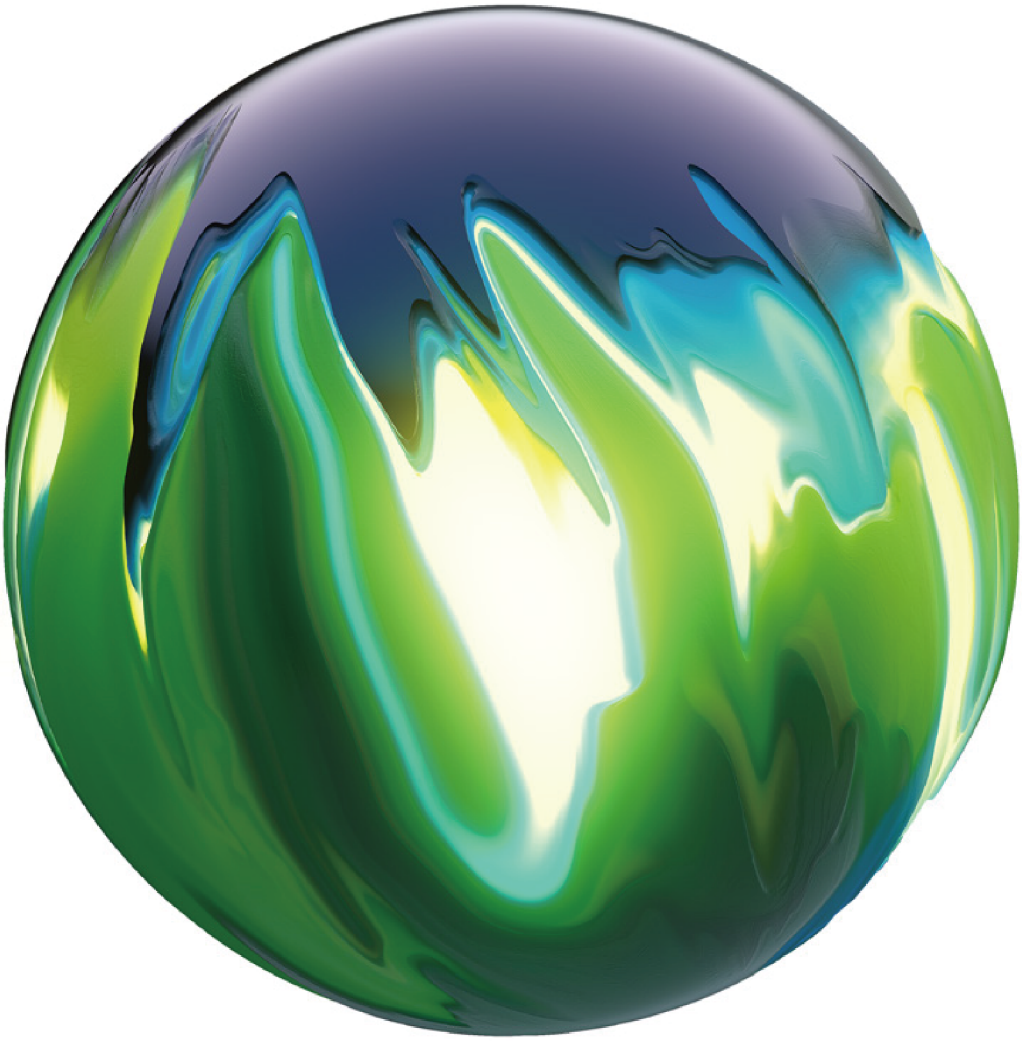
Deloitte.



사이버의 미래 2021 서베이

복잡해지는 사이버 생태계, 시야 확보가 시급하다

Emily Mossburg 외 7인 / 딜로이트 사이버

차례

개요 4
복잡성을 들여다볼 시야를 확보하라

디지털 전환 8
사이버와 전환이라는 과제

고객 경험 12
개인 맞춤인가 침해인가? 개인정보의 윤리적 활용

제로 트러스트 18
경계 없는 환경 확보

신흥 기술 22
신흥 기술 스펙트럼 연결하기

산업 중심적 사이버 26
만병통치약은 없다

결론 30
깨끗한 시야 확보

서베이 방법론

딜로이트는 웨이크필드 리서치(Wakefield Research)와 공동으로 '딜로이트 2021 사이버의 미래 서베이'를 실시했다. 서베이는 2021년 6월 6일부터 8월 24일까지 연 매출 5억 달러 이상인 기업의 고위 임원 약 600명을 대상으로 온라인으로 실시됐다. 서베이 대상자는 최고정보보호책임자(CISO) 약 200명, 최고정보관리책임자(CIO) 100명, 최고경영자(CEO) 100명, 최고재무책임자(CFO) 100명, 최고마케팅책임자(CMO) 100명으로 구성됐다.

복잡성을 들여다볼 시야를 확보하라

오늘날 우리는 사방이 사이버로 둘러싸인 세상에 살고 있다. 특히 원격 근무가 확산하면서 각종 디지털 전환 계획의 실현 속도가 점차 가팔라지고 있다. 기술 혁신과 이러한 혁신이 창조하는 문화는 엄청난 속도로 발생해, 기하급수적으로 급증하는 위험을 이해, 측정, 대응하려는 우리의 능력으로는 도저히 따라잡기가 힘들다.

위험이 급증하는 환경에서도 우리 고객들은 디지털 전환(digital transformation)과 클라우드 전환(migration to the cloud)을 계속 우선순위로 삼고 있다. 단순히 효율성을 개선하는 데 그치지 않고 조직 전반의 데이터 흐름을 통해 새로운 방식으로 가치가 창출되고 각기 다른 사업분야가 연결되고 고객 정보의 활용이 풍부한 고객 경험으로 이어진다. 이번 서베이 결과 또한 이러한 클라우드 전환이 대세임을 시사했다. CFO 응답자의 94%는 재무 시스템 또는 전사적자원관리(ERP)를 클라우드로 이전하는 방안을 검토 중이라고 답했다.

고위 임원

600 명 대상

연 수익

5 억 달러 이상 기업

본사 위치

40% 북남미

28% EMEA

32% 아시아태평양

현재 동향

오늘날 기업들은 경쟁력을 유지하기 위해 온프레미스(on-premise) 인프라에 하이브리드 정보화기술(IT) 및 제3자 클라우드 제공업체의 서비스를 접목시켜 다양한 기술과 서비스를 복합적으로 활용하고 있다. 기업의 사이버 환경이 이처럼 첨단화, 통합화하면서 기존의 인하우스 IT 아키텍처와 전혀 다른 새로운 관리 방식이 필요하게 됐다. 이번 서베이에서 상당히 많은 CIO와 CISO(41%)가 디지털 전환뿐 아니라 점차 복잡해지는 하이브리드 생태계 전반에 대한 시야 확보를 가장 중대한 과제로 꼽았다.

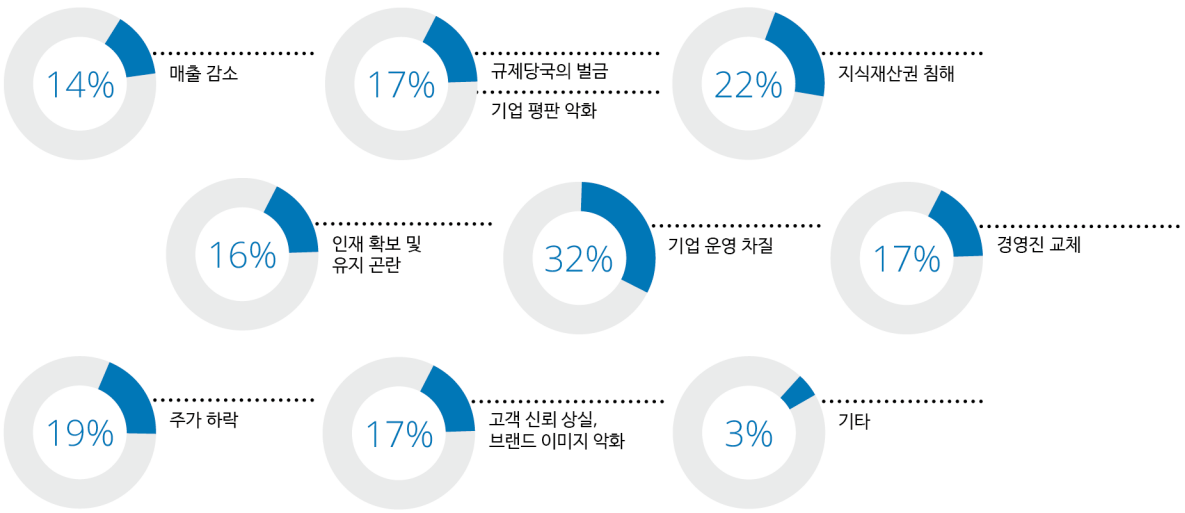
시장 압력은 이전부터 존재했지만, 팬데믹이 원격 근무를 고용의 한 가지 영구적인 특징으로 선포하는 역할을 했다. 크고 작은 기업들이 빠르게 업무 환경을 전환하면서 공격 노출면(attack surface)도 가파르게 확장됐다. 확장 속도가 워낙 빨라 이에 따른 보안 문제를 숙고할 시간이 거의 없을 정도이다. 이에 따라 당연히 사이버 공격도 증가했다. 이번 서베이 응답자의 69%는 2020년 초부터 2021년 5월까지 자사가 경험한 사이버 위협이 '증가했다' 또는 '대폭 증가했다'고 답했다. 이러한 추세는 산업과 지역을 막론하고 일관되게 나타났다. 또 응답자의 32%는 이에 따른 가장 큰 여파로 운영 차질을 꼽았고, 지식재산권(IP) 침해(22%), 주가 하락(19%)이 뒤를 이었다.

신뢰 배제, 상시 인증

서베이 응답자들은 조직 전반의 사이버보안 관리를 가로막는 가장 큰 장벽으로 복잡한 영역을 넘나드는 데이터 관리(44%)와 조직 차원에서 사이버 위험을 더욱 우선시할 필요성(31%)을 꼽았다. 다행히 현재 제로 트러스트(Zero Trust) 아키텍처는 실행 가능하다. 제로 트러스트는 단순한 개체 인증 대신 지속적 위험 파악에 기반한 실시간 접속 결정 방식을 사용하는 것으로, 이를 통해 경계가 급속도로 무너지는 오늘날의 생태계 속에서 효과적으로 대응할 수 있다. 아키텍처의 모든 구성 요소가 취약하고 모든 계층을 보호해야 한다는 전제로 시작하기 때문이다.

최근 연산 능력의 발전으로 제로 트러스트의 존재감과 도입이 확대되면서 각 기업의 문화가 더욱 광범위하게 변화하고 있다. 사이버의 역할과 중요성이 커지고 있는 것이다. 제로 트러스트는 단순히 기술적 해결 방식에 그치지 않고 씨줄과 날줄처럼 교차된 일련의 솔루션을 제공함으로써 적대적 행위 및 이에 따른 사업 위험을 들여다볼 수 있는 시야와 함께 이러한 위험을 줄이기 위해 필요한 변화에 대한 통찰력도 제공한다. 결론은 IT 부서와 비즈니스 부서 간 협력뿐 아니라 전사적 교육과 훈련이 필요하다는 것이다.

