
CISO

새로운 정보보안 최고 책임자(CISO)

전략적 보안조직을 이끌기

저자 Taryn Aguas, Khalid Kark, Monique François
일러스트레이션 Lucy Rose

사이버 위협을 감시하고 격퇴하며 대응하는 동시에 컴플라이언스 요건을 준수하는 것은 정보보안 최고 책임자(Chief Information Security Officer: CISO) 혹은 그와 같은 임무를 맡은 사람과 그 팀에게 주어진 명백한 책임이다. 그러나 비즈니스 환경은 급격히 진화하고 있다. 빈번하게 인용되는 통계 중엔 "세계에서 유통되는 자료 중 90%는 지난 2년간 만들어진 것"이라는 말[1]도 있다. 연결성의 폭발적인 증가는 기업에 고객 유치와 제품 개발을 위한 새로운 기회를 부여한다. 그러나 동시에 이들 기회에는 숨은 위험도 있다. 고객 정보, 지적재산, 브랜드 자산이 진화하면서 정보 유출의 새로운 목표물이 되어 주주 가치와 기업 실적에 직접적인 영향을 미치고 있다. 이에 대응하기 위해 경영진은 보다 강력하고 전략적인 리더십 역할을 수행할 수 있는 CISO를 필요로 한다. 이 새로운 역할은 단순히 규정 준수를 감시하고 집행하는 역할을 넘어서 사업에 실질적으로 도움을 주고, 보다 전략적으로 정보 위험을 관리하며, 전사에 걸쳐 사이버리스크 책임을 공유하는 문화를 육성해야만 한다.

CEO와 여타 고위 경영진들이 CISO의 역할 확대를 매우 반길 수 있지만, 역설적이게도 이 동일한 경영진들이 부지불식간에 조직의 진보를 방해하고 있을 수 있다. 기업 경영진들은 사이버 보안의 필요성을 이해한다고 주장하겠지만 정보보안조직 그리고 때때로 구체적인 사이버보안 조치에 대한 그들의 지원을 사실상 얻기 힘들기 때문이다. 예를 들어, 경영진 중 70%가 자사의 현재 보안 솔루션에 대해 자신감을 표하지만 이에 공감하는 정보기술(IT) 전문가들은 50%에 불과하다.[2] 그렇다면 이러한 조직 내 불일치의 원인은 무엇인가?

CISO는 새로운 기술, 전략에 대한 집중, 경영진과의 소통 확대로부터 혜택을 볼 수 있다는 것을 알고 있지만, 이를 진척시키기 위해 시도할 때마다 번번이 헛바퀴 도는 경험을 하곤 한다. 우리는 딜로이트[3]의 CISO Lab 활동[4] 및 추가 연구에서 얻은 인사이트를 바탕으로 CISO가 비즈니스와 조화를 이룬 보다 주도적인 보안 조직을 구축하려 할 때 가장 일반적으로 직면하는 장애물을 탐구하고, CISO가 조직에 전략적인 공헌자가 되기 위해 취할 수 있는 조치를 설명하려 한다.

경고 신호를 인식하라

경영진과 IT 전문가들이 CISO의 조직 내 권한 확대에 대해 의견이 상충할 경우, 경고 신호를 평가하는 것이 중요할 수 있다. 조직 내에서 CISO의 역할을 격상시켜야 할 필요성이 몇 가지 신호로 나타날 수 있다.

리더십과 자원의 결핍. 보안 조직의 리더가 정식 보안 훈련을 받지 않은 사업 혹은 IT 감독자로서, 전술적이고 운영 중심적인 접근방식을 취한다는 인상을 주거나 사이버 리스크 관리보다는 컴플라이언스 활동에 대부분의 시간을 할애할 수 있다. 부서가 산업평균 대비 예산 규모가 작고 제한된 자원과 기술만을 가지고 있거나 보안 프로그램이 적절하게 정의되지 않았으며 확립된 절차나 통제가 없을 수 있다.

보안 침해. 자료나 시스템이 손상된 실질적 침해 사고는 시스템적인 문제, 운영상의 실패, 그리고 잠재적으로는 보안을 경시하는 문화의 징후일 수 있다. 해이한 규정 준수, 부족한 내부 감사, 측정기준과 투명성의 부족은 모두 잠재적인 보안 문제를 나타내는 조짐이 될 수 있다.

비즈니스와의 엇박자. 사업부서는 보안팀을 파트너보다는 경찰관으로 간주할 수 있다. 사업부 수장을 이해하고 협력하려는 노력을 하지 않는 CISO와 보안팀은 기업의 목표 달성에 걸림돌이 되는 경우가 잦아 직원들이 보안팀과 보안조치를 회피하는 결과로 이어진다.

조직 구조상의 문제. 보안조직의 구조가 적절히 정의되지 않거나 IT부서내 몇 단계 아래 깊이 파묻혀 있을 수 있다. 최근 조지아공과대학(Georgia Institute of Technology)이 수행한 설문조사는 이러한 문제를 조명했다. 조직에서 관련 업무를 담당하는 응답자 중 오직 22%만이 CISO가 CEO에 직접 보고한다고 말했고 40%는 여전히 CIO에 보고한다고 답했다.[5] 또한 보안조직이 IT, 리스크관리부서, 법무부서, 운영부서 등 어디 속하건 간에 여타 사업 영역과 고립되어 통합은 고사하고 다른 부서들의 기능을 이해, 인지하는 데 애를 먹을 수 있다.

이중 어느것도 조직 내에서 어떠한 문제가 점증하고 있음을 나타내는 신호가 될 수 있다. 잠재되어있던 신호가 정보유출 혹은 여타 사이버보안의 침해의 형태로 발현되면서 조직은 위기 모드로 돌입한다. 여기서 다음과 같은 질문을 제기할 수 있다: 왜 더 이상의 발전이 이뤄지지 않는가?

