TONE at the TOP®

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

제106호 | 2021년 8월

사이버보안이라는 괴물에 맞서

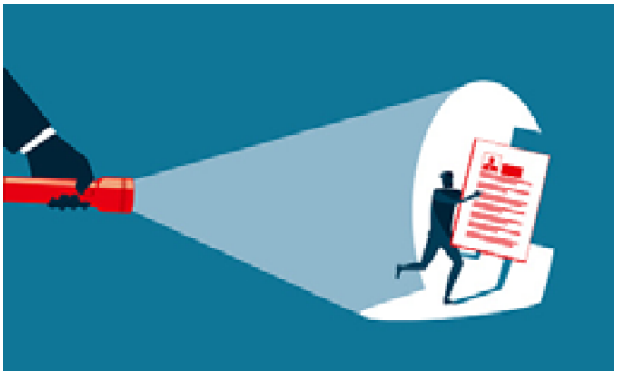
사이버 리스크는 전(全) 산업에서 조직의 규모와 무관하게 영향을 미치며, 이제 일상이 된 것으로 보인다. 2021년 글로벌 이사회와 임원진을 대상으로 실시한 설문조사에서 사이버 위협은 10대 리스크의 하나로 부상했고, 응답자들은 2030년에도 사이버 위협이 주요 리스크일 것으로 예상했다. 실제로 글로벌 사이버범죄는 매년 15%씩 증가할 것으로 예상되며, 그 피해액은 2025년까지 연간 10조5천억 달러에 달할 것으로 사이버시큐리티 벤처스 (Cybersecurity Ventures)는 예측하고 있다. 한 사이버 리서치 회사는 이를 "사상 최대의 경제적 부의 이전(移轉)"이라고 부른다.

사이버보안 이벤트는 랜섬웨어, 원격 근무 자원에 대한 공격, 공급망 공격, 피싱 또는 다른 범죄의 형태를 취할 수 있다. 이러한 이벤트는 기업의 업무를 마비시킬 수 있고, 기업 가치를 크게 증발시킬 수 있고, 기업 이미지를 훼손하거나 채무를 발생시킬 수 있다. 데이터 유출의 비용은 크며, 증가일로에 있다. IBM 데이터에 따르면 2021년 평균은 424만 달러로, 1년만에 거의 10% 증가했다.

설상가상으로 COVID-19 팬데믹은 아직 완전히 파악되거나 해소되지 않은 새로운 취약성을 탄생시켰다.

위험의 관리

이처럼 많은 위험 속에서, 사이버 리스크에 대한 감시를 강화하기 위해 이사회가 취할 수 있는 조치가 많이 있다. 그리고 이 프로세스에서 내부감사는 중요한 파트너가 될 수 있다. 내부감사팀은 조직의 사이버보안 전문가와 협력하며



조직의 계획이 의도한 대로 실행되고 있으며 임무에 적절하다는 객관적 검증을 제공할 수 있다. "내부감사팀은 이사회에 대형 리스크 노출이나 그에 대한 방심이 존재하는지 말해줄 수 있다"고 딜로이트 리스크 및 재무 자문 (Deloitte Risk and Financial Advisory)에서 은퇴한 시니어 파트너이자 CIA 샌디 펀드맨 (Sandy Pundmann)은 말했다.

사이버 리스크의 해결을 돕는 이사회의 전략은 다양하다. 펀드맨과 다른 이들은 이사회가 조직의 사이버리스크 프로파일에 대한 날카로운 이해를 유지하고 감시자로서의 역할을 적극 수용하고 강점, 약점 및 취약성에 대해 분명하게 이해하고 있음을 보장하기 위해 건강한 회의론을 펼칠 것을 권고하고 있다.

감시 역할을 정립하고 정기 업데이트 일정을 수립. 오늘날 자격을 갖춘 이사회 멤버가 리더인 사이버보안 전담 위원회를 설치한 이사회의 비율은 10% 미만이지만, 2025년까지 40%로 증가할 것으로 가트너 (Gartner, Inc.) 설문조사는 예상한다. 이러한 전망은 펜데믹 동안의 디지털비즈니스 확산, 재택 근무 도입 및 그로 인해 생긴 잠재적 리스크에 기인한 것일수도 있다.

번역자: 이은주

삼성전자 내부감사팀 근무,

SC제일은행 내부감사부 근무, 한국씨티은행 내부감사부 근무, 2003~한국외국어대학교 통번역대학원 영어과 졸업, 한-영 통역자-제주, 금융, IT, 법률 등 다양한 분야의 한-영 통역사활동

세계내부감사인협회(IIA) 소개

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

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.

현재 사이버보안 감시의 책임은 경영진 및 여러 위원회에 분산되어 있는 경우가 빈번하기 때문에 책임 소재를 명확히 밝히기 어려울 수 있다고 펀드맨은 말했다. 감시의 책임은 한 위원회에 전적으로 부여하되, 이 위원회는 모든 회의에서 이 주제를 논의해야 한다고 그녀는 덧붙였다. 또한 사이버보안은 최소 연 2회 전원 이사회 안건으로 상정되어야 한다.