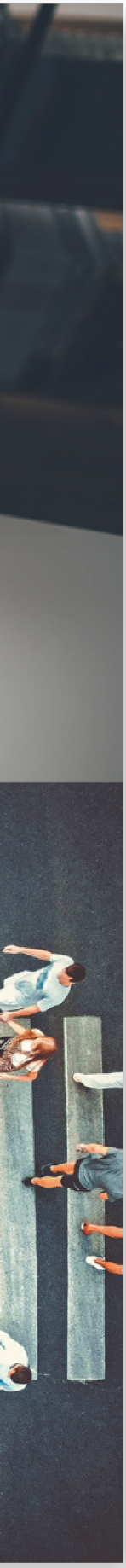
그림1
사이버 침해사건에 따른 가장 큰 여파*



*최대 두 개 복수 응답 허용, 백분율 총합이 100% 초과

"지금은 급격한 진화가 발생하는 과도기다. 현재 기업들이 마주한 최대 과제는 하이브리드 IT와 디지털 전환이다. 이로 인해 환경이 한층 다각화되고 복잡해진다. 더욱 분명한 시야 확보, 특히 클라우드 도입과 관련한 시야 확보가 기업들의 최우선사안으로 떠오르고 있다."

-Emily Mossburg,
딜로이트 글로벌 사이버 리더



사이버 방어 재정비

해커들의 수법이 갈수록 교묘해지고 의약품 특허, 엔지니어링 및 제품 특허, 고객 정보를 비롯한 중요 데이터 등 자산의 시장 가치에 대한 이들의 이해도 높아지면서, 기업들은 사이버 방어 예산을 지속적으로 확대하고 있다. 이번 서베이에서 자사 연 매출액이 300억 달러 이상인 응답자의 약 75%가 2021년 사이버보안 지출액이 1억 달러를 넘을 것으로 예상했다.

남은 과제는 이러한 투자를 통해 점차 복잡해지는 생태계에서 증폭되는 위험에 대해 보다 분명한 시야를 확보하는 것이다. 이를 위해 기술과 전문성을 확보하는 데 그치지 않고 조직 전체의 변화를 추진해 조직 내부뿐 아니라 파트너사와 제3자 공급업체까지 포함하는 프로그램화된 지배구조를 촉진해야 한다.

기술 변화와 맞물려 CISO의 역할도 변하고 있다. 사이버가 기업 조직 곳곳에 스며들면 조직도에서 CISO의 위치를 반드시 수정해야 한다. 보고 체계를 간소화할 뿐 아니라 CEO와 더욱 긴밀히 협력할 수 있는 위치를 부여해 CISO가 사업 우선순위를 더욱 잘 이해하고 현재 발생하는 혁신을 제대로 파악할 수 있도록 해야 한다. CISO가 이처럼 새로운 운영자 역할을 맡음으로써 조직 전반에 더욱 많이 개입하게 되면, 사이버팀은 필요한 요구 사항과 기술 솔루션, 통제 시스템을 처음부터 혁신 계획에 포함시킬 수 있다. 이를 통해 계획 착수 단계에서 발생하는 위험뿐 아니라 제품과 서비스 개발 전 단계의 위험을 최소화할 수 있다.

이처럼 사이버가 기업 문화에 미치는 영향이 더욱 심오해지는 점을 반영해 2021년 서베이는 사이버를 직접 감독하는 리더뿐 아니라 CEO, CFO, CMO, CIO, CISO 등 사이버의 역할 확대로 가장 큰 혜택을 누릴 수 있는 리더들까지 포함해 대상 범위를 확대했다. 비록 지역별, 산업별 차이는 있으나 이들 리더들은 비슷한 정서를 표출했다.

미래를 내다보는 눈

단순한 조직적 혹은 기술적 솔루션만으로는 현대 비즈니스를 떠받치는 통합 생태계의 점차 복잡해지는 양상을 제대로 파악할 수 없다. 하지만 조직, 문화, 운영 방식을 모두 통합하면 사업 계획의 핵심 부문, 기업 문화, 지속적으로 진화하는 기술 생태계에 사이버를 내재화할 수 있다.

본고에서는 이러한 방식을 탐구함과 동시에, 현재 생태계의 복잡성이 창출하는 위험을 파악하는 조직의 능력과 더불어 차세대 기술 진화로 인해 상호연결성이 지속적으로 심화하는 환경에서 미래를 내다보는 조직 능력의 중요성을 강조하고자 한다.

사이버와 전환이라는 과제

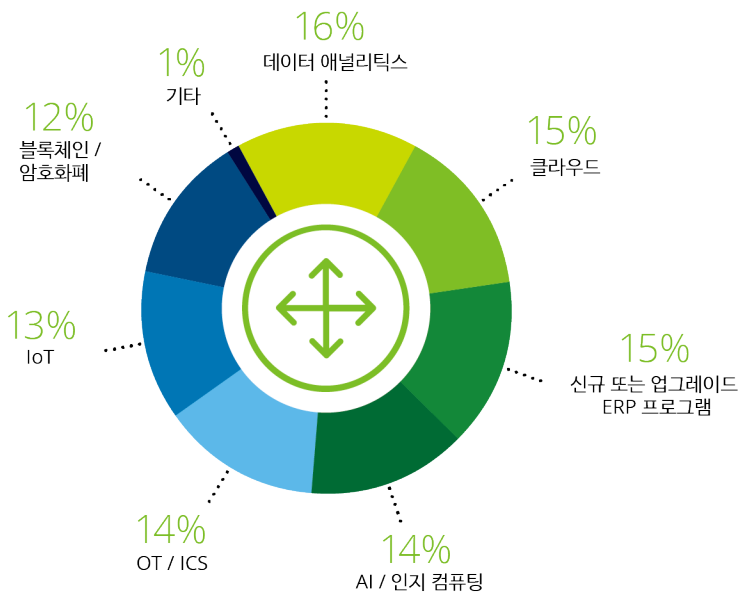
산업군을 막론하고 경쟁력을 유지하려면 새로운 서비스와 제품을 신속히 개발, 출시해야 한다.

혁신 사업 모델은 기존의 프로세스를 단순히 디지털화하는 데 그치지 않고 공급망을 아우르며 참신한 고객 경험을 창출한다. 다만 이러한 전환으로 인해 기업은 새로운 형태의 사이버 위험에 노출되기 때문에, 진화하는 사업 모델을 보호하기 위해 새로운 사이버 전략이 필요하다. 이러한 위험을 관리하기 위해 고위 임원과 이사회 위원들은 변화를 수용하고, 사업 분야를 통틀어 효과적 지배구조를 창출하고, 리스크 관리 프로세스를 발전시켜 제3자의 사업까지 포함해 새롭게 연결된 사업 영역을 철저히 파악할 수 있는 시야를 확보해야 한다. 이를 성공적으로 수행하기 위해 고위 경영진의 의지가 반드시 필요하고, 보안에 대한 효과적 투자를 단행한 후 경영진이 사이버 위험을 제대로 이해해야 한다.

향후 12개월간 디지털 전환 계획의 순위를 묻는 질문에 서베이 응답자들은 데이터 애널리틱스(16%)를 1위로 꼽았고, 클라우드(15%)와 신규 또는 업그레이드 ERP 프로그램(15%) 등을 우선순위로 꼽았다. 또 올해 해당 질문의 항목에 운영기술(OT)·산업제어시스템(ICS)이 포함됐고 14%의 응답자들이 이를 최우선순위로 지목한 것은 범 산업적으로 공장 및 운영 기술 환경의 디지털화와 현대화가 진행 중임을 시사했다.

변화의 속도와 규모는 가히 혁명적이다. COVID-19 팬데믹으로 전 세계가 온라인으로 달려가자, 이러한 변화는 즉각 뚜렷이 모습을 드러냈다. 상당한 인력이 갑자기 원격 근무로 전환하면서 전체 사업 부문은 거의 즉각적으로 전환됐다. 다행히 클라우드와 섀도 IT(shadow IT)부터 ICS까지 이러한 전환에 필요한 디지털 생태계는 대부분 구축된 상태여서 빠른 규모 확대가 가능했다. 하지만 이러한 전환 뒤에 도사린 수많은 사이버 위험은 쉽게 눈에 띄지 않았으며, 현재 적절한 수준으로 이러한 위험을 이해하고 완화할 수단을 가진 기업도 거의 없는 실정이다.

그림2
기업들의 디지털 전환 계획 우선순위



고위 임원과 이사회는 디지털 전환으로 자사가 노출될 실제 위험을 파악하고 다른 종류의 위험과 동등한 노력을 기울여 해당 사이버 위험을 관리할 지렛대를 확보하는 것을 주요 목표로 삼아야 한다.

-Matthew Holt,
글로벌 사이버 전략 &
전환 리더, 딜로이트 사이버

사이버 위험의 이해

오늘날 사이버 위협은 사업 전체에 영향을 미치며 운영에 차질을 빚고 힘들게 쌓아 올린 기업 명성을 한 순간에 무너뜨리기 때문에, 이사회가 사이버 위험을 파악하는 것이 매우 중요하며 이들의 이해를 돕기 위해 쉬운 용어를 사용할 필요가 있다. 이사회가 이미 익숙한 위험과 사이버 위협을 비교할 줄 알아야 하기 때문이다. 사이버 위험 프로파일 분석은 재무 건전성을 파악하는 것과 유사한 방식이 될 필요가 있다.

이사회가 해당 기업이 노출된 사이버 위험의 성격과 규모를 파악하기만 한다면 해로운 위험을 최소화하기 위해 어디에 투자해야 할지 알 수 있다.

이번 서베이 응답자 41%는 사이버 성숙도 평가를 기준으로 사이버 투자 결정을 내릴 수 있다고 답했고, 35%는 리스크 정량화 툴을 도입했다고 답했으며, 23%는 자사의 사이버 리더십 경험에 의존한다고 답했다. 새로운 또는 기존의 애플리케이션에 대해 얼마나 자주 위험 분석 및 위협 모델링을 실시하느냐는 질문에 CIO와 CISO 응답자 37%는 분기별, 29%는 월별로 실시한다고 각각 답했다. 이러한 평가를 실시할 책임은 대체로 CIO와 CISO에게 있지만, 더욱 넓은 범위의 이해관계자들이 그러한 노력의 의미와 중요성을 이해하는 것이 중요하다.

전력질주?

기업 경영진이 규모의 경쟁에만 사활을 걸다 보면 사이버 위험을 제대로 이해하지 못한 채 결과에만 주력하는 디지털 전환 노력을 펼치기가 십상이다. 시장 확보 경쟁에만 열을 올리면 시야가 좁아져 중요한 사각지대를 놓치게 된다.