전략적인 보안조직을 만드는 데 있어 도전과제

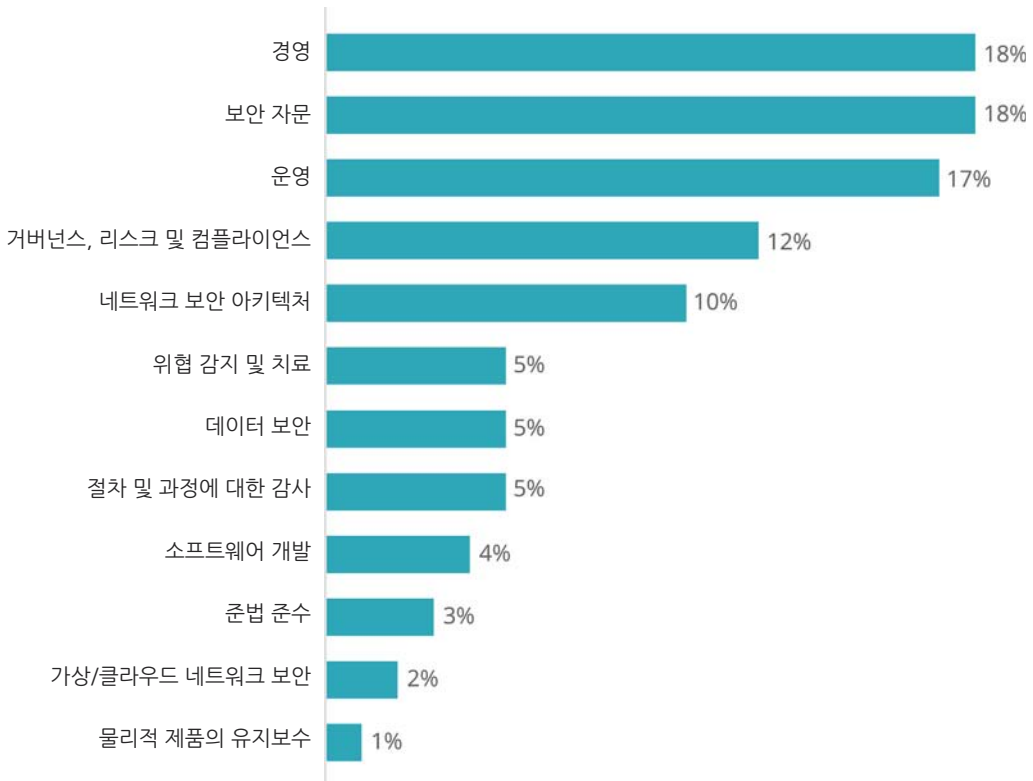
왜 기업들은 사이버 보안을 강화하는 데 애를 먹을까? 어떤 요인들이 CISO로 하여금 기업에서 보다 전략적인 역할을 맡지 못하게 할까? 그 원인은 보안조직, 사업부서 그리고 둘 사이의 의사소통에 있을지 모른다.

내부를 바라보기: CISO가 거울을 들여다봐야 할 때는 언제인가

딜로이트의 CISO Labs 자료에 따르면 사업과 더 잘 통합되는 역량의 구축은 CISO들 사이에서 지속적인 우선순위였다. CISO 중 90% 이상이 보안조직과 사업부 사이에 전략적 조율이 개선되길 바랐으나 거의 절반(46%)이 이의 달성을 위한 능력이 부족하다고 우려했다.[6] 그 이유는 무엇일까?

좁은 시야. 대부분의 CISO는 해당 분야를 전공한 혹은 경력을 쌓은 기술 전문가이기 때문에 일반적으로 사업 전반에 대한 지식과 경험에 한계가 있다. 많은 CISO들은 관리직에 오르기 전 물리적 제품의 유지보수나 소프트웨어 개발부터 컴플라이언스 관련 활동, 위협 감지/대응, 네트워크 보안 아키텍처(그림1)[7]까지 다양한 부문에서 활동했다. 만약 이들이 사업이나 사업개발 기술을 포함한 경영 훈련을 받지 못했을 경우, 이런 좁은 시야로 인해 사이버 위협을 단순한 기술적 필요요건이 아닌 사업상 중대한 리스크로 인식하는 CISO의 능력이 떨어질 수 있다. 후자의

그림 1. CISO들의 과거 전문가적 역할



참고: 이 수치는 현 CISO들이 보안조직으로 이동하기 전 맡고 있던 직무들을 보여준다.

출처: 프랭크 딕슨(Frank Dickson), 마이클 수비(Michael Suby), 2015 (ISC)2 글로벌 정보보안 인력 연구(The 2015 (ISC)2 global information security workforce study), 프로스트 & 설리번(Frost & Sullivan), 2015, p. 36.

그래픽: Deloitte University Press | DUPress.com

경우 전사를 아우르는 전략적 플레이어가 되기 위해 필수적인 능력이다.

소통과 협력. CISO는 또한 사업부 리더들과 의사소통하고 협력하는 데 어려움을 겪을 수 있는데, 이의 일부 원인은 그들과의 상호작용 및 관계가 제한되어 있기 때문이다. 이러한 문제는 경영진들의 인식 때문에 더욱 악화된다. 딜로이트 CISO Labs 참여자들 대부분(79%)은 "사이버 위협이 기술적 문제거나 컴플라이언스 활동이라고 생각하는 경영진들과 함께 시간을 보낸다"고 답했다. 결과적으로 대부분의 CISO는 "보안 추진계획에 동의를 얻고 설득하는 데 많은 시간을 투자해야 한다".[8]

그러나 경영진과의 관계는 사업에서 발생하는 일을 이해하고 가장 큰 리스크가 어디에 있는지 파악하는 데 필수적이다. 예를 들어, 조직 내 모든 데이터 하나하나를 보호하는 것은 사실상 불가능하기 때문에 보안 책임자는 어떤 자료가 기업에 가장 중요하고, 어디에 그 자료가 있으며, 만약 그 자료가 분실되거나 손상되었을 때 어떤 영향이 미치는지를 파악하기 위해 사업부와 협력할 필요가 있다. 이 같은 활동은 분명하게 정의된 의사소통 경로가 없을 때 어려울 수 있다. 보안 부문은 고객 서비스(여타 주요 부서에 고객 수요와 트렌드에 관한 정보를 정기적으로 제공한다)나 재무(주주들에게 조직 전반에 걸친 재무 자료를 전달한다) 부서들과 다르게 사업부문과 긴밀히 협력하거나 소통하지 않는다.

