TONE — at the — TOP®

최고경영진, 이사회, 감사위원회에 거버넌스 관련 주제에 대한 간결한 정보를 제공

사이버 회복력과 이사회의 역할

귀사는 다음에 있을 사이버공격에 대비되어 있는가? 대부분의 조직은 앞으로의 사이버 공격을 예상하고 있으며, 2024 시스코 사이버보안(2024 Cisco Cybersecurity Readiness Index)에 따르면 비즈니스 및 사이버보안 리더 중 73%가 사이버 장애로 인해 향후 12~24개월 내에 업무 혼란이 있을 것으로 예측한다.

사이버공격은 민감 데이터의 유출, 운영 중단, 제3자 관계 및 회사 평판의 손상 등 많은 잠재적 결과를 가져온다. IIA의 2025 리스크 인 포커스(2025 Risk in Focus) 보고서에서 내부감사 리더들은 사이버보안에 2위와는 현저한 차이가 있는 최고 리스크 등급을 부여했다. 또한 내부감사가 가장 많은 시간과 노력을 투자하는 분야로 사이버보안을 언급했다.

보고서에 따르면, 사이버보안은 조직이 3년 후에도 직면할 것으로 리더들이 예상하는 최대 리스크로 남아 있으며 디지털 파괴(인공지능 포함)는 과거 설문조사 순위에서 빠르게 상승하여 2위를 차지했다. 보고서는 "AI가 전 세계적으로 사이버보안과 부정행위(fraud) 리스크를 증가시키고 있다"고 말한다. 사이버보안은 AI가 가장 부정적인 영향을 미칠 수 있는 분야로 평가되었다.

공격의 발생 여부가 아니라 언제 발생할지가 관건인 환경에서 사이버 회복력은 기업이 장애를 견뎌내는 데 중요하다. 기업은 사이버공격으로부터 스스로를 보호하기 위해 많은 노력을 기울일 수 있지만, 공격에 대응하고 복원할 준비도 갖춰야 한다.

사이버 회복력이란 "사이버 자원을 이용하거나 사이버 자원에 의해 활성화된 시스템에서 발생하는 악조건, 스트레스, 공격 또는 유출을 예상하고, 견뎌내고, 복구하고, 적응할 수 있는 능력이다. 사이버 회복력의 목적은 사이버 자원에 의존하는 임무나 비즈니스 목표를 경쟁적인 사이버 환경에서 달성할 수 있게 하는 것이다." — 미국 국립표준기술연구소(National Institute of Standards and Technology)

이사회에 대한 새로운 기대

규제당국과 주주들은 사이버보안에 대한 이사회의 책임을 검토하고 이사회 구성원의 조직 취약성 감시에 대해 새로운 기대를 수립하고 있다.

확정된 규칙인 사이버보안 리스크 관리, 전략, 거버넌스 및 사고 공시(Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure)에 따라 미국 증권거래위원회(Securities and Exchange Commission)는 상장 기업에 대한 공시 요건을 제시하며 특히 중대한 사이버보안 사고에 대한 공시와 등록기업이 이러한 리스크를 평가, 식별 및 관리하는 방법에 대한 정기 공시, 그리고 이를 평가하고 관리하는 경영진의 역할에 대해 언급하고 있다. 해당 규칙은 또한 사이버보안 리스크에 대한 이사회의 감시를 공시하도록 요구한다.

맥킨지(McKinsey)의 기사 "이사회: 산업을 위한 사이버보안의 최종 방어선"("Boards of Directors: The Final Cybersecurity Defense for Industrials")에 따르면, 이사회는 감시 역할의 일환으로 임직원이 사이버보안에 대한 엄격한 기준을 수립하도록 해야 한다. 그런 다음 사이버보안 노력을 모니터링하여 목적이 달성되었는지, 사이버보안에 대해 책임지는 부서가 있는지 확인해야 한다. 기사는 "이사회는 이러한 이니셔티브가 계획되고 예산이 배정되도록 하는 최후의 방어선이다"라고 언급한다.