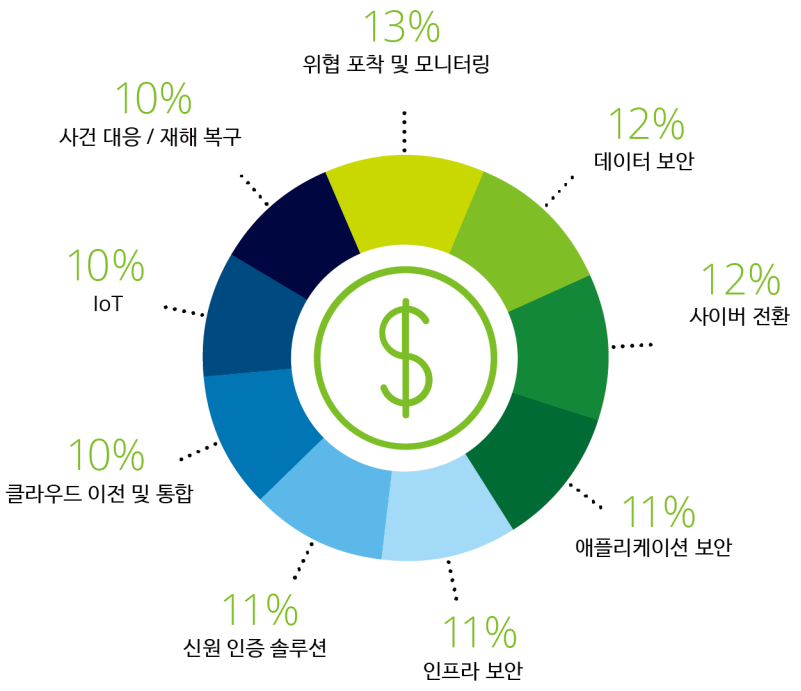
고객 접점부터 지능형 공장, 원격 근무 직원들의 기기까지 사이버가 모든 곳에 스며들어 있는 지금, 바이러스 퇴치 소프트웨어와 패스워드를 관리하는 IT 부서의 비밀주의 시대는 끝났다. 네트워크 운영을 지속하는 것만으로는 더 이상 충분하지 않으며, 더욱 광범위하고 심도 깊은 사고가 필요하다.

오늘날 CISO에게는 모든 사업 부문에 영향을 미치고, 조직 전체로부터 정보를 수집하고, 고위 경영진 및 이사회와 직접 소통할 수 있는 권한이 필요하다. 전략적으로 가장 중요한 조직의 우선순위와 자산을 적절히 보호하기 위한 자원과 인력 투자가 필요한 것은 두말할 것도 없다.

대부분의 CFO는 이러한 투자의 타당성에 동의하지 않을 것이다. 대규모 사이버 투자의 성과는 대개 '제로'이기 때문이다. 사이버 투자의 최대 성과는 사이버 사건이 단 한 건도 일어나지 않는 것이다. 그렇다면 CISO가 사이버 예산을 어떻게 정립해야 하는가? 지난 2019년 서베이에서 CISO와 CIO 응답자들은 사이버 예산이 다양한 사이버 프로그램에 골고루 할당됐다고 답했다. 2021년 서베이에서도 이러한 추세는 변하지 않아, 비슷한 응답이 나왔다. 고위 임원들은 사이버 위험 관리를 위한 만병통치약은 없음을 알아야 한다.

따라서 위협 분석 정보, 포착 및 모니터링, 사이버 전환과 더불어 데이터 보안에 대한 관심이 증가할 수록 사이버 예산도 확대된다. 전 세계 CISO와 CIO는 자사의 사이버 방어를 구축하기 위해 ▲클라우드 내 또는 클라우드를 위한 사이버 솔루션 규모 확대 ▲사이버 및 기술 회복력 ▲인공지능(AI) 주도 위협 평가 및 파악에 지속적으로 투자하고 있다.

그림3
기업 사이버 예산은
전반적인 위험 완화를 위해
고르게 분배된다



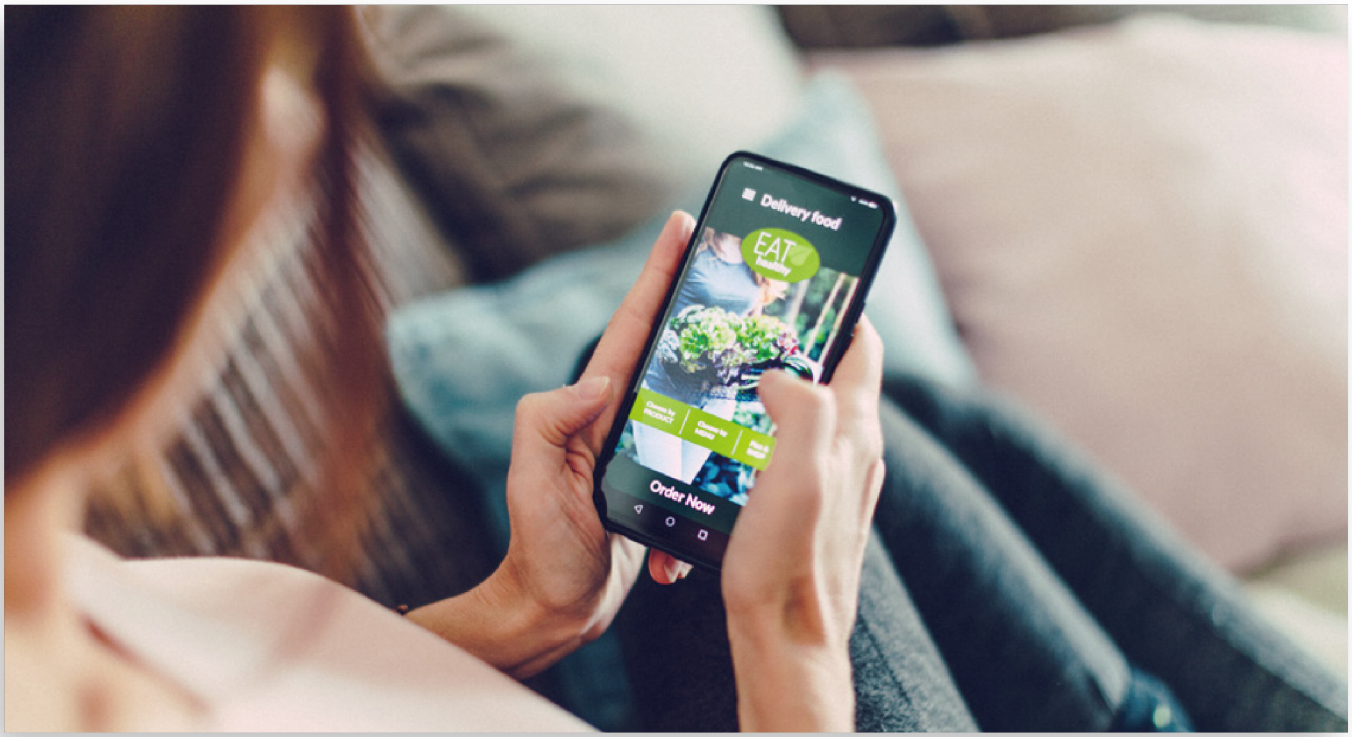
올바른 사이버팀 만들기

이사회나 고위 임원에게 사이버 보안 전문가가 되라고 주문하기는 현실적으로 어렵다. 하지만 이사회는 사이버팀을 구성해 이들을 통해 생태계 시야를 확보하고 이들로부터 이해할 수 있는 용어로 적절한 정보를 얻을 수 있다. 핵심 인력 채용은 이사회 또는 고위 경영진 수준에서 결정돼야 한다.

개인 맞춤인가 침해인가? 개인정보의 윤리적 활용

사람들은 개인화된 맞춤형 경험을 기대한다. 음식 배달부터 여행, 헬스케어까지 과거 자신의 사용 이력에 기반한 매끄러운 경험을 원한다. 하지만 가는 곳마다 따라다니며 관심도 없는 제품이나 서비스의 쿠폰을 끊임없이 뿌려 대는 마케터는 원치 않는다.

개인정보를 보호하면서 고객 데이터를 어떻게 관리하고 온라인과 대면 경험을 어떻게 연결하는지에 따라 기업의 수익과 손실, 심지어 장기적 생존 여부까지 결정된다.



설계부터 개인정보보호를 고려하라

고객을 상대하는 모든 프로젝트는 처음부터 개인정보보호와 보안을 반드시 염두에 두어야 한다. 우선 고객과 이 정도의 친밀한 관계를 맺는 것이 사업 모델에 얼마나 중요한가를 자문해 보라. 적절한 수준의 서비스를 제공하기 위해 필요한 정보의 종류를 신중하게 파악하라. 그리고 이러한 정보에 접근할 필요가 있는 관리자와 데이터 저장 및 보호 방식을 파악하라. 이번 서베이에서 CMO 응답자 중 대다수(85%)가 글로벌 데이터 보안 규제 준수를 측정 및 입증할 수 있다고 답했다.

방만한 데이터 수집을 경계하라

나중에 유용할 것이라는 기대만으로 데이터를 방만하게 수집하면 자원을 낭비하게 돼 결국 실패할 가능성이 높다. 고객들은 분명한 혜택을 얻을 수 없다면 개인정보를 내놓으려 하지 않는다. 진정한 맞춤형 인간적 경험을 창출하기 위해 데이터를 수집하고 효과적으로 활용해야 성장을 촉진시킬 수 있다. 또 역으로 보자면 더 많은 데이터를 가질수록 마주하게 되는 위험도 늘어난다. 결국 균형을 잘 맞추는 것이 가장 바람직하다. 이번 서베이에서 CMO 응답자들 사이 고객 경험을 맞춤화하기 위해 데이터를 수집해야 한다는 의견과 개인정보 유출을 막기 위해 데이터를 수집하지 말아야 한다는 의견이 정확히 반으로 갈렸다.

그림4
글로벌 데이터 보안 규제 준수를 측정 및 입증할 수 있는가?

가치와 신뢰

오늘날 사람들은 개인정보가 지닌 고유한 가치를 인지하고 있다. 개인정보를 넘겨주는 것을 일종의 투자로 보고 이에 따른 보상을 원하는 것이다. 개인정보를 제공하면 삶이 더 편해져야 한다. 그리고 가치 있는 모든 것이 그러하듯 개인정보 또한 안전하게 보호돼야 한다. 또한 사람들은 개인정보가 언제 어떻게 사용되는지 선택할 수 있도록 대리 시스템을 요구하고 있다. 기업들이 이와 관련한 약속을 충실히 이행하면 고객과의 관계는 한층 심화된다.

귀사에 대한 고객의 신뢰도는 이들의 행동에서 나타난다. 고객 신뢰도와 비즈니스 빈도수는 밀접한 연관성이 있다. 고객은 신뢰할 수 있다고 판단하는 기업의 경우 제품 및 서비스를 재구매할 확률이 540%나 상승한다. 이와 비슷한 고객의 행동은 소셜미디어에서도 나타난다. 결과적으로 신뢰받는 기업은 경쟁사를 월등히 앞선다. 예를 들어, 신뢰받는 기업은 지난 1년간 두 배 강한 회복탄력성을 보였다.*

이번 서베이에서 CMO 응답자 91%는 자사가 데이터 수집과 신뢰 창출 간 균형을 '매우' 또는 '어느정도' 맞추고 있다고 답했다. 하지만 고위 임원들도 CMO들의 이처럼 높은 자신감을 공유하고 있을까? 사각지대를 간과하지 않도록 협력에 기반한 접근법이 분명 필요한 대목이다.

