TONE — at the — TOP®

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

사이버 위협의 경감

사이버보안은 현대의 리스크 환경에서 영구적인 위협이 되었으며 이사회가 다면적이고 지속적으로 진화하는 사이버 보안 위협을 적절히 감시해야 한다는 압력은 점증하고 있다. NACD 이사회 설문조사(Board Survey)[1]에서 이사회 이사의 총 70%가 사이버보안을 "전략적, 전사적 리스크"라고 말했다. 사이버보안에는 광범위한 문제가 포함되는데 개인정보 보호, 랜섬웨어, 맬웨어, DoS 또는 피싱 공격, 부적절한 사이버보안 정책, 장애 대응 및 복구 계획 등을 포함하여 모두 중요한 사안이다.

조직은 또한 침해 사실에 대해 보고할 것을 요구하는 새로운 규정에 직면해 있다. 예를 들어, 중요 인프라에 대한 사이버 장애 보고법(Cyber Incident Reporting for Critical Infrastructure Act)[2]은 연방 사이버 보안 및 인프라 보안 기관(Cybersecurity and Infrastructure Security Agency)이 사이버 공격 중에 피해자에게 지원을 제공하고, 동향을 파악하고, 다른 잠재적 피해자와 정보를 공유할 수 있도록 보고할 것을 요구한다. 증권거래위원회(Securities and Exchange Commission)는 상장 기업의 사이버보안 리스크 관리, 전략, 거버넌스 및 장애 보고와 관련된 공시를 표준화하는 규정[3]도 제안했다.

조직에 독립적이고 객관적인 검증 및 조언을 제공하는 내부감사는 이사회가 사이버 리스크를 다루는 데 강력한 자원이 될 수 있다. PwC 보고서[4]에 따르면 "많은 기업이 내부감사를 활용하여 복원력 및 대응을 포함한 사이버 프로세스 및 통제를 검토하고 있다."

보안 강화의 단계

이사회가 직면한 사이버보안 위협과 관련하여, 내부감사가

기여할 수 있는 영역이 여럿 존재한다.

리스크의 인식. 사이버 위협은 기업의 리스크 순위에서 상위권으로 이동했다. "사이버공격의 점증하는 정교함과 다양성은 조직의 브랜드와 평판을 지속적으로 파괴하여 종종 막대한 재정적 영향을 초래한다"고 세계내부감사인협회(IIA)의 온리스크(OnRisk)2022[5]는 전한다. 이사진, 최고경영진 및 최고감사책임자(CAE)와의 인터뷰를 기반으로 한 온리스크 보고서는 사이버보안을 올해 최고의 리스크로 식별했다.

불행히도 일부 기업의 리더들은 이러한 위협을 완전히 인식하지 못할 수 있다. 온리스크 보고서에서 특히 우려되는 점은 CAE, 이사진 및 최고경영진이 사이버보안에 부여한 리스크 관련성 간의 차이였다. CAE의 97%가 사이버보안을 조직과 매우 관련성이 높은 리스크로 평가했지만(7점 척도에서 6~7로 평가) 이사진은 87%만이, 최고경영진은 77%만이 관련성이 매우 높다고 평가했다.

CAE들이 부여한 높은 관련성 등급은 사이버보안 문제에 대한 높은 인식 수준을 나타낸다. 조직에 대한 내부감사의 총체적인 지식을 감안할 때 이는 놀라운 일이 아니다. 이사회는 재무 및 컴플라이언스 리스크를 넘어 리스크 검증을 활용하고 개선하기 위해, 내부감사를 통해 사이버보안 문제를 설명

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

세계내부감사인협회 소개

세계내부감사인협회 (IIA)는
전세계 170여개국에서
20만 명 이상의 회원들을 위해 봉사하는
감사직 종사자들의 단체이다.
IIA는 내부 감사직의 최고 수호단체이자
세계적으로 인정받는 표준의 주창자로서,
주요 연구와 교육을 실시하고 있다.

IIA 주소

1035 Greenwood Blvd. Suite 149 Lake Mary, FL 32746 USA

무료 구독

www.theiia.org/tone을 방문하여 무료 구독을 신청하세요.

