



2027년 사이버 보안 전망

전략적 거버넌스와 디지털 자율성을
기반으로 한 회복탄력성

forv/s
mazars

서문

사이버 보안 환경이 빠르게 변화하고 있습니다. 새로운 기술이 잇따라 등장하면서 규제는 더욱 복잡해지고, 사이버 위협은 한층 정교해졌습니다. 기업은 이제 보안을 단순한 기술적 문제로만 여길 것이 아니라, 경영 차원의 의제로 바라봐야 합니다. **앞으로의 변화에 대응하려면 명확한 거버넌스를 바탕으로 혁신을 주도하고, 변화하는 환경에 유연하게 적응할 수 있는 역량을 갖춰야 합니다.**

이번 보고서는 기업들이 급변하는 사이버 보안 환경 속에서 어떤 선택을 해야 하는지 살펴봅니다. 기술을 적극적으로 활용하는 동시에 규제 변화, 지정학적 불안정성, 디지털 주권 등 글로벌 이슈에 대응하며 조직의 회복력과 자율성을 높일 수 있는 방안을 집중적으로 다룹니다.

사이버 보안은 더 이상 혁신이 끝난 뒤 점검하는 분야가 아닙니다. 새로운 기술 도입과 사업 추진 단계에서부터 고려해야 할 핵심 요소입니다. 보안을 혁신 전략과 실행 계획 전반에 자연스럽게 녹여낸 기업일수록 변화하는 위협에 유연하게 대응할 수 있으며, 기업들의 중요한 자산 보호는 물론 디지털 경제에서 경쟁력을 강화할 가능성이 큼니다.

2027년을 앞둔 지금, 디지털 전환과 사이버 보안은 더 이상 분리해서 바라볼 수 있는 별개의 과제들이 아닙니다. AI는 위협 환경을 변화시키고 있으며, 업무 환경의 변화와 다양한 규제, 디지털 주권에 대한 논의로 인해 그 환경은 더 복잡해지고 있습니다. 이러한 변화가 동시다발적으로 밀려오면서 기업들은 새로운 위협과 요구사항에 직면하고 있으며, 이전보다 더 전략적인 판단을 내려야 하는 상황에 처해 있습니다.

“AI의 확산과 초연결 생태계의 등장, 지정학적 긴장, 갈수록 복잡해지는 규제 환경은 사이버 위협의 진화를 더욱 가속화하고 있습니다. 그러나 이에 대응하기 위한 기본 원칙은 달라지지 않습니다. 가장 중요한 자산을 우선적으로 보호하는 위험 기반 접근법이 여전히 핵심이며, 단순히 규제를 준수하는 데 만족하기보다 조직의 회복력을 얼마나 강화하고 있는지를 사이버 보안의 기준으로 삼아야 합니다.”



와디 므세디
사이버 보안 총괄
포비스 마자르

서문

최근의 사이버 보안 사고는 기업에 분명한 메시지를 던지고 있습니다. 사이버보안은 더 이상 IT 부서만의 단순한 문제가 아니라 고객신뢰와 사업의 연속성을 유지하고 규제를 준수하며 이를 통해 창출해 나갈 기업가치에 직접적인 영향을 미칠 수 있는 기업의 핵심 경영과제입니다.

국내 금융권에서는 최근 시중은행들과 제2금융권의 금융기관들에 대한 외부 공격으로 인한 정보유출 사고가 확인됐습니다. 해당 정보유출에 감독당국은 전산시스템 전반에 대한 보안 점검을 요청하였고, 추가 피해가 발생함에 따라 금융권의 공동대응체계를 강화하고 유사사고 확산 가능성을 차단하기 위한 조치를 강구하고 있습니다.

특히 이번 정보유출 사고는 금융기관들의 핵심 전산망뿐만 아니라 정보가 저장되는 장소 및 관련 개체들이 다양해짐에 따라 그 공격 경로가 확장되고 있음을 확인할 수 있었습니다. 이에 따라 기업들은 개별 기업들의 현황을 고려하여 보안 관리의 범위를 재점검해야 할 필요성이 커지고 있습니다.

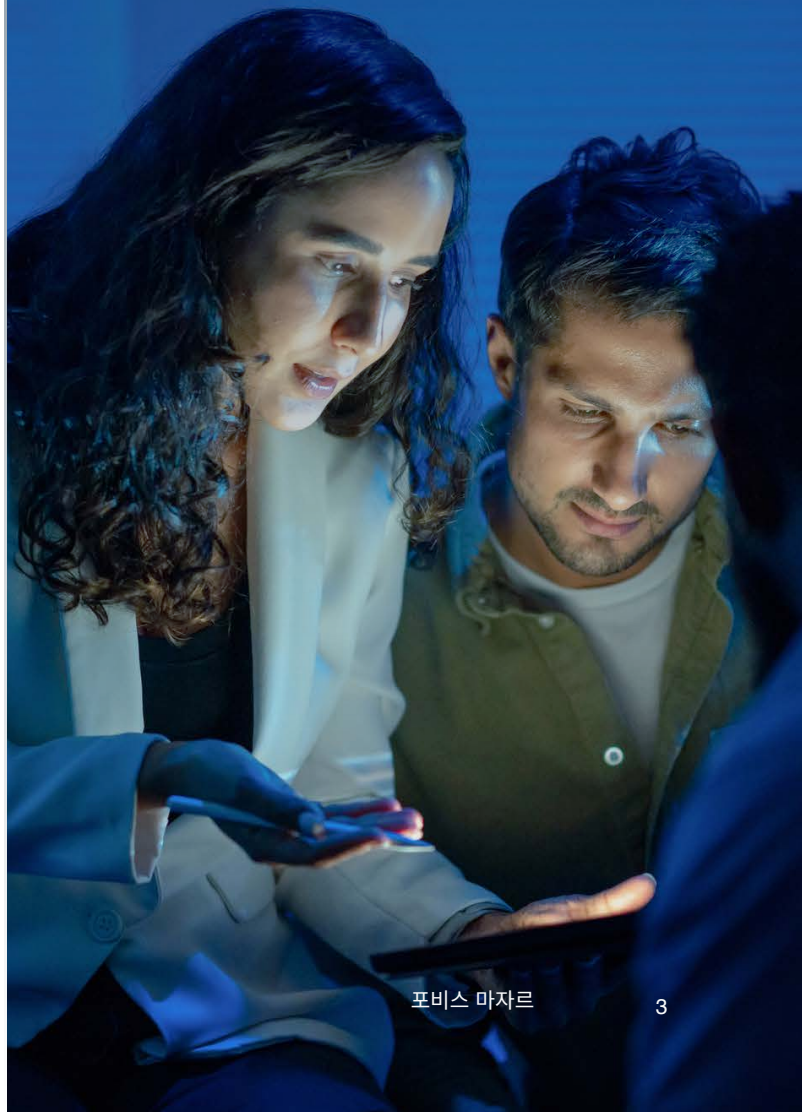
또한 AI의 확산은 보안사고와 관련된 위협 환경을 파악하는 데 어려움을 주고 있습니다. 최근 금융권 침해사고에서도 AI 활용 가능성이 제기돼 당국이 그 원인과 공격 수법을 조사하고 있는 상황입니다. 이제 경영진은 기업에 충분한 보안 솔루션의 적용 여부를 넘어 기업의 핵심 자산과 관련된 기업 IT 환경의 외부 접점을 충분히 파악하여야 합니다. 그리고 기업이 서비스를 제공받는 제3자 업체들에서 초래될 수 있는 위험들을 관리하며 사고 발생 시 기업의 핵심 사업을 신속히 회복할 수 있는지를 점검해야 합니다.

이와 관련하여 이번 보고서에서는 기업의 공급망, AI, 관련된 규제 상황, IT·OT 융합과 보안 투자 등 주요 사이버 보안과 관련된 과제를 살펴봅니다.



심규택
파트너, 감사 및 금융서비스
한국의 포비스 마자르

앞으로 기업의 경쟁력을 가르는 기준은 빠르게 변화하는 위협 상황들에 얼마나 준비가 되어 있고 사고 이후에도 사업과 이해관계자들의 신뢰를 얼마나 안정적으로 지켜낼 수 있는가에 있을 것입니다. 지금이 바로 우리 조직의 사이버보안 리스크와 그 대응 역량을 객관적으로 진단하고, 핵심 자산과 사업을 중심으로 투자 우선순위와 실행 로드맵을 재점검해야 할 시점입니다.