인재 부족. 보안 인재의 부족 역시 CISO가 큰 그림에 집중할 수 없게 만들 수 있다. CISO가 갈피를 잡지 못하고 흔들리는 첫 번째 이유는 팀원들이 너무 부족하거나 충분한 경험을 갖춘 인재가 부족하기 때문이다.[9] 보안은 여전히 고도로 전문화된 새로운 기술로서 많은 수요가 따른다. 2015년 프로스트 앤 설리번(Frost & Sullivan)의 조사에 따르면 응답자 중 62%가 자신들의 조직이 충분한 수의 보안 전문가를 보유하지 못했다고 답했다. 2년 전의 56%에 비해 더 높아진 수치다. 게다가 프로스트 앤 설리번은 2020년까지 약 150만 명의 보안 전문가가 부족할 것이라고 전망했다.[10]

"적절한 능력을 가진 사람을 찾는 것은 쉽지 않다. 그러나 더 큰 문제는 시장이 '구매자의 시장'이라는 사실이다. 직급을 막론하고 거의 모든 사이버 전문가들은 어디서 일할지 결정할 수 있는 많은 선택권을 가지고 있다. 이들을 유치하는 데 성공하기 위해, 우리가 가진 양질의 기업 문화와 이들이 할 수 있는 공헌의 가치를 그들에게 분명하게 전달할 수 있어야 한다"

- 스튜어트 타이틀(Stewart Title) CISO 제나디 비슈네베스키(Genady Vishnevetsky)

외부를 바라보기: 조직 내에서 CISO가 넘어야 할 고개

CISO와 그 팀에 국한되는 문제를 넘어 보안 책임자들은 더 넓은 사업부문에서 불어오는 역풍에 직면한다. 비즈니스 프로그램 리더들은 종종 보안의 전통적인 기능 그 이상을 이해하는 데 시간과 자원을 투자해야 할 가치를 못 느끼는 경우가 많다. 이와 대조적으로, 그들은 고객관계관리(Customer Relationship Management: CRM) 시스템의 구현 같은 다른 기술적 영역에는 보다 거리낌 없이 참여할 수 있다. 왜냐면 그 기저에 깔린 사업적 문제를 쉽

게 파악할 수 있기 때문이다. 우리의 연구결과는 조직 차원에서 사이버리스크에 집중하지 못하는 두 가지 주요 원인을 보안에 대한 잘못된 인식과 상충되는 의제들이라고 가리킨다.

보안에 대한 잘못된 인식. 많은 사업부문과 최고 경영진들이 컴플라이언스와 보안을 동일시하는데, 특히 규제가 많은 산업일수록 이러한 인식이 강하다. 딜로이트 CISO Labs에 따르면, CISO 중 79%가 사이버리스크가 기술적 문제거나 컴플라이언스 활동이라고 생각하는 이들과 시간을 보낸다고 답했다.[11] 그러나 규정을 준수한다고 해서 모든 사이버리스크를 해결하거나 조직을 안전하게 지킬 순 없으며 그러한 사고방식은 사이버리스크를 무척 협소하고 부적절한 방식으로 이해하는 조직 문화를 만들 수 있다.

상충되는 의제들. 사업부 리더들은 기업 보안의 중요성을 격상시켜야 할 역할이 있지만, 많은 이들이 이런 역할을 기껏해야 무관심하게 보고 있다. 최근 쓰레트트랙(Threat Track)의 설문조사에 의하면 최고 경영진 중 74%는 CISO가 경영진 회의에 참석하거나 조직 내 지도부의 반열에 올라야 할 필요가 없다고 생각했다.[12] 아마도 그 이유는 사업부문의 임무가 새로운 상품 및 서비스의 창출, 판매와 매출의 증대, 그리고 그 과정에서의 비용 통제이기 때문일 것이다. 이러한 활동의 결과는 일반적으로 보안 측면에서 평가되지 않고 책임을 지지도 않기 때문에, 경영진들은 성장을 위한 그들의 전략적 의제와 그들이 유발하게 되는 사이버리스크를 서로 연관 짓지 않는다.

전략적인 보안 조직을 향한 단계

보다 전략적이고 비즈니스의 통합된 파트너 역할을 하는 보안 조직을 만들기 위해서는 CISO의 역할에 대한 새로운 관점과 사이버리스크를 공유하는 문화의 조성이 모두 필요하다.

CISO의 역할 격상하기

사이버리스크 프로그램이 기업에 제공하는 가치를 높이기 위해서는 균형 잡힌 접근법이 필요하다. 성공적인 CISO는 기술자, 보호자, 조언자, 전략가라는 CISO의 '네 가지 역할' 전반(삽입글 CISO의 '네 가지 역할' 참고)[13]에 대한 우선순위와 도전과제의 균형을 어떻게 맞출지를 조기에 결정한다. 네 가지 역할 모두 중요하지만 CISO는 기술자와 보호자라는 전통적 역할에서 한발 더 나아가라고 도전 받고 있다. CISO의 일상의 행동과 활동이 전략가와 조언자 역할로 기울어진다면 다른 고위 경영진들도 그러한 방향으로 인식할 가능성이 크다.

전략가와 조언자의 특징을 파악하기

오늘날 CISO의 시간과 자원의 상당 부분이 위협을 관리하고 대응하는 데 할애된다. CISO는 전형적으로 보안 도구 및 기술의 실행을 감독 및 지시하고, 디지털 자산의 유출을 감지 및 차단하며, 사이버 사고의 리스크를 관리하고 사고에 대처하는 데 집중해왔다. 어떤 것이 더 중요하고 덜 중요한지를 구분하는 것은 무척이나 어려워서 사이버리스크를 하나의 덩어리로 묶거나 모든 환경을 보호하려고 시도하는 결과로 이어질 수도 있다.