규제보다 윤리가 우선

기업의 지속가능한 환경 정책과 적극적 사회 문제 해결 노력에 지지를 보내기 위해 소비자들이 구매자로서의 영향력을 행사하는 추세가 확산되고 있다. 소비자들은 기업이 개인정보를 사용하는 방식에도 이러한 영향력을 행사하고 있다.

과거 기업들은 의무와 금지 사항에 대해 규제당국의 규정과 지침만을 따랐다. 세계 각국의 다양한 법규를 준수하는 것은 여전히 중요하다. 하지만 귀사가 개인정보의 활용 목적을 제대로 설명하지 않는다면 소비자들이 개인정보를 기꺼이 공유할 것이라 더 이상 기대할 수 없을 것이다. 게다가 이에 대한 설명은 평이한 용어로 소비자들이 이해하기 쉽게 제시돼야 한다.

세계 어느 곳에 위치하건 신뢰를 DNA에 내재하고 고객의 개인정보 권리를 지키겠다는 의지를 분명히 제시하는 기업은 고객의 신뢰 강화라는 성과를 거둘 수 있다. 사용자 동의서를 단순하고 이해하기 쉽게 작성해 고객들이 개인정보를 손쉽게 열람, 삭제, 이동할 수 있도록 해야 한다. 귀사가 신중하고 사려 깊은 개인정보보호 정책을 수립하고 앞으로의 방향을 분명히 제시한다면 고객들은 기꺼이 개인정보를 내줄 것이다.

*딜로이트 HX TrustID 연구, 2020년 10월~2021년 6월

그림5
귀사의 마케팅 부서는 데이터 수집과 신뢰 창출 간 균형을 얼마나 잘 맞추고 있는가?

신뢰를 등불로 삼아라

귀사가 창출하려는 고객 경험의 개요를 수립하고
이를 위해 필요한 데이터와 필요하지 않은 데이터를 파악하라.
모든 조직 구성원이 신뢰 창출의 책임을 지도록 하라.

01
설계 단계부터 개인정보보호를 고려하라

02
수집한 정보를 활용하라. 필요하지 않은 데이터는 수집하지 말라.

03
사일로를 해체해 정보를 접근 가능하게 만들어, 조직 전체에서 자유로운 정보의 흐름을 창출하라.

04
신뢰를 낳는 매끄러운 경험을 창출하라.

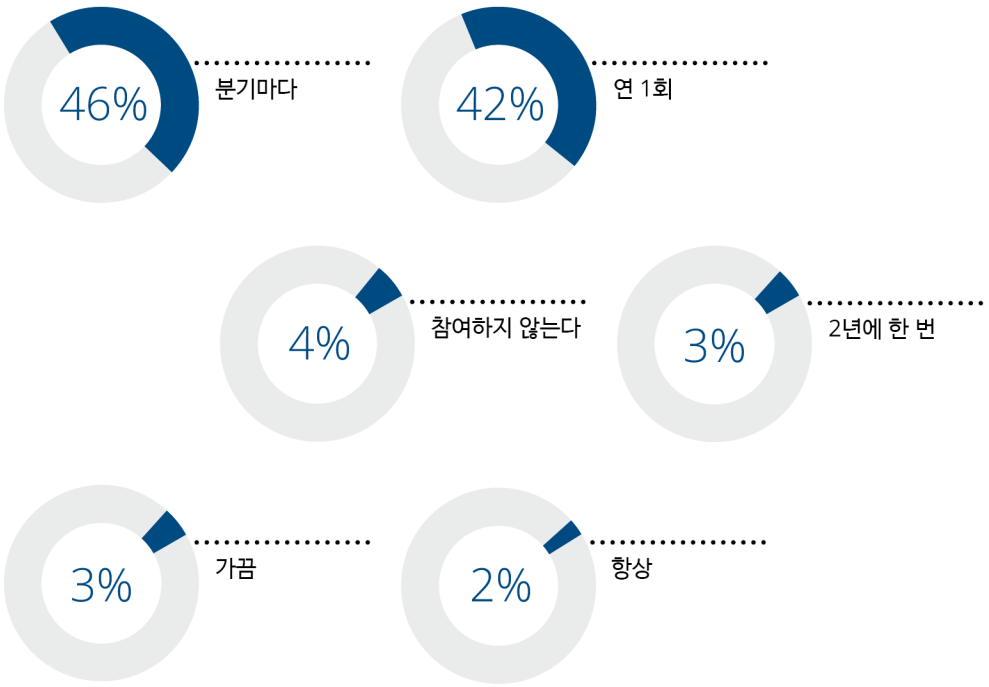
05
정보 유출이 발생한다면, 실수를 만회하고 더 강한 신뢰를 창출할 기회로 전환하라.

06
커뮤니케이션 부서가 모든 부문에 필수적으로 관여하도록 하라.

사일로를 해체하라

CMO와 고객 경험 책임자들은 브랜드와 마케팅 요구에 기반해 결정을 내리고 실행 직전 단계에서야 데이터가 올바른 방식으로 수집됐는지 CISO의 검토를 받는다. (그리고 대부분의 경우 CISO의 대답은 '올바르지 않다'이다.) 모든 구성원이 각기 다른 팀에 속해 있다. 한 팀은 가능한 한 많은 데이터를 수집하는 것이 목표인 반면 다른 팀은 필요한 정보만 수집해 이를 보호하는 것이 임무이다. 접근법을 개선하려면 이들이 모두 한 자리에 모여 매끄러운 고객 경험을 제공하기 위해 필요한 정보를 수집하는 것과 자사와 고객 모두의 위험을 완화할 필요성 사이 적절한 균형을 찾아야 한다. 각기 다른 고객 경험의 점을 선으로 연결하기 위해 데이터를 활용하기에 앞서, 기업은 사일로(silo, 부서 비밀주의)를 벗어나 연결점을 찾을 수 있는 사람들이 필요하다. 이는 양방향으로 추진돼야 한다. 개인정보보호 정책과 커뮤니케이션이 점차 브랜드 의도와 메시지의 핵심 요인이 되고 있는 만큼, 이를 설계할 때 마케팅 부서와 협업하면 도움이 될 수 있다.

그림6
귀사의 '사이버 침해사건 대응' 계획 및 시험에 얼마나 자주 참여하는가?



데이터 유출에 적극 대응하라

아무리 조심해도 데이터 유출은 발생하기 마련이다. 데이터 유출은 만일의 사태로 상정하고 항상 대비해야 한다. 아무 준비 없이 사건이 발생하면 상황을 더욱 악화시킬 수 있다. 귀사의 대응 방식은 귀사가 어떠한 브랜드인지 명확히 보여준다. 데이터 유출 시나리오를 시험하는 사이버팀과 함께 사고 대응 계획을 리허설해보고 협업을 통해 회복 계획과 관련 커뮤니케이션 전략을 수립해야 한다.

이번 서베이에서 CMO 응답자 46%는 분기에 한 번씩 사이버 사건 대응 계획과 시험에 참여한다고 답해, 사이버 부서와 충분히 협력하기 위한 조치가 취해졌음을 시사했다. 다만 지역별로 차이는 있었다. 아르헨티나, 독일, 호주의 CMO 응답자들이 다른 국가에 비해 사이버팀과 더욱 높은 수준의 통합을 이룬 것으로 나타났다.

데이터 유출이 발생하면 고객에게 상황을 정확히 전달할 수 있도록 충분한 정보를 필수적으로 제공해야 한다. 이에 대응하기 위해 고객에게 제공할 서비스를 분명히 제시하고, CEO가 직접 보내는 서한, 선물, 여타 보상 등 귀사의 메시지를 가장 잘 전달할 수 있는 커뮤니케이션 채널을 파악하라.

상황이 심각하기는 하지만 고객과 제대로 소통하면 오히려 고객과의 관계를 강화할 수 있는 전화위복이 될 수 있다. 고객의 이익을 우선하며 어려운 상황을 잘 이겨내면 귀사의 명성은 빠르게 회복돼 더욱 큰 신뢰를 얻게 될 것이다.

> "고객과 기업은 개인정보보호, 보안, 신원 인증에 대한 입장이 서로 다르다. 고객은 다음의 사안을 알고 싶어한다. 이 기업이 나에게 최상의 이익을 주려 하는가? 나의 정보를 나에게 이익이 되도록 사용하는가, 아니면 기업에 이익이 되도록 사용하는가? 개인정보를 안전하게 보호하기 위해 최선을 다하고 있는가?"
>
> -Annika Sponselee,
> 글로벌 데이터 &
> 개인정보보호 리더, 딜로이트 사이버

경계 없는 환경 확보

기존의 레거시 환경에서 IT 자원은 명확히 규정된 경계 안에 갇혀 있었다. 외부에 존재한다면 어떤 것도 신뢰할 수 없지만, 내부에 존재하든 것은 모두 어떠한 의심도 없이 태생적 신뢰를 얻는 구조다. 하지만 지금 우리는 모든 것이 서로 연결되는 초(超)연결 세상에 살고 있다. 오늘날 대부분의 기업은 경계가 무너진 상태다.

이번 서베이 응답자 72%는 지난 한 해에만 자사가 1~10건의 사이버 침해 사건 및 유출 사태를 겪었다고 답했다. 기업의 보안을 위해 더 이상 아무것도 믿지 못하는 상황이 됐다. 오늘날의 과제는 '태생적 신뢰를 완전히 제거하는 방법을 알아내는 것'이다. 이는 현대 보안 아키텍처를 구축하는 방식에 혁명적 변화라 할 수 있다. 다행히도 제로 트러스트가 이 임무를 수행할 역량을 갖추고 있다.

제로 트러스트를 도입하는 이유

01 급격한 디지털화로 IT의 복잡성이 심화되고 비용이 증가하고 있다.

02 원격 근무가 확산하면서 장소와 기기의 제한을 받지 않는 업무 환경을 요구하는 수요가 창출되고 있다.

03 디지털 제품과 서비스 발전으로 인해 클라우드 도입으로 방향이 전환하고 있다.

04 사업 협력과 공급망 통합이 더욱 개선되고 용이해져야 한다는 요구가 나오고 있다.

05 현재의 사이버 방어 능력으로는 극도로 교묘한 사이버 공격을 막기에는 역부족이다.

제로 트러스트 개시

제로 트러스트는 단 하나의 기술 또는 솔루션이 아니며, '신뢰를 배제하고 상시 인증한다'(Never trust. Always verify)는 기본 원칙을 따르는 아키텍처 정책의 묶음이다. 제로 트러스트는 전통적 경계 기반 또는 성벽과 해자(castle and moat, 기업의 중요한 자산이 하드웨어 방식으로 고정되고 경직된 보안 체계 안에서 보호되는 것을 의미) 보안 관리 방식을 버리고 필요 시 개별 자원과 소비자 간 신뢰가 구축되는 방식으로 전환하는 개념이다. 끊임없이 재인증되는 내외부 요인에 기반해 신뢰 연결 구조가 수립된다.

