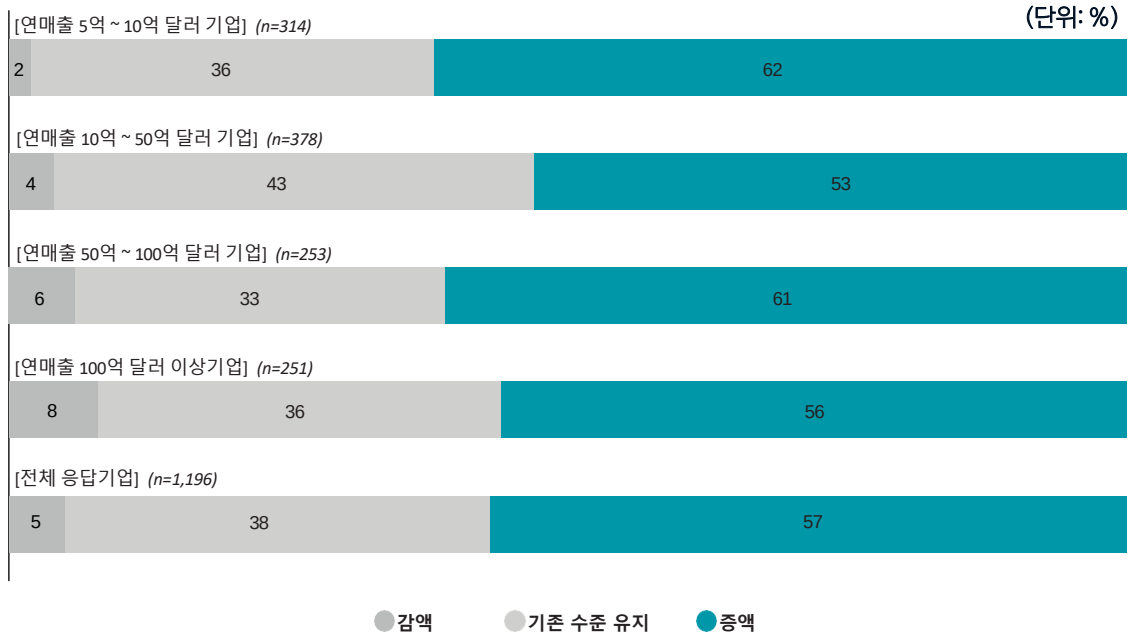
비즈니스 및 기술 운영, 그리고 리더십 전반에 걸쳐 지속적으로 사이버 보안 도입/투자를 우선시하고 구축하는 것은 조직이 전략적 성과를 성공적으로 달성하기 위해 필수적이다.

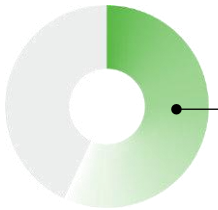
사이버 성숙도가 높은 조직은 사이버 보안이 단순한 IT 문제가 아니라 조직의 모든 기능과 수준에서 통합이 필요한 비즈니스 핵심 필수 요소임을 이해하고 있다. 이러한 강력한 사이버 보안 연결을 촉진함으로써 조직은 사이버 보안과 관련된 협업, 정보 공유, 의사 결정 역량을 강화할 수 있다.

이러한 접근 방식은 리더들이 비즈니스 목표를 달성하는 동시에 사이버 위험을 효과적으로 완화하며 정보에 기반한 전략적 결정을 내리도록 만든다.

사이버 보안을 기업 기능과 리더십 역할에 통합하여 강력한 사이버 보안 연결을 구축한 조직은 디지털화가 가속화되는 상황에서 기업의 자산, 명성, 전반적인 회복력(resilience)을 더욱 잘 보호할 수 있다.

그림3: 기업규모별 사이버 보안 예산 증액 계획 비율





57%

응답자가 향후 1~2년 이내 사이버 보안 예산을 증액할 것이라 답했다.

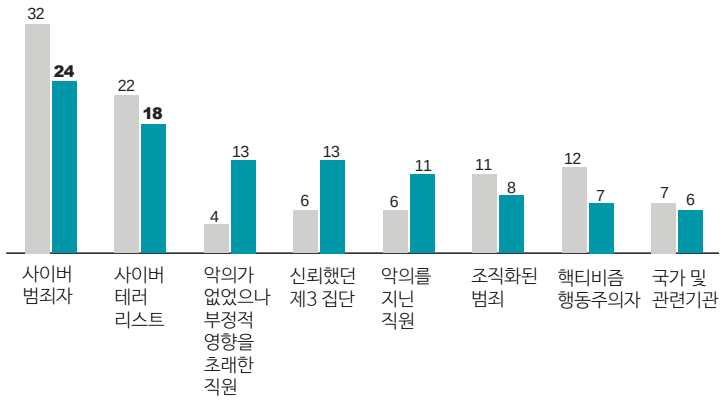
기업은 규모, 보유 데이터 유형, 온라인 영향력, 공급망 구조 등 다양한 요인에 따라 그 성격이 다르기 때문에 사이버 보안 위협의 성격도 각기 다릅니다. 모든 기업이 자신을 노리는 이들이 누구이며 그 이유와 그들의 운영 방식을 이해하는 것을 포함해 사이버 보안 위협에 대한 인텔리전스 전략을 갖추는 것이 중요합니다. 잠재적 공격자의 동기와 전술을 이해하는 것은 효과적인 보안 조치를 위해 필수적입니다.

— Gary Harbison, Chief Information Security Officer, Johnson & Johnson

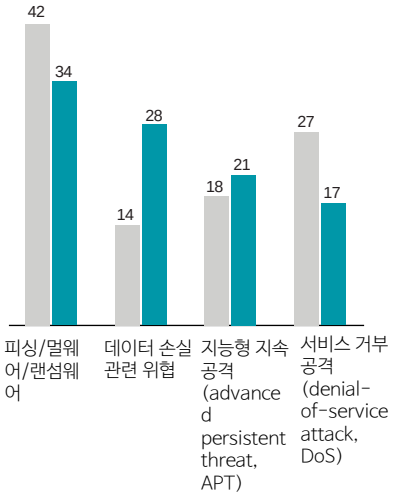
조사 결과, 응답자들은 평균적으로 매년 1억 4,700만 달러에서 2억 6,600만 달러를 IT에 지출하고 있으며, 그중 19%인 3,900만 달러가 사이버 보안 관련 활동에 할당되고 있다. 응답자들은 향후 12~24개월 내에 이 지출을 3% 증가시킬 것으로 나타났다.

그림4: 사이버 보안 위협 행위의 주체, 유형 및 위협 시도 횟수

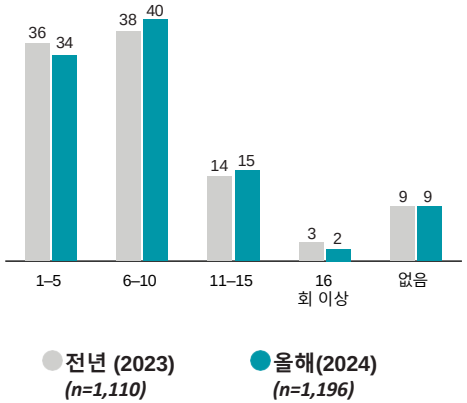
사이버보안 위협 주체 (%)



사이버보안 위협 유형 (%)

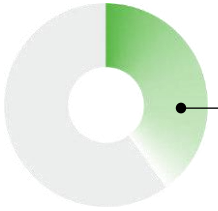


사이버보안 위협 횟수 (건, %)



전년 (2023) *(n=1,110)*

올해(2024) *(n=1,196)*



40%

응답자들은 6~10회의 사이버보안 위협을 겪었다고 답했다.

사이버 공격이 확대되고 있으며, 생성형 AI와 관련된 새로운 위협과 사이버 위험도 증가하고 있다. 이전 조사와 유사하게, 사이버 범죄자와 테러리스트가 주요 위협 세력으로 확인되었으며, 응답자의 42%가 이를 다양한 위협 요인 중 가장 걱정하는 요인으로 꼽았다.

또한 정치적 또는 사회적 목적을 추구하는 핵티비스트(Hactivist, Hacker + Activist), 금전적 이득을 위해 악의적 활동을 저지르는 사이버 범죄자, 그리고 개인적 불만이나 이익을 위해 행동하는 내부자 등도 위협의 주체인 것으로 나타났다.

사이버 공격자가 사용하는 도구와 기술로는 피싱, 멀웨어, 가장 큰 위협 기술로 나타났다(34%). 이는 이전 조사보다 8% 포인트 하락한 수치로, 데이터 손실과 관련된 위협이 크게 증가한 것과 맞물려 있다. 데이터 손실 위협 보고는 이전 조사에서 14%에서 이번 조사에서는 28%로 상승했다.

한편, 응답자의 40%는 지난 1년간 6~10건의 사이버 보안 침해를 당했다고 밝혔으며, 이는 이전 조사보다 2% 포인트 증가한 수치이다.
공격이 지속적으로 증가하는 것은 놀라운 일이 아니다. 위협 행위자가 접근할 수 있는 공격 표면이 계속해서 확장되고 있기 때문이다.

또한 생성형AI의 출현으로 인해 발생하는 새로운 사이버 위험에 대한 응답자들의 대응을 추적해봤다. 분석 결과, 이러한 위험에 대한 인식은 사이버 성숙도가 높은 조직에서 더 두드러지게 나타났다.
가장 사이버 성숙도가 높은 조직들이 사이버 보안 전략에 영향을 미칠 것으로 보는 주요 생성형AI 관련 위험 4가지는 다음과 같다.

- 생성형 AI 출력값의 설명 가능성 (82%)
- 생성형 AI 알고리즘이 정보 무결성 위험을 유발할 가능성 (81%)
- 생성형 AI와 인간의 협업과 관련된 통제의 효과적인 개발 (81%)
- 데이터 오염(예: 생성형 AI 출력에 영향을 미치기 위해 훈련 데이터 세트를 손상시키는 행위) (80%)

더 많은 조직이 프로세스를 자동화하고 공급업체 및 기타 제3자와 데이터를 공유함에 따라 새로운 취약점이 발생할 수 있다. 이처럼 점점 더 복잡해지는 디지털 인프라와 생태계는 새로운 공격 기회를 제공한다.

다양한 기업에 걸쳐 있는 모든 것과 모든 사람이 서로 연결되면서 보안 위험이 확대되고 있습니다. 우리의 전체 공급망을 관리하는 능력의 수준을 고려해 보세요. 네트워크에 접촉하는 모든 사람이 보안 및 통제를 처리할 수 있는 동일한 능력과 역량을 갖추도록 어떻게 보장할 수 있을까요?