주요 인사이트

선도적인 기업들은 사이버 보안을 단순한 비용이 아닌 경쟁력의 원천으로 바라보고 있으며, 이를 통해 비즈니스 성과와 연결할 수 있는 방안을 적극적으로 탐색하고 있습니다.

디지털 주권에 대한 관심이 지속적으로 증가하고 있지만, 글로벌 기업에게는 완전한 통제권보다 안정적으로 사업을 운영할 수 있는 자율성을 확보하는 것이 더 현실적이고 필수적인 과제가 되고 있습니다.

유럽에서는 디지털 보안 및 보안 관련 규제가 강화되는 추세인 반면, 미국에서는 규제를 완화하려는 움직임이 나타나고 있습니다. 이러한 상반된 환경에서도 위험 기반 접근법은 효과적인 규제 대응의 핵심 원칙으로 자리 잡고 있습니다.

운영기술(OT)과 기업 IT 환경의 경계가 점점 희미해지면서 새로운 사업 기회가 열리고 있지만, 이에 따른 보안 위험도 증가하고 있습니다.

AI는 공격자와 방어자 모두의 역량을 한층 강화하며 새로운 경쟁 구도를 형성하고 있습니다. 기업은 AI 기반 위협에 맞서기 위해 AI를 활용함과 동시에 조직 특성에 맞는 거버넌스 체계도 마련해야 합니다.

데이터 거버넌스는 여전히 효과적인 사이버 보안 전략의 기초입니다. 그러나 일률적인 통제보다 위험 수준과 사업 특성을 고려한 균형 있는 접근이 중요합니다.

사이버 보안 팀은 안정성과 민첩성을 동시에 확보해야 하며, 이를 위해서는 지속적인 투자와 인력 역량 강화가 필수적입니다.



글로벌 사이버 보안 현황

사이버 보안이 공급망의 핵심 과제로 떠오르는 이유

사이버 보안은 이제 공급망 관리의 핵심 요소로 자리 잡고 있습니다. 최근 기업들은 협력사를 평가할 때 가격이나 기술력 외에도 보안 수준을 중요한 기준으로 고려하고 있습니다. 실제로 제안요청서(RFP) 검토와 입찰 과정에서 사이버 보안 요건 충족 여부를 검증하는 절차가 일반화되고 있으며, 기준에 미치지 못하는 기업은 초기 검토 대상에서 제외되는 경우가 늘어나고 있습니다.

이러한 변화는 공급망과 기술 환경이 복잡해질수록 더욱 뚜렷하게 나타나고 있습니다. 보안 수준이 높은 기업은 위험 관리뿐만 아니라 평판과 신뢰 측면에서도 경쟁 우위를 확보하게 됩니다. 특히 B2B 시장에서 이러한 현상이 더욱 명확하게 나타나며, 많은 기업이 공급업체 선정 시 높은 수준의 보안 요건을 요구하고 있습니다. 이를 충족하지 못하면 사업 기회 자체를 잃을 수 있는 위험도 있습니다.

복잡한 공급망으로 인해 데이터가 어디에 저장되고, 어떤 경로로 처리되는지 명확하게 알기 어려워지면서 기업이 데이터 흐름을 완벽히 파악하기 어려워졌습니다. 이러한 정보의 공백은 보안 취약점으로 이어질 수 있으며, 특히 AI에 의해 새로운 형태의 데이터 공유 및 처리방법이 적용된 경우, 이러한 가시성의 부족은 중요한 보안취약점을 야기시킬 수 있습니다. 또한, 기업의 핵심 시스템과 클라우드 플랫폼 및 외부 서비스 간 상호연결성이 지속적으로 증가하면서 잠재적인 보안 공격의 대상이 확장되고 있고, 이러한 보안 위협을 극복하는 것이 전체 기술환경 전반의 가시성 확보에 의존하도록 되고 있습니다.

궁극적으로 기업들은 이제 개별 기업의 사이버 보안을 넘어 전체 기술환경 전반의 잠재적인 위협들을 모니터링하고 관리하도록 요구되고 있습니다. 이러한 요구들이 반영되어 EU에서는 외부의 서비스공급자와 공급망 차원의 사이버보안 위협을 보다 강화된 방법으로 관리하도록 하는 디지털운영복원력법안(DORA)과 NIS2 지침이 제정되었습니다.

위와 같이 외부의 서비스 공급자 및 공급망의 책임이 해당 기업으로 공유되는 방향으로의 변화는 이전보다 복잡해진 제3자 관리체계(TPRM)의 도입을 이끌고 있습니다. 제3자의 사이버보안체계에 대한 점수화를 통해 이를 관리하는 도구의 등장은 시장의 새로운 부담이 되고 있습니다. 기업들은 사이버보안의 성숙도가 계약을 수주하고, 파트너십을 유지하면서 고객의 신뢰를 유지할 수 있는 능력에 직접적인 영향이 미친다는 것을 체감하고 있습니다.



글로벌 사이버 보안 현황

디지털 주권과 디지털 자율성: 사이버 보안을 둘러싼 새로운 지정학

사이버 보안이 이제 국가 주권과 직결된 중요한 문제로 자리 잡고 있습니다. 사이버 공격이 국가의 전략적 수단으로 활용되면서 각국 정부는 중요 데이터의 저장 위치, 핵심 디지털 서비스를 운영하는 주체, 기업이 의존하는 기술 등을 더욱 면밀히 살펴보고 있습니다. 실제로 Volt Typhoon과 같은 조직은 향후에 활용할 수 있는 가능성을 보고 민간 인프라에 장기간 잠복해온 것으로 알려져 있으며, 2024년 CrowdStrike 장애 사태는 특정 외부 서비스 제공업체에 대한 과도한 의존이 얼마나 큰 리스크가 될 수 있는지를 보여줬습니다. 특히 해당 서비스가 다른 국가의 법과 규제의 영향을 받는 경우라면 이러한 우려는 더욱 커질 수 있습니다.

정책적 대응도 빠르게 이뤄지고 있습니다. 특히 유럽에서는 데이터 현지화 요건, 소버린 클라우드 구축, 다양한 규제 강화가 활발히 추진되고 있습니다. NIS2와 DORA도 운영 복원력과 공급망 보안을 핵심 과제로 강조하고 있습니다. 이러한 흐름은 유럽에만 국한되지 않습니다. 전 세계적으로 사이버 보안에 대한 기대 수준이 높아지면서, 단순히 규정을 준수하는 것을 넘어 실제 위기 상황에서도 핵심 업무를 지속하고 신속히 복구할 수 있는 역량을 입증하는 것이 중요한 과제가 되고 있습니다.

그러나 디지털 주권을 지나치게 강조하면 공급업체 생태계가 분절되고, 동일한 인프라에 대한 중복 투자가 증가할 수 있습니다. 또한 검증된 기술에 대한 접근성이 제한될 가능성도 있습니다. 오히려 특정 국가나 특정 공급업체에 대한 의존이 심화되어 새로운 형태의 위험이 발생할 수도 있습니다. 극단적인 경우, 한 국가의 정책 변화가 사업 지속성 자체에 영향을 미칠 수도 있습니다.

따라서 기업의 목표는 단순히 디지털 주권을 확보하는 것이 아니라 디지털 자율성을 추구하는 데 있습니다. 디지털 자율성이란 디지털 의존 관계를 명확히 이해하고 필요한 경우에 기술을 직접 제어하거나 다른 대안으로 전환할 수 있는 역량을 말합니다. 즉, 특정 기술이나 공급업체에 무조건적으로 의존하지 않으면서도 변화하는 환경에 유연하게 대응할 수 있는 선택권을 확보하는 것이 중요합니다.

결국 중요한 것은 디지털 주권이 아니라 디지털 자율성입니다. 디지털 자율성을 스스로 이해하고 통제할 수 있는 역량이야말로 규제 당국과 고객, 투자자들이 필요로 하는 회복력을 보여주는 보다 실질적인 기준입니다.

기업이 고려해야 할 사항



민감한 데이터가 실제로 저장되고 처리되는 위치를 파악해야 합니다. 계약서에 명시된 내용만으로는 충분치 않으며, 백업 시스템이나 유지보수 지원 체계까지 포함해 데이터가 어떤 경로로 저장·처리되는지 전체 흐름을 파악해야 합니다.



공급업체의 지정학적 리스크도 살펴봐야 합니다. 주요 계약 상대방뿐 아니라 공급망의 하위 협력업체와 기술 의존 관계까지 확인해야 합니다. 눈에 잘 띄지 않는 의존성이 예기치 않은 큰 위험 요인이 될 수 있기 때문입니다.