실시간 접근 제어

마침내 우리는 실시간으로 위험에 기반한 역동적 접근 제어 결정을 전달할 수 있는 연산 능력과 기술을 갖추게 됐다.

이제 더 이상 '접근 허용' 또는 '접근 금지'의 이분법이 아니다.
모든 연결 요청은 집합적 전후 관계 요인을 반영해 인증돼 위험 기반 접근 결정을 도출한다.

- 소스 연결 요청의 출처가 인증 또는 권한을 받은 사용자인가?
- 출처나 정체가 확인된 안전한 기기인가?
- 요청하는 사용자가 거의 항시 이 지역에서 연결하는가?
- 연결 시간이 사용자의 히스토리와 일치하는가?
- 접근을 허용하기에 앞서 고려해야 할 다른 신호나 위협 정보가 있는가?

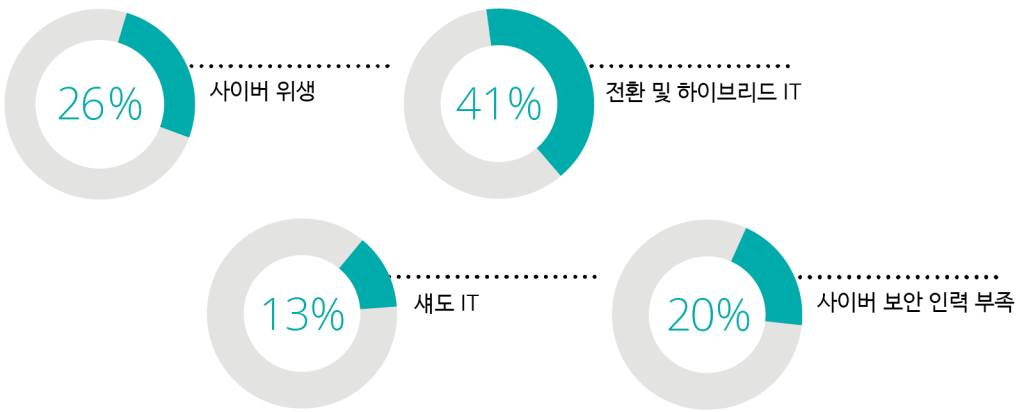
"제로 트러스트 개념을 도입하려면 대대적인 '제거와 대체'가 필요할 것이라는 우려는 오해다. 한 걸음 물러서서 목표한 상태를 달성하기 위해 반복적이고 점증적 단계를 전략적으로 고찰하는 것이 중요하다."

-Andrew Rafla,
미국 제로 트러스트 리더, 딜로이트 사이버

현재 상황

이번 서베이는 조직 전체의 사이버 위험을 관리하기 위해 CIO와 CISO가 짊어져야 할 과제를 제시한다. 가장 큰 과제로는 전환과 하이브리드 IT가 꼽혔으며, 사이버 위생, 인력 부족, 섀도 IT 등이 근소한 차이로 뒤를 이었다. 이러한 과제는 디지털 전환이 가속화됨에 따라 더욱 복잡해진다. 처음부터 다시 시작해, 디지털 전환의 가속화를 뒷받침할 보안 아키텍처를 구축해야 한다. 지금 당장 행동에 나서라!

그림 7
조직 인프라 전반의 사이버보안 관리를 위해 가장 힘겨운 과제는 무엇인가?



한 걸음씩 차근차근

대부분 기업은 알게 모르게 제로 트러스트 경로를 밟고 있다. 전술, 전략, 아키텍처 등 어떤 요인이 주도하느냐에 따라 접근법에 차이가 있을 뿐이다. 제로 트러스트는 모든 산업과 섹터에 중요한 의미를 지니지만, 만병통치약은 없다. 제로 트러스트는 수년에 걸친 투자가 필요한 계획이며, 부서와 IT, 다양한 사이버 영역 간 사일로를 무너뜨리는 완전한 탈바꿈이다. 제로 트러스트 여정에서는 누구도 위험과 장애물을 피할 수 없으며, 이를 이겨내고 성공을 손에 쥐기 위해서는 강력한 리더십 지원과 투자, 조직 전체의 협조가 필요하다.

우선 귀사와 관련이 있는 비즈니스 원동력, 기존 역량, 실제 사례를 파악할 필요가 있다. 사이버의 기본 또한 잊지 말아야 한다. 무엇을 지키고자 하는가? 이러한 자산은 어디에 존재하는가? 누가(신원), 그리고 무엇이(기기) 이러한 자산에 접근할 수 있어야 하는가? 접근한다면 어떠한 조건이 있어야 하는가? 이러한 질문에 답하기 위해 조직은 IT 자산 관리와 데이터 거버넌스 역량을 우선시해 자산 및 데이터의 범주와 중요성을 파악해야 한다. 또한 접근 제어 정책을 세울 때 이러한 전후 사정을 활용해야 한다. 이후 목표를 규정하고 이를 E2E(end-to-end) 전략에 내재하면 분명 원하는 사업 결과를 달성할 수 있다. 하지만 이러한 여정은 결코 쉽지 않다. 이번 서베이 응답자들은 조직 전반의 사이버 보안 관리의 가장 큰 장애물이자 과제로 '데이터 관리·경계 및 복잡성 증대'를 꼽았다.

제로 트러스트는 단순한 기술 솔루션을 넘어선 문화적 변화에 속한다. 조직 전체의 변화는 과소평가할 수 없다. 커뮤니케이션과 역할 중심 훈련, 인식 개선, 운영 프로세스 수정 등 연성 요인들이야말로 변화에 성공하는 열쇠다. 대체로 그러한 프로그램을 이행하려면 강력한 리더십, 전담 아키텍처, 기술적 업무 흐름, 설득력 있는 리더 등의 지원을 발판으로 비즈니스 전략에 부합하는 전략을 세워야 한다. 그래야 모든 이해관계자의 의지와 노력을 한 데 모을 수 있다.

엄청난 장점

제로 트러스트를 기업 전략에 내재하면 여러 가지 전략 우위를 확보할 수 있다. 운영 복잡성을 줄이고 생태계 통합을 간소화함으로써 다음과 같은 이점을 누릴 수 있다.

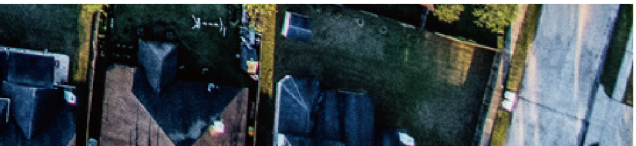
- 고객 경험 개선
- 사업 민첩성 강화
- 사업 회복력 강화
- 공격 노출면 축소
- 비용 감축 실현
- 비즈니스 파트너와 협력 강화
- 클라우드 도입 가속화

성공으로 가는 길

대형 첨단기술 기업들이 제로 트러스트의 성숙기로 향하는 여정을 주도하며, 이러한 원칙을 응용해 보안 서비스를 개발, 운영, 제공하고 있다. 다른 선도 기업들은 제로 트러스트 전략을 도입해 사업 우선순위, 디지털 전환, 리스크 전략을 뒷받침하고 있다. 귀사의 아키텍처를 현대화할 때 선도 기업들의 혁신 및 엄청난 규모 확대 방식을 이해하면 귀사의 디지털 전환을 이끌어가는 데 도움이 된다. 변화가 일어나고 있음은 부인할 수 없다. 제로 트러스트 전환을 위한 방향키를 빨리 잡을수록 귀사의 여정은 더욱 안전해진다. 남들이 이끄는 대로 끌려가느니 운전석에 앉아 귀사의 운명을 스스로 결정하는 것이 훨씬 바람직하다. 당장 제로 트러스트 여정을 시작하라.

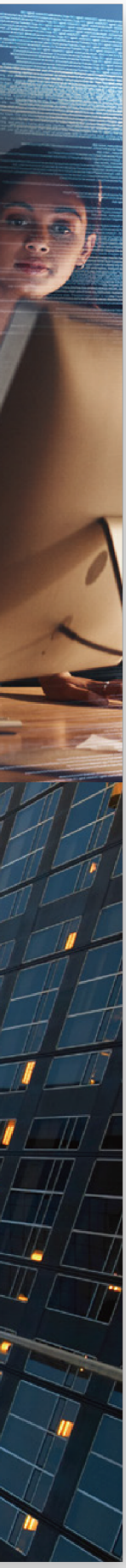
"이제 제로 트러스트 원칙을 100% 활용해 현대적 보안 아키텍처를 구축해야 할 때가 왔다. 이를 통해 디지털 전환을 따라잡고 실현할 수 있다."

-Marius Von Spreti,
글로벌 제로 트러스트 리더,
딜로이트 사이버



"상당수 기업이 이미 자사 환경에 존재하는 기존 기술을 연결할 때 수반되는 리스크를 간과하고 있다. 기존 기술에 연결성을 부여하면 생태계 전반에서 공격 노출면이 확대된다."

-Dana Spataru,
글로벌 사이버 신흥 기술 리더,
딜로이트 사이버



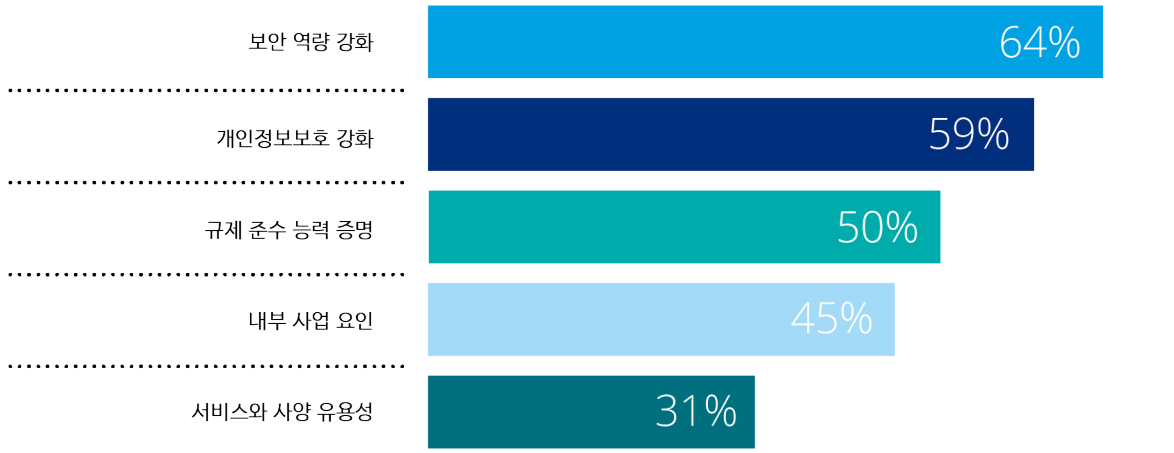
신흥 기술 스펙트럼 연결하기

퀀텀 컴퓨팅, 5세대(5G) 네트워크, 디지털 트윈 등 첨단 기술이 헤드라인을 장식하고 있지만, 실상을 제대로 들여다보면 OT 등 수십년 간 제조 환경에서 함께 해 온 다수의 브라운필드(brownfield) 기술이 여전히 활약하고 있다.