게다가 CISO의 사이버리스크에 대한 이해와 수용 범위는 사업부문 리더의 그것과는 상당히 다를 수 있다. CISO는 리스크 축소의 관점에서 생각하지만, 사업부문 리더는 신규 시장에 기존 상품을 소개하고, 신사업 추진을 위해 외부 파트너를 들이고, 인수나 합병을 진행하면서 매일 리스크를 취한다. 실제로 더 많은 리스크를 수용할 수 있는 능력은 사업의 기회를 확대하는 반면 리스크를 배제하면 사업 기회의 상실로 이어질 수 있다. 이러한 관점에서 CISO의 역할은 경영진과 직원들이 사이버리스크를 인지하고 이해하도록 돕고 이해를 바탕으로 결정할 수 있게 준비시키는 것이다. 어떤 경우 조직의 혁신 의제는 보안 통제에 대한 보다 유연한 시각이 필수적일 수 있다. 사업의

CISO의 네 가지 역할

CISO는 보안 기술을 관리(기술자)하며 기업자산을 보호(보호자)하는 필수적인 역할을 수행하며 동시에 보안전략을 수립(전략가)하고 보안의 중요성에 대해 경영진에게 조언(조언자)하는 데 좀더 노력하도록 기대 받고 있다(그림 2 참조).

기술자. 기술자로서의 CISO는 보안의 기술적 아키텍처의 설계, 개발, 배치를 지도해, 보안 표준을 주입하고 혁신적인 대응책을 시행한다. 기술자는 변화하는 위협을 감지하고 모니터링하는 솔루션을 지원할 수 있는 플랫폼을 신중하게 선정하고 시행하며, 외부에서 제공된 서비스를 매끄럽게 운영되는 프레임워크에 통합시킨다. 또한 기술자는 미래의 보안 및 비즈니스 니즈에 부합할 수 있도록 보안 아키텍처의 설계가 유연하고 확장 가능하도록 만든다. 이들은 조직이 고수해야 하는 보안정책 및 표준을 개발 및 유지관리하고 플랫폼이 이러한 요건들을 만족시킬 수 있도록 CIO와 협력한다.

보호자. 보호자로서의 CISO의 책임은 설치된 보안 프로그램, 절차, 통제의 효과성을 모니터링하는 것이다. 보호자는 통제가 의도대로 작동하고, 데이터가 안전하며, 정보가 적절히 공유되고 있는지 등의 여러 사항을 고려한다. 보호자는 데이터의 기밀성, 무결성, 가용성을 보호하는 절차를 감시하고 전반적인 보안 프로그램을 추진한다. 이들은 또한 이해관계자들에게 정보를 제공하고 컴플라이언스 및 규제 요건을 충족시키기 위해 정보보안리스크를 측정하고 보고한다.

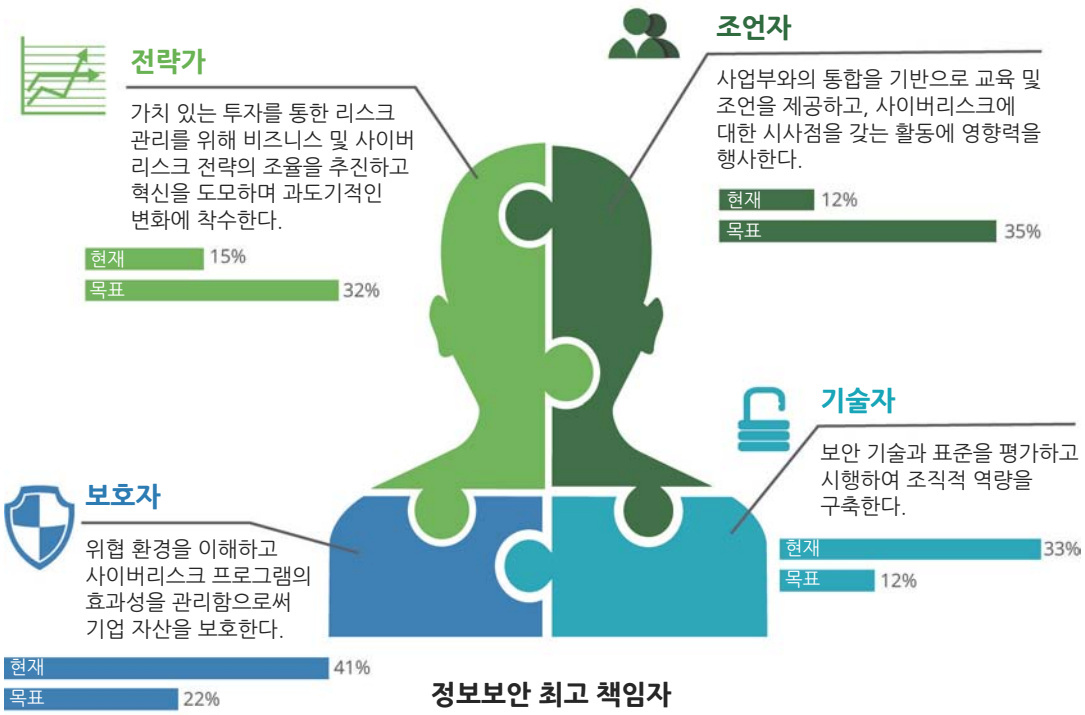
전략가. 전략가로서의 CISO는 모든 사이버리스크 투자에 있어서 최고로 중요한 설계자다. 전략가는 사업 전략과 정보 보안 전략을 조율하고, 기업 자산을 보호해 보안 투자에 대한 가치를 포착하기 위해 사업부문과 파트너 관계를 맺는다. 이러한 역할을 통해 CISO는 깊은 비즈니스 지식을 확보하며, 어떻게 리스크 관리가 비즈니스에 도움이 되는지에 대한 비즈니스 중심적인 조언을 제공하는 신뢰받는 파트너로서 활동한다. 전략가는 어떠한 사업 운영과 정보 자산이 기업의 최고 가치가 되는지 잘 알고 있고, 정보보안에 대한 투자를 우선시하는 전략적 거버넌스를 시행하며, 조직의 우선순위를 실행하고 기대하는 결과가 도출될 수 있도록 보안 및 비즈니스 자원과 예산을 확실히 조율한다.

조언자. 조언자로서의 CISO는 새로운 또는 부상하는 위협이 어떤 영향을 끼치는지 이해하고 있으며 기업이 새로운 전략을 실행할 때마다 발생하는 사이버리스크를 파악하는 데 기여한다. 조언자는 기업이 계속해서 보안에 대한 의사결정과 리스크 경감 역량을 향상시킬 수 있도록 한다. 또한 조언자는 조직이 사이버 위협을 해결하기 위해 어디에 초점을 맞춰야 할지 알고 있으며, 기업의 리스크 수용 범위와 사이버보안 활동을 조율하는 리스크 기반의 전략적 로드맵을 만든다. 조언자는 상당한 정치적 자산을 보유하고 있으며 보안 인식을 고취하기 위해 중요 이해관계자들의 협조를 요청하고, 교육을 제공하며, 관여하고, 조정한다.