공급업체의 위치와 적용되는 법률 체계도 중요한 평가 요소입니다. 핵심 서비스를 제공하는 기업이 속한 국가와 그들이 준수해야 할 법률 및 규제가 조직이 감당해야 할 법적·지정학적 리스크를 변화시킬 수 있습니다.



규제준수를 넘어선 회복력에 대한 입증도 필요합니다. 디지털 주권은 중요한 고려사항이지만, 최종 목표는 아닙니다. 조직의 전반적인 회복력 전략의 일환으로 취급되어야 하며, 실제 사고 발생 시 핵심 업무의 안정적 유지와 복구 가능성이 더욱 중요합니다.

“자율성 확보라는 목표를 위해 디지털 주권 확립을 중간 요소로 삼는 기업이 결국 더 강한 경쟁력을 갖게 될 것입니다. 의존 관계를 명확히 이해하고, 신뢰할 수 있는 파트너사를 선택하며, 예상치 못한 장애나 위기 상황에서도 운영을 지속할 수 있는 능력을 입증할 수 있는 기업은 규제를 준수하는 것에 그치지 않고 실질적인 회복력을 갖추게 됩니다.”



야코프 헤슬러
글로벌 컨설팅 총괄
포비스 마자르

“사이버 공간에서는 평시와 위기 상황의 경계가 점차 흐려지고 있습니다. 국가 차원의 공격 주체들은 당장의 이익을 노리기보다, 앞으로의 영향력을 확보하기 위해 민간 인프라에 미리 침투해 자리를 잡고 있습니다. 이러한 변화는 디지털 서비스에 의존하는 모든 조직이 사이버 위험을 바라보는 관점을 다시 생각하게 만들고 있습니다.”



조지 라가리아스
수석 이코노미스트
포비스 마자르



글로벌 사이버 보안 현황

DORA와 NIS2는 사이버 보안 규제를 어떻게 바꾸고 있는가

DORA와 NIS2는 유럽의 사이버 보안 규제 환경을 빠르게 변화시키고 있습니다. 기존에는 법적 준수를 문서로 입증하는 데 초점을 맞췄던 반면, 이제는 기업이 얼마나 안정적으로 운영하고 위기 상황에서 신속하게 대응할 수 있는지를 증명하는 방향으로 변화하고 있습니다. 특히 여러 국가에서 사업을 운영하는 글로벌 기업에게 DORA와 NIS2를 동시에 충족하는 일은 2027년의 주요 과제 중 하나로 손꼽힙니다.

유럽 시장에서는 촘촘한 규제 환경으로 인해 기업들의 부담이 가중되고 있습니다. 현재 100개가 넘는 디지털 관련 법률과 지침이 있으며, 계속해서 새로운 의무와 요구사항이 추가되어 복잡한 규제가 만들어지고 있습니다. 여러 차례 시행이 연기됐던 NIS2는 이제 본격적인 집행 단계에 들어섰고, 앞으로 시행될 Cyber Resilience Act(CRA)는 디지털 요소가 포함된 제품에도 일정 수준 이상의 사이버 보안을 요구할 예정입니다. NIS2가 규정이 아닌 지침이라는 점도 기업들이 어려움을 겪는 이유 중 하나입니다. 회원국마다 NIS2의 원칙을 자국 법률에 반영하는 방식이 조금씩 다르기 때문에 한 국가에서 수행한 규제 대응 업무를 다른 국가에 그대로 적용하기 어렵습니다. EU가 추진 중인 디지털 옴니버스는 이러한 복잡성을 줄이고 기업 규모와 위험 수준에 맞춘 보다 합리적인 규제 체계를 마련하는 것을 목표로 하고 있지만, 아직 실질적인 진전은 없는 상태입니다.

반면 미국은 정반대의 상황입니다. 미국은 규제를 완화하는 기조를 유지하고 있으며, 유럽과 같은 포괄적인 연방 차원의 사이버 보안 규제 체계는 존재하지 않습니다. 규제는 주로 특정 산업이나 정부 분야에 집중돼 있으며,

대표적인 사례가 국방 관련 사업자를 대상으로 하는 사이버보안 성숙도 모델 인증(CMMC)입니다.

다만 이마저도 시행이 지연되고 있으며, 그 영향은 금융 서비스 IT 분야를 비롯한 여러 산업에 영향을 미치고 있습니다. 미국에는 연방 차원의 개인정보보호법이 없어 주마다 서로 다른 규제를 따르고 있고, 현재 정치적 상황을 고려하면 전국 단위의 통합 법안이 등장할 가능성은 낮아 보입니다. 그러나 규제가 적다고 해서 기업의 부담이 줄어드는 것은 아닙니다. 어떤 규정은 지나치게 구체적이고, 어떤 부분은 기준이 모호하여 기업이 스스로 판단해야 합니다. 결국 기업들은 각기 다른 규제 체계와 기대 사이에서 나아갈 방향을 설정해야 하며, 이는 글로벌 기업일수록 더욱 부담스러운 과제로 남게 됩니다.

위험 기반 접근법은 어떻게 비즈니스 지속성을 지원하는가

이처럼 복잡한 규제 환경은 산업에 새로운 부담을 안기는 동시에 새로운 기회를 창출하기도 합니다. 최근 도입된 많은 규제가 조직의 회복력과 비즈니스 지속성을 강화하는 데 도움을 주는 것은 사실입니다. 그러나 규제를 준수하기 위한 작업과 문서화 과정은 이미 인력이 부족한 보안 조직에 상당한 부담이 됩니다.

보다 효과적으로 관리하기 위해 위험 기반 접근법을 적용하는 것이 중요합니다. 위험 기반 사이버 보안 전략은 조직이 실제로 중요한 위험을 우선순위를 두고 자원을 배분할 수 있도록 돕습니다. 이를 통해 규제 준수가 보안 활동을 지배하기보다는 보안 전략을 뒷받침하는 역할을 수행하도록 합니다.

“규제 준수는 위험 기반 사이버 보안 프로그램의 여러 구성 요소 중 하나에 불과합니다. 특정 법률이나 프레임워크가 사업 일부의 위험 수준에 영향을 줄 수는 있지만, 그것이 조직 전체의 보안 전략을 결정해서는 안 됩니다.”



톰 톨러턴
CMMC 부문 리드, 수석 컨설턴트
미국의 포비스 마자르

글로벌 사이버 보안 현황

운영기술(OT) 보안이란 무엇이며, 왜 공격의 표적이 되고 있는가

운영기술(OT)은 전 세계의 핵심 인프라와 산업 현장을 움직이는 기술입니다. 발전소, 제조설비, 교통 시스템, 상하수도 시설 등 물리적 설비를 관리하고 운영하는 시스템이 대표적인 예입니다. 최근 OT 환경이 디지털 기술과 연결되면서 운영 효율성은 높아졌지만, 동시에 사이버 위협에 더 많이 노출되고 있습니다. 특히 전통적인 IT 시스템에 비해 보안 투자가 상대적으로 부족했던 만큼 새로운 위협에 직면하게 되었습니다.

전통적으로 OT는 오랫동안 엔지니어링과 관련된 사항으로 여겨져 왔으며, 사이버보안은 큰 우선순위가 아니었습니다. 이 때문에 정교한 보안 체계를 갖추기보다 외부 네트워크와 분리된 환경에서 운영되어 왔습니다. 그러나 최근 들어 중요한 기반시설의 OT 환경을 겨냥한 공격이 증가하고 있으며, 국가 차원의 공격 조직들은 보호 수준이 낮은 OT 환경을 주목하며 목표로 삼고 있습니다. 실제로 2025년 12월에는 베네수엘라와 폴란드의 인프라 시설을 겨냥한 공격 시도가 보고되었습니다. 또한 M&S와 Jaguar Land Rover 사례처럼 사이버 공격이 기업 운영 및 비즈니스 지속성에 직접적인 영향을 미친 사례가 잇따르면서, OT 환경에 대한 가시성과 관리 수준에 대한 요구가 커지고 있습니다.