위협의 수준을 인지. 사이버보안은 IT 이슈 그 이상이다. "장애 발생 전이건 발생한 도중이건, [사이버보안을] 최고정보책임자 (CIO)와 기술 팀에만 맡기면 안된다"고 맥킨지 (McKinsey) 팟캐스트에서 영국 국립 사이버 보안 센터 (National Cyber Security Centre)의 전임 디렉터 존 노블 (John Noble)은 말했다. "리더는 편리, 보안 및 비용 사이의 갈등을 관리하는 방법을 결정해야 하며, 이사회가 프로세스에 이의를 제기하고 검증해야 하는 것은 바로 이 영역이다."

보다 철저한 분석. 이사회는 조직이 정기적으로 사이버 리스크 평가결과를 점검 및 보완하고 있는지 알아야 한다. 내부감사팀에게 최초의 평가 또는 프로젝트, 공격, 침투 감사를 실시해 달라고 요청하는 경우가 많은데 이것은 첫걸음일 뿐이라고 펀드맨은 경고한다.
기업은 사이버 이벤트를 예방 및 적발하고 그에 대응하기 위해 다면적인 전략을 필요로 한다. 이러한 노력은 공격의 발생과 그에 맞서 취하는 조치의 효과성, 장애 및 대응의 모니터링 방식, 전사적 대응의 역학관계와 성공여부를 파악하기 위해 회사가 취하는 상시적 조치의 평가를 포함해야 한다. 전체적인 전략은 해당 위원회에서 평가할 수 있지만 그에 대한 논의는 전원 이사회에서 이루어져야 한다고 그녀는 말했다.

딜로이트 간행물에 언급되었듯이, 사이버리스크에 대항하는 제1선은 사업 부문과 IT로 구성되어 있고 이들은 일상적인 결정 및 운영상의 리스크를 다룬다. 조직의 제2선은 정보 및 테크놀로지 리스크를 관리하는 리더십으로, 거버넌스와 감시를 담당한다. 내부감사부서가 보안 조치 및 그 성과의 독립적인 점검을 실시하며 제3선의 역할을 하는 경우가 증가하고 있다.

이러한 리스크의 차이점이 무엇인지 이해. 조직과 그 이사회는 리스크에 익숙하지만 사이버보안은 두 가지 점에서 다르다. 첫째, 사이버보안은 매우 특화되어 있고 위협은 계속 변화하여 이사진 대부분의 전문성을 넘어서고 있다. 둘째, 대부분의 조직은 인터넷을 사용하고 있기 때문에 리스크와 그 영향이 다면적이고 복잡하다. "인터넷 접속은 기업의 가치 제공에 있어 필수적이며, 인터넷 접속에 의존하는 모든 거래는 태생적으로 안전하지 못하다"고 사이버 리스크 디렉터 네트워크 (Cyber Risk Director Network)의 패널 토론에서 한 참가자는 말했다. "이는 이사회가 여태 다뤄온 리스크의 어떤 측면에도 해당되지 않는 점이다."

이사진을 위한 질문

- 이사회는 조직의 사이버보안 위협과 사이버 리스크를 해결 및 관리하기 위해 취해지는 조치에 대해 얼마나 자주 업데이트를 얻고 있는가?
- 조직은 사이버보안을 IT 우려사항에 국한시키지 않고 전사적 리스크 이슈로 다루고 있는가?
- 이사회는 사이버 리스크를 적극적으로 모니터링하고 있는가? 아니면, 달리 언급되지 않는 한 다 잘 되고 있다고 가정하는가?
- 이사회는 사이버보안 전담 위원회를 두고 있는가? 아니면 감사 위원회와 같은 다른 위원회가 사이버보안 감시 책임을 맡고 있는가?

현실성 추구. *내부감사, 다른 경영진 또는 외부인이 실시할 수 있는* 모의 훈련을 통해 이사회와 경영진은 사이버 공격을 시뮬레이션하여 조직이 어떻게 대응하는지, 투자자는 어떻게 통보받는지, 고객이나 비즈니스 파트너는 어떤 영향을 받는지 감독할 수 있다 (펀드맨은 최대한 실제 상황 같은 모의 훈련을 위해 CIO 및 CEO에게만 이 상황이 시뮬레이션임을 알려달라고 요청한 위원회와 일한 적도 있었다). 조직이 대응을 평가하고 나면, 이사회는 시행되었거나 진행 중인 변경사항에 대해 업데이트를 얻을 수 있다.

또다른 귀중한 훈련에서는 내부감사가 중심적인 역할을 할 수 있다: 성숙도 모델 시각화는 비전문가의 평범한 표현으로 사이버 리스크에 대해 기업차원의 개요를 제공하고 조직의 현주소와 나아가야할 방향을 비교한다. 모든 리스크를 모니터링하고 그에 대응하는 것은 불가능하기 때문에, 이러한 훈련을 통해 가장 중요한 타겟을 정하고 조직이 해당 영역에서 예방 및 적발을 강화할 수 있는지 명확히 하는데 도움이 될 수 있다고 펀드맨은 말했다.