전혀 새로운 것이든 오래 전부터 도입된 것이든, 인터넷에 연결돼 있고 실제와 디지털 세계가 상상 가능한 거의 모든 방법으로 더욱 연결되는 방식을 취한다면 '신흥 기술'이라 부른다. 의료기기부터 운송 및 교통, 농업까지 모든 분야에서 디지털 변형이 이뤄지고 있다. 이는 우리가 거의 모든 것을 만들고 사용하는 방식을 완전히 변화시킴과 동시에 전에는 결코 상상할 수 없었던 보안 위험을 가져온다.

CIO와 CISO는 향후 3년간 신흥 기술을 도입할 이유로 보안 역량 강화(64%), 데이터 보호 역량 강화(59%), 규제 부합 능력 강화(50%) 등을 꼽았다.

그림 8
신흥 기술을 도입하는 이유는 무엇인가? *



*복수 응답 허용, 백분율 총합이 100% 초과

증폭되는 연결성

원래 인터넷으로부터 고립돼 있던 OT 공간은 최근 수많은 랜섬웨어 공격을 받고 있다. 이로 인해 즉각 생산에 차질이 빚어지자 연결성의 취약성에 관심이 쏟아졌다. 특히 COVID-19를 계기로 공장과 설비를 원격으로 관리하는 기업이 늘면서 이러한 상황은 더욱 심화됐다.

의료기기부터 자동차, 심지어 도시 전체까지 모든 연결 생태계가 유사한 특징의 리스크를 안고 있음을 이해할 필요가 있다. 의료 기기는 각 병원의 온프레미스 플랫폼 용으로 만들어졌지만, 이제는 인터넷을 통해 가정에서 사용되고 있다. 전 세계에서 화석연료 자동차를 빠르게 대체할 것으로 기대되는 전기차는 대부분 구동을 위해 연결성이 필요하다. 이러한 커넥티드 차량은 전 세계 곳곳에 흩어져 있는 수많은 공급업체가 제공하는 부품으로 만들어지는데, 모든 공급업체가 이러한 부품에 보안 장치를 설계하는 것은 아니다. 각 도시가 서비스와 중요 인프라 연결을 확대하면서, 클라우드 제공업체부터 플랫폼 운영업체까지 수많은 제3자 업체들과 파트너십을 맺고 있다. 이 모든 상황으로 인해 공격 노출면이 확대되고, 위험은 증폭되며, 책임 경계가 모호해진다.

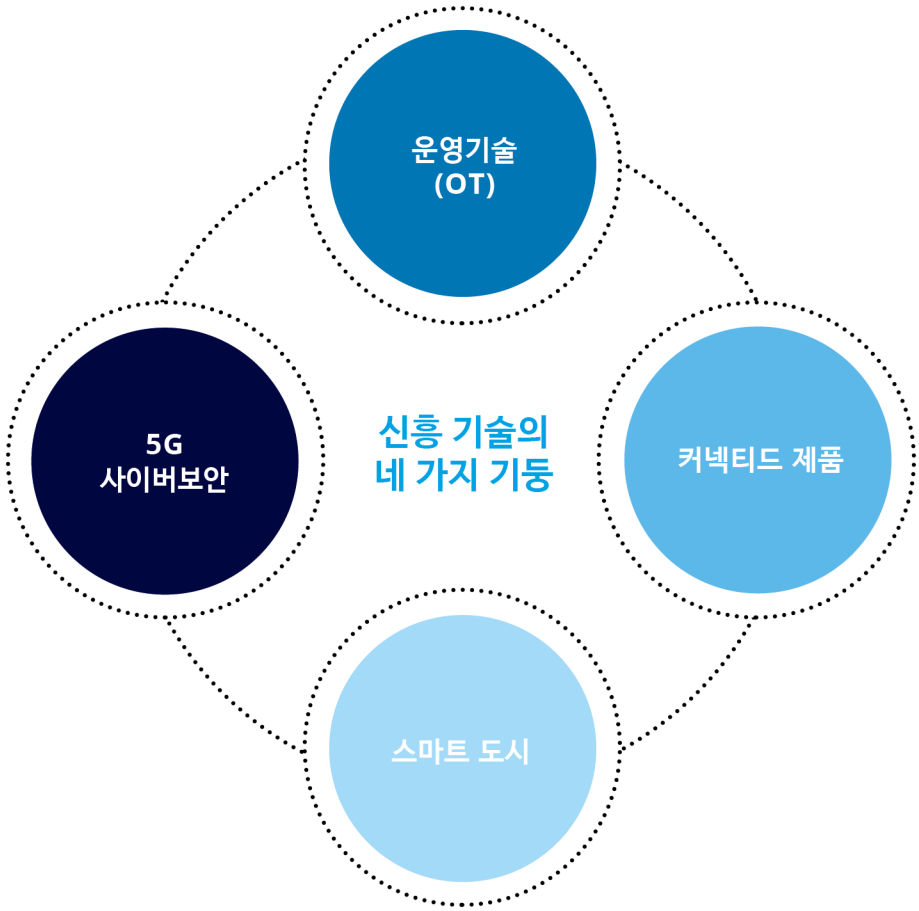


그림 9
끊임없이 나타나는 신흥 기술을 아우를 수 있는 환경을 단순화하기 위해 딜로이트 사이버는 다음의 네 가지 주요 요인에 초점을 맞춘다

이들 네 가지 주요 요인은 실행 과정에서 맞닥뜨리는 대부분의 시나리오에 적용할 수 있다.

보이지 않아도 파악하라

규모가 작고 100% 디지털화를 달성한 기업은 사이버 위험을 한 눈에 파악할 수 있다. 반면 복잡하게 상호 연결된 생태계를 지닌 대기업의 경우 사이버 위험을 한 눈에 파악할 수 있는 능력을 단시간 내 키우기가 어렵다. 하지만 조직 내 각 부문이 각자의 영역 내에 있는 프로세스의 보안에 대해 책임을 지도록 하면 이 문제를 해결할 수 있다. 구성원 모두가 생태계 내 각각의 영역에서 보안을 강화한다면, 사이버 위험을 총체적으로 파악할 수 없을지라도 전체 위험을 줄일 수 있다.

각 기업이 이를 수행하는 속도는 기술의 유형과 복잡성에 따라 달라지지만, 기본적 보안을 효율적으로 유지하고 정보를 안전하게 공유한다는 목표는 같다. 현재 제시된 솔루션은 단순하다. 부문별 프로세스를 정렬해 장기적으로 효율성과 효과를 개선하는 것이다. 이러한 정렬 작업을 빨리 할수록 보안 또한 빨리 성숙할 수 있다. 중앙화, 분산화 모델 모두 효과적이겠지만, 결국에는 단일한 통합적 사이버 위험 시각으로 수렴돼야 한다.

비즈니스의 핵심

거버넌스 관점에서 신흥 기술 스택(stack)은 매우 복잡할 수 있지만, 누군가는 보안 문제를 완벽하게 파악해야 한다. 이사회의 이해와 지지를 얻으면 기술을 확보하고 관리하는 것뿐 아니라 올바른 전략 파트너십을 수립하는 데 도움이 된다. 기존 IT와 달리 신흥 기술은 핵심 비즈니스와 긴밀히 연결돼 있다는 점에서 이를 달성하기가 더 용이하다.

예를 들어, 제조사가 자사 OT에 사이버 공격을 받는다면 이는 단순히 CISO만의 문제가 아님이 단번에 드러난다. 생산이 중단되면 즉각 운영 책임자의 문제가 되고, 수익이 악화되면 당장 CFO와 CEO의 문제가 되며, 기업 이미지가 추락하면 CMO의 문제가 된다.

자산으로서의 보안

위의 시나리오를 역으로 생각해 보면, 신흥 기술 덕분에 비즈니스 리더들이 사이버 보안의 순기능을 더욱 명확히 알 수 있게 된다. CEO가 설계 자체에 보안을 포함한 제품을 늘리고자 하는 의지를 보인다면 이러한 제품은 연결성이 심화되는 세상에서 상품성이 더 강화될 것이다. 이제 비즈니스 리더들은 보안을 생각할 때 비용 발생이 아니라 가치 창출을 떠올리게 될 것이다. 이를 통해 다운타임(downtime) 감축 방안을 찾기 위한 논의가 프로세스 개선을 모색하는 논의로 확대될 수 있다. 물론 보안은 필요한 사안이고 논의의 중심 의제가 되겠지만 결국에는 부차적 이슈가 될 것이다.

> "최근 발생한 대형 사이버 공격은 해킹 능력이 고도로 발전한 결과라는 것이 통념이지만, 대부분 사이버 공격은 기본적 보안 통제와 위생이 부재한 결과이다. 이는 전혀 복잡한 일이 아니다."
>
> -Dana Spataru,
> 글로벌 사이버 신흥 기술 리더,
> 딜로이트 사이버

만병통치약은 없다

범 산업적으로 사이버는 계속 톱3 기업 위험 요인에 들고 있다. 이사회와 경영진뿐 아니라 사이버 위험을 관리하는 책임자들도 이러한 인식을 공유하고 있다. 모든 산업의 기업들은 IP와 고객 신뢰의 취약성을 갈수록 절실히 체감하고 있다.

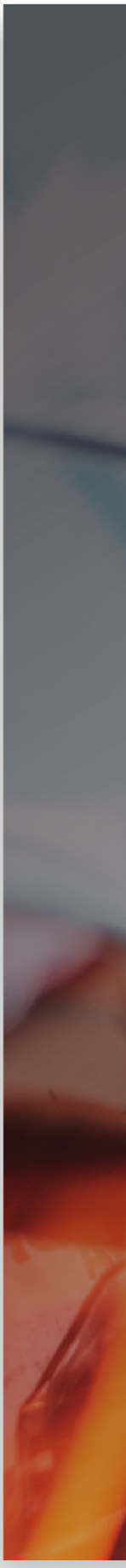
하지만 제각각인 사이버 규제 환경과 지역 간 차이 등 여러 요인들로 인해 산업별 디지털 전환 양상도 천차만별이다. 팬데믹을 계기로 공급망 보안과 원격 근무로 부각된 제로 트러스트 필요성 등 공통적 테마가 나타나기는 했지만, 모든 산업의 사이버 문제를 한 번에 치료할 수 있는 만병통치약은 없다.