하지만 여기에는 딜레마가 존재합니다. 보이지 않는 환경을 기업들이 관리할 수도 없음에도 불구하고 많은 기술 리더들은 OT 네트워크를 충분히 파악하지 못하고 있다고 답하고 있습니다. 그래서 기업들은 위협을 효과적으로 파악하고 관리하기 위해 OT 시스템을 다른 시스템과 연결하고, 데이터 수집 도구와 모니터링 플랫폼을 도입하며, IT 환경과의 연계를 확대하고 있습니다. 문제는 이러한 연결 과정이 새로운 위협을 만들어낼 수 있습니다. OT 환경이 기업 IT 시스템, 클라우드 플랫폼, 원격 유지보수 솔루션과 연결됨에 따라 과거에는 물리적 분리로 보호받던 시스템이 외부 위협에 노출될 가능성이 커지고 있습니다. 즉, 가시성을 높이기 위해 만든 연결 경로가 오히려 새로운 공격 경로가 될 수 있다는 것입니다. 또한, OT 시스템은 일반적인 IT 시스템보다 수명이 길고, 오래된 장비와 레거시 시스템이 여전히 존재하는 경우가 많습니다. 따라서 IT 환경에서는 일반적으로 사용하는 보안 접근법을 그대로 적용하기 어려운 경우도 빈번합니다.

그럼에도 불구하고 OT 자산 보호는 선택이 아닌 필수 과제가 되고 있습니다. 특히 국가 기반 시설을 운영하는 조직은 디지털 규제를 통해 OT 보안을 강화하는 방향으로 나아가고 있습니다.

“OT 환경의 가시성을 높이는 것은 중요하지만, 그 과정에서 신중한 접근이 필요합니다. 오랫동안 독립적으로 운영되던 시스템을 적절한 거버넌스와 통제 없이 연결하면, 조직은 파악하고 관리하려 했던 운영상 위험을 오히려 증가시킬 수 있습니다.”



폴 트루잇
사이버 보안 부문 책임자, 수석
컨설턴트
미국의 포비스 마자르

글로벌 사이버 보안 현황

AI는 사이버 보안을 어떻게 바꾸고 있는가

AI는 사이버 보안의 양상을 근본적으로 바꾸고 있습니다. 공격자는 AI를 활용해 보다 정교하고 표적화된 공격을 대규모로 수행하고 있으며, 방어 측은 AI를 활용해 위협 탐지 능력을 강화하고 대응 과정을 자동화하여 보안 수준을 높이고 있습니다.

그동안 AI는 기회와 위협이라는 관점에서 논의되어 왔지만, 이제 이러한 관점만으로는 AI의 영향을 충분히 설명하기 어렵습니다. AI는 단순히 기술 혁신을 넘어 사이버 보안 환경 전반을 재편하는 구조적인 변화를 이끌고 있습니다. 공격과 방어 양측 모두 AI 중심의 생태계를 형성하고 있으며, 취약점 탐색부터 공격 수행까지 자동화 기술이 빠르게 발전하고 있습니다. 그 결과 사이버 공간에서는 새로운 형태의 경쟁이 벌어지고 있으며, 공격자와 방어자 간의 격차도 점차 확대되고 있습니다.

비대칭적인 경쟁 구도

이러한 격차는 단순히 기술 수준의 차이 때문만은 아닙니다. 실제로는 기술 자체보다 이를 어떻게 활용하느냐가 더 중요하게 작용합니다. 공격자와 방어자가 비슷한 수준의 AI 기술을 가지고 있더라도, 공격자가 훨씬 유리한 위치에 설 수 있습니다. 공격자는 시스템 운영이나 서비스 중단을 걱정할 필요가 없으며, 변경 관리나 규제 준수 의무도 없고, 경영진에게 결과를 보고해야 할 필요도 없습니다. 반면 방어자는 조직을 보호해야 하는 입장이기 때문에 각종 정책과 절차, 규제 및 윤리 기준을 준수해야 합니다. 이는 필수적인 과정이지만, 동시에 의사결정과 대응 속도를 늦추는 요인이 되기도 합니다. AI를 활용하는 공격자들은 이와

같은 틈을 노리고 있으며, AI가 공격 환경을 얼마나 빠르게 변화시키고 있는지는 여러 사례를 통해 확인할 수 있습니다.

- **증가하는 공격 규모와 현실성:** 사이버 공격의 규모는 계속 커지고 있으며, 특히 AI를 활용한 사기와 사회공학 공격이 급증하고 있습니다. 딥페이크는 이제 단순한 기술 시연이나 화제를 넘어서 실제 비즈니스 위협으로 대두되고 있습니다. 대표적인 사례로 엔지니어링 회사 Arup은 임원을 사칭한 딥페이크 화상회의에 직원들이 속아 약 2,500만 달러를 송금하는 피해를 입기도 했습니다.
- **스스로 변형하는 악성코드:** 최근에는 메타모픽 악성코드의 위협도 커지고 있습니다. 메타모픽 악성코드는 실행 과정에서 스스로 코드를 변조해 탐지를 회피합니다. 기존 보안 시스템이 주로 활용해 온 시그니처 기반 탐지 방식만으로는 대응이 점점 어려워지고 있으며, 보안 조직은 알려진 패턴보다 실제 행위와 이상 징후를 중심으로 위협을 식별하는 방향으로 변화하고 있습니다.
- **완전 자동화된 공격 체계:** 에이전트형 AI의 발전으로 인해 공격 자동화는 새로운 차원에 도달했습니다. 이제는 일부 과정에 한정되지 않고 공격 준비부터 실행까지 전체 절차를 자동화할 수 있는 수준에 가까워지고 있습니다. 이런 환경에서는 아무리 숙련된 인력으로 구성된 보안 팀이라도 공격 속도를 따라잡기는 어렵습니다. 따라서 기업들은 공격 발생 이후의 대응에서 벗어나 보다 선제적인 접근 방식을 채택해야 합니다. 취약점을 신속히 보완하고 지속적으로 시스템을 모니터링 하며, 침해 발생 시 가장 큰 피해를 초래할 수 있는 핵심 시스템과 데이터를 우선적으로 보호해야 합니다.

“에이전트형 AI가 공격을 자동화하는 환경에서는 인간만으로 대응하기 어렵습니다. 방어자는 AI를 활용해 대응 역량을 확대하고 속도를 높여야 합니다. 이는 선택이 아니라 필수입니다.”



알리술탄 키르기즈바예프
파트너, 데이터·AI 역량센터 총괄
포비스 마자르

글로벌 사이버 보안 현황

[IBM의 Cost of a Data Breach 2026 보고서에 따르면](#), AI 기반 탐지 및 대응 시스템을 활용하는 기업은 데이터 침해 시 평균 비용을 약 40% 절감했으며, 사건당 약 193만 달러의 손실을 줄인 것으로 나타났습니다. 공격자들이 사용하는 AI 기술은 방어 측에서도 유용하게 활용될 수 있습니다. 실제 공격 상황을 가정해 조직 보안 체계를 점검하고 취약점을 미리 발견하는 데 도움을 주고 있습니다.

현재 기업들은 단순 자동화를 넘어 에이전트형 AI에 주목하고 있습니다. 이는 위협 탐지에 그치지 않고, 위협을 격리하고 대응 조치까지 수행하는 AI를 의미합니다. 중요한 의사 결정은 여전히 사람이 검토하고 승인하는 방식으로 운영됩니다. 에이전트형 AI는 사이버 보안의 오래된 딜레마를 해결하는 데도 도움이 될 수 있습니다. AI를 안전하게 활용하려면 명확한 통제 기준과 가이드라인이 필요하지만, 사이버 공격은 본질적으로 예측할 수 없는 모습을 띠고 있습니다. 모든 가능성을 사전에 정의하고 대응책을 마련하는 것은 현실적으로 어렵습니다. 하지만 공격자는 이러한 제약 없이 자유롭게 움직일 수 있습니다. 적절한 통제 체계 아래 운영되는 에이전트형 AI는 예상치 못한 공격에도 반자동적으로 대응하여 방어 공백을 최소화할 수 있습니다.

다만 효율성이 높아진 만큼 위험도 함께 커지고 있습니다. 공격자가 사용하는 AI 에이전트는 별도의 승인 절차 없이 작동할 수 있지만, 방어용 AI는 반드시 책임 있는 통제 체계 안에서 운용돼야 합니다.

“인간의 개입을 완전히 배제하는 것은 매우 우려스럽습니다. AI 에이전트는 모든 입력값을 충분히 검증할 수 있어야 하며, 시스템 전반에서 오용이나 악용을 방지할 수 있는 통제 장치도 갖춰야 합니다.”