리스크에게 기습당하지 않기. 테크놀로지의 수용이 확대됨에 따라, 새롭게 등장하는 낯선 테크놀로지에 수반되는 리스크도 증가하고 있다. 새로운 ERP 시스템 조차도 간과해서는 안될 보안상의 도전과제를 제기할 수 있다고 펀드맨은 언급했다. 많은 기업이 새로운 시스템에 문제가 생기고 나서야 이슈 대처 계획을 수립하는 우를 범한다. "사이버 및 통제 전략을 위해 보안 계획을 수립했는지 처음부터 확인해야 한다"고 그녀는 말했다.

인수합병에 관련된 조직도 새로운 취약성에 노출될 수 있다. "기업 인수 중이라면, 비즈니스 결합 과정에서 어떤 리스크를 무릅쓰고 있는지 자문해보라"고 그녀는 조언했다. 공급망이나 다른 외부 업체와 협력하는 기업도 해당 업체로부터 기인한 리스크에 노출될 수 있다. 또한 조직은 준법 감시 영역에서 사이버보안 공시에 대한 미국 증권거래위원회 (Securities and Exchange Commission) 요건과 같은 유관 규정을 알고 있어야 한다.

내부감사 자원의 활용

사이버 위협은 벅찬 도전과제일 수도 있지만 내부감사는 조직의 리스크에 대해 고유하고 독립적인 시각과 그를 다루는 최선의 방법을 제공할 수 있다. 사이버보안 이슈의 모니터링에 적극적이고 내부감사가 제공할 수 있는 가치를 전적으로 활용하는 이사회는 사이버보안 리스크를 효과적으로 해결하기에 더 나은 입장에 있어야 한다.

귀사의 이사회가 놓치고 있는 것은?

60%의 조직에 이사회 멤버이거나 임원급인 사이버보안 수장이 없다.

59%의 조직이 사이버보안과 영업 부문의 관계는 잘해야 중립적이며, 불신하거나 관계가 아예 존재하지 않는다고 말한다.

20%의 이사회가 이사회에 제출된 사이버보안 리스크 및 경감 대책이 조직을 주요 사이버 공격으로부터 보호할 수 있다고 확신한다.

36%의 조직이 신사업 이니셔티브의 기획 단계에서부터 사이버보안을 고려한다고 말한다.

출처: *"6대 리스크: 조직의 사이버 회복력에 대한 이사회의 착각을 드러내는 핵심 질문 (The Risky Six: Key Questions to Expose Gaps in Board Understanding of Organizational Cyber Resiliency)"* IIA Global 및 EY, 2021년 3월 30일.

1 *Executive Perspectives on Top Risks for 2021 and 2030*, Protiviti and NC State University'sERM Initiative, 2021.

2 *"Cybercrime to Cost the World $10.5 Trillion Annually by 2025,"* Steve Morgan, *Cybercrime Magazine*, November 13, 2020.

3 *Cost of a Data Breach Report*, IBM, 2021.

4 *"Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025,"* Gartner press release, January 28, 2021.

5 *"Boards and Cybersecurity,"* McKinsey and Company podcast, February 2, 2021.

6 *"Cybersecurity and the Role ofInernal Audit: An Urgent Call to Action,"* Sandy Pundmann, Deloitte, 2017.

7 *"Cybersecurity: An Evolving Governance Challenge,"* Harvard Law School Forum onCorporate Governance, March 15, 2020.

8 *"Commission Statement and Guidance on Public Company Cybersecurity Disclosures,"* Release Nos. 33-10459; 34-82746, Securities and Exchange Commission, February 26, 2018.

간단 여론 조사

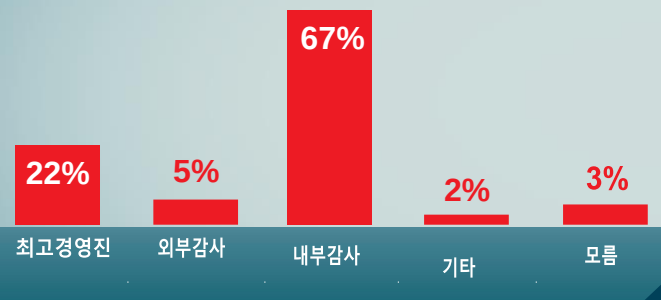
귀사의 이사회에는 사이버보안 전문성을 갖춘 멤버가 있습니까?

- ❑ 있다
- ❑ 없다
- ❑ 모르겠다

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

간단 여론 조사 결과

리스크 관리 및 내부통제의 효과성 검증을 위해 이사회는 일차적으로 누구에게 의지합니까?



출처: Tone at the Top June 2021년 설문조사