—Patrick Milligan, Chief Information Security Officer, Ford Motor Company

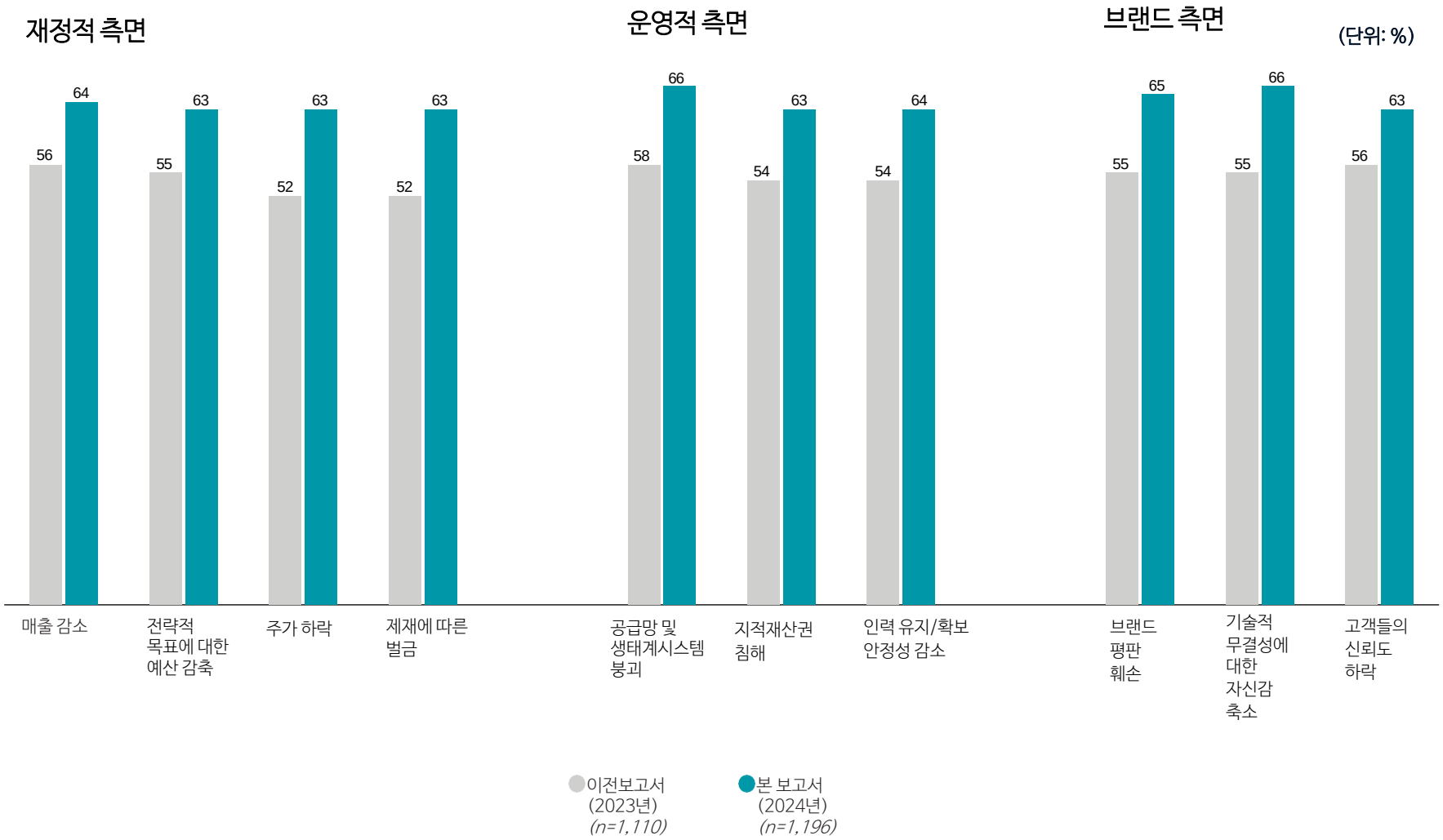
사이버 프로그램에서 얻을 수 있는 이점에 대한 기대가 커짐에 따라 기술 무결성이 응답자들 사이에서 가장 큰 우려 사항으로 떠오르고 있다. 조직들은 재정적 측면, 운영적 측면, 브랜드 측면 등 3가지 영역에 걸쳐 부정적인 영향을 받는 것으로 나타났다.

응답자들은 이전 보고서(2023년 보고서) 결과 보다 3가지 측면 모두 부정적인 영향을 더 많이 받고 있다고 답했다. 이러한 증가세는 2가지 함의를 가지고 있다.

첫째, 조직들이 사이버 공격으로 인한 영향을 보다 포괄적으로 보고하고 있을 가능성이 있으며, 이는 인식의 확장을 의미한다.

둘째, 생성형 AI 및 기타 첨단 기술로 인해 공격 범위가 확장되고 빈도가 증가했으며, 이는 향후 강력한 사이버 보안 계획의 필요성을 분명히 보여주고 있다.

그림5: 재정, 운영, 브랜드 측면에서 사이버 위협이 미치는 부정적 영향



사이버 사고로 인한 이러한 부정적인 결과는 조직들이 사이버 보안 이니셔티브를 통해 달성할 것으로 기대하는 긍정적인 비즈니스 성과와 극명하게 대조된다. 조사에 따르면, 사이버 보안 이니셔티브로 인해 얻을 것으로 기대하는 주요 결과는 다음과 같다
: (1) 지적 재산 보호 (2) 위협 탐지 및 대응 개선 (3) 효율성 및 민첩성 증가

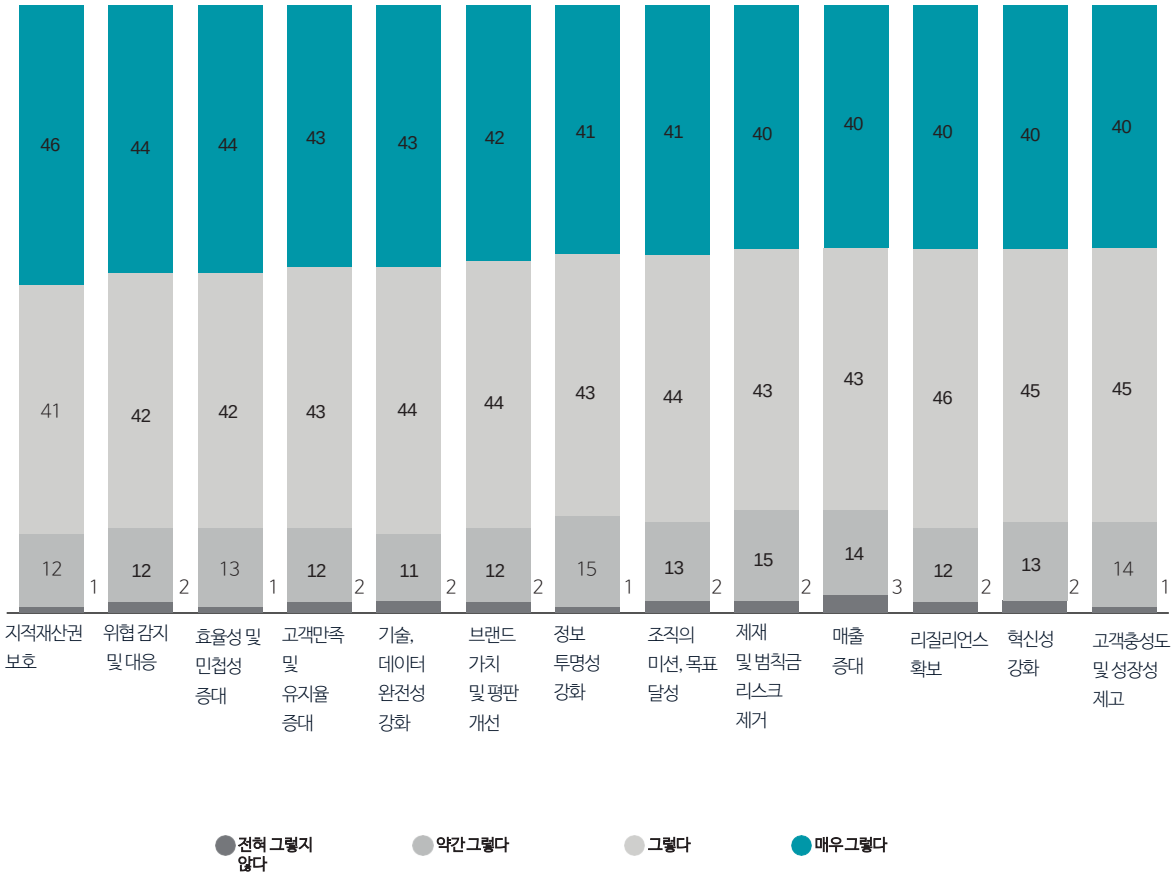
사이버보안 이니셔티브로 기대되는 이점 (산업군별)

사이버 기능의 주요 책임자인 CISO에게 이러한 기대가 집중되고 있으며, 이들은 비즈니스 기대치를 관리하고 달성하는 데 막대한 업무를 수행해야 한다.

사이버 보안을 통해 위험과 부정적인 영향을 최소화하고 가능한 많은 이점을 극대화하여 궁극적으로 신뢰할 수 있는 데이터를 활용하여 성장 추진에 있어 보다 안전하고 회복력 있는 조직을 만들어가야 한다.

그림6: 사이버보안 이니셔티브 및 조치를 통한 긍정적 영향 기대치

(단위: %)



(n=1,196)

조사에 따르면, 응답자들은 조직 내에서 대부분의 사이버 보안 활동에 대해 CISO(최고정보보호책임자)가 주로 책임을 지고 있으며, CIO(최고정보책임자)도 중요한 역할을 하고 있다고 답했다.

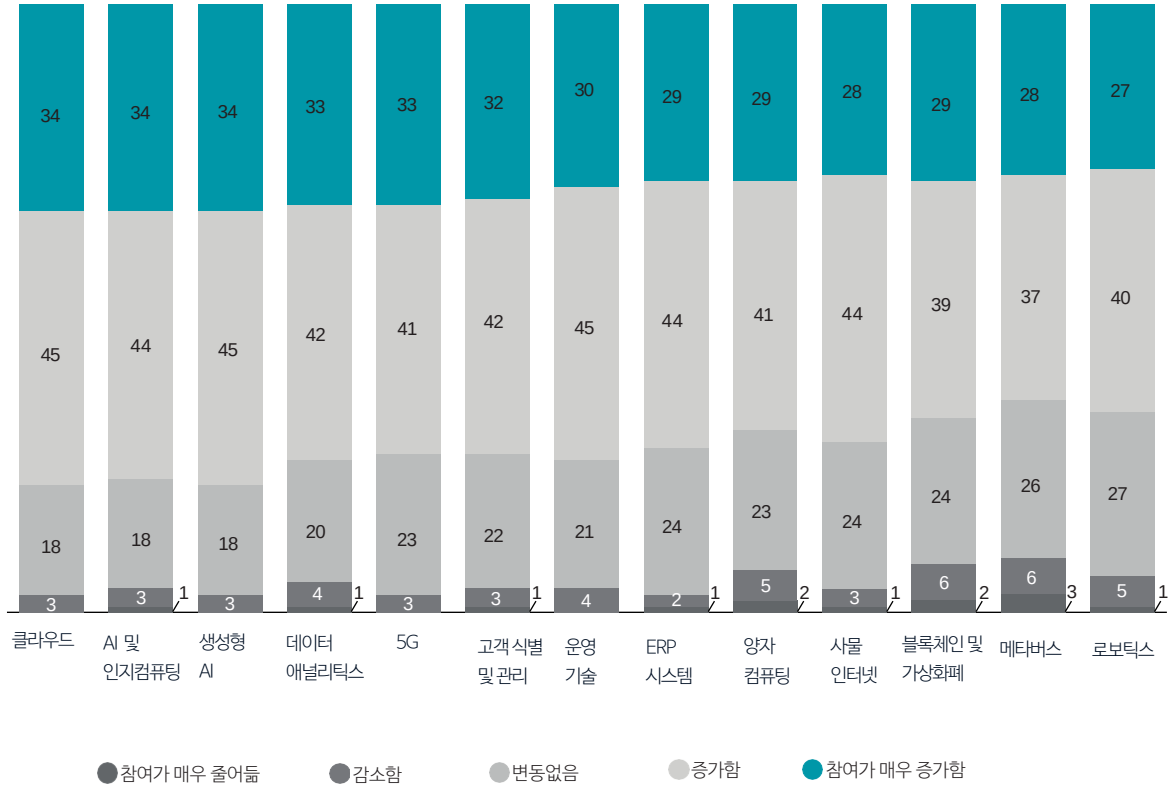
종종 CISO는 CIO 또는 CTO에게 보고하지만, 약 5분의 1의 CISO는 CEO에게 직접 보고하고 있는 것으로 나타났다. 이는 비즈니스와 정보보안의 연결성이 점점 높아진다는 것을 나타내는 중요한 신호로, C-레벨 및 경영진 전반에 걸쳐 CISO의 영향력이 확대되고 있음을 보여준다.

CISO 또는 그와 동등한 리더의 영향력은 다른 방식으로도 확대되고 있는 것으로 보인다. CISO는 기술 역량에 대한 전략적 비즈니스 논의에 점점 더 많이 참여하고 있으며, 이는 비즈니스 가치를 창출하는 데 있어 CISO의 중요성이 커지고 있음을 반영한다.

비즈니스 의사결정에 있어 CISO의 참여는 이제 선택 사항이 아니다. 약 3분의 1의 응답자는 지난 1년 동안 클라우드, AI/인지 컴퓨팅, 생성형 AI, 데이터 분석, 5G, 고객 신원 및 접근 관리와 같은 기술 역량에 대한 전략적 논의 부문에서 CISO의 참여가 크게 증가했다고 답했다.