손 앤드류
매니저, IT 리스크 및 컴플라이언스
미국의 포비스 마자르

AI는 방어 수단인 동시에 새로운 공격 표면이기도 합니다. 새로운 AI 서비스가 추가될 때마다 잠재적인 보안 위험도 함께 생겨납니다. 최근 빈번히 발생하고 있는 프롬프트 인젝션 공격은 이러한 위험을 명확히 보여줍니다. DPD와 McDonald's의 사례에서 확인할 수 있듯이 AI의 취약점은 평판 리스크뿐만 아니라 실제 데이터 유출로도 이어질 수 있습니다. 따라서 AI 거버넌스와 데이터 프라이버시를 따로 관리하던 방식에서 벗어나 정책, 통제 체계, 공급업체 관리를 아우르는 통합적인 접근이 필요합니다.

글로벌 사이버 보안 현황

AI 도입 과제와 실질적인 전략

에이전트형 AI를 도입할 때 가장 중요한 과제는 입력 데이터가 신뢰성을 검증하고, 의미 있는 수준의 인간 감독을 유지하는 것입니다. 그러나 모든 의사 결정 과정에 사람의 승인을 거치도록 설계해서는 안 됩니다. AI의 효과적인 활용과 적절한 통제 사이에서 균형을 찾는 것이 중요합니다.

사이버 보안처럼, AI 거버넌스도 위험 기반 접근법을 따라야 합니다. 모든 위협을 완벽하게 차단하는 것은 현실적으로 불가능하며, 자동화된 공격이 늘어날수록 이는 더욱 분명해집니다. 보안 내재화는 여전히 가장 효과적인 위험 관리 원칙으로 꼽힙니다. 다만 보안을 강화할수록 사용 편의성은 떨어지고, 서비스 출시 속도에도 영향을 줄 수 있습니다. 따라서 보안, 사용자 경험, 비즈니스 민첩성 사이에서 적절한 균형을 찾는 것이 중요합니다.

“완벽함을 목표로 하면 오히려 보안은 떨어집니다. 보안은 비즈니스의 발목을 잡게 되고, 현업은 규정을 우회하는 방법을 찾게 되며, 보안 담당자는 대응에 쫓겨 본연의 역할을 수행하지 못하게 됩니다.”



안톤 유누소프
사이버 보안 부문 총괄
영국의 포비스 마자르

사이버 보안의 목표는 모든 위협을 제거하는 것이 아닙니다. 오히려 조직에 가장 중요한 핵심 자산, 즉 ‘Crown jewels’이 무엇인지 파악하고 그 중요도에 맞춰 보호하는 것이 더 현실적이고 효과적인 접근 방식입니다. 또한 사이버 보안 조직은 통제와 규제에만 집중하는 부서가 아니라, 조직이 AI를 안전하고 신속하게 활용할 수 있도록 지원하는 비즈니스 파트너로서의 역할을 해야 합니다.

위험 수준에 맞는 거버넌스 적용: AI 활용하는 사례마다 위험 수준이 달라집니다. 따라서 모든 기술에 동일한 위험 평가 체계를 적용하되, 각 사례의 위험도를 고려해 통제 수준을 조정해야 합니다. 모든 AI 서비스를 동일한 기준으로 관리하려 하면 오히려 비효율이 커지고 실패 가능성도 높아질 수 있습니다.

인간의 감독 체계 유지: AI 에이전트의 역할을 명확히 설정해야 합니다. 위협 탐지나 격리, 일부 시스템의 차단까지는 AI가 담당할 수 있지만, 중요한 판단은 인간이 검토하고 결정하도록 설계해야 합니다. 이와 함께 입력값에 대한 철저한 검증 체계도 갖춰야 합니다.

AI 거버넌스와 데이터 프라이버시 통합 관리: AI 관리 체계와 개인정보 보호 체계를 분리하기 보다는 정책, 통제 기준, 공급업체 관리 전략을 하나의 프레임워크 안에서 관리하는 것이 바람직합니다.

보안 인력에 대한 투자: 새로운 공격 기법과 방어 기술이 빠르게 발전하는 가운데 보안 조직의 역량 강화를 필수적으로 고려해야 합니다. 오늘날의 역량 격차는 기술뿐 아니라 전문성에서도 발생하므로 이에 대한 투자가 중요합니다.

글로벌 사이버 보안 현황

양자 컴퓨팅: 패러다임 전환에 대비하기

양자 컴퓨팅이 대부분의 기업에 당장 직접적인 위협이 되는 것은 아닙니다. 그러나 그 파급력이 워낙 크기 때문에, 위협이 현실화된 이후가 아니라 지금부터 대비를 시작해야 합니다.

양자 컴퓨팅이 가져올 보안 위협

양자 컴퓨팅이 초래하는 위협은 일반적인 사이버 보안 위협과는 다른 시간적 차원에서 발생합니다. 현재의 암호 체계가 무력화될 정도의 양자 컴퓨터가 널리 활용되기까지는 시간이 걸릴 수 있습니다. 하지만 공격자들은 이미 이러한 미래에 대비하고 있습니다. 그 대표적인 예로 “Steal now, decrypt later” 전략이 있습니다. 공격자는 현재 암호화된 데이터를 미리 수집해 보관한 뒤, 향후 충분한 성능의 양자 컴퓨터가 등장하면 이를 복호화해 활용하려고 할 수 있습니다. 따라서 오늘 유출된 데이터라도 미래에는 민감한 정보가 그대로 노출될 수 있다는 점이 문제로 대두됩니다.

“사이버 범죄자들은 이미 양자 컴퓨팅 시대를 준비하고 있습니다. 기업들 역시 지금부터 대비해야 합니다. 공격자들은 당장 양자 컴퓨터를 소유하지 않더라도, 오늘 암호화된 데이터를 탈취한 후 미래에 관련 기술이 충분히 발전했을 때 이를 복호화할 수 있습니다. 따라서 중요한 질문은 ‘양자 컴퓨팅이 언제 현 암호 체계를 무력화할 것인가’가 아니라 ‘우리 데이터가 언제까지 기밀성을 유지할 수 있는가’입니다.”



안톤 유누소프
사이버 보안 부문 총괄
영국의 포비스 마자르

이러한 현실을 감안하면 기업들은 양자 컴퓨팅 위협이 본격화되기 전에 양자내성암호 체계로의 전환을 준비해야 합니다. 이를 위해서는 먼저 현재 사용 중인 암호화 기술을 파악하고, 위험 수준을 평가하며, 주요 공급 업체의 전환 계획을 검토해야 합니다. 미국 국립표준기술연구소(NIST)는 2024년 8월 양자내성암호 표준을 최종 확정할 이후 관련 암호화 도구와 전환 가이드라인을 순차적으로 공개하고 있습니다. 기업의 입장에서는 위협이 현실화되기 전에 준비하는 것이 사후 대응보다 훨씬 효과적입니다.

기업은 다음과 같은 단계로 양자 컴퓨팅 시대에 대한 준비를 시작할 수 있습니다.



암호화 자산: 어떤 시스템과 데이터가 암호화 기술에 의존하고 있는지 전반적으로 검토해야 합니다. 이를 통해 양자 컴퓨팅으로 인해 영향을 받을 수 있는 영역을 파악할 수 있습니다.



우선 보호 자산: 암호화 체계가 무력화될 경우 가장 큰 영향을 받을 데이터와 시스템이 무엇인지 우선순위를 정해야 합니다. 고객 정보, 지식재산권, 금융 정보, 핵심 운영 데이터 등이 대표적인 대상이 될 수 있습니다.



전환 계획 수립: 양자내성암호 기술이 상용화되고 적용 가능한 시점에 맞춰 새로운 암호화 알고리즘으로 전환할 수 있도록 로드맵을 마련해야 합니다. 단순한 기술 교체가 아니라 장기적인 변화 관리 관점에서 접근할 필요가 있습니다.



공급망의 준비: 양자 전환은 개별 기업만의 과제가 아닙니다. 협력사와 기술 공급업체 역시 전환을 준비하고 있는지 확인해야 하며, 공급망 전반의 대응 수준도 함께 관리할 필요가 있습니다.

글로벌 사이버 보안 현황

데이터 전략, 전환 및 거버넌스

AI 활용이 확대되면서 “잘못된 입력은 잘못된 결과를 낳는다(Garbage in, garbage out)”는 원칙이 그 어느 때보다 중요해지고 있습니다. AI의 의사결정은 결국 데이터 품질에 좌우되기 때문에, 데이터 거버넌스는 이제 사이버 보안의 핵심 요소로 자리 잡고 있습니다. 데이터 거버넌스가 미흡하면 단순한 정보 관리 문제를 넘어 다양한 보안 위험으로 이어질 수 있습니다. 실제로 사고 대응 과정에서 기업들은 존재조차 몰랐던 데이터가 관리되지 않는 위치에 저장돼 있거나, 접근 권한이 불분명하게 관리되는 상황을 뒤늦게 발견하는 경우가 많습니다.