민첩성을 끌어올리려면 CISO는 위협을 조기에 감지하고 잠재적인 사이버공격에 대한 대비를 강조할 수 있도록 보다 미세하게 조정된 노력을 이끌어가야 한다. (조직이 어떻게 리스크에 초점을 맞춘 모니터링 프로그램을 향해 진화할 수 있는지에 관한 보다 세부적인 논의를 보려면 본서의 '보안 모니터링부터 사이버리스크 모니터링까지' 기사를 참고)[14]

대화의 중심을 보안에서 리스크로 전환하라 (전략가의 역할)

그림 2. CISO의 네 가지 역할



출처: 딜로이트 CISO Labs의 연구결과

그래픽: Deloitte University Press | DUPress.com

보다 전략적인 역할을 취하기 위해 CISO는 대화의 중심(언어뿐 아니라 사고방식까지)을 보안 및 컴플라이언스에서 리스크 전략과 관리로 전환시켜야 한다. CISO는 리스크로 초래될 수 있는 피해와 손실의 부정적 측면을 넘어 경쟁 우위, 사업 성장, 매출 확대 등과 같은 긍정적 효과의 잠재력 측면에서 리스크를 이해할 수 있어야 한다. 예를 들어, 대형 유통업체에서 일하는 한 CISO는 3단계 계층의 리스크 모형을 이용해 이사회에 사이버리스크를 시각화해 보여줬고 가장 치명적인 리스크에 대한 경감 계획을 논의했다. 또한 그는 사업적 혜택의 맥락에서 사업부 리더들이 수용하기로 결정한 리스크와 그 이유에 대해 이사회에 추가 보고했다.

위험을 측정하고 보고하라 (전략가와 고문의 역할)

속담에도 있듯이 무언가를 실행하려면 그 대상을 측정할 수 있어야 한다. 사이버보안에서는, 측정이 되어야 주목을 받을 수 있다. 그러므로 CISO는 사업부 리더가 의미를 도출할 수 있는 정보를 제공하는 측정 기준을 정의할 수 있어야 한다. 첨단기술 대기업의 한 CISO는 과거 복도에서 CEO와 마주쳤을 때 보안팀이 지난달 125,000건의 악성코드 공격을 막았다고 이야기했던 사연을 들려줬다. CEO의 대답은 "그게 당신의 일 아닌가요?"였다. CISO는 자신이 적절한 맥락을 제공하지 않고 불쑥 수치를 말해버렸다는 사실을 깨달았다.

이러한 문제를 피하기 위해 한 대형 금융기관의 CISO는 보안계량지표들의 목록을 만들었다. 여기에는 각 지표마다의 수용범위 상하한 값이 포함된다. 그런 다음 6개월에

사이버리스크의 조직적 특성을 형상화하기 위한 질문

1. 조직에서 가치의 주요 동인은 무엇인가? 그리고 이들은 어떻게 보호되고 있는가?
2. 오늘날 우리가 가장 많이 노출되어 있는 위협과 취약성은 무엇인가?
3. 중요한 자산을 보호하기 위한 기본 역량과 실행중인 실무 방안을 어느 정도까지 갖추고 있는가?
4. 얼마나 효과적으로 사이버 사고를 모니터링하고 감지하고 있는가?
5. 효과적으로 사이버 사고에 대응하고 복구할 수 있는가? 대응 계획을 갖추고 있으며 이를 테스트하고 있는가?
6. 어떠한 측정 지표가 우리가 효과적으로 기업을 보호하고 있다는 사실을 입증해 주는가?

걸쳐 이해관계자들과 함께 각 사업영역별 맞춤 사이버리스크 대시보드를 만들었다. 이를 통해 조직은 리스크 대응 우선순위를 정하고 어느 영역에서 리스크 수용이 가능한 지를 이해할 수 있었다.

세계경제포럼(World Economic Forum: WEF)이 공개한 보고서에 따르면 사이버리스크에 관한 대화는 세 가지 변수를 저울질 한다. 시스템의 취약성, 위협받는 자산의 가치, 공격자의 정교함 수준이 그것이다.[15] 이들 세 가지 요소를 대화에 끌어들이면 사업부 리더들에 미치는 사이버 위협의 상대적인 중요성을 부각시키게 된다. (이러한 대화를 쉽게 풀어 나가기 위해 삽입글 '사이버리스크의 조직적 특성을 형상화하기 위한 질문'을 참고) 더 이상 대화는 컴플라이언스 문제에 국한되지 않는다. 대신에 사업부 리더들은 사업을 방해하는 위협의 비용과 현재 환경에서 발생할 수 있는 보안사고의 가능성을 이해할 수 있다.

리스크 측정지표와 사업의 가장 급박한 문제를 조율할 수 있는 CISO의 의견을 전략적 리더들이 경청할 가능성이 크다. 직관적인 대시보드를 통해 이들 인사이트를 쉽게 소화할 수 있게 만드는 것은 CISO의 중요성을 더욱 강화하는 데 도움을 줄 수 있다.

인재 수요 해결하기

만약 CISO가 보다 전략적인 역할을 담당하길 원한다면 운영 및 기술적 활동을 지원할 보안 관련 인재의 부족과 같은 조직적 문제를 해결해야 할 필요가 있다. 이는 CISO가 자질구레한 일들을 처리하는 데만 신경 쓰게 할 수 있는 핵심 문제다. 최근 수행된 블랙햇(Black Hat) 조사에 따르면 약 73%의 조직들이 보다 숙련된 보안관련 인재를 필요로 하는 것으로 나타났다. 이 결과는 딜로이트 CISO Labs의 설문조사 데이터와 밀접하게 연관되는데 조사에 참여한 CISO의 75% 이상이 자신들의 우선순위 업무를 지원할 숙련된 자원과 효율적인 팀 체계가 부족하다고 언급했다.[16]

조직의 인재풀을 구축하기 위해 CISO는 기존의 기술을 활용하고, 이해관계자들과 더 잘 통합하며, 미래 인재 파이프라인 보강을 계획하는 보안에 특화된 인재 전략의 개발에 초점을 맞춰야 한다.