사이버공격은 조직이 평상시처럼 업무를 계속하기 어렵게 만들기 위해 고안되었다. 사이버 회복력은 정보를 얻고 대비하는 것이므로, 위기 발생 시 선택과 우선순위가 명확하다. PwC의 사이버 리스크의 감시: 이사회의 역할(Overseeing Cyber Risk: The Board's Role)에 따르면, 조직의 철저한 대비를 위해 이사회는 경영진이 모의 훈련(Tabletop Exercise)에서 주기적으로 검증하는 위기 관리, 사고 대응 및 재해 복구 계획서가 존재하는지 확인해야 한다. 이러한 훈련은 위기 시에 경영진의 의사결정을 명확히 하기 위해 역할과 책임을 명확히 수립하는 데 중점을 두어야 한다.

많은 이사회가 경영진이 제출한 사이버 스코어카드나 대시보드를 받게 되는데 여기에는 현재의 리스크와 사이버보안 목표에 대한 진행상황이 강조되어 있다. PwC는 이사회 보고서의 일부가 될 수 있는 몇 가지 영역을 지적한다.

- 다개년 전략 계획 및 당해 연도 경영 계획
- 금액 및 인원으로 세분된 사이버보안 자원 할당 내역
- NIST 사이버보안 프레임워크(NIST Cybersecurity Framework)와 같이 인정된 프레임워크를 이용한 성숙도 평가
- 정기 업데이트되는 기간 시스템 목록
- 조직의 주요 사이버 리스크 요약
- 조직에서 경험한 중대한 보안 사고에 대한 검토
- 직원 교육 및 의식 제고 노력에 대한 정보
- 사이버 보험 가입에 대한 정보를 포함하여 조직의 사고 대비 프레임워크에 대한 세부 정보
- 제3자의 사이버리스크 전략에 대한 세부 정보
- 조직의 노력을 동종업체와 비교한 정보
- 관련된 주요 법규의 동향에 대한 세부 정보
- 최근의 사이버공격에서 얻은 교훈

조직을 공격으로부터 보호하는 것도 중요하지만, 이사회는 보호만으로는 조직이 이미 알고 있는 문제만 해결할 수 있다는 점을 기억해야 한다. 안타깝게도 AI를 이용한 신기술로 무장한 혁신적인 사이버 범죄자들은 피해를 입힐 새로운 방법을 끊임없이 찾아낸다. 결과적으로, "사이버 리스크를 적절히 완화하기 위해 리더는 회사가 계속 운영될 수 있도록 신속하게 대응하고 복구할 수 있는 견실한 계획을 갖춰야 한다"고 MIT의 뉴스 기사는 보도한다. "이제 기업의 이사회도 사이버보안에 대한 책임이 있다"("Now Corporate Boards Have Responsibility for Cybersecurity, Too.")

세계내부감사인협회 소개

세계내부감사인협회(IIA)는 전 세계 230,000명 이상의 회원에게 서비스를 제공하고 전 세계적으로 185,000명 이상에게 공인내부감사사(CIA) 인증을 수여한 비영리 국제 전문가 협회이다. 1941년에 설립된 IIA는 표준, 인증, 교육, 연구 및 실무적 지침 분야에서 내부감사직종의 리더로 전 세계적으로 인정받고 있다. 자세한 내용은 **theiia.org.** 참조.

IIA 주소

1035 Greenwood Blvd.Suite 401
Lake Mary, FL 32746 USA

무료 구독

theiia.org/Tone을 방문하여 무료 구독을 신청하세요.

독자 피드백

질문이나 의견은 다음 이메일로 보내주세요:
Tone@theiia.org.