독자 피드백

질문 및 의견은 다음 주소로 보내주세요
Tone@theiia.org

하고 잠재적 영향을 정량화할 수 있다. 리스크 커버리지의 실패를 강조하고, 새로운 리스크를 모니터링하고, 사이버보안을 위해 신 기술과 도구를 최대한 활용하는 것이 이에 포함될 수 있다.

3선 모델(Three Lines Model)의 가치 활용. IIA의 3선 모델[6]을 통해 조직은 목표 달성을 지원하는 데 가장 효과적이고, 사이버보안을 포함하여 강력한 거버넌스 및 리스크 관리를 촉진하는 구조와 프로세스를 식별할 수 있다. 3선 모델은 다음의 주체가 수행하는 주요 역할을 파악한다.

≫ 이해당사자에 대해 조직 감시의 책무를 지니는 지배기구(governing body).
≫ 조직의 목표를 달성하기 위해 행동하는 경영진.
≫ 목표 달성에 대해 독립적이고 객관적인 검증을 제공하는 내부감사.

연구에 따르면 3선 간의 협력은 사이버보안 리스크 관리의 효율성에 긍정적인 영향을 미친다. ISACA 저널[7]의 기사에 따르면 내부감사는 가치있는 검증을 제공하고 위협과 취약성을 식별할 수 있다. 여기에는 사이버보안의 동향 및 이해당사자의 기대치 식별, 초기 사이버 리스크 평가 수행과 효과적인 감사 기준의 정의가 포함될 수 있다. 지적사항을 보고하고 조언을 제공하는 가운데 "감사인은 [이사회]가 감시를 수행하는 데 크게 도움이 될 수 있다"라고 기사는 말한다.

내부감사의 정보 최적화 보장. 많은 조직에서 감사위원회는 사이버 위협을 포함한 모든 유형의 리스크를 다룰 책임이 있다.[8] 그러나 일부 조직에서는 여러 가지 이유로 사이버 이슈를 다른 위원회에 배정한다. 조직의 규모와 업종, 직면한 위협에 따라 별도의 사이버보안 위원회, 리스크 위원회, 기술 위원회, 지명 및 거버넌스 위원회 또는 다른 위원회가 사이버 이슈를 감시할 수도 있다. 이사회는 감사위원회가 사이버 이슈까지 다룰 여력이 없거나, 무엇보다도 사이버 이슈를 감시하는 데 필요한 전문성이 없다고 판단할 수 있다.

일반적으로 내부감사는 감사위원회에 보고한다. 내부감사가 사이버보안을 담당하는 위원회에 보고하지 않는 경우, 조직은 사이버 리스크와 관련된 귀중한 권고사항 및 검증을 놓칠 수 있다. 어느 위원회가 되었건, 사이버 이슈의 감시 주체와 보고 관계를 유지할 때 내부감사의 통찰력이 제대로 이해되고 조치로 실행될 수 있다.

숨겨진 위협 식별. 사이버보안 노력에 피해를 주고, 잠재적으로 재난을 야기할 수 있는 미미한 수준의 감시 때문에 이사회는 놀랄 지 모른다. 내부감사는 조직의 감사 계획이 간과된 위협을 얼마나 잘 식별하고 새로운 리스크를 발견할 수 있는지 이사회가 결정하는 데 도움이 되는 통찰력을 제공할 수 있다. 딜로이트(Deloitte) 보고서[9]에 따르면 경영진이 일반적으로 과소평가하는 사이버 위협 중 일부는 다음과 같다.

≫시스템에 여전히 로그인할 수 있는 퇴사자의 범위 및 회사 시스템에 접속할 수 있는 외부 공급업체의 수. 두 경우 모두 기업은 얼마나 많은 미확인 및 외부 사용자가 무단으로 접속할 수 있는지 거의 알지 못할 수 있다.

이사진을 위한 질문

≫우리 조직은 사이버보안과 관련된 전략 기획 시 내부감사의 통찰력 및 조언을 최대한 활용하고 있는가?