현재의 인력 강화하기

기업이 채용했거나 현재 CISO 팀에 소속돼 있는 개인들은 조직의 니즈에 부응할 수 있도록 자신들의 기술을 연마

할 필요가 있다. 그 동안 조직들이 취해온 한 가지 방법은 필요한 특정 기술의 확보를 위한 기술기관 및 대학과의 관계 구축으로, 조직의 목적과 목표에 부합하는 대학생들과의 관계 수립과 기술 개발에 초점을 맞춘 인턴십 프로그램을 수립하기도 했다. 전문성 개발을 위한 또 다른 방안은 사이버리스크에 관한 '워 게임(War game)' 훈련에서 찾을 수 있다.[17] 이는 특정한 사이버 취약점에 대한 조직의 준비 수준을 테스트할 뿐 아니라 직원들에게 그러한 사고에 대응할 수 있는 실무 경험을 제공할 수 있도록 고안된 모의 시나리오다.

사업부문과 통합하기

사이버 보안 및 리스크가 아닌 분야에 있어, 광범위한 '내부 협력 네트워크'를 가진 개인이 독자적으로 일하는 개인보다 일반적으로 뛰어난 성과를 보인다는 사실이 수많은 연구를 통해 입증됐다. 이들 연구는 엔지니어링, 연구, 컨설팅과 같은 분야에서 유효한 것으로 검증됐다.[18] 이러한 관점에서 봤을 때 CISO는 사이버리스크 전문가와 사업부 리더 모두의 기술을 향상시키는 보다 높은 차원의 비즈니스 협력에 초점을 맞출 필요가 있다.

CISO는 또한 각 사업부문 내 사이버리스크 챔피언을 지정하거나 사업부서에 부합하는 사이버리스크 담당직원을 배치하는 방식의 통합 모델 개발을 고려할 수 있다. 인적 자원의 통합은 직원들이 보안 문제와 관련해 어디로 찾아가야 할 지 알 수 있도록 돕고, 비즈니스 전략과 관련 사이버리스크 관리 요건에 대한 보안 전문가의 이해와 인식을 촉진할 수 있다. 현실적으로 사이버 보안은 모든 직원들의 우선순위가 되어야 한다. 그리고 CISO의 기능이 조직 내에서 어떤 위치를 점하는지에 상관없이 어디서 긴밀한 관계가 존재할 수 있는지 이해하고, 책임에 대한 혼란을 피하며 통합과 협력을 개선하기 위한 역할을 명확히 규정하는 것이 중요하다.

미래의 사이버리스크 책임자 확보하기

장기적으로, CISO 승계 계획 및 조직 전반에 걸쳐 해당 CISO를 대리할 수 있는 다른 책임자들의 발굴을 고려하는 것이 중요하다. 매니저 직급 이상의 이러한 후보자들을 조기에 파악하고 교차 훈련 시킬 필요가 있으며, 단지 보안 부문에 국한할 것이 아니라 다른 사업부문 전반에 걸쳐 찾아봐야 한다. 최근에 조지 워싱턴 대학교 경영대학원(George Washington University's School of Business)은 학교 내 사이버 및 국토안보 센터(Center for Cyber and Homeland Security)와 협력해 조직의 미래 지도자들을 '글로벌 경제, 혁신, 정책을 추진할 수 있는 심도 있는 지식, 자원, 네트워크'로 무장시켜 차세대의 사이버 도전과제에 맞설 수 있도록 하는 특화된 '사이버 보안 MBA' 프로그램을 마련했다.[19]

이와 같은 훈련은 CISO 후보자들이 지도자 역할을 맡기 전에 사이버리스크 관련 부서 내외에서 신뢰를 더 쌓을 수 있도록 해주고, 보안 전문가는 순전히 기술적, 전술적인 면에만 치중한다는 인식을 변화시키는 데 도움을 줄 수도 있다.

리더십 교육, 관여, 그리고 주인의식

CISO는 어떻게 기업 전반에 걸친 문화적 변화의 독려 및 보안 관련 주인의식 공유에 대한 경영진의 지원과 관여를 확보할 수 있는가?

소통 전략과 계획의 개발

CISO의 소통 계획은 비전과 목표에 직접적으로 부합해야 하며 각 기능 영역 혹은 경영진의 역할에 대해 어떠한 형태의 성공이 이뤄질지 보여줄 수 있어야 한다. 소통은 조직의 모든 영역으로 확장되어야 하며 다른 사업 및 기능과 관련된 메시지 전달과 통합되어야 한다. 의사소통에서 강

이사회에서의 의사소통

사이버리스크는 이사회 임원들이 감독하기 특히 힘들다고 느낄 수 있는 비즈니스 문제다. 보다 적절하고 관련성이 있는 소통을 하기 위한 노력의 일환으로 다음 사항들에 메시지의 초점을 맞추는 것을 고려하라.

- **최우선 사이버리스크.** 현재의 리스크 평가 결과가 특히 현재 비즈니스 상 가장 우선적인 문제와 관련이 있을 때 평가 결과와 그에 대응하는 리스크 경감 및 통제관리 활동에 대해 이야기하라.
- **프로그램의 성숙도.** 위협 환경 및 동종 업체들의 상황과 관련 지어 조직의 성숙도를 설명하라.
- **떠오르는 위협.** 자사 혹은 동종 기업들을 공격하고 있는 주체가 누구며 어떤 교훈을 얻었는지 파악하라. 랜섬웨어(Ransomware)의 확산이나 세간의 이목을 끄는 데이터 침해와 같은 새로운 사건이나 트렌드, 그리고 그들이 조직에 어떤 영향을 미칠 수 있는지 설명하라.
- **감독 및 규제 사항.** 공개된 감독 및 규제 사안에 대한 갱신된 정보를 제공하라.
- **공공 혹은 민간 파트너십.** 산업 단체에 대한 참여와 법 집행기관이나 정보기관과의 협력을 명심하라.