번역: 이은주(CIA)

- 삼성전자 내부감사팀 근무
- SC제일은행 내부감사부 근무
- 한국씨티은행 내부감사부 근무
- 2003~한국외국어대학교 통번역대학원 영어과 졸업
- 한-영 통역사, 제조, 금융, IT, 법률 등 다양한 분야의 한-영 통역사 활동

내부감사: 신뢰할 수 있는 사이버보안 파트너

이사회는 내부감사부서가 사이버보안 노력에 기여할 수 있는 가치를 이해해야 한다. 내부감사는 사이버보안 전략, 거버넌스, 통제에 대해 고유하고 객관적이며 독립적인 검증 및 자문 서비스를 제공한다. 앞서 언급된 PwC의 기사는 "많은 회사가 내부감사인을 통해 회복력과 대응을 포함하여 사이버 프로세스와 통제장치를 점검한다"고 언급한다.

내부감사부서는 사이버 장애 복구 및 대응 감사를 포함하여 여러 방법으로 사이버 회복력 제고에 기여할 수 있다. 작년의 리스크 인 포커스 보고서는 내부감사인이 추가할 수 있는 가치 중 일부를 설명하는데, 이 리스트는 오늘날에도 유효하다:

- 이사회를 포함한 비즈니스의 핵심 부분에서 의식, 지식 및 스킬 수준을 평가하여 사이버 방어 대응이 적절하고 최신인지 확인한다.
- 최고정보보안책임자(CISO), 최고정보책임자(CIO) 및 이사회 간의 보고선을 평가하여 리스크와 권고사항을 명확하게 전달하고 필요시 최상위로 에스컬레이션할 수 있는지 확인한다.
- 시뮬레이션 테스트 피싱 캠페인과 기타 의식 제고 활동의 빈도, 적시성, 효과성과 직원 참여 수준, 직원이 교육 및 후속조치 프로세스에 얼마나 잘 통합되어 있는지 여부를 평가한다.
- 시나리오 실행을 통해 이사회에 거버넌스 책임에 대한 교육을 제공하고 경감 프로세스가 완전하고 효과적인지 테스트한다.
- IIA의 3선 모델(Three Lines Model)에 따라 내부 통제 환경의 효과성과 제1선 및 제2선에 통제장치가 제대로 내포되어 있는지 평가하며 직원이 혼란스럽거나 거슬린다고 생각하여 무시, 망각, 회피할 가능성이 있는 관행에 특히 주의를 기울인다.
- 조직의 거버넌스 구조가 3선 간의 협업을 얼마나 원활히 기능하게 하는지 평가한다.
- 조직이 사이버보안 및 기술 규제의 글로벌 동향을 충실히 모니터링하는지 여부와 미래의 요건 충족을 위해 내부 통제가 유연하게 변경될 수 있는지 확인한다.

