위험 대비 또는 위험

COHESITY

중견 기업의 사이버 레질리언스 격차

사이버 공격은 더 이상 고립된 사건이 아니라 디지털 세계의 지속적인 특징입니다. 전 세계적으로 갈수록 중견 기업이 표적이 되면서, 매일 새로운 경각심을 일깨우는 일이 이어지고 있습니다. 어떤 사업체도 안전하지 않으며, 위협의 빈도와 정교함이 증가함에 따라 측정 가능한 재정, 운영, 평판상의 손실을 초래하는 중대한 사이버 공격이 급증하고 있습니다.

직원 수가 **1,000~1,999**명인 기업의 **IT** 및 보안 운영 의사결정자 약 **1,000**명을 대상으로 실시한 글로벌 설문조사에서 이러한 현실이 드러납니다.

75%
중대한 사이버 공격을 경험했음.

55%
지난 12개월 내 공격을 받음.

1/4
여러 차례 공격을 받은 적이 있음

피해의 상처는 깊게 파고들며 비용은 급격히 쌓여갑니다.

85%
매출 손실

36%
고객 이탈

76%
상장 기업으로서 재무 전망을 수정해야 했음

92%
법적 또는 규제적 제재를 받았음

82%
지난 12개월 내 몸값을 지불했음

명백한 증거가 있음에도 불구하고, 많은 조직들이 자사의 레질리언스를 과대평가합니다.

47%
자사의 사이버 레질리언스 전략에 대해 완전한 확신을 가지고 있음

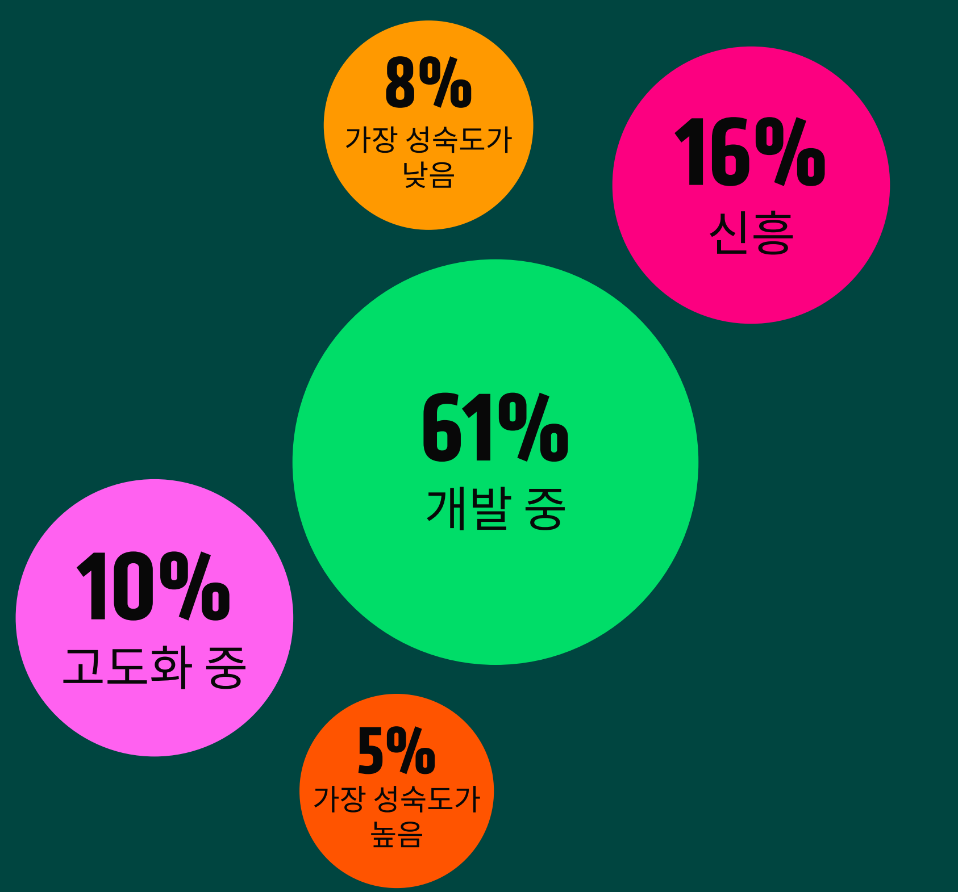
대부분은 대응과 복구라는 동등하게 중요한 기능보다 예방과 탐지를 여전히 우선시합니다.

NIST 사이버 보안 프레임워크에 기반한 순서.
박스 크기는 사이버 레질리언스 투자 비율이 높은 순서부터 낮은 순서로 표시됩니다.

#3	#1	#2	#4	#5
식별	보호	탐지	대응	복구

신뢰도와 소비 패턴은 이야기의 일부에 불과합니다

진정한 레질리언스는 이를 뒷받침하는 실천과 역량에 달려 있습니다. 실제 성능 기준에 따라 평가했을 때, **데이터 보호, 데이터 복구, 위협 탐지 및 조사, 애플리케이션 레질리언스, 데이터 위협 최적화라는** 다섯 가지 핵심 영역에서 성숙도를 보여주는 조직은 단 5%에 불과합니다.



사이버 레질리언스를 지닌 대부분의 기업에게 있어서, 레질리언스는 체계적이고 포괄적인 것입니다. 다른 모범 사례와 더불어 민감한 데이터의 전 세계적 백업, 다중 인증 및 관리자 제어 강제 적용, 위협 인텔리전스 극대화, 교정을 통한 복구 보안, 규정 준수 보호 조치의 일관된 이행을 보장하고 있습니다.

하지만 성숙도는 멈춰 있는 것이 아닙니다.

53%
레질리언스 전략에 성장의 여지가 있음을 인정함

레질리언스 강화의 필요성에 대한 인식이 자동화와 AI를 동력으로 하는 차세대 진화를 주도하고 있습니다. 위협이 더욱 빠르고 복잡해짐에 따라 자동화는 탐지 가속화, 대응 효율화, 복구 강화의 핵심 요소입니다.

56%

사이버 공격 이후 얻은 주요 교훈 중 하나로 탐지, 대응, 복구 전반에 걸친 자동화 개선을 꼽음

37%

AI가 위협을 탐지하고 대응하는 방식에서 중심적인 역할을 수행하며, 일부 자율적인 의사결정을 내리는 기능도 포함될

99%

2026년까지 데이터 보안 운영을 지원하기 위해 AI를 사용할 계획임

위험에 대비하고 계십니까?

- 중견 기업을 위한 **Cohesity**의 **사이버 레질리언스 솔루션**에 대해 알아보세요.
- **레질리언스 스코어카드**로 **사이버** 레질리언스 **성숙도**를 평가하십시오
- **5단계 사이버 레질리언스 실행 계획**으로 수준을 높이십시오

Vanson Bourne은 2025년에 북미, 아시아태평양, 유럽, 라틴아메리카 지역에서 직원 수 1,000명 이상의 조직을 대표하는 IT 및 보안 리더 3,200명을 대상으로 설문조사를 실시했습니다. 응답자 중에는 직원 수가 1,000~1,999명인 중견 기업에 재직하는 977명의 참가자가 포함되었습니다.

COHESITY VansonBourne

COHESITY
cohesity.com
1-855-926-4374
서울시 강남구 테헤란로 152 강남파이낸스센터 28층
6200013-001-KO 7-2026