그림7: CISO(최고정보보호책임자)의 기술 관련 비즈니스 의사결정 참여 증가

(단위: %)



(n=1,196)

경영진 중 CISO의 영향력이 커지고 조직이 사이버 역량을 강화하려 함에 따라, CISO는 이사회와 C-레벨 경영진에게 보안 취약점, 위험 시나리오, 그리고 더 높은 회복력을 위한 조치를 조언하고 교육하는 중요한 파트너가 될 것으로 예상된다.

앞으로 CISO는 조직의 전체 사이버 보안 전략을 이끌 뿐만 아니라, 다른 C-레벨 경영진과 긴밀히 협력하여 보안 이니셔티브를 비즈니스 목표에 맞추는 전략적 지침을 제공할 것으로 보인다.

사이버 보안에 집중하는 C-레벨 경영진 중 단 34%만이 C-레벨과 이사회가 사이버 보안을 적절히 관리할 수 있을 것이라는 강한 확신을 가지고 있는 것으로 나타났다.

분석에 따르면, 사이버 성숙도가 높은 조직은 CISO의 역할이 C-레벨 및 이사회와의 소통에 있어 필수적이며, 사이버 보안 위험을 효과적으로 해결하는 데 핵심이라는 점을 이해하고 있다.

딜로이트는 CISO의 역할이 커지고 있는 이 같은 추세를 확인하며, 사이버 위협의 진화, 기술 역량, 사이버 보안의 비즈니스 통합을 고려할 때 조직들이 CISO의 역할을 더욱 강화하는 조치를 가속화할 것을 권장하는 바이다.

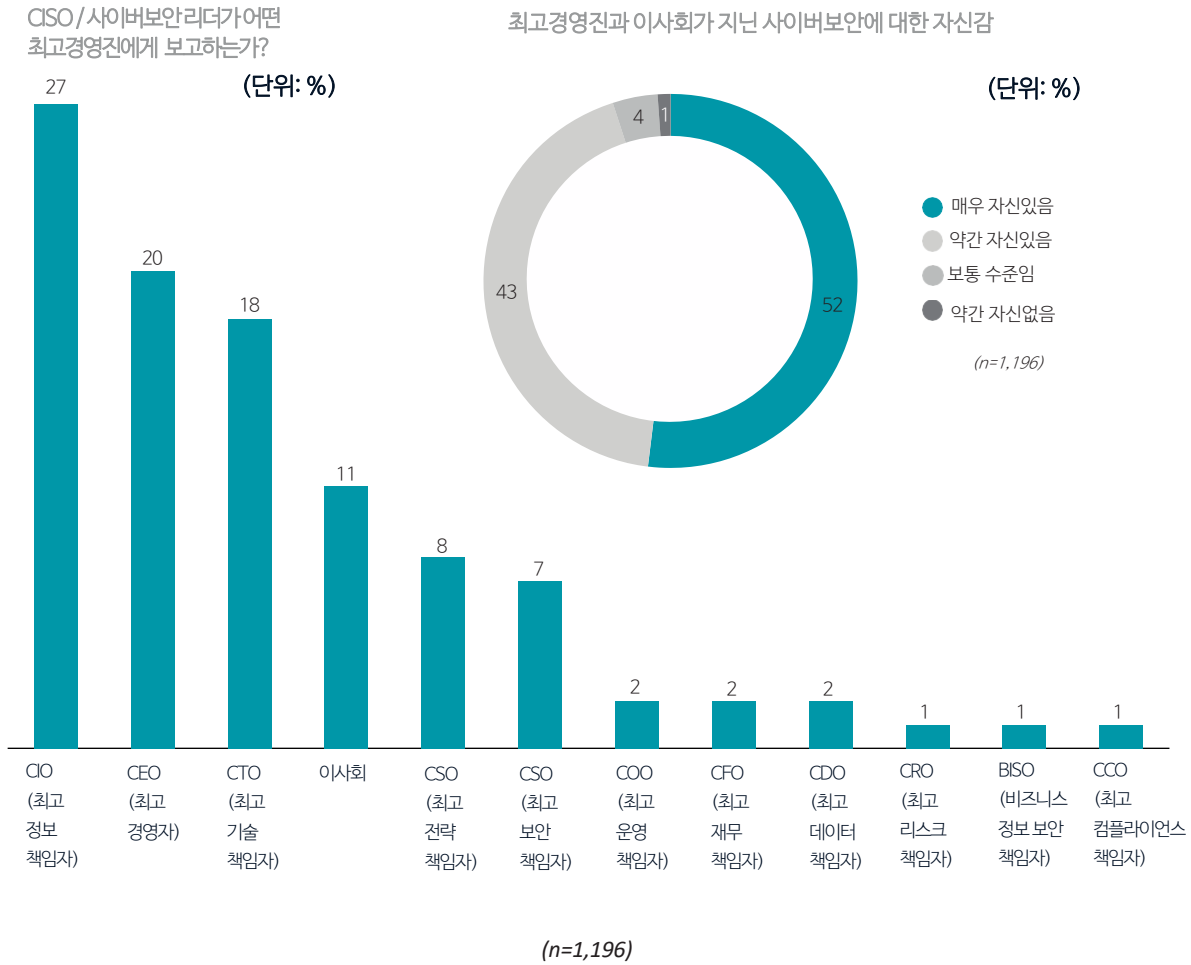
대부분의 사람들이 CISO의 역할이 진화하고 있으며 CISO가 중요한 자리에 있다고 말하지만, 여전히 C-레벨 경영진이 오늘날의 복잡한 사이버 환경을 자신 있게 헤쳐 나갈 수 있다는 확신은 부족하다.

이러한 낮은 확신은 CISO가 위험과 위협, 그리고 조직의 대응 능력에 대해 효과적으로 교육하면서 C-레벨이 오늘날의 사이버 환경의 복잡성을 실감하게 되었음을 의미한다.

우리에게 중요한 변화는 보안을 솔루션 구축 후가 아닌 구축 전에 논의에 포함시키는 것입니다. 우리는 종종 발생하는 '평가 중 보안'이 아닌 '설계 단계부터 보안'을 추구하고 있으며, 이는 보안을 전체 비즈니스의 전략적 부분으로 통합해야 함을 의미합니다.

—Director General, Cyber and IT Security, Government and Public Services Agency

그림8: CISO의 보고 대상 경영진 / 최고경영진과 이사회가 지닌 사이버보안에 대한 자신감



(n=1,196)

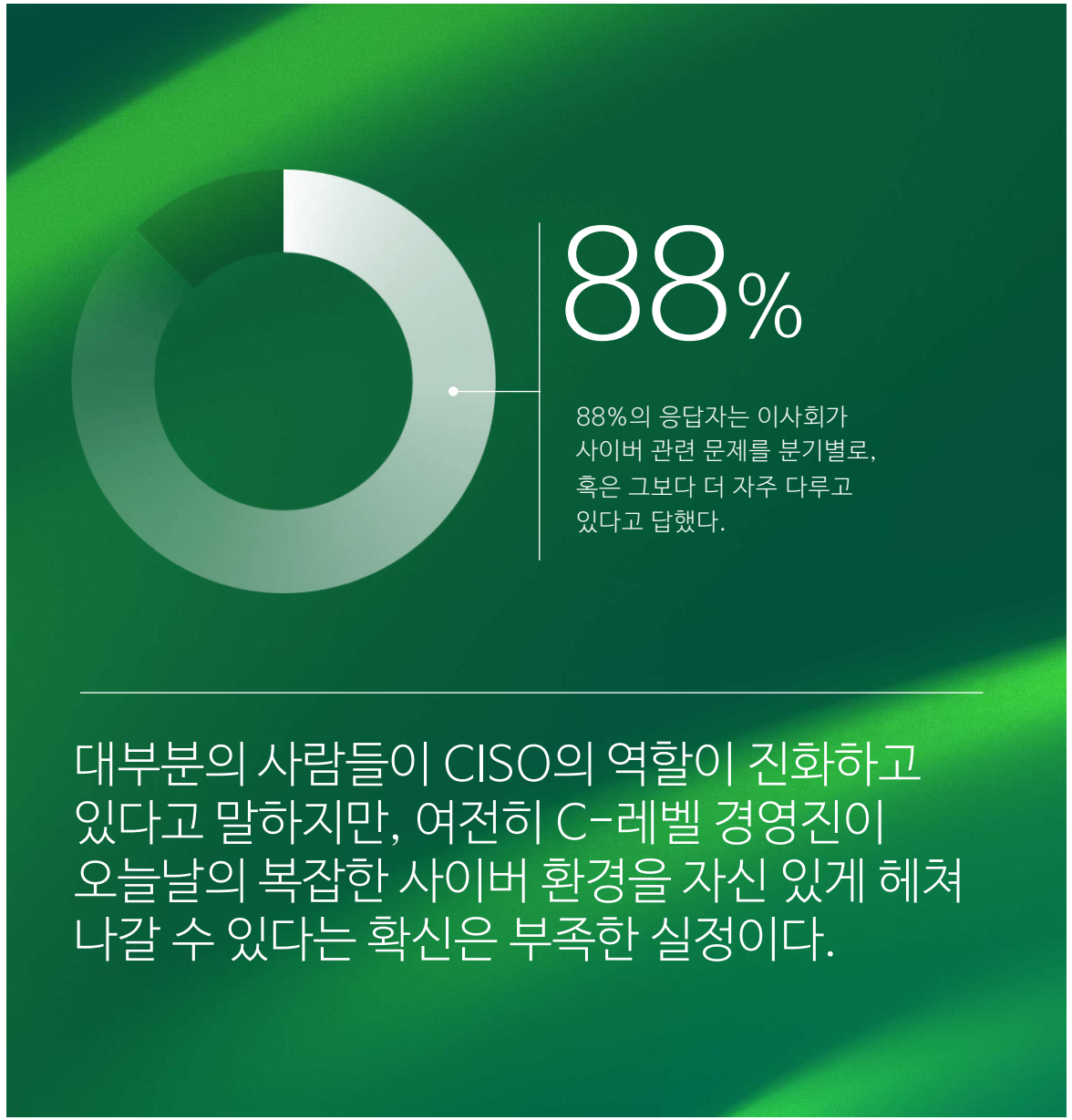
사이버 보안은 대부분의 조직에서 이사회 의제의 기본 요소로 자리 잡고 있으며, 응답자의 88%가 이사회가 분기별 또는 그보다 더 자주 사이버 관련 문제를 다루고 있다고 답했다. 그러나 CISO가 전략적 위험과 이에 따른 조치에 대해 자문하고 이사회를 교육할 사항들은 여전히 많이 남아있다.

딜로이트는 이사회 논의를 한층 발전시키기 위해 기술 리더들이 기술 관련 특수 용어를 비즈니스적인 용어로 바꿔 언급하고, CFO와 긴밀히 협력해 비즈니스 영향을 명확히 설명하기를 권장한다.

또한 보고 및 벤치마킹 구조를 일관되게 마련하고, 공동 발표를 하거나 심층 기술 세션을 통한 워크숍을 진행하며, 피드백 루프를 생성하고 이러한 활동을 소규모 이사회 세션과 회의로 확장시킬 것을 권장하는 바이다.

우리는 이사회와 분기별로 사이버 보안 관련 사안에 대한 업데이트를 진행하고 있는데, 이는 몇 년 전에는 없었던 일입니다. 논의의 빈도뿐만 아니라 깊이도 지금 훨씬 더 깊어졌다고 할 수 있습니다. 이제 이사회가 질문하는 주요 주제에 대해 훨씬 더 깊이 다루고 있으며, 이를 위해 더 많은 시간을 할애하고 있습니다.

—Chief Information Security Officer, Financial Services Corporation



사이버 보안은 기술 기반 프로그램 및 비즈니스의 디지털 전환과 통합되고 있다. 디지털 전환의 경계가 흐려지는 것처럼 사이버 보안의 경계도 흐려지고 있는 것이다.

조직이 파트너 및 기타 제3자와 데이터 및 시스템 접근 권한을 공유함에 따라 보안과 프라이버시 우려에 대응하는 것이 조직의 최우선 과제가 되고 있다.

궁극적으로 비즈니스 성장, 고객 신뢰, 데이터 신뢰, 그리고 디지털 신뢰는 사이버 보안에 달려 있다. 이에 따라 많은 조직이 사이버 보안을 비즈니스 및 기술 기능 전반에 통합하는 과정에 있다.