진화하고 확대되는 리스크

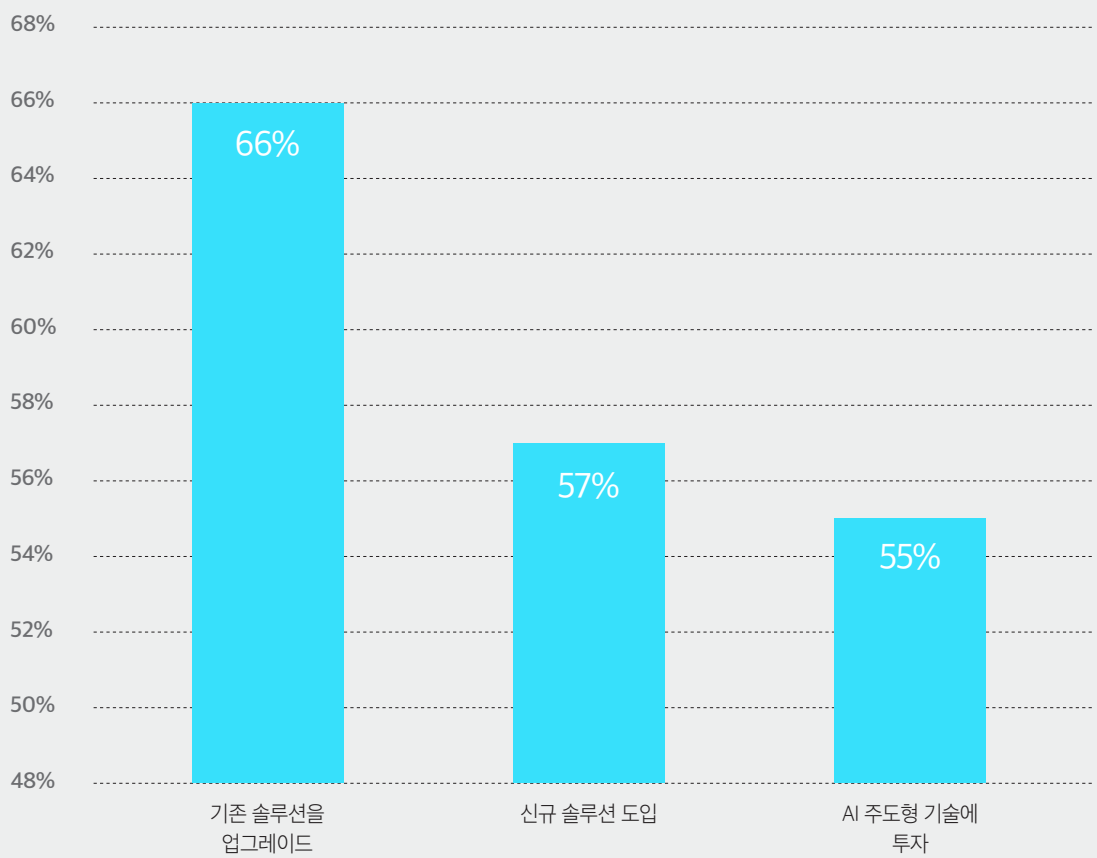
신기술의 빠른 발전에 따라, 사이버공격을 보다 쉽게 자행할 수 있게 해주는 많은 새로운 툴이 등장하고 있다. 연방 정부의 사이버보안 및 인프라 보안국(Cybersecurity and Infrastructure Security Agency) 책임자인 젠 이스털리(Jen Easterly)에 따르면, AI와 유사 도구는 사이버보안 노력을 향상시킬 수 있지만 피싱과 스팸, 협박과 테러, 허위정보와 선거 개입을 간단하게 만들 수도 있다. 그녀는 또한 생성형 AI가 사이버 공격자에게 새로운 기회를 제공하고 기술적 정교성이 낮은 사이버범죄자도 큰 혼란을 일으킬 수 있게 해 준다고 지적한다.

이사회 구성원은 사이버공격을 예방하고 공격 발생 후 대응의 민첩성을 평가하는 최선의 방법에 대한 귀중한 정보와 조언을 얻기 위해 내부감사부서에 의지해야 한다. 내부감사인은 조직이 공격으로부터 가장 성공적으로 복구하는 데 도움이 되는 통제 환경 및 식별된 리스크에 대한 독립적인 평가를 제공할 수 있다.

이사진을 위한 질문

- 다른 조직의 대처 방법을 포함하여, 새로운 사이버 위협을 어떻게 모니터링하고 있는가?
- 조직은 자체 사이버 회복력을 어떻게 측정하고 평가하는가?
- 공격에 대한 대비와 잠재적 대응을 조정하기 위해 이러한 정보를 어떻게 활용하고 있는가?
- 재해 복구 계획은 무엇인가? 과거에 얼마나 원활하게 작동했는가? 이러한 경험에서 무엇을 배웠는가?
- 어떤 부서가 사이버 회복력 전략에 대해 직접적인 책임을 지는가?
- 전체 임직원이 사이버 회복력의 필요성과 이를 위해 자신이 할 수 있는 역할을 이해하고 있는가?

기업은 사이버보안을 어떻게 강화하고 있는가?



출처: *2024 Cisco Cybersecurity Readiness Index.*