이처럼 데이터에 대한 가시성이 부족하면 기업 스스로 인지하지 못하는 공격 표면이 생길 수 있습니다. 어떤 데이터가 어디에 있는지 파악하지 못한다면 적절한 조치를 적용하기도 어렵습니다. 또한 이러한 문제는 보안 위험뿐 아니라 규제 준수 측면에서도 부담을 가중시킬 수 있습니다.

제3자 위험관리(TPRM)와 데이터 공유

데이터 공유가 확대되고 복잡해지면서 제3자 위험관리(TPRM)의 중요성도 커지고 있습니다. 오늘날의 공급망은 여러 단계의 협력사와 서비스 제공업체로 구성되어 있어 데이터가 실제로 어디서 처리되고 어떻게 보호되는지 파악하기 쉽지 않습니다. 이러한 복잡성은 기업의 사이버 보안 노출 범위를 넓히는 요인이 될 수 있습니다. 효과적인 제3자 위험관리를 위해서는 다음과 같은 요소가 필요합니다.

- ✓ **보안 통제를 위한 서비스 수준 협약(SLA):** 계약서에는 보안 및 규제 준수 요건을 명확히 명시해야 합니다. 또한 공급업체의 자체 보고에만 의존하기보다, 가능한 경우 감사 권한도 계약에 포함하는 것이 바람직합니다.
- ✓ **정기적인 평가 및 지속적인 모니터링:** TPRM은 일회성 점검으로 끝나서는 안 됩니다. 공급업체의 위험 수준을 지속적으로 모니터링하고 정기적으로 재평가해야 합니다. 감사 권한 역시 실제로 활용할 때 의미가 있습니다.
- ✓ **위험도에 따른 차등 관리 체계:** 모든 공급업체가 동일한 수준의 위험을 초래하는 것은 아닙니다. 따라서 기업은 공급업체의 중요도와 위험 수준에 따라 관리 체계를 차등 적용해야 합니다. 특히 핵심 시스템이나 중요 데이터를 다루는 공급업체에는 보다 강화된 관리와 감독 체계를 적용하는 것이 중요합니다.

데이터 보안 및 거버넌스를 실제로 구현하는 방법

데이터 거버넌스를 개선하려는 기업이라면 거창한 정책을 만드는 것보다 실질적인 논의와 점검부터 시작하는 것이 더 효과적입니다. 예를 들어, “만약 지금 휴대전화와 컴퓨터를 사용할 수 없다면 어떻게 될까?”같은 단순한 질문으로도 비즈니스 지속성 점검을 시작할 수 있습니다. 기술 부서뿐만 아니라 비기술 부서도 이러한 논의에 참여하다보면, 자연스럽게 데이터 의존도와 핵심 자산, 보호가 필요한 영역에 대한 대화로 발전할 수 있습니다.

이런 대화 중심 접근은 정책 수립에도 적용할 수 있습니다. 사이버 보안 조직은 정책이 실제 사용자 기준으로 충분히 이해하기 쉽고 실행 가능한지를 점검해야 합니다. 아무리 잘 설계된 정책이라도 현업 구성원이 이해하지 못하면 실효성을 기대하기 어렵기 때문입니다. 또한 교육과 협업은 데이터 거버넌스의 중요한 기반입니다. 임직원은 정책을 이해하고 실천할 수 있어야 하며, 거버넌스 담당 조직은 현업의 업무 특성과 운영 환경을 충분히 이해해야 합니다. 이러한 상호 이해가 뒷받침될 때 비로소 조직에 적합하고 효과적인 데이터 보호 체계를 구축할 수 있습니다.

“보안 조직은 현업 부서와 긴밀히 협력하며 데이터 활용 목적과 업무 환경을 이해해야 합니다. 그래야 조직에 맞는 현실적인 해결책을 제시하고 정책의 필요성도 효과적으로 설명할 수 있습니다. 구성원들이 보안 조치의 이유를 이해하고, 보안 조직이 업무 현실을 충분히 이해하고 있다고 느낄 때 정책 준수도 훨씬 자연스럽게 이뤄집니다.”



크리스토퍼 호크
이사
독일의 포비스 마자르

글로벌 사이버 보안 현황

데이터를 안전하게 보호하면서도 업무 효율성과 혁신을 해치지 않는 균형을 찾는 것은 데이터 거버넌스의 핵심 과제입니다. 지나치게 엄격한 정책은 오히려 구성원들이 우회적인 방법을 찾게 만들고, 그 과정에서 새도우 IT와 같은 새로운 위험이 발생할 수 있습니다. 효과적인 업무 지원 체계를 구축하려면 기술적 통제만으로는 부족합니다. 조직 문화와 구성원의 인식 변화도 함께 이루어져야 합니다. 특히 현업 부서와 긴밀하게 협력하면 서로의 요구사항과 제약 조건을 더 잘 이해할 수 있으며, 모니터링과 같은 보안 통제를 통해 사용자 행동을 더 효과적으로 파악할 수 있습니다.

사이버 보안 조직과 전문성

사이버 보안 분야의 전문가들은 지금 매우 큰 도전에 직면해 있습니다. 기술은 빠르게 발전하고 있지만 필요한 역량을 갖춘 인재를 여전히 부족하기 때문입니다. 기업들은 전통적인 보안 원칙뿐 아니라 AI, 클라우드 등 새로운 기술 환경까지 이해할 수 있는 인재를 찾고 있습니다. 그러나 이러한 역량을 모두 갖춘 전문가를 찾기는 쉽지 않습니다.

특히 최고정보보호책임자(CISO)의 역할은 최근 몇 년간 크게 변화했습니다. 과거에는 기술 전문가로서의 역할이 중심이었다면, 이제는 경영진의 일원으로서 비즈니스 관점에서 의사결정에 참여해야 합니다. 규제 대응, 이사회 보고, 전략 수립 등 역할의 범위가 넓어지면서 사이버 보안은 단순히 기술 부서의 책임을 넘어 경영 과제로 자리 잡고 있습니다.

이러한 변화에 힘입어 CISO의 보상 수준도 높아지고 있습니다. 하지만 이것은 현대의 보안 리더에게 요구되는 기술 전문성과 비즈니스 역량을 모두 갖춘 인재를 찾기가 더욱 어려워지고 있음을 의미하기도 합니다. 이에 따라 일부 기업은 가상 CISO를 도입해 내부 역량을 보완하고, 외부 전문가의 경험과 관점을 활용하는 방법을 채택하고 있습니다.

혁신 과제

사이버 보안 인력 관리에서 가장 큰 과제 중 하나는 혁신적인 아이디어와 관리 역량을 동시에 갖춘 인재를 찾는 일입니다. 특히 중견·중소 규모의 조직에서는 이러한 문제가 더욱 크게 나타납니다. 기술이 빠르게 발전할수록 보안 전문가는 새로운 기술을 지속적으로 배우면서도 보안의 기본 원칙을 지켜야 합니다.

SI와 양자 컴퓨팅 분야는 이러한 문제를 잘 보여주는 대표적인 사례입니다. 최첨단 기술과 보안이 교차하는 영역인 이 분야를 깊게 이해하는 전문가는 여전히 드뭅니다. 이런 상황에서 기업들은 신뢰할 수 있는 자문사와 외부 전문가의 도움을 통해 부족한 전문성을 보완하려고 합니다. 전략 수립에서 실행에 이르기까지 외부 전문가는 내부 팀과 협력하여 역량 격차를 줄이는 데 기여할 수 있습니다.

지속가능한 사이버 보안 조직 구축

개별 전문가를 채용하여 조직을 운영하는 전통적인 방식은 지속가능성이 점점 낮아지고 있습니다. 우수 인재 확보 경쟁이 치열해지면서 인건비 부담이 증가하고, 기술의 변화 속도가 빨라져 내부 인력만으로는 최신 위협과 기술 동향을 따라가기가 점점 어려워지고 있습니다.

자동화와 AI가 보안 조직의 업무 효율성을 높이는 데 중요한 역할을 하고 있지만, 모든 문제를 해결하기에는 한계가 있습니다. 최근에는 공유 서비스 모델을 활용하는 사례도 늘고 있습니다. 특히 M&A 환경에서는 모회사나 투자사가 자회사에 공통된 보안 서비스와 지원 체계를 제공하는 방식이 점차 확산되고 있습니다.