비즈니스 전반에 걸친 사이버 통합 조직들은 기술 역량을 강화하고 보안을 유지하는 것뿐만 아니라 새로운 제품과 서비스를 창출하는 방식에도 변화를 주고 있는 상황이다.

예를 들어, 80% 이상의 응답자가 제품 개발 초기 단계에서 프라이버시 관련 사항을 통합하고 있다고 답했으며, 이는 고객 데이터 보호와 디지털 신뢰 증진에 도움이 될 수 있다.

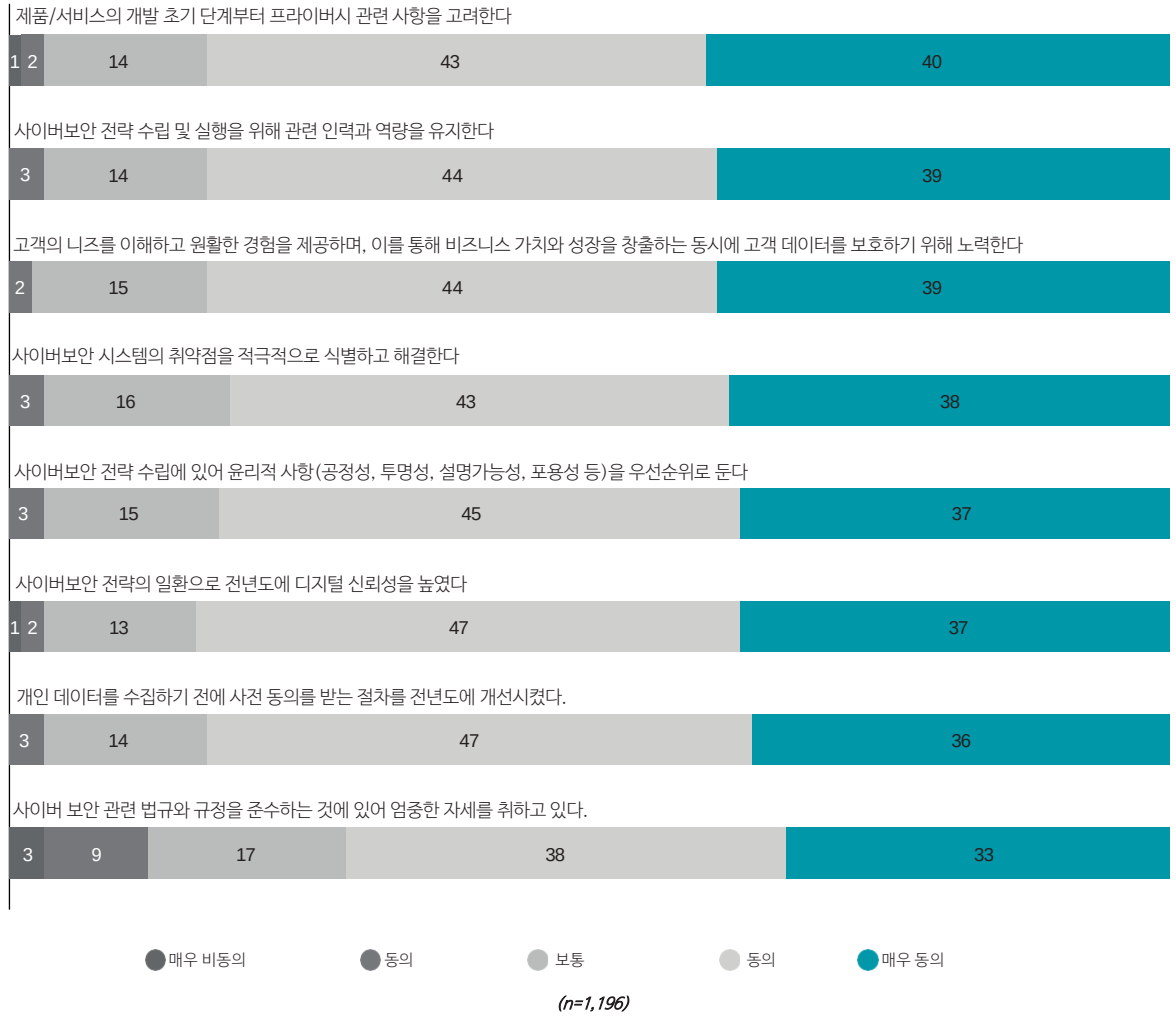
이러한 고려 사항은 DevSecOps(개발/보안/운영) 프로세스가 새로운 성숙 단계에 이르렀음을 보여주며, 사이버 보안 리더들이 제품 설계 및 개발 팀에 성공적으로 통합되고 있음을 시사한다.

저는 항상 사이버 보안을 하나의 지원 요소로 봅니다. 고속도로에서 빠르게 달리고 싶다면, 범퍼와 브레이크가 잘 작동하는지, 차량의 여러 기능이 제대로 작동하는지 확인해야 도로 위에 안전하게 있을 수 있습니다. 사이버 보안은 이러한 범퍼나 브레이크 역할을 하여 인터넷 속도로 달릴 수 있도록 지원하는 것입니다.

—Vivek Khindria, SVP Cyber Security, Network, and Technology Risk, Loblaw

그림9: 사이버보안과 다른 비즈니스 활동의 통합 수준

(단위: %)



(n=1,196)

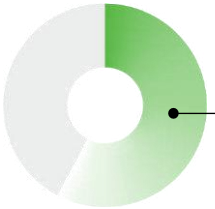
사이버 보안이 비즈니스의 다양한 측면에 통합되면서 지출에서도 이러한 변화가 나타나고 있다.

앞서 언급한 바와 같이, 응답자의 절반 이상(58%)은 사이버 보안 지출이 디지털 전환, IT 프로그램, 클라우드 투자와 같은 다른 예산과 통합되기 시작할 것으로 예상하고 있다. 동시에, 또 다른 다수(55%)는 여전히 지출이 별도로 분리된 상태로 유지될 것으로 보고 있다.

이 두 가지 다수 의견은 상충되지 않는다.

응답자의 25%는 사이버 보안 지출의 미래에 대해 통합된 지출과 분리된 지출 모두를 선택했다. 이러한 이중성은 사이버 보안 지출이 전용 예산뿐 아니라 IT, 디지털 전환, 비즈니스 영역 및 제품 예산 등 여러 우선순위에 걸쳐 분산된 것을 보여주며, 이는 딜로이트가 여러 조직에서 목격하는 현상이다.

즉, 사이버 보안 지출은 다양한 우선순위에 걸쳐있으며, 리더들이 이를 재정적으로 지원하기 위해 다양한 '동시적 지출 모델'을 탐색할 필요가 있음을 시사한다.

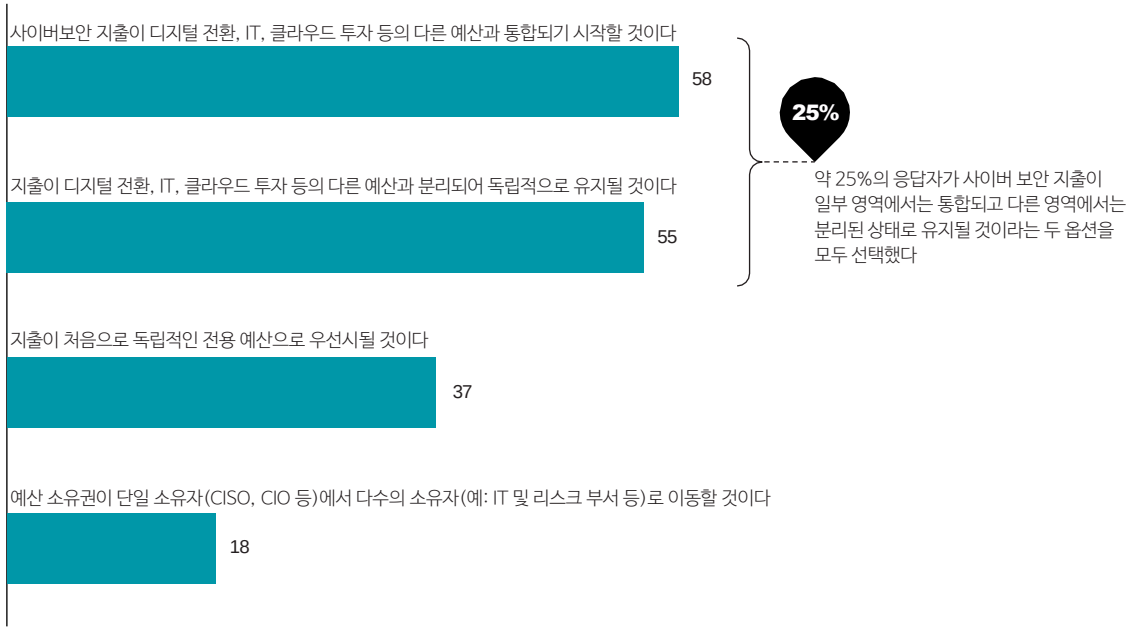


58%

사이버 보안 지출이 다른 예산과 통합되기 시작할 것으로 예상하고 있다

그림10: 사이버 보안 지출과 디지털 전환이 교차하는 지점

(단위: %)



(n=1,196)

* 반올림으로 인해 총합이 100%가 되지 않을 수 있음.

사이버 보안 예산의 통합이 진행되는 추세는 사이버 보안이 비즈니스 목표를 추진하는 데에 필요한 주요 요소라는 새로운 현실과 맞물려 있다.

설문 조사 결과에 따르면 사이버 보안은 클라우드(48%), 생성형 AI(41%), 데이터 분석(41%) 같은 영역에서 조직의 기술 역량 투자를 보호하는 데 중요한 역할을 하고 있다.

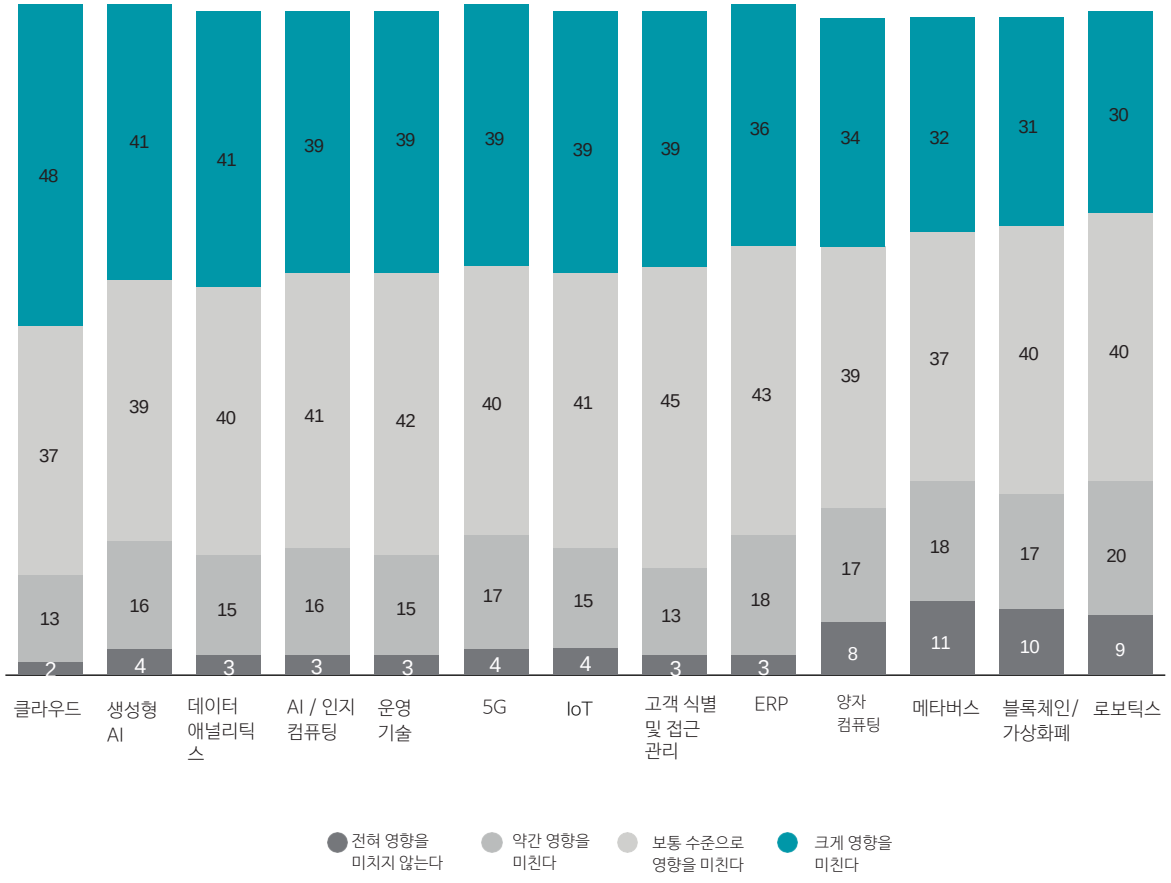
우리 그룹은 글로벌하게 운영되므로 보안 강화를 디지털 전환을 촉진하기 위한 필수 활동으로 보고 있습니다. 우리는 JFE 보안 통합 및 대응 팀이라는 내부 조직을 설립하여 예산과 인력 등 자원을 할당하고, 인적, 기술적, 물리적 측면에서 필요한 조치를 시행하고 있습니다.