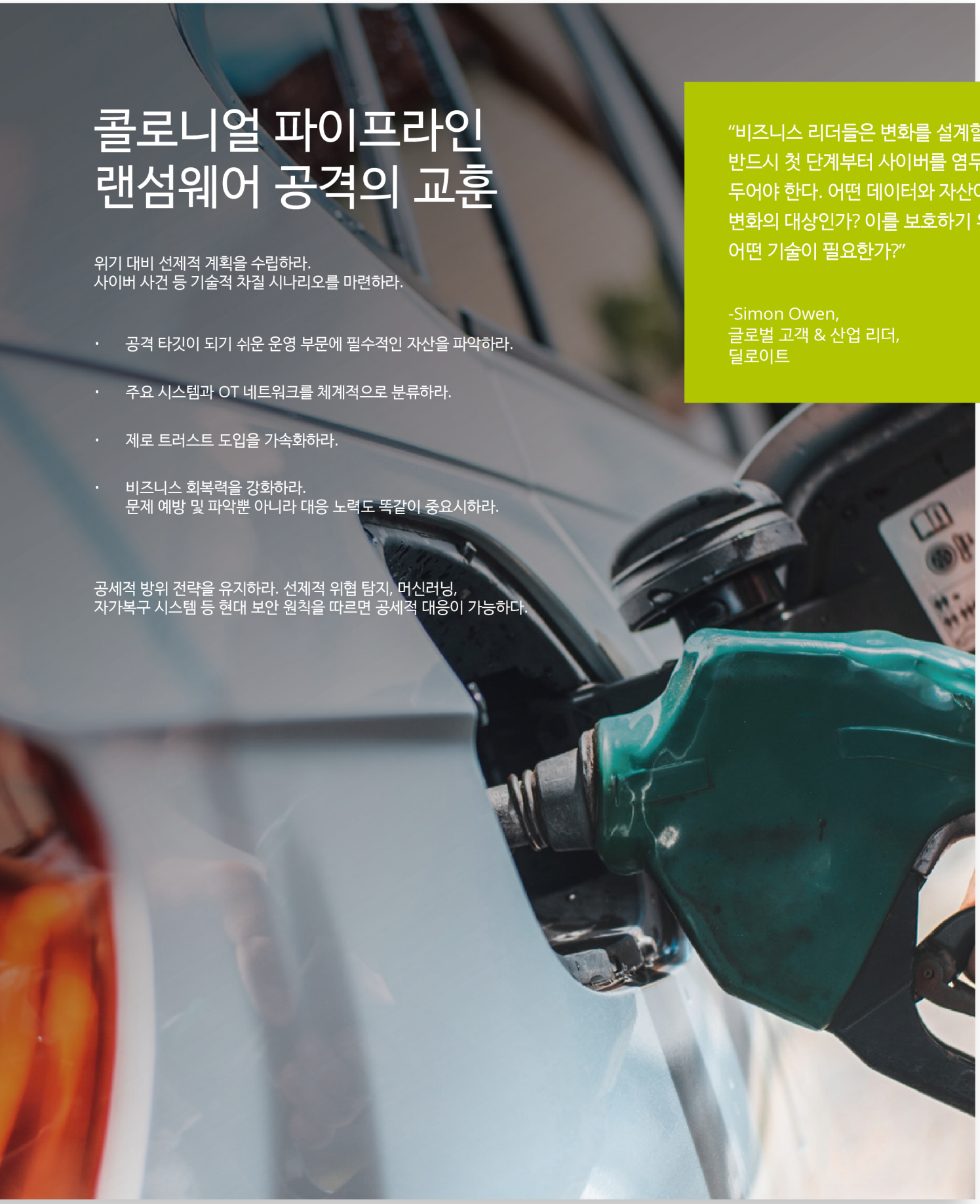
어떤 방향을 선택하든 범 산업적으로 점차 중요해지는 관심사는 반드시 파악하고 있어야 한다. 현재 각국 정부는 광범위한 사이버 위협에 대응하기 위한 규제 노력을 강화하고 있기 때문에, 첨단 보안 계획이 반드시 필요하다. 규제 당국이 변화를 주도하지 않는다 하더라도, 기술 연결성과 개인 맞춤화가 심화되면서 디지털 생태계의 재설계를 피할 수 없게 됐다. 또 모든 산업이 사이버 위협에 취약하다는 인식이 확산되면서 지식을 공유하려는 노력 또한 확대되고 있다. 다른 산업에서 적용 가능하고 효과를 보인 솔루션이 내가 속한 산업에서도 중요한 사례가 되는 것이다.

규제 폭발

일부 산업에서는 사이버 공격이 엄청난 규제 대응으로 이어졌다. 지난 2021년 5월 미국 동부 최대 휘발유, 경유 및 항공유 송유관 회사인 콜로니얼 파이프라인(Colonial Pipeline)이 랜섬웨어 공격을 받은 후 행정명령과 에너지 기업의 사이버 보안 개선을 위한 지침이 쏟아져 내렸다.

에너지 자원 및 산업(ER&I) 섹터에서는 탈탄소화라는 장기적 목표를 달성해야 할 필요성과 함께 사이버 방어를 강화해야 한다는 단기적 시급성이 동시 압박으로 작용하고 있다. 최근 미국 정부는 최근 전력 부문 탈탄소화 목표 시점을 2035년으로 제시했는데, 에너지 산업이 이처럼 타이트한 목표를 달성하려면 대대적 디지털화 노력이 불가피하다. 이 과정에서 5G 전환과 커넥티드 기술 등으로 대거 전환이 이뤄지면서 에너지 산업 자체의 사이버 보안 수요도 증가하고 있다.





콜로니얼 파이프라인 랜섬웨어 공격의 교훈

위기 대비 선제적 계획을 수립하라.
사이버 사건 등 기술적 차질 시나리오를 마련하라.

- 공격 타깃이 되기 쉬운 운영 부문에 필수적인 자산을 파악하라.
- 주요 시스템과 OT 네트워크를 체계적으로 분류하라.
- 제로 트러스트 도입을 가속화하라.
- 비즈니스 회복력을 강화하라.
  문제 예방 및 파악뿐 아니라 대응 노력도 똑같이 중요시하라.

공세적 방위 전략을 유지하라. 선제적 위협 탐지, 머신러닝,
자가복구 시스템 등 현대 보안 원칙을 따르면 공세적 대응이 가능하다.

"비즈니스 리더들은 변화를 설계할 때 반드시 첫 단계부터 사이버를 염두에 두어야 한다. 어떤 데이터와 자산이 변화의 대상인가? 이를 보호하기 위해 어떤 기술이 필요한가?"

-Simon Owen,
글로벌 고객 & 산업 리더,
딜로이트

기회와 위험 사이 균형 잡기

생명과학과 헬스케어 부문에서는 환자와 직접 소통하는 새로운 모델로 인해 사이버 보안 수요가 증가하고 있다. 헬스케어 제공업체들이 고객의 건강 개선 상황을 모니터링할 방법을 모색하고 있고 생명과학 기업들이 환자의 건강 개선을 위해 환자 중심 서비스에 주력하고 있는 가운데, 원격 기기와 애플리케이션 사용으로 데이터 보호와 개인정보보호 문제가 중요해지고 있다.

이러한 고객 모니터링과 애플리케이션 사용으로 데이터가 급속도로 축적되면서, 기업들은 클라우드 기반 데이터 레이크(data lake)를 만들어 연구개발(R&D), 치료와 지원, 환자의 치료 지속, 제품 출시 등에 도움이 되는 인사이트를 얻을 수 있다. 하지만 이러한 기술 발전은 사이버 보안 문제를 수반한다. 따라서 관련 생태계는 데이터를 보호, 암호화, 익명화하고 유출을 막을 수 있도록 설계 및 수립돼야 한다.

일반적으로 글로벌 생명과학 기업들은 지역마다 상이한 규제의 칼날보다 해킹 공격을 더욱 두려워한다. 고객과 소통할 때 신뢰를 구축하고 유지하는 것이 매우 중요하고, IP를 보호하는 것은 생명과학 기업의 사활이 걸린 일이다.

지식 공유

사이버 위협은 어디에나 존재하고 팬데믹을 계기로 이에 대한 취약성이 여실히 드러남으로써 각 산업 내부의 지식 공유 방식에 변화가 생겼다. 브랜드 명성 악화는 사이버 공격의 부작용으로 남겠지만, 사이버 사건에 대한 정보를 공유하는 것은 가치 있고 유용한 일이자 브랜드 명성을 회복하는 데 도움이 되는 치유의 단계로 인식되고 있다. 기업들은 사이버 보안 문제를 비밀로 유지한다 한들 경쟁우위를 확보하는 데 도움이 되지 않고 오히려 산업 전체에 악영향을 줄 수 있음을 알게 됐다.

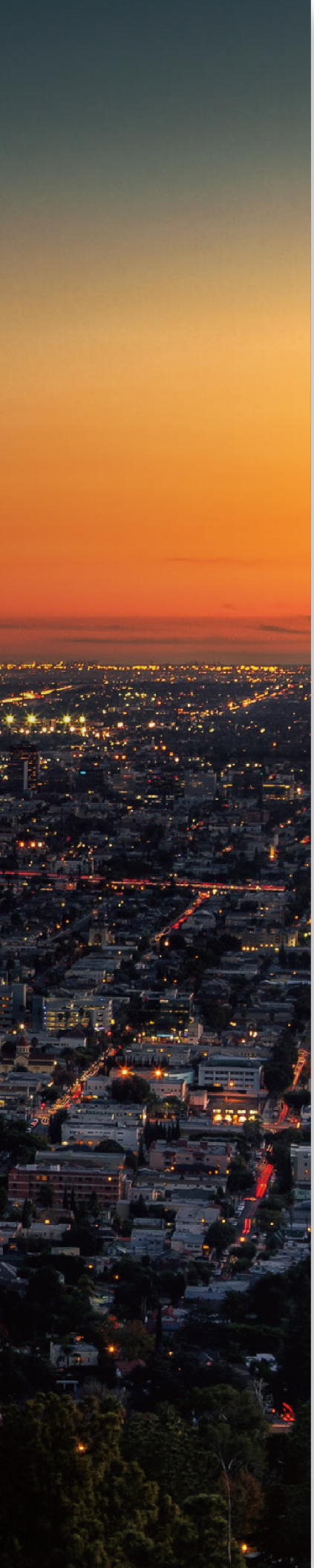
각국 정부도 집단 방어의 중요성을 인정하고 정보 공유를 위한 민관 협력체 구축을 지원하고 있다. 미국 정보공유분석센터(ISAC)가 대표적인 예다. 한편 각 기업의 CISO들은 물밑에서 서로 정보를 주고받고 있다. 동종 산업 내 동료들과 정보를 공유하는 것이 보다 일반적이지만, 금융 서비스와 석유 및 가스 산업처럼 성숙한 산업부터 생명과학과 제조업까지 덜 성숙한 산업까지 산업 간 정보 공유도 시작됐다. 또 사이버 보안 경험을 가진 CISO들은 산업 간 이동하는 경우가 많다. 이를 통해 근 시일 내 산업 간 글로벌 정보 공유가 더욱 활발해질 것으로 기대된다.

"생명과학 기업, 대형 은행, 에너지 기업을 막론하고 가장 난감한 문제는 초점을 맞춰야 할 부분을 찾는 것이다. 완전무결한 보안은 전혀 현실적이지 않다. 기업 리더들은 위험 정보에 기반해 가장 먼저 보호할 자산과 후순위로 남겨둬도 되는 자산을 취사 선택해야 한다. 그리고 이러한 결정을 신속하게 내려야 한다. 이후 조직 내외 여건을 살피며 끊임없이 재검토를 해야 한다. 고인 물이 되지 말라."