또한 외부 파트너사와의 협력 가치도 커지고 있습니다. 경험이 풍부한 외부 전문가와 협력하면 검증된 방법론을 활용할 수 있을 뿐만 아니라, 부족한 전문성을 보다 효율적인 비용으로 보완할 수 있습니다. 결국 지속가능한 사이버 보안 조직을 구축하기 위해서는 내부 인력, 자동화 기술, 외부 전문성을 균형 있게 활용하는 것이 중요합니다.

“이제 CISO는 보안을 넘어 비즈니스를 이해해야 합니다. 사이버 보안의 중요성을 경영 관점에서 설명하고, 경영진과 원활하게 소통하며, 보안 전략을 사업 목표와 일치시킬 수 있어야 합니다. 그러나 이러한 역량은 기술 지식만으로 충분하지 않습니다. 많은 기업이 필요로 하는 이런 인재를 경험, 리더십, 소통 능력을 모두 갖추어야 하지만 쉽게 찾기 어려운 것이 현실입니다.”



안 마토

디지털 신뢰 분야 수석 자문 위원, 전 파트너
네덜란드의 포비스 마자르

글로벌 사이버 보안 현황

사이버 보안 성과 측정

기업들은 이제 사이버 보안의 성과를 더 이상 단순한 기술적 지표로만 평가하지 않습니다. 보안 투자로 인해 예방된 위험, 장애 대비 수준, 강력한 보안 능력이 새로운 비즈니스 기회를 어떻게 창출하는지를 중요하게 보고 있습니다. 이러한 변화는 보안 예산을 확보하는데도 중요한 의미가 있으며, 경영진은 단순한 보안 활동 자체보다 비즈니스 성과에 미치는 영향을 알고 싶어합니다. 따라서 사이버 보안 조직은 투자 효과를 측정하고 설명할 수 있어야 하며, 이를 통해 ROI를 보다 명확하게 입증할 필요가 있습니다.

비용이 아닌 투자로 바라보는 사이버 보안

사이버 위협이 증가하고 기술 환경이 복잡해지면서 보안 관련 비용도 계속 증가하고 있습니다. 이로 인해 사이버 보안은 종종 비용만 발생시키는 분야로 인식되기도 합니다. 그러나 선도적인 기업들은 사이버 보안을 비용이 아닌 전략적 투자로 바라보고 있습니다.

많은 기업이 탄탄한 보안 역량이 경쟁 우위로 이어질 수 있다는 사실을 체감하고 있습니다. 특히 B2B 시장에서는 고객들이 공급업체를 선택할 때 보안 수준을 중시하며, 뛰어난 보안 체계가 차별화 요인으로 부상하고 있습니다. 규제가 강화되면서 공급망 전반에 대한 책임도 커진 만큼, 기업들은 협력업체의 보안 역량을 이전보다 훨씬 중요한 평가 요소로 보고 있습니다. 하지만 이러한 흐름이 단순히 규제 때문인 것은 아닙니다. 최근에는 연이어 발생한 대형 사이버 사고로 인해 서비스 중단이나 데이터 유출이 기업에 미치는 영향을 시장이 민감하게

받아들이고 있습니다. 그 결과, 고객들은 공급업체 선정 과정에서 보안 요구사항을 더욱 강화하고 있습니다. 결국 사이버 보안 조직의 역할은 단순히 보안 통제를 운영하는 데 그치지 않습니다. 강력한 보안 역량이 수주 기회 확대, 고객 신뢰 확보, 비즈니스 지속성 강화에 어떤 가치를 제공하는지 구체적으로 설명할 수 있어야 합니다. 이러한 가치를 정량적으로 보여주고 효과적으로 전달하는 조직은 경영진과 실무 부서의 공감과 지원을 보다 쉽게 받을 수 있습니다.

“사이버 보안을 필수 비용으로만 여겨온 시대는 저물고 있습니다. 이제 사이버 보안은 기업의 경쟁력을 좌우하는 전략적 차별화 요소가 되고 있습니다.”



제프리 더 브라윈
이사
네덜란드의 포비스 마자르

사이버 보안은 고객만 중요하게 보는 요소가 아닙니다. 보험사들은 기업의 보안 수준을 주요 평가 항목으로 삼고 있으며, 금융기관 역시 기업의 사이버 보안 대응 역량을 리스크 평가에 적극 반영하고 있습니다. 그 결과 탄탄한 보안 체계를 갖춘 기업은 보험 가입과 자금 조달 측면에서 실질적인 이점을 얻을 수 있습니다. 사이버 보안 투자가 비용이 아닌 경영적 가치로 이어질 수 있다는 점을 보여주는 대표적인 사례라고 할 수 있습니다.

글로벌 사이버 보안 현황

사이버 보안 가치 측정



중요한 것을 측정하라

선도적인 기업들은 더 이상 취약점 수나 탐지 건수와 같은 전통적인 보안 지표에만 의존하지 않습니다. 대신, 그들은 사이버 보안이 비즈니스 성과와 이해관계자의 신뢰에 미치는 영향을 평가하는 데 집중하고 있습니다.

주요 측정 항목은 다음과 같습니다.

- **복구 목표 시간:** 보안 사고 발생 후, 업무를 정상적으로 운영할 수 있는 복구 속도
- **비즈니스 영향 지표:** 보안 사고가 매출, 고객 관계, 시장 경쟁력에 미친 실제 영향 평가
- **이해관계자 신뢰 지표:** 보안 역량이 고객, 투자자, 파트너사와의 신뢰 형성에 얼마나 기여하는지
- **혁신 지원 역량:** 보안 체계가 새로운 사업과 혁신을 얼마나 효과적으로 뒷받침하는지



사이버 보안 ROI 극대화

사전 예방적 보안 체계에 투자하는 기업은 사고가 발생한 후 대응하는 방식에 의존하는 기업보다 더 나은 일관된 성과를 보이고 있습니다. 그러나 조직의 규모가 아무리 커도 자원은 제한적이므로, 투자 효과를 극대화하고 위험을 최소화하기 위해서는 우선순위를 명확히 설정해야 합니다.

- **위험 기반 우선순위 설정:** 모든 자산을 동일하게 보호하기보다 조직에서 가장 중요한 자산에 인력과 예산을 집중해야 합니다.
- **보안 내재화:** 시스템과 업무 프로세스를 설계하는 단계부터 보안을 반영해야 합니다. 구축 후 보안 기능을 추가하는 방식보다 훨씬 효과적이고 경제적입니다.
- **통합적 접근:** 개별 문제에 대해 각각의 솔루션을 도입하기보다는 여러 요구사항을 아우를 수 있는 통합적인 보안 체계를 구축하는 것이 중요합니다.
- **자동화와 운영 효율화:** 단순히 인력을 늘리기보다는 사람의 역량을 확장할 수 있는 도구와 프로세스에 투자해야 합니다. 특히 지속적인 모니터링 체계는 보안 가시성을 확보하는 데 중요한 역할을 합니다.
- **임직원 교육:** 정기적인 교육과 인식 제고 프로그램은 사람의 실수로 인한 사고와 사회공학 공격의 위험을 줄이는 데 도움이 됩니다.
- **사고 대응 역량 강화:** 실제 사고가 발생하기 전에 대응 체계를 구축하고 반복적으로 점검해야 합니다. 위기 상황에서는 계획의 존재보다 준비 수준이 더 중요합니다.
- **공유 서비스 활용:** 필요한 경우 공유 서비스나 가상 CISO를 활용해, 상시 채용이 어려운 전문 분야에서 비용 효율적으로 전문성을 얻을 수 있습니다.

글로벌 사이버 보안 현황

2027년, 기업은 사이버 회복력을 어떻게 강화해야 하는가

2027년 이후 사이버 회복력은 단순히 공격을 방어하는 능력을 의미하지 않습니다. 예기치 못한 장애와 공격을 미리 대비하고, 사고 발생 시에도 핵심 업무를 지속하며, 변화하는 위협 환경에 유연하게 적응할 수 있는 능력이 더욱 중요해질 것입니다.

무엇보다 보안 내재화는 더 이상 선택 사항이 아니라 필수 요건으로 자리매김할 전망입니다. 기업은 고객, 규제기관, 보험사에 보안이 철저히 적용되고 있다는 것을 지속적으로 증명해야 합니다.

AI 활용이 확대될수록 이러한 변화는 더욱 중요한 의미를 띠게 됩니다. AI 시스템은 설계 단계에서의 의사결정이 실제 운영 환경에 적용된 이후에야 보안 문제로 드러날 수 있습니다. 따라서 보안 내재화 원칙을 충분히 적용하지 못한 기업은 보안 성과뿐 아니라 시장 신뢰와 규제 대응 측면에서도 불리한 위치에 놓일 수 있습니다.