그 결과, 우리는 공급망 전반에 걸쳐 사이버 보안을 강화시켰으며 궁극적으로는 전 세계 사회의 전반적인 사이버 보안 강화에도 기여하고 있습니다.

—Akira Nitta, Chief Information Security Officer, JFE Steel

그림11: 사이버 보안이 기술 투자 확보 측면에 영향을 미치는 정도

(단위: %)

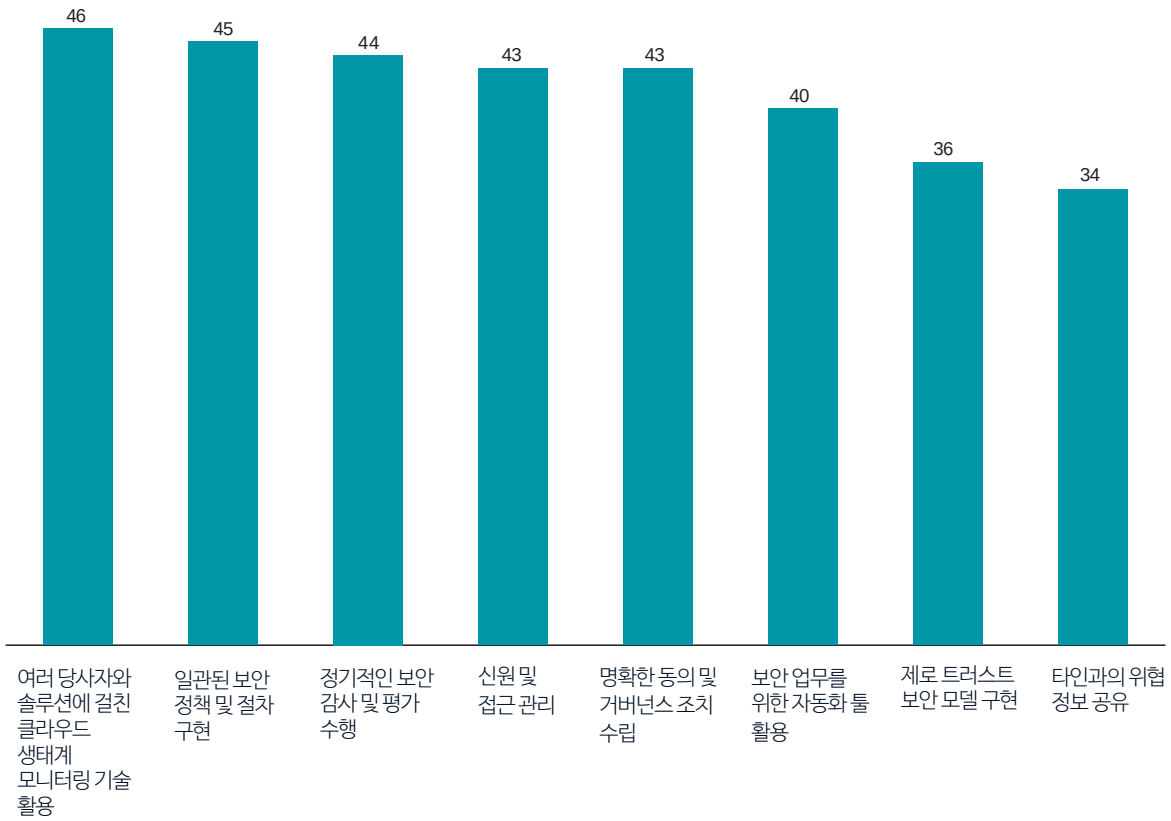


(n=1,196)

* 반올림으로 인해 총합이 100%가 되지 않을 수 있음.

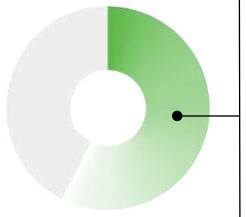
그림12: 클라우드 에코시스템의 복잡성을 줄이기 위한 사이버 보안 조치

(단위: %)



(n=1,196)

사이버 보안은 조직의 클라우드 환경을 단순화하고 보안을 강화하는 중요한 역할을 한다. 클라우드 생태계의 복잡성을 줄이기 위해 응답자들이 취하는 주요 사이버 보안 조치에는 여러 당사자와 솔루션에 걸친, 클라우드 생태계 모니터링 기술 활용(46%), 일관된 보안 정책 및 절차 구현 (45%), 정기적인 보안 감사 및 평가 수행 (44%) 등을 포함한다.



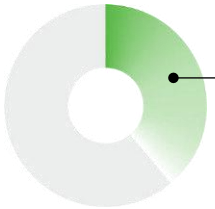
46%

응답자는 여러 당사자와 솔루션에 걸쳐 클라우드 생태계를 모니터링하는 기술을 사용하고 있다고 보고했다.

AI의 중요성을 고려하여, 이번 설문 조사에서는 사이버 성숙도 지수에 AI를 포함시켰다. 조직들이 AI를 활용하여 사이버 보안 역량을 강화하려는 주요 방법으로는 디지털 인프라 모니터링, 고급 시뮬레이션, 그리고 자동화된 보안이 포함된다.

인공지능으로 생성된 콘텐츠는 사이버 공격자들이 훨씬 적은 시간 투자로 맞춤형 콘텐츠를 생성할 수 있게 해준다. 이제 신뢰할 수 있는 출처를 가장하여 취약점을 이용하는 인공지능으로 생성된 콘텐츠들이 기업을 타겟으로 한 공격의 도구가 되고 있다. 이러한 문제는 빠르게 악화되고 있다.

그러나 이러한 상황은 기업이 다가오는 인공지능으로 생성된 콘텐츠의 물결에 무력하다는 것을 의미하지 않는다. 선도적인 기업들은 피해자가 되지 않기 위해 사전 조치를 취하고 있다.



39%

응답자들은 평균적으로 사이버 보안 프로그램에서 AI 기능을 대규모로 사용하고 있다고 보고했다.

AI의 미래가 발전하는 것처럼 사이버의 미래도 함께 발전하고 있다. 조직들이 새로운 AI 솔루션을 활용하여 사이버 보안의 부담을 줄이고 있기 때문이다.

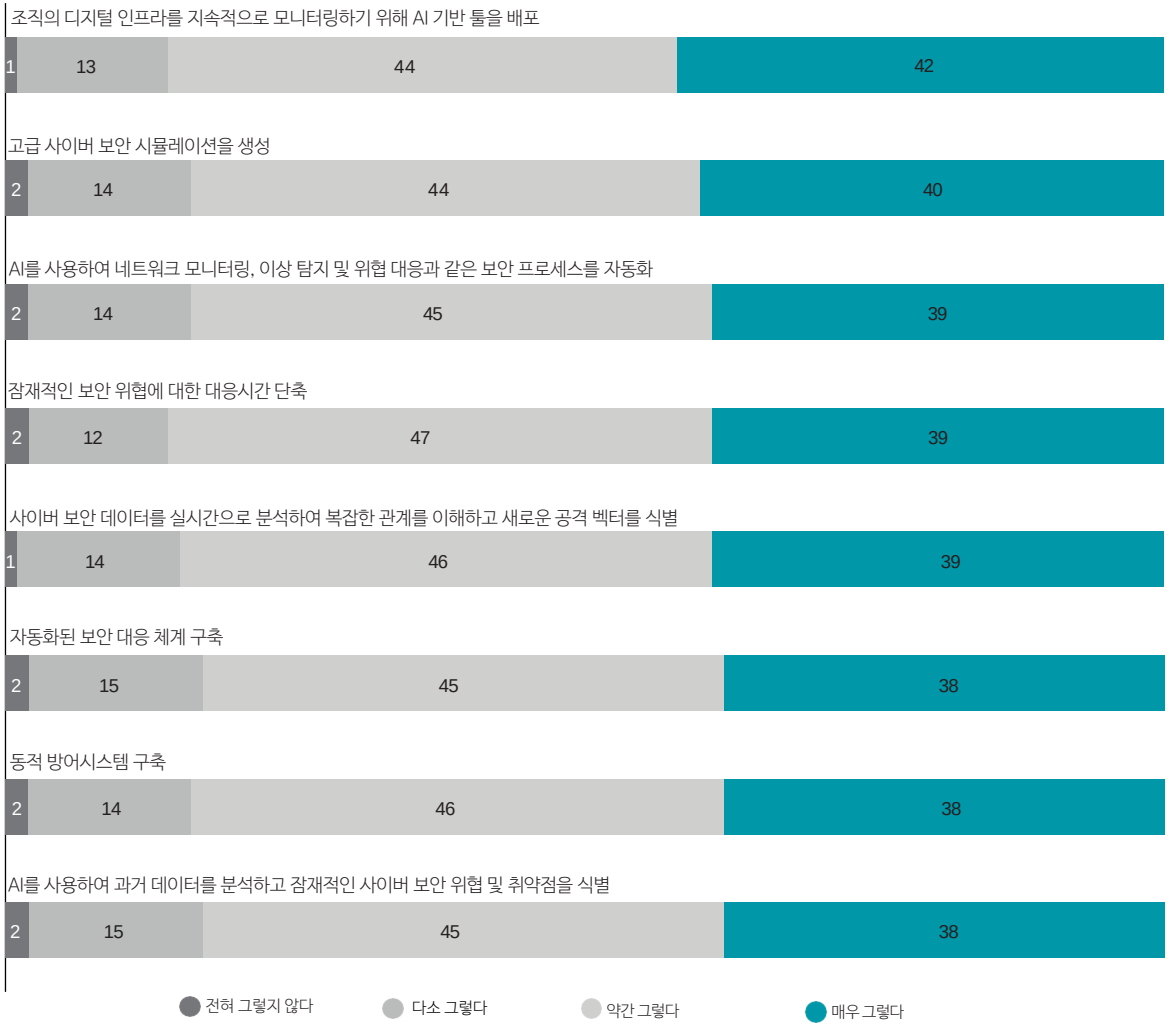
설문 조사에 따르면, 응답자의 평균 39%가 사이버 보안 프로그램에서 AI 기능을 대규모로 사용하고 있다. 동시에 응답자들은 AI와 관련된 우려를 표명하며, 지속적인 기술 혁신에 발맞추기 위해 사이버 보안 전략을 업데이트할 필요성을 강조하고 있다.

물론, 핵심은 나쁜 사람들을 차단하는 것입니다. 하지만 우리는 이러한 새로운 기술(예: AI)이 우리 환경에 미치는 영향을 살펴보아야 합니다. 어떻게 하면 AI를 안전한 방식으로 적용하고 사용할 수 있을지, 그리고 AI를 사용하여 우리의 사이버 프레임워크 내에서 보안을 더 잘 제공할 수 있을지를 고민해야 합니다.