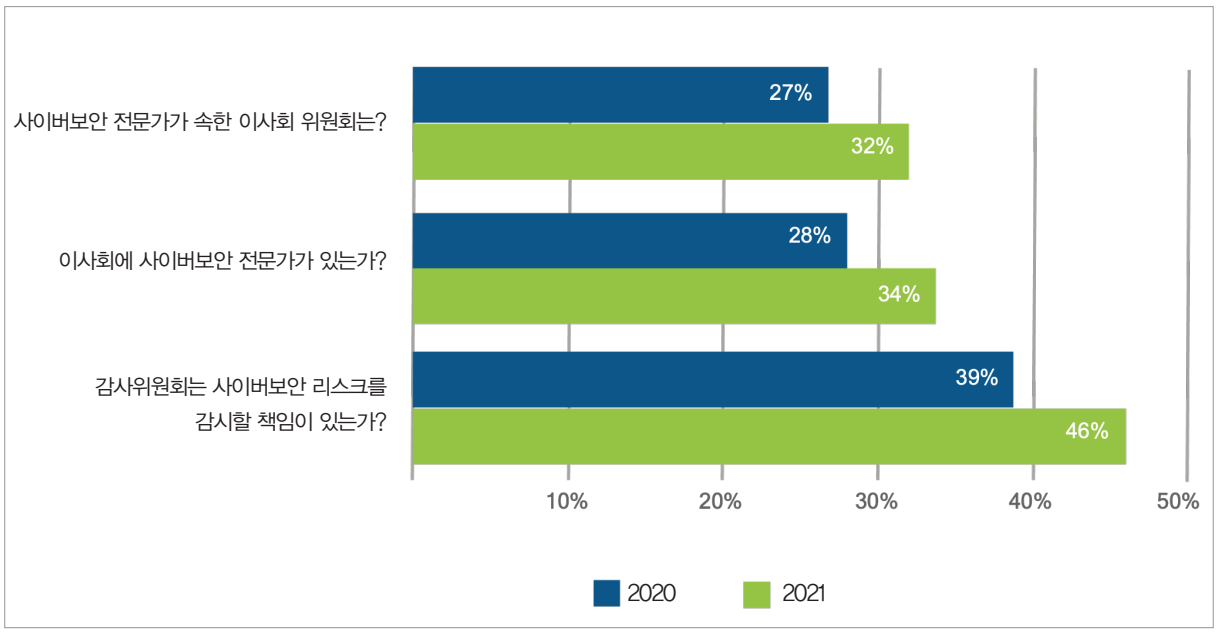
≫사이버보안을 위해 적절한 인력을 배치하고 자금을 지원했는가?

≫조직은 사이버보안과 관련하여 재정적 측면에서 리스크 허용 범위를 정의했는가?

≫특정 위원회가 사이버보안 감시를 담당하는가?

≫이사진은 사이버 침해가 발생한 경우 적용되는 회사의 절차를 이해하고 있으며 사이버 침해 발생 시 자신의 역할이 무엇인지 알고 있는가?

〈S&P 500 기업 중 다음을 공시하는 기업의 비중〉



출처 : 2021 Audit Committee Transparency Barometer, Center for Audit Quality, 2021년 11월.

≫기업이 사용하는 클라우드 계정의 수. 클라우드 이용률이 높을수록 사이버 공격의 기회도 늘어날 수 있다. 딜로이트 보고서는 인프라 복원력, 서비스 중단시간, 성능 및 기타 지표는 물론 준법 상태와 독립적인 통제 평가에 대해 클라우드 서비스 제공업체에게 문의할 것을 조직에 권고한다.

≫조직에서 경험한 사이버 침해의 실제 총 건수

회사에서 사이버공격을 거의 경험하지 못했다면, 직관적으로 이것은 사고가 감지되지 않고 있다는 경고 신호일 수 있다. 내부감사 부서는 이러한 유형의 경고 신호가 모니터링되고 있는지 확인하는 데 도움을 줄 수 있다.

비즈니스 파트너 간의 문제 해결. 가트너(Gartner)는 2025년까지 조직의 60%가 제3자 거래 및 비즈니스 계약 시 사이버보안 리스크를 고려할 것으로 예측한다.[10] 오늘날에는 보안 및 리스크 관리 리더의 23%만이 제3자 사이버보안 노출을 실시간으로 모니터링하며, 검사 범위도 전체 공급망이 아닌 직속 공급업체와 납품업체로 제한된다.