-Simon Owen, 글로벌 고객 & 산업 리더, 딜로이트

깨끗한 시야 확보

비즈니스 세계의 모든 분야에서 진행 중인 디지털 전환은 사람과 프로세스에 새로운 가능성을 열어주는 놀라운 실현 요소임과 동시에 위험을 증폭하고 퍼뜨리는 수단이기도 하다. 기업들이 전례 없는 글로벌 과제에 직면한 바로 이 시점에 실시한 이번 딜로이트 서베이는 참신한 시사점을 제시한다.



복잡성은 계속될 것이다. 하이브리드 업무 환경은 영구적으로 자리잡고, 클라우드는 거의 모든 형태의 기업에 중요한 수단이 될 것이며, 기기와 애플리케이션은 더욱 진화하면서 연결성이 강화될 것이다.

기업은 명확히 규정된 경계가 없는 생태계 전반을 들여다볼 수 있는 시야를 반드시 확대해야 한다. 그렇지 않으면 운영 차질, 명성 악화, 주가 하락 등 치명적 손실을 피할 수 없다. 하지만 복잡성이라는 문제를 해결하기 위한 솔루션 또한 결코 단순하지 않다.

사이버 보안의 책임을 윗선으로 끌어올려라

기업들은 사이버 보안을 사업 위험의 모든 부문에 흡수시켜야 한다. 그렇지 않으면 디지털 전환의 가치를 눈 앞에서 놓치게 되고 공격에 대한 취약성만 키우게 될 것이다.

이를 위해 우리가 제시하는 가장 중요한 해결책은 CISO가 CEO에게 직접 보고할 수 있도록 전권을 부여하는 것이다. 이렇게 되면 CISO는 자사의 모든 사업 부문을 파악할 수 있다. 이는 양방향으로 작용해야 하므로, CISO는 이사회가 이해할 수 있는 방식으로 위험 평가 결과를 설명해야 한다. CISO는 CEO와 이사회에 보고하는 것 외에도 신규 사업 개발 작업에 처음부터 참여해 적절한 사이버 거버넌스가 수립되도록 해야 한다.

사일로를 깨뜨려라

기술 발전으로 조직 내에서 정보가 자유롭게 이동할 수 있게 된 만큼, 사람도 이를 따를 필요가 있다. 부서 간 단절을 조장하는 사일로를 깨뜨려 사이버에 관해 협업하는 것이 매우 중요하다. 새로운 계획을 시작할 때 전략, 제품개발, 규제 담당, IT, 마케팅 부서가 모두 한 자리에 앉아 필요한 데이터 자산뿐 아니라 보안과 개인정보보호 요건을 파악해야 한다. 계획의 설계 단계부터 보안과 개인정보 보호를 포함해야 차후 골치 아픈 문제를 피할 수 있다.

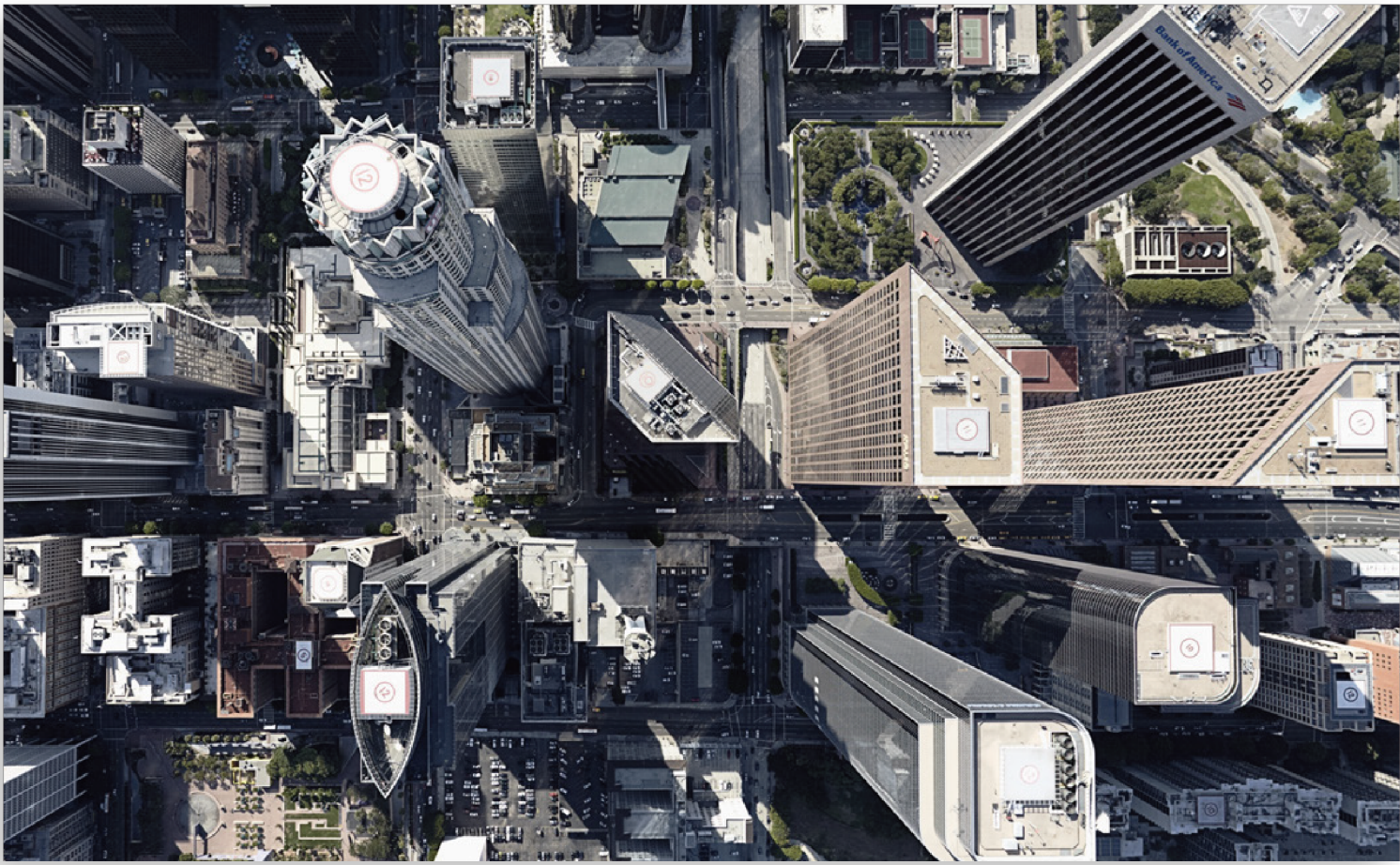
제로 트러스트를 실행하라

복잡성은 현실이다. 사용자와 여타 개체를 인증하는 과거의 방식에 의존하면 해커들의 공격에 취약해져 재앙을 피할 수 없다. 다행히도 지속적으로 위험을 평가하고 실시간으로 접근 제어 검토를 응용할 수 있는 능력을 복잡한 아키텍처에 설계할 수 있다.

제로 트러스트는 기술적 혁신이자 문화적 혁신이다. 사람들의 행동 습관을 바꾸려면 소통과 훈련이 필요하다. 제로 트러스트를 통해 혁신과 비즈니스 전략을 안전하게 실행할 수 있다. 제로 트러스트 도입이 디지털 전환 노력에 큰 도움이 된다는 사실을 모든 구성원이 제대로 이해할 필요가 있다.

자산으로서의 보안

데이터는 디지털 전환의 혈액과도 같다. 데이터의 기능 방식을 이해하는 것도 중요하지만, 데이터가 비즈니스 성과와 고객 경험을 창출하는 방식을 알아야 장기적으로 데이터가 창출하는 가치를 이해할 수 있다. 모범적 데이터 거버넌스, 세심한 개인정보보호 정책, 강력한 보안을 갖춘 기업들은 고객과 파트너사의 신뢰를 얻는다. 사이버 보안을 비용으로만 생각하기 쉽지만, 새로운 초연결성의 세상에서 사이버 보안이 브랜드와 주주 가치에 미치는 영향을 반드시 고려해야 한다. 보안을 이행하는 것은 일개 프로젝트가 아니며, 처음부터 끝까지 데이터와 커뮤니케이션, 비즈니스 교류를 신중히 다루겠다는 약속이다.



지식 공유

사이버 보안을 관리하는 단순한 단일 솔루션은 없지만, 디지털 전환 여정의 기업들이 마주한 위협은 이미 상당수 공유되고 있다. 만연한 사이버 공격에 면역을 갖춘 산업이나 지역은 없지만, 상호 지식 공유를 통해 사건 발생 시 효과적으로 대응하는 법을 서로에게 배울 수 있다. 이를 위해 다른 기업들과 경험 및 지식을 공유하는 것은 전반적인 보안 환경을 개선하기 위해 매우 중요하다.

위험과 보상

귀사의 사이버 예산 규모가 크든 작든, 본고에서 제시하는 접근법을 활용하면 자원을 보다 효과적으로 활용할 수 있다.

디지털 전환에 수반되는 복잡성과 무수한 위험에만 시선이 가기 쉽지만, 이에 따른 긍정적 측면 또한 간과해서는 안 된다. 필요한 시야를 확보하고, IT를 통해 조직의 민첩성이 강화되고, 고객의 신뢰를 얻고, 복잡성을 완전히 파악해 대응할 수 있다는 자신감을 얻게 되면, 전혀 새로운 차원의 보상을 받게 될 것이다.

저자

Emily Mossburg
Global Cyber Leader

+1 571 766 7048
emossburg@deloitte.com

Simon Owen
Global Clients & Industries Leader

+44 20 7303 5133
sxowen@deloitte.co.uk

Annika Sponselee
Global Data & Privacy Leader

+31882882463
asponselee@deloitte.nl

Dana Spataru
Global Emerging Technologies Leader

+31882888882
dspataru@deloitte.nl

Matthew Holt
Global Strategy & Transformation Leader

+393351421906
maholt@deloitte.it

Marius von Spreti
Global Zero Trust Leader

+49 89 290365999
mvonspreti@deloitte.de

Ashley Reichheld
US Customer & Marketing Leader

+1 617 449 5067
areichheld@deloitte.com

Andrew Rafla
US Zero Trust Leader

+1 201 912 6535
arafla@deloitte.com

연락처

Emily Mossburg
Global Cyber Leader

+1 571 766 7048
emossburg@deloitte.com

Dave Kennedy
Asia Pacific Risk Advisory Leader

+61 2 8260 4295
davekennedy@deloitte.com.au

Yuichiro Kirihara
Asia Pacific Cyber Clients & Industries Leader

+818033672805
ykirihara@deloitte.com

Amir Belkhelladi
Canada Cyber Leader

+1 514 393 7035
abelkhelladi@deloitte.com.ca

Peter Wirnsperger
Central Europe Cyber Leader

+49 40 320804675
pwirnsperger@deloitte.de

Neils van de Vorle
North South Europe Cyber Leader

+31882882186
nvandevorle@deloitte.nl

Cesar Martin
Spain Cyber Leader

+34 914 381 416
cmartinlara@deloitte.es

Deborah Golden
United States Cyber Leader

+1 571 882 5106
debgolden@deloitte.com

Interested to learn more?
Drop us a note and we'll connect you to the right people:
Futureofcybersurvey@deloitte.com

Deloitte.