—Director General, Cyber and IT Security, GPS Agency

그림13: AI가 사이버 보안 프로그램에서 활용되는 방식

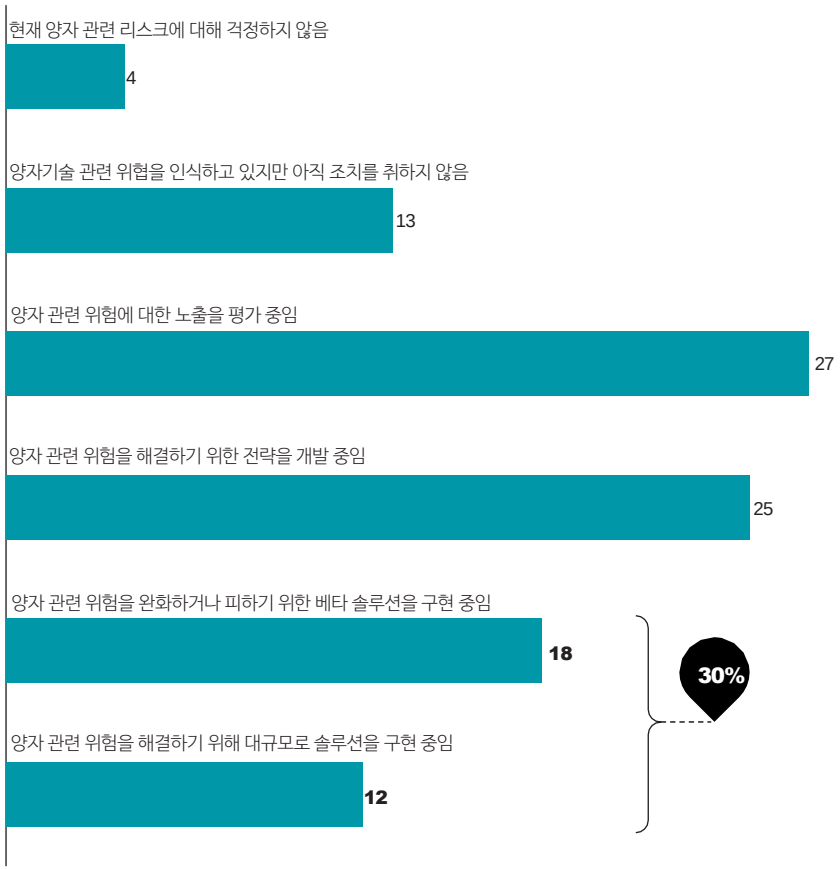
(단위: %)



(n=1,196)

그림14: 양자(Quantum) 기술과 사이버 보안 준비에 대한 조직들의 생각

(단위: %)



(n=1,196)

조직들이 AI 관련 위험과 기회를 다루는 한편, 다른 파괴적인 기술들도 발전하고 있으며 널리 사용될 수 있는 방향으로 나아가고 있다.

양자 기술과 관련된 사이버 보안 준비가 많은 조직에서 더 큰 화두가 되고 있으며, 양자 컴퓨팅이 현실에 가까워지고 있다.

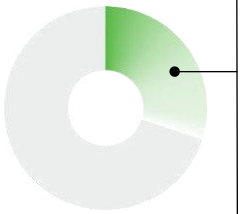
이는 향후 몇 년 내에 주류가 될 것으로 예상되며, 사이버 공격자들이 암호를 푸는 데 사용할 수 있는 강력한 새로운 도구를 제공한다.

데이터에 따르면 응답자의 약 83%가 양자 관련 위험을 평가하거나 전략 개발, 파일럿 솔루션 구현, 또는 대규모 솔루션 구현과 같은 어떤 형태의 조치를 취하고 있다. 대다수(52%)의 응답자는 여전히 위험 노출을 평가하고 양자 관련 리스크 대응 전략을 개발하는 한편,

다른 응답자(30%)는 초기 채택자로서 솔루션을 구현하기 위해 결정적인 조치를 취하고 있다.

이 수치는 이 문제에 대한 분명한 모멘텀을 보여준다. 리더들은 위험 잠재력을 이해하고, 데이터 및 시스템 거버넌스를 검토하며, 비즈니스 운영에 대한 취약성을 우선시하고, 암호화 알고리즘 업데이트를 위한 로드맵을 개발함으로써 도전에 앞서 나갈 수 있다.

이를 통해 조직들은 수년이 걸리는 사이버보안 이니셔티브에서 앞서 나가고, 보다 넓은 기업 변혁을 통해 그리고 계약 메커니즘 업데이트를 통해, 새로운 알고리즘을 체계적으로 도입할 수 있다.



30%

응답자 중 30%는 초기 채택자로서 솔루션을 구현하기 위해 단호한 조치를 취하고 있다고 보고했다

사이버 성숙도가 높은 조직은 더 큰 자신감을 느끼고 사이버 행동 및 투자에서 더 많은 이점을 실현하고 있다.

사이버 성숙도 지수

딜로이트는 전 세계 수천 개 조직과의 협업 경험을 바탕으로 높은 사이버 성숙 조직을 중간 및 낮은 사이버 성숙 조직과 구분하였다.

이러한 사이버 리더 집단을 식별하고 사이버 보안이 비즈니스 성공과 가치에 얼마나 기여하는지를 보다 완전히 이해하기 위해, 실천 사례에 기반한 기준을 사용하여 조직을 평가하거나 지수화하였다:

- **강력한 사이버 보안 계획:** 사이버 위협에 대응하고 방어하기 위한 전략적, 운영적, 전술적 계획을 수립한다.

- **주요 사이버 보안 활동:** 정성적 및 정량적 위험 평가, 업계 벤치마킹, 사고 대응 시나리오 계획 등이 포함된다.

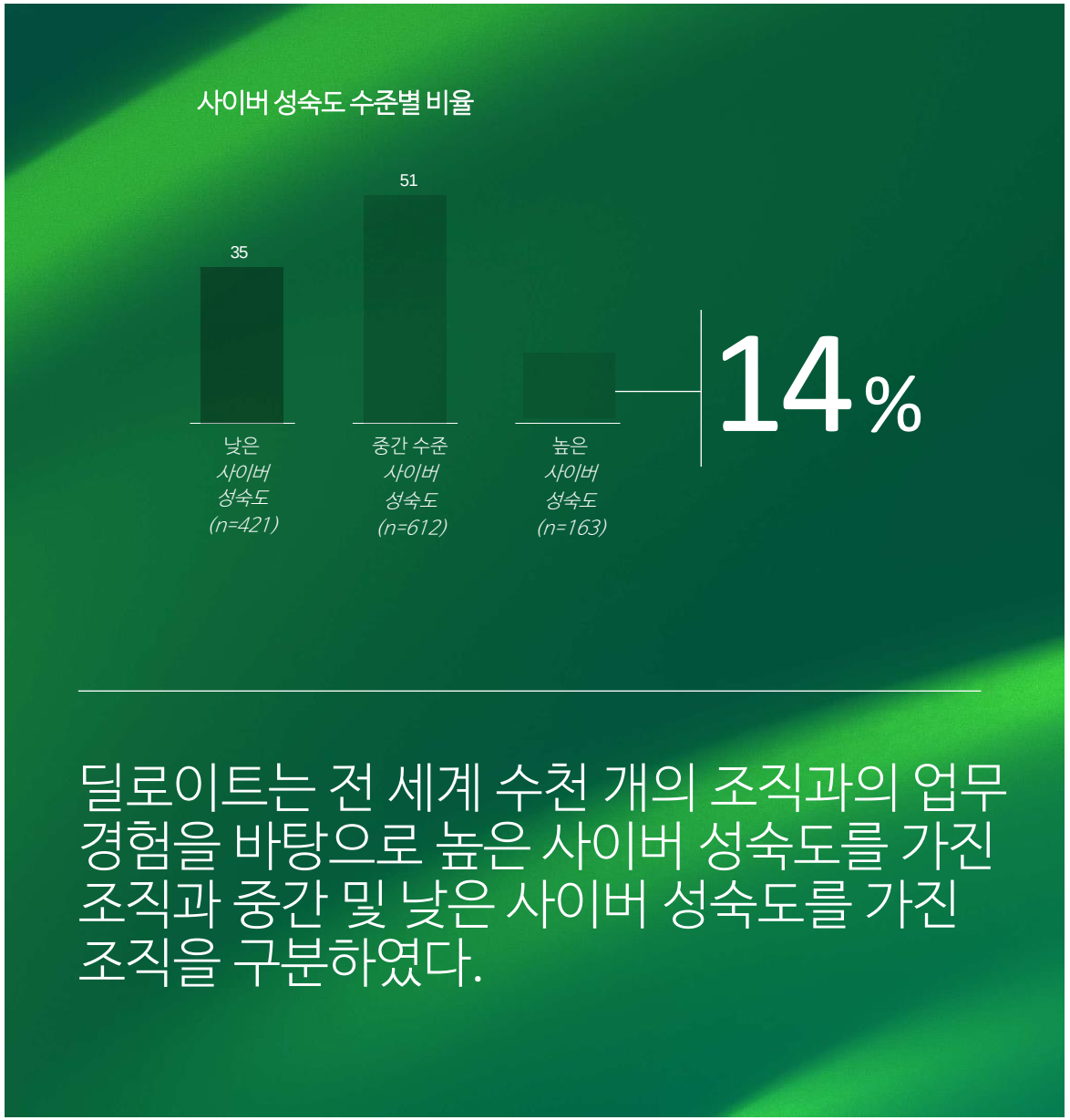
- **효과적인 이사회 참여:** 사이버 관련 문제를 정기적으로 다루는 조직의 이사회가 그 예시이다.

- **사이버 보안 프로그램 내 AI 기능 적용:** 최소한 여덟 가지 사이버 AI 관련 행동 중 다섯 가지를 대규모로 수행하는 조직에 초점을 맞춘다.

이번 조사에서 마지막 기준인 AI 기능은 기술과 비즈니스의 발전 및 사이버 성숙도가 무엇을 의미하는지를 반영하기 위해 새롭게 추가되었다.

사이버 성숙도 지수에 AI 요소를 포함함으로써, 사이버의 미래를 선도하고 있는 엘리트 집단의 조직을 정의할 수 있다.

사이버 성숙도가 높은 조직은 조사에 참여한 응답자의 14%를 차지한다. 이들이 사이버 보안에 접근하는 방식은 기업 리더들이 자사의 사이버 및 비즈니스 가치를 높이는 데 사용할 수 있는 중요한 교훈을 제공한다.



딜로이트는 전 세계 수천 개의 조직과의 업무 경험을 바탕으로 높은 사이버 성숙도를 가진 조직과 중간 및 낮은 사이버 성숙도를 가진 조직을 구분하였다.