이사회가 고심하는 많은 결정들—신상품, 신시장, 혹은 M&A든 간에—은 기술이나 보안과 직접적인 관련은 없지만 사이버리스크에 대한 중요한 시사점을 가지고 있다. 이사회와 소통할 때 CISO의 가장 중요한 목표는 사전에 이와 같은 문제들의 검토를 적극적으로 지원하는 신뢰할 만한 조언자가 되는 것이다.

조해야 할 점은 조직 내부뿐만 아니라 다른 유사한 기업이나 정부기관에서의 보안 관련 동향이다. 직원들이 이 같은 동향의 영향에 대해 이해할 수 있도록 맞춤화된 방식으로 동향에 대한 토론을 진행해야 한다. 데이터 보안에 대한 직원들의 책임과 관련된 추가적인 업무조언이나 상기는 이런 메세지를 강조하는 데 도움이 된다.

경영진이나 이사회와 같은 최고위 간부들과 소통할 때는 메시지 전달이 핵심을 찌르고 듣는 사람들의 화제에 부합하도록 해야 한다(삽입글 '이사회에서의 의사소통' 참조). 계획은 프레젠테이션이든 소셜 미디어 캠페인이든, 또는 기타 수단이든 리더십과 조직간의 대화를 어떻게 수립해야 하는지를 제시해야 한다. 이는 더 광범위한 문화적 변화를 위한 분위기를 조성하는 중요한 단계다.

리스크와 보안에 대한 새로운 시각을 분명히 하고 정당화하며 또한 직원들을 독려하고 고무해 이를 받아들이도록 하는 것이 목표다. 한 CISO는 자신의 메시지와 이야기를 조직의 간부와 나머지 사람들에게 잘 정리하여 전달하기 위해 자신의 팀에 두 명의 풀타임 언론인을 고용한 적이 있다.[20]

감성적인 연대를 통해 직원들의 주인의식 강화하기

심리학, 행동경제학, 마케팅 분야의 연구들은 이성보다 감정이 인간의 행동을 주도한다는 사실을 반복해서 보여주고 있다. 이성적인 주장만으로는 습관을 깨뜨리기 어렵기 때문에 CISO는 반드시 경영진을 고무해야만 하고, 그 결과 경영진들이 직원들로 하여금 자신의 행동과 관점을 변화시키는 어려운 일을 수행하도록 독려하게 해야 한다.

딜로이트 유니버시티 프레스(Deloitte University Press)에 실린 '방침에 따르기: 정보화 시대에 보안 행동 강화하기(Toeing the line: Improving security behavior in the information age)' 기사는 위험한 관행 혹은 리스크를 내포한 조직 문화를 변화시킬 수 있는 네 가지 행동 요소들에 대해 설명하고 있다.[21]

1. **정책을 통한 학습.** 직원들이 숙지할 정책을 제공하는 것은 자연스러운 첫 번째 단계이다. 이러한 정책은 주창하는 가치를 대변하고자 인위적으로 만들어낸 것들이다. 그러나 집단이 정책에 따르지 않는다면 정책만으로는 충분히 행동을 변화시킬 수 없을 것이다.

2. **멘토링 제공.** 사회적 신호는 사람들이 무엇을 가치 있게 여기고 어떻게 순응해야 하는지 결정하는 데 강

표 1. 전략적 보안 조직을 향한 여정에서 CISO의 역할 단계 요약

도전과제	이를 극복하기 위한 단계
좁은 시야	• 비즈니스에 대한 보다 전체적인 대화를 촉진하기 위해 대화의 중심을 보안에서 리스크로 옮겨라. • 리스크를 부정적인 것으로 분류하는 시각을 버려라. 계산된 리스크는 새로운 사업 기회로 이어질 수 있다.
소통과 협력	• 사이버리스크 전문가와 비즈니스 리더를 포함하는 여러 업무부서를 아우르는 팀을 개발함으로써 사업부문과 통합하라. • 심리학과 행동경제학의 교훈을 통해 인간의 행동과 사고에 직접 전달하는 의사소통을 실현하라. • 프레젠테이션과 소셜 미디어, 경영진의 성공 사례와 같은 수많은 소통 채널을 활용하라.
인재 부족	• 팀의 기술력을 향상시키기 위해 대학 및 전문 조직과의 파트너십을 추구하라. • 시뮬레이션과 게이밍 시나리오를 이용해 당신의 팀이 고위험 사건에 대비할 수 있도록 하라. • 리더십 잠재력을 가진 '비기술' 직원들을 사이버리스크에 정통하도록 훈련시켜라.
보안에 대한 잘못된 인식	• 현재의 리스크 수준을 보여주는 대시보드를 이용하라. • 소통과 이야기를 통해 컴플라이언스와 사이버리스크 관리 사이의 차이를 경영진에게 교육하라.
상충되는 의제	• 사업에 대한 이해도를 높이고 조직의 전략가 및 조언자로서 행동하라. • 경영진 및 이사회와의 관계 형성을 통해 보안 인식을 고취하라. 우선순위가 높은 비즈니스 활동에 부합하는 리스크 측정 지표를 제공하라. • 소통과 이야기를 통해 공유 책임을 촉진하는 감성적 연대를 생성하라.

보안과 리스크에 대한 인식, 사이버리스크에 대한 공유된 주인의식, 사이버리스크에 대한 복구능력을 조성하는 환경의 중요성은 더욱 커질 것이다. 전략적, 기술적 수준을 넘어 더 앞서갈 수 있는 CISO는 이사회, CXO, 각 사업부문 책임자를 포함한 전사의 리더들로부터 신뢰와 지지를 받게 될 것이다.

력한 영향을 끼친다. 새로운 사이버 보안의 문화적 속성을 내재화한 경영진은 사이버 보안을 직접 보고 받고 직원들에게 강력한 예시를 제공한다. 경영진은 자신들의 사이버보안 행동 변화와 관련한 직접적인 경험과 직면했던 도전들을 공유할 때, 더욱 진정성을 가지게 되며 그들의 경험은 다른 직원들이 비슷한 장애를 극복하는 데 도움이 될 수 있다.

3. **단체 학습.** 소통 방법을 개발하는 소비자 마케터의 업무를 본받아라. 예를 들어, 직원들간의 협력을 보다 증진하기 위해 업무환경에서 영향력 있는 사이버 방어법을 강조하는 조직내의 성공사례를 임원이 제시하는 것을 고려할 수 있다.