온리스크 2022에 따르면 CAE, 최고경영진 및 이사진의 의견은 다시 한번 일치하지 않았다. CAE는 이 영역에서 조직의 역량을 37%로 평가했지만 임원진은 53%, 이사진은 57%로 평가했다. 이 영역에 대한 CAE의 신뢰도가 낮은 이유는 이 리스크에 부여한

관련성 등급이 더 높은데서 비롯된 것으로 해석될 수 있다. CAE는 이사진보다 17 포인트 더 높은 리스크 관련성을 부여했다(77% 대 60%).

어떤 경우든 이사회는 이 분야에서 내부감사의 의견 및 경험을 최대한 활용할 수 있도록 해야 한다. 내부감사는 조직 전체 부서와 함께 일하기 때문에, 특정 공급업체나 전체 공급망에서 관련되었거나 식별된 사이버 리스크를 이사회에 알릴 수 있다. 조직의 비즈니스 파트너가 사이버보안 보호 장치의 신뢰성에 대한 확신을 원할 때 내부감사는 그들이 찾는 데이터 및 검증을 제공할 수 있다.

자원의 최적화

벅찬 사이버보안 이슈와 씨름하는 가운데 조직은 모든 기존 리소스를 최적화해야 한다. 이사회는 효율성 및 효과성을 제고할 수 있는 기회를 식별함으로써 내부감사인이 조직 전체에 가져올 수 있는 가치를 이해하고 활용하여 회사의 보안 수준을 제고시킬 수 있다

미주

1. Principles for Board Governance of Cyber Risk, National Association of Corporate Directors, Internet Security Alliance, and World Economic Forum, In Collaboration with PwC, March 2021.

2. https://www.cisa.gov/circia

3. https://www.sec.gov/rules/proposed/2022/33-11038.pdf

4. Overseeing Cyber Risk : The Board's Role, PwC,January 2022.

5. OnRisk 2022 : A Guide to Understanding, Aligning, and Optimizing Risk,The Institute of Internal Auditors, 2021.

6. The IIA's Three Lines Model: An Update of the Three Lines of Defense, The Institute of Internal Auditors,July 2020.

7. "How Effective Is Your Cybersecurity Audit?," Matej Drašček, et al., ISACA Journal,June 1, 2022.

8. "Cybersecurity: An Evolving Governance Challenge," Harvard Law School Forum on Corporate Governance, Phyllis Sumner, et al., March 15, 2020.

9. Internal Audit: Risks and Opportunities for 2022, Deloitte, 2021.

10. Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem, Sam Olyaei, et al., Gartner,January 24, 2022.

간단 여론 조사

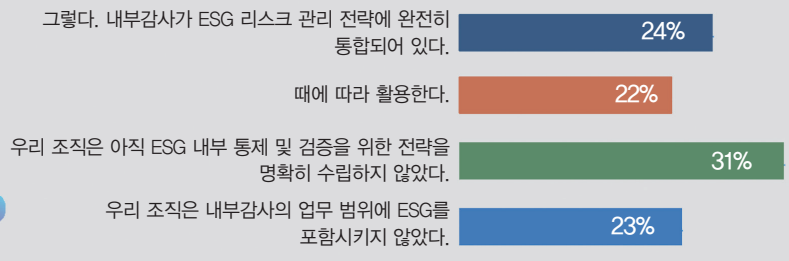
귀하의 조직에서 사이버보안 리스크 관리를 감시하는 이사회 위원회는 누구인가?

- ■ 감사위원회
- ■ 사이버보안 위원회
- ■ 기술 위원회
- ■ 지명 및 거버넌스 위원회
- ■ 기타

www.theiia.org/Tone 사이트를 방문하여 응답하고, 다른 사람들의 응답도 확인하세요.

간단 설문 조사 결과

귀하의 조직은 ESG 검증을 위해 내부감사를 활용하는가?



출처 : Tone at the Top June 2022 설문조사