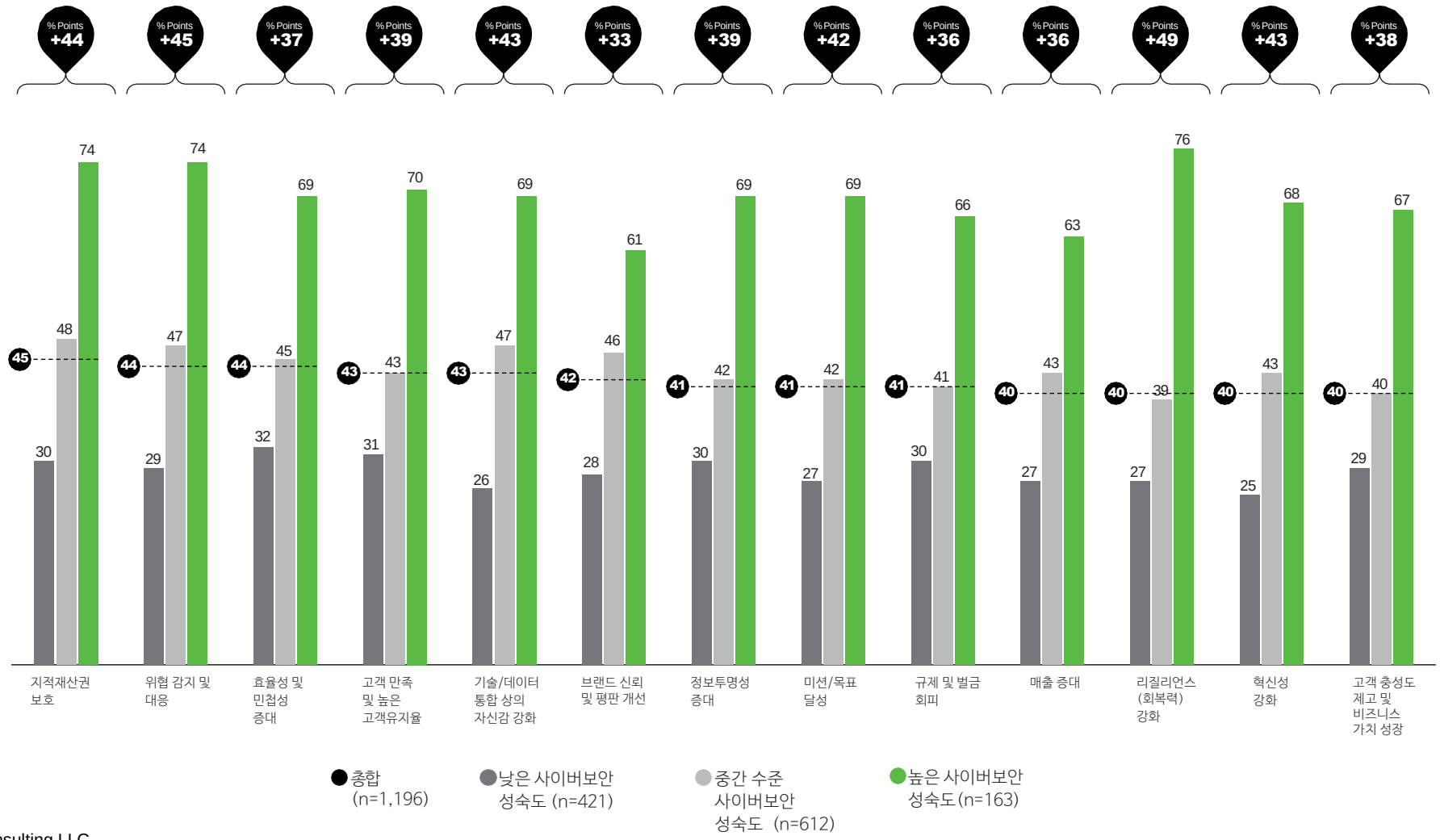
높은 사이버 성숙도를 가진 조직의 응답자들은 사이버 보안 조치로 얻는 잠재적 이점에 대해 높은 감각을 가지고 있다. 평균적으로, 높은 사이버 성숙도를 가진 조직의 응답자는 낮은 사이버 성숙도를 가진 조직의 응답자보다 긍정적인 결과를 기대할 가능성이 2.4배 더 높다(중간 사이버 성숙도를 가진 조직의 응답자와 비교하면 1.6배 더 높다).

이러한 이점 중 일부는 조직의 회복력 강화(76%), 위협 탐지 및 대응 개선(74%), 그리고 지식 재산 보호(74%)를 포함한다. 이 세 가지 분야에서 높은 사이버 성숙도를 가진 조직의 응답자들의 기대치는 낮은 사이버 성숙도 그룹과 비교해 상당히 차이가 난다.

그림15: 사이버보안 활동으로 조직이 기대하는 이점

(단위: %)

높은 사이버보안 성숙도 조직과 낮은 성숙도 조직간 차이



높은 사이버 성숙도를 가진 조직조차도 사이버 침해와 사고의 부정적인 결과에서 완전히 자유롭지 않다. 분석에 따르면, 평균적으로 높은 사이버 성숙도를 가진 조직은 사이버 위협을 탐지하는 능력이 더 강하고 이에 따른 보고 요구 사항을 준수하는 성실성도 더 높다.

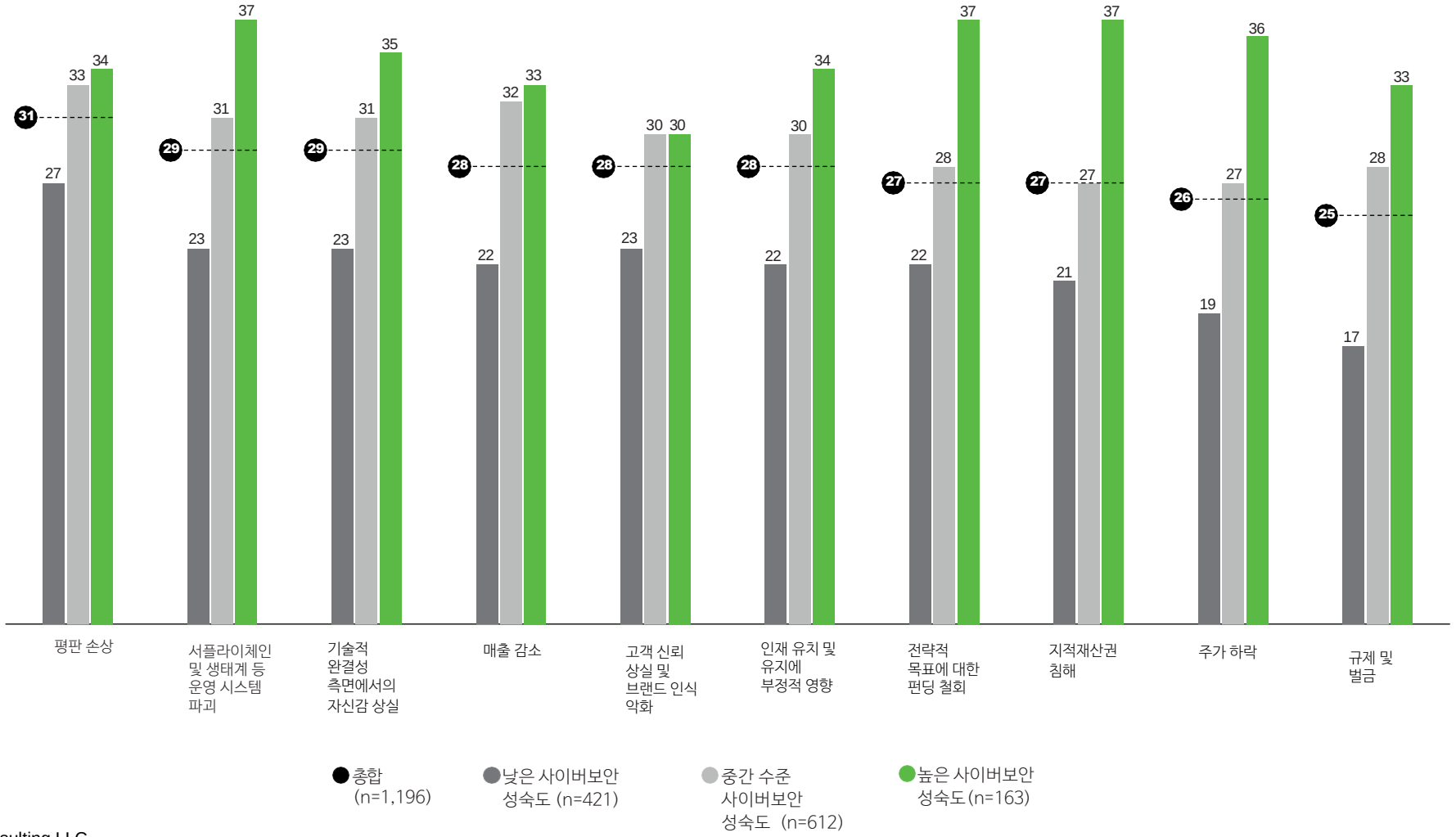
예를 들어, 높은 사이버 성숙도를 가진 조직 응답자의 25%가 지난 1년 동안 11건 이상의 사이버 보안 사고를 보고했으며, 이는 전체 응답자보다 8%포인트 높은 수치이다. 이는 부정적으로 보일 수 있지만, 이러한 조직은 위협을 더 효과적으로 식별하고 대응할 수 있는 강력한 위협 탐지 기능을 갖추고 있을 가능성이 크다.

침해 및 사고에 대한 인식이 높은 것 외에도 이러한 조직들은 사이버 보안 수반되는 비용을 이해하고 있으며, 평균적으로 높은 사이버 성숙도를 가진 그룹은 낮은 성숙도를 가진 그룹에 비해 재무적, 운영적, 브랜드 관련 영향의 범위를 인정할 가능성이 13%포인트 더 높다.

이러한 높은 이해도는 사이버 보안이 비즈니스 및 기술 환경 전반에 걸쳐 통합되고 지속적 성장을 만들 수 있는 '선순환'을 촉진한다.

그림16: 사이버 위협이 초래하는 부정적 결과들에 대한 인지 역량

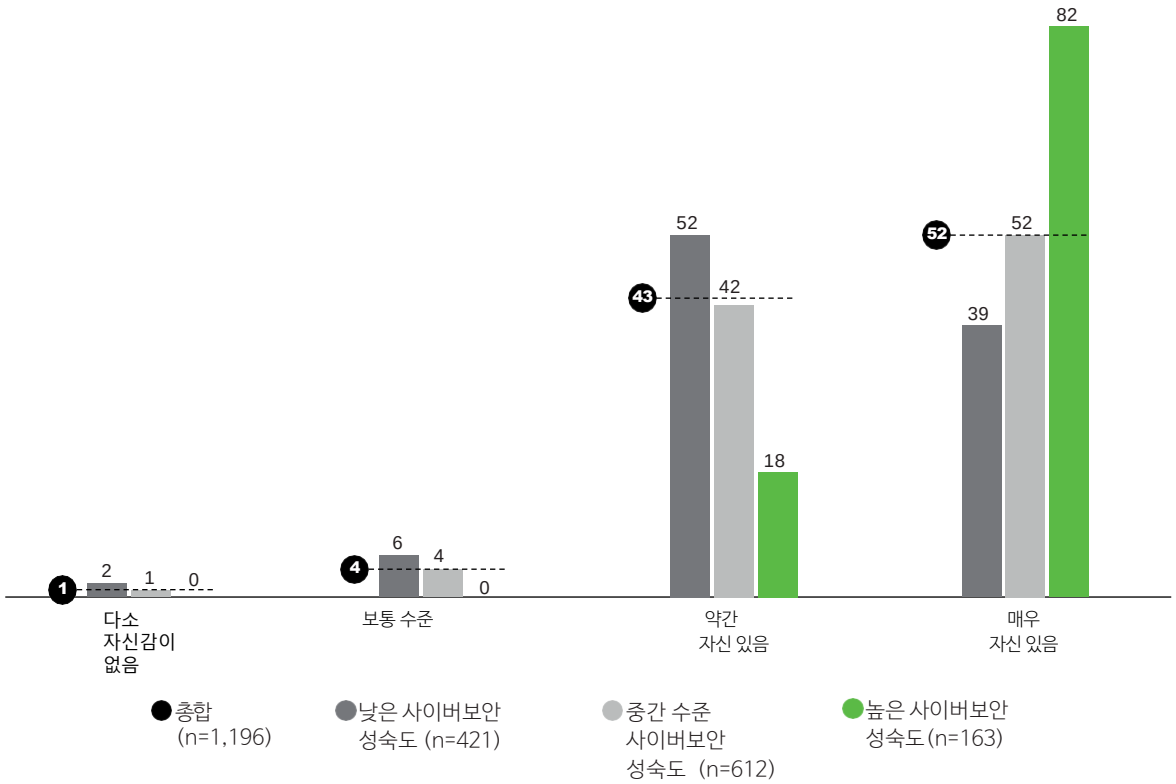
(단위: %)



사이버 성숙도가 높은 조직의 응답자들은 C-suite의 사이버 보안 준비 태세에 대한 자신감이 매우 높다.
이들은 사이버 성숙도가 낮은 조직의 응답자들에 비해 C-suite와 이사회가 사이버 보안 요구사항을 효과적으로 처리할 수 있는 능력에 매우 자신감을 가질 가능성이 두 배 더 높다.