4. **일상 업무를 통한 학습.** 개별 직원들의 일상적인 책임을 더욱 큰 목표와 조직의 사이버 복구능력에 연결시키는 것은 매일매일의 업무에 의미를 부여할 수 있다. 이는 또한 보다 높은 차원의 헌신과 참여를 이끌어 낼 수 있다. 열정을 불태우는 직원들이 있는 기업은 높은 생산성과 이익을 창출해 내곤 한다.

이들 단계는 CISO가 조언자로서의 역할을 다 하면서 기업 전반에 걸쳐 신뢰를 쌓고 직원들이 스스로 리스크를 적절히 파악하고 경감할 수 있도록 보안 지식, 요건, 데이터에 대한 권한을 부여해주는 업무 환경을 수립하는 데 도움이 될 수 있다.

견인력, 가속도, 전략적 방향 확보하기

기술의 발전과 함께 사이버리스크가 증가하고 진화함에 따라 CISO, 조직 리더, 직원들에 대한 요구도늘어날 것이다. CISO는 사이버 위협에 대한 두려움으로 혁신을 방해하는 대신에 조직을 도와 목표를 달성하는 역할을 하도록 노력해야 한다. 보안과 리스크에 대한 인식, 사이버리스크에 대한 공유된 주인의식, 사이버리스크에 대한 복구능력을 조성하는 환경의 중요성은 더욱 커질 것이다. 전략적, 기술적 수준을 넘어 더 앞서갈 수 있는 CISO는 이사회, CXO, 각 사업부문 책임자를 포함한 전사의 리더들로부터 신뢰와 지지를 받게 될 것이다. 이는 사이버리스크에 대한 인식 문화를 생성하고 유지하기 위한 선도적 노력의 중요한 첫 단계다. 표 1은 전략적 보안조직 구축에 필요한 나머지 단계들을 간추려서 제시한다.

CISO는 리더십 테이블에서 한 자리를 확보하고, 사이버리스크 관리에 대한 공동 책임의식 부여에 기여하며, 조직의 리더와 직원들이 그러한 책임을 다할 수 있는 방법에 대해 지침을 제시함으로써, 전략적 보안 조직을 향한 여정에서 중요한 추진체의 역할을 할 수 있다. **DR**

타린 아구아스(Taryn Aguas)*는 딜로이트 & 투쉬 LLP의 프린시펄로 사이버보안과 기술 리스크 관리를 전문으로 하며 딜로이트 CISO Labs를 이끌고 있다.*

칼리드 카크(Khalid Kark)*는 딜로이트 컨설팅 LLP의 디렉터로 CIO 프로그램에 대한 리서치와 인사이트의 개발을 이끌고 있다.*

모니크 프랑수아(Monique François)*는 딜로이트 컨설팅 LLP 의 매니징 디렉터로 기업이 복잡한 변화를 헤쳐나가도록 조언해온 20년 이상 경력을 지니고 있다.*

Endnotes

1. "Big data, for better or worse: 90% of world's data generated over last two years," *Science Daily*, May 22, 2013, https://www.sciencedaily.com/releases/2013/05/130522085217.htm.
2. Barkly, *2016 cybersecurity confidence report*, http://cdn2.hubspot.net/hubfs/468115/Barkly_Cybersecurity_Confidence_Report.pdf, accessed April 11, 2016.
3. As used in this article, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.
4. The Deloitte CISO Labs are immersive one-day workshops that encourage CISOs to think from a new perspective and develop a plan for success by focusing on the three most important resources a CISO has to manage: time, talent, and stakeholder relationships.
5. Jody R. Westby, *Governance of cybersecurity: 2015 report*, Georgia Tech Information Security Center, October 2, 2015, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/tech-briefs/governance-of-cybersecurity.pdf.
6. Deloitte CISO Labs data, 2015.
7. Frank Dickson and Michael Suby, *The 2015 (ISC)² global information security workforce study*, Frost & Sullivan, 2015, p. 3.
8. Deloitte CISO Labs data, 2015.
9. Ibid.
10. Dickson and Suby, *The 2015 (ISC)² global information security workforce study*, p. 36.
11. Deloitte CISO Labs data, 2015.
12. ThreatTrack Security Inc., *No respect: Chief information security officers misunderstood and underappreciated by their C-level peers*, June–July 2014, https://www.threattracksecurity.com/resources/white-papers/chief-information-security-officers-misunderstood.aspx.
13. Deloitte CISO Labs data, 2015. The "four faces of the CISO" concept is adapted from the framework presented in Ajit Kambil, *Navigating the four faces of a functional C-level executive*, Deloitte University Press, May 28, 2014, http://dupress.com/articles/crossing-chasm/.
14. Adnan Amjad, Mark Nicholson, Christopher Stevenson, and Andrew Douglas, "From security monitoring to cyber risk monitoring: Enabling business-aligned cybersecurity," *Deloitte Review* 19, July 2016, http://dupress.com/articles/future-of-cybersecurity-operations-management.
15. World Economic Forum in collaboration with Deloitte, *Partnering for cyber resilience: Towards the quantification of cyber threats*, January 2015, http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.
16. Black Hat, *2015: Time to rethink enterprise IT security*, July 2015, https://www.blackhat.com/docs/us-15/2015-Black-Hat-Attendee-Survey.pdf; Deloitte CISO Labs data, 2015.
17. Cat Zakrzewski, "Cybersecurity training, military style," *Wall Street Journal*, March 13, 2016, http://www.wsj.com/articles/cybersecurity-training-military-style-1457921566.
18. Jim Guszcza, Josh Bersin, and Jeff Schwartz, "HR for humans: How behavioral economics can shape the human-centered redesign of HR," *Deloitte Review* 18, Deloitte University Press, January 25, 2016, http://dupress.com/articles/behavioral-economics-evidence-based-hr-management/.
19. George Washington University, "World executive MBA with cybersecurity," http://business.gwu.edu/programs/executive-education/world-executive-mba/, accessed April 12, 2016.
20. Deloitte CISO Labs data, 2015.
21. Joe Mariani et al., *Toeing the line: Improving security behavior in the information age*, Deloitte University Press, January 28, 2016, http://dupress.com/articles/improving-security-behavior-in-information-age-behavioral-economics/.