빠르게 변화하는 기술 환경에 대응하기 위해서는 거버넌스 역시 달라져야 합니다. 새로운 기술과 위협이 나타날 때마다 별도의 체계를 만드는 대신, 핵심 원칙을 유지하면서도 새로운 환경에 유연하게 적용할 수 있는 거버넌스 구조가 필요합니다. 회복력이 높은 조직은 조직 간 경계를 넘어 일관되게 작동하는 관리 체계를 구축하고, 지속적으로 학습하며, 새로운 위협과 기회를 선제적으로 파악합니다.

기술 환경이 급격하게 변화하는 상황에서는 회복력 있는 기업들이 특정 기술이나 플랫폼에 지나치게

의존하기보다는 변화 자체를 견딜 수 있는 능력을 구축하는 데 집중하고 있습니다. 이를 위해서는 위험 기반 접근법을 지속적으로 적용하고, 가능하다면 특정 도구나 공급업체에 종속되지 않는 아키텍처를 마련하며, 기술보다는 역량 중심의 인재 육성을 위해 투자해야 합니다.

생태계 전반을 고려한 위험 관리

2027년의 사이버 회복력은 기업 내부만 보호한다고 확보되지 않습니다. 공급망 파트너사는 물론 기술 공급업체, 서비스 제공업체, 나아가 공동 인프라를 사용하는 다른 기업들까지 포함한 전체 생태계의 보안을 함께 고려해야 합니다.

생태계 차원의 위험 관리를 위해서는 다음과 같은 요소가 중요합니다.

- **위험 정보 공유:** 여러 조직에 영향을 미칠 수 있는 위협을 조기에 식별하고 대응할 수 있도록 파트너사와 관련 정보를 공유하고 협력해야 합니다.
- **공동 사고 대응 체계 구축:** 사고 발생 시 조직 간 경계를 넘어 협력할 수 있는 대응 체계를 마련해야 합니다.
- **표준화된 위험 평가 체계 활용:** 공통된 프레임워크와 지표, 용어 체계를 활용해 위협을 평가하고 소통해야 합니다. 이를 통해 조직 간 위험 수준을 보다 일관되게 이해할 수 있습니다.
- **집단 방어 역량 강화:** 업계 차원의 협의체나 공동 대응 프로그램에 참여해 위협 정보를 공유하고 공동 방어 체계를 발전시켜야 합니다.

“진정한 회복력은 변화에 얼마나 유연하게 대응할 수 있는지에서 드러납니다. 회복력이 높은 조직은 새로운 기술과 비즈니스 모델을 수용하기 위해 기존 거버넌스 체계를 반복적으로 재설계하지 않습니다. 대신 변화에 맞춰 자연스럽게 확장할 수 있는 거버넌스 구조를 갖추고 있습니다.”



폴 트루트
사이버 보안 부문 책임자, 수석 컨설턴트
미국의 포비스 마자르

보안을 기반으로 한 혁신

2027년 이후 성공하는 기업은 지금부터 대비를 시작한 곳일 것입니다. 이러한 기업들은 갈수록 복잡해지는 위협 환경에 대응하기 위한 역량을 강화하고, 효과적인 파트너십과 유연한 거버넌스 체계를 갖추는 데 집중할 것입니다. 동시에, 신기술이 제공하는 기회를 기민하게 포착하고 활용할 것입니다. 결국 미래의 경쟁력은 변화하는 위협에 효율적으로 대응하는 능력뿐 아니라, 변화 속에서 새롭게 등장하는 기회를 얼마나 신속하게 실행 가능한 결과로 전환시키는지에 의해 결정될 것입니다.

“앞으로의 사이버 보안은 보안과 혁신 사이에서 균형을 선택하는 문제가 아닙니다. 두 목표를 함께 달성하는 것이 핵심입니다. 이를 위해서는 장기적인 관점의 전략 수립과 투자, 그리고 사이버 보안을 조직 전체의 공동 책임으로 바라보는 협력 문화가 뒷받침되어야 합니다.”



얀 마토
디지털 신뢰 수석 자문위원, 전 파트너
네덜란드의 포비스 마자르

앞으로 나아가기 위한 핵심 과제

변화에 유연하게 대응하되, 기본 원칙은 흔들리지 않아야 합니다: 기술은 계속 발전하고 변화하겠지만 사이버 보안의 기본 원칙은 크게 달라지지 않습니다. 기업은 새로운 기술을 빠르게 수용할 수 있는 민첩성을 갖추는 동시에, 일관된 보안 수준을 유지할 수 있는 체계도 함께 마련해야 합니다.

인재와 파트너십에 지속적으로 투자해야 합니다: 2027년 이후의 사이버 보안 과제는 많은 조직이 내부 역량만으로 감당하기 어려운 수준으로 발전할 가능성이 높습니다. 따라서 전문 인력을 지속적으로 육성하는 한편, 부족한 역량을 보완할 수 있는 전략적 파트너십도 적극적으로 활용해야 합니다.

보안과 가치를 비즈니스 관점에서 입증해야 합니다: 보안 프로그램의 성과는 기술 지표만으로 설명하기 어렵습니다. 보안역량이 비즈니스 지속성, 고객 신뢰, 매출 기회, 운영 효율성에 어떤 영향을 미치는지 보여줄 수 있어야 합니다. 이를 위해 보안 담당자 역시 기술 역량뿐 아니라 비즈니스에 대한 이해를 함께 갖춰야 합니다.

조직을 넘어 생태계 관점에서 접근해야 합니다: 어느 기업도 혼자만의 힘으로 완전한 회복력을 확보할 수는 없습니다. 공급망 파트너와 기술 공급업체, 서비스 제공업체 등 전체 생태계가 연결돼 있는 만큼 사이버 보안 역시 공동의 과제로 접근해야 합니다. 효과적인 대응을 위해서는 정보 공유와 협력, 그리고 유기적인 대응 체계가 뒷받침되어야 합니다.



Contacts

심규택

파트너, 감사 및 금융서비스
한국의 포비스 마자르
gyu-taek.sim@forvismazars.com

조지 라가리아스

수석 이코노미스트
포비스 마자르
george.lagarias@mazars.co.uk

와디 므세디

사이버 보안 총괄
포비스 마자르
wadi.mseddi@forvismazars.com

알리술탄 키르기즈바예프

데이터·AI 역량센터 총괄
포비스 마자르
ali-sultan.kirgizbaev@forvismazars.com

안톤 유누소프

사이버 보안 부문 총괄
영국의 포비스 마자르
anton.yunussov@mazars.co.uk

크리스토퍼 호크

이사
독일의 포비스 마자르
christopher.hock@forvismazars.com

야콥 헤슬러

글로벌 컨설팅 총괄
포비스 마자르
jakob.haesler@forvismazars.com

얀 마토

디지털 신뢰 분야 수석 자문위원, 전 파트너
네덜란드의 포비스 마자르
jan.matto@forvismazars.com

제프리 더 브라윈

이사
네덜란드의 포비스 마자르
jeffrey.debruijn@forvismazars.com

폴 트루잇

사이버 보안 부문 책임자, 수석 컨설턴트
미국의 포비스 마자르
paul.truitt@us.forvismazars.com

손 앤드류

매니저, IT 리스크 및 컴플라이언스
미국의 포비스 마자르
sean.andrews@us.forvismazars.com

톰 톨러턴

CMMC 부문 리드, 수석 컨설턴트
미국의 포비스 마자르
tom.tollerton@us.forvismazars.com

Forvis Mazars Group SC는 선도적인 글로벌 전문 서비스 네트워크인 Forvis Mazars Global의 독립 회원사입니다. 감사, 세무 및 자문 서비스를 제공하며, 100개 이상의 국가에서 국제 통합 파트너십으로 운영되고 있습니다. 전 세계 40,000 명 이상의 전문가들이 전문성과 문화적 이해를 바탕으로, 다양한 규모의 기업이 비즈니스 성장의 전 과정을 성공적으로 이끌어갈 수 있도록 지원합니다.

포비스 마자르 새빛회계법인은 Forvis Mazars Group SC의 독립 회원사로서 120명 이상의 전문가들이 회계감사, 세무, 자문, 아웃소싱 서비스를 제공하며, 글로벌 네트워크의 전문 역량을 바탕으로 국내외 기업에게 최적의 솔루션을 제공하고 있습니다.

© 2026년 10월

forvismazars.com/kr

forvis
mazars