그림17: C-suite와 이사회의 사이버 보안 해결 역량에 대한 자신감

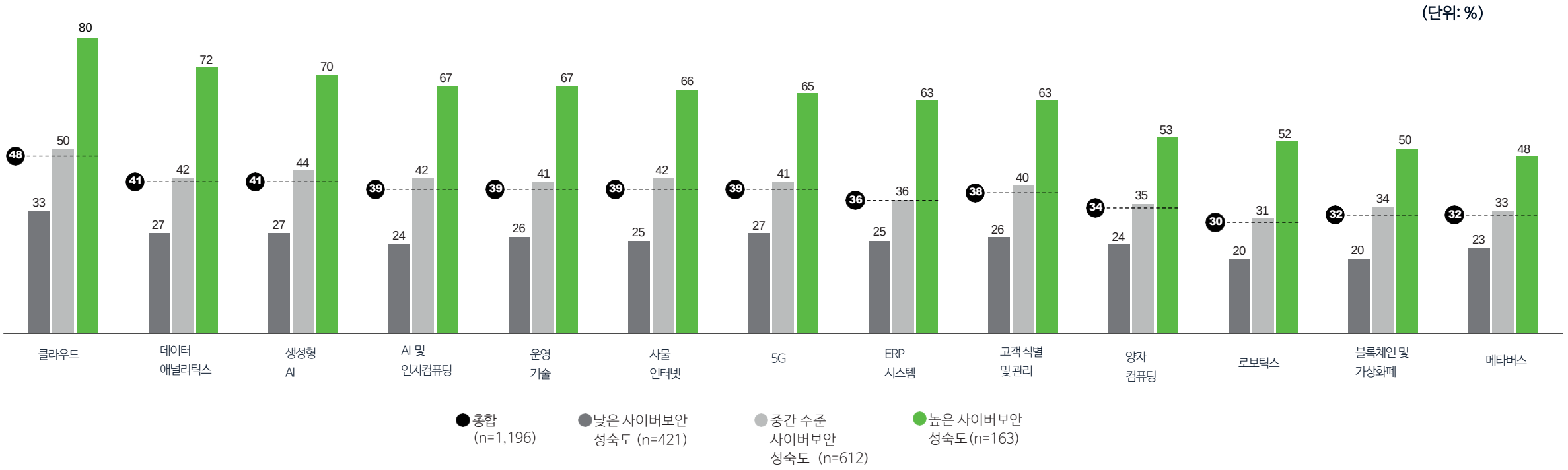
(단위: %)



사이버 성숙도가 높은 조직은 사이버 보안을 활용하여 기술 역량에 대한 투자를 확보하고, 디지털 전환에 대한 전략적 논의에 CISO를 포함시키는 데 더 능숙한 것으로 보인다.

평균적으로, 사이버 성숙도가 높은 조직의 응답자는 낮은 사이버 성숙도 그룹의 응답자보다 사이버 보안이 기술 역량에 대한 투자 확보에 큰 역할을 한다고 말할 가능성이 2.5배 더 높다. 이러한 투자 확보가 이루어지는 주요 분야는 클라우드, 데이터 분석, 생성 AI, 운영 기술(예: 산업 제어 시스템) 및 AI/인지 컴퓨팅을 포함한다.

그림18: 기술 역량 개발/증진에 있어 사이버 보안이 큰 역할을 한다고 생각하는 비율



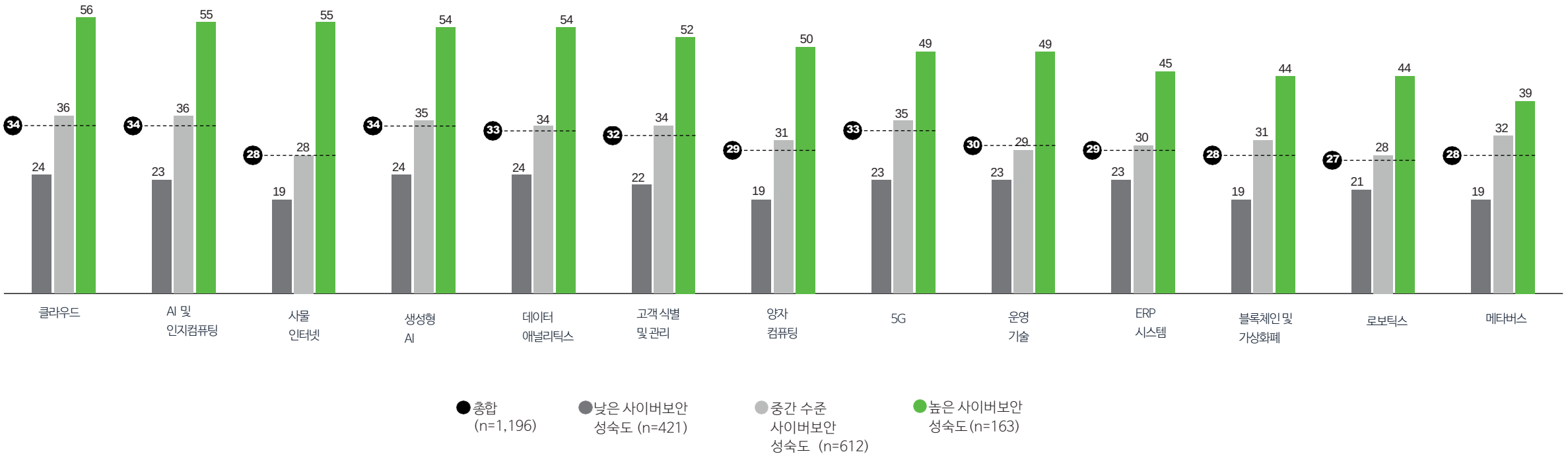
기술 역량에 관한 전략적 논의 측면에서, 사이버 성숙도가 낮은 그룹에 비해 성숙도가 높은 그룹은 CISO 또는 사이버 보안 리더의 참여가 크게 증가했다고 말할 가능성이 2.3배 더 높다. 사이버 성숙도가 높은 조직에서는 클라우드, AI/인지 컴퓨팅, 사물인터넷(IoT), 생성형AI, 데이터 분석과 같은 분야에서 CISO의 참여가 가장 두드러진다.

CISO의 역할은 진화하고 있다. 이들은 회사가 데이터 기반 의사 결정을 내릴 수 있도록 적절한 전략을 도입하여 적극적으로 이끌어야 한다. 이는 경영진과의 소통이 증가함을 의미한다. CISO는 기술적 전문성뿐만 아니라 경영진 수준의 사고방식과 비즈니스 감각을 갖추어 사이버 전략이 비즈니스에 어떤 영향을 미칠지 보여줄 수 있어야 한다.

— Gary Harbison, Chief Information Security Officer, Johnson & Johnson

그림19: CISO(최고정보보호책임자)가 각 기술 분야의 전략적 의사결정 및 논의에 참여한다고 답한 비율

(단위: %)



사이버의 미래에 관한 인사이트

조직 전분야에 걸친 사이버 보안 강화

미래의 사이버 환경에서 성공하기 위해 조직은 새로운 트렌드를 이해하고 무엇보다도 비즈니스에 측정 가능한 영향을 미칠 수 있도록 실행에 옮겨야 한다.

사이버 보안에 필요한 필수 요소를 강화하고, 연결과 협력을 촉진하며, 더 큰 회복력을 구축해야 한다. 사이버 보안이 전략적 비즈니스 가치의 요소로 점점 더 주목받는 상황에서, 리더들은 사이버 보안이 단순한 IT 문제가 아니라 조직 전체의 모든 기능과 수준에 통합되어야 하는 비즈니스 필수 과제임을 인식해야 한다.

조직이 더 강력한 리더십을 확립하고 사이버 연결을 강화함에 따라, 비즈니스 요구가 사이버 보안과 맞닿는 모든 영역에서 협업, 정보 공유, 의사 결정이 더욱 원활해질 수 있다. 이를 통해 리더들은 비즈니스의 현실을 깊이 반영한 전략적 결정을 내릴 수 있다.

궁극적으로, 사이버 보안을 우선시하고 전사적으로 사이버 보안과의 강력한 연결을 구축함으로써, 조직은 중요한 자산과 명성을 더욱 잘 보호하고, 점점 더 디지털화되는 세상에서 전반적인 회복력을 강화할 수 있다.

한때, 기업 IT 부서의 주요 보안 책임자로 여겨졌던 CISO의 역할은,

이제 핵심 비즈니스 운영부터 브랜드 평판까지 전체 조직을 보호하면서 혁신과 비즈니스의 미래를 지원하는 방향으로 진화하고 있다.

CISO부터 다른 경영진과 이사회에 이르기까지 사이버보안 이슈에 대한 리더십의 참여와 역량을 강화해야 한다.

사이버 보안 위험을 비즈니스 목표와 함께 효과적으로 다루기 위해서는 전체 경영진과 이사회가 정기적으로 사이버 보안 논의에 참여해야 한다.

CISO는 이사회와 조직에 사이버 관련 중요한 통찰과 지침을 제공함으로써, 사이버 보안 분야의 지속적인 투자를 받을 수 있다.

전략과 거버넌스를 기반으로 예산을 통합하려는 노력이 필요하다. 사이버 보안 예산이 다른 디지털 전환 투자 예산과 통합되는 추세는 중요한 변화이다. 앞으로 더 많은 부서가 자금 계획에 사이버 보안을 포함할 가능성을 시사한다.

이 통합된 접근 방식은 보다 포괄적인 전략과 전체적인 보안 성과를 개선할 수 있다. 더 넓은 의제를 지원하고 사이버 보안에 대한 목표를 정의하는 명확한 거버넌스 프레임워크를 수립해야 한다.

전략에 관해서 우리가 성숙해지고 있는 것 중 하나는 결과를 시작점으로 삼는 것입니다. 즉, 우리가 몇 년 후에 어디에 있고 싶은지를 항상 생각하는 것입니다. 저는 보안 분야에서 2년 이상 앞서 전략을 수립하는 것이 바람직하다고 생각합니다. 왜냐하면 위협이 변하고 기술이 변화하는 등 많은 것들이 바뀔 것이기 때문입니다. 그래서 우리는 결과를 염두에 두고 사이버 보안 체계를 구축하고 있으며, 이는 정말 중요합니다.

—Chief Information Security Officer, Life Sciences and Health Care Company

딜로이트 산업 전문가

사이버 보안 및 리스크

딜로이트는 사이버 리스크 대응을 위한 정보보호 및 개인정보보호 자문, 정보보안 인증,
기술적 취약점 진단 및 대책 수립, 정보보호 전략 수립, Cyber Incident 대응 등의 서비스를 제공하고 있습니다.
수많은 유형의 리스크를 사전에 방지해 기업 운영의 든든한 조력자 역할을 수행합니다.

서영수 파트너
Cyber 리더 |
Cyber Risk & Compliance

Tel : 02 6676 1929 |
E-mail : youngseo@deloitte.com

유선희 파트너
Cyber |
Cyber Risk & Compliance

Tel : 02 6676 2956 |
E-mail : sunhyou@deloitte.com

이상훈 이사
Cyber |
Cyber Risk & Compliance

Tel : 02 6676 2937 |
E-mail : sanghunlee@deloitte.com

Cyber Service Offerings	주요 서비스
Cyber Governance & Compliance	• 정보보안 인증 및 자문(ISO27001, ISMS-P, SOC 2/3, WebTrust 등) • 전자서명인증 평가
Privacy Governance & Compliance Data Protection & Compliance	• 정보보호/개인정보보호 자문 • 수탁사 진단 • 상시 보안 자문
Application Security Security Architecture Cyber Cloud	• 개발 보안(시큐어코딩 등) • 시나리오 기반 모의해킹 • 인프라 취약점 진단 • 클라우드 보안 진단

Cyber Service Offerings	주요 서비스
Cyber Strategy Emerging Technologies	• 정보보호 전략 수립 • OT 보안 전략 수립 • 중장기 마스터플랜 수립
Technology Resilience Crisis & Incident Response	• Crisis Management • BCM • 사이버 침해사고 대응

Deloitte.

전 세계 경제·산업·경영 트렌드와 인사이트를

실시간으로 확인하세요!

- MZ세대 소비자, ESG, 경제전망 등 **이슈 분석 리포트**
- CEO·CFO 분기 서베이, 자동차구매의향지수 등 **경영·산업 동향 지표**
- 딜로이트 전문가의 생생한 경험이 녹아있는 **영상 콘텐츠**
- 채용공고, 임직원 브이로그, 이벤트 안내 등 **다양한 딜로이트 소식**

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. Insights

성장전략부문 대표	딜로이트 인사이트 리더	딜로이트 인사이트 편집장	연구원	Contact us
손재호 Partner	정동섭 Partner	박경은 Director	양원석 Senior Consultant	krinsightsend@deloitte.com
jaehoson@deloitte.com	dongjeong@deloitte.com	kyungepark@deloitte.com	wonsukyang@deloitte.com	