Deloitte.

2022년 6월

Center for Board Effectiveness

On the board's agenda | US
A new chapter in cyber

Escalating risk, regulatory focus can drive board oversight of governance

An SEC proposal issued in March 2022 to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting has sparked increased discussions about cyber risk in many corporate boardrooms. At many companies, boards are asking questions about what measures they should consider taking that would help to enhance governance and improve risk management, which may also help prepare the company to meet likely new requirements.

Even before the proposal was issued, oversight of cybersecurity risk had become an increasing area of focus for boards. A survey by Deloitte and the Center for Audit Quality of 246 audit committee members published in January 2022 found that two-thirds of participants with oversight responsibility for cybersecurity expected to spend more time on the topic in the coming year.[1] In addition, 62% identified cybersecurity as one of the company's top risks to focus on in 2022.[2]

1. Deloitte and Center for Audit Quality, "*Audit Committee Practices Report: Common Threads Across Audit Committees*," January 2022.
2. Ibid.

On the board's agenda | US
사이버보안의 새로운 장

리스크 고조 및 규제집중에 대응하는 이사회의 거버넌스 감독

지난 3월에 발표된 사이버보안 리스크관리, 전략, 거버넌스 및 사고 보고와 관련된 공시 강화 및 표준화를 위한 SEC 제안으로 인해 많은 기업의 이사회에서 사이버 리스크에 대한 논의가 증가했습니다. 많은 기업의 이사회는 거버넌스를 강화하고 리스크관리를 개선하며 기업이 새로운 요구사항 등을 충족할 수 있도록 준비하기 위해 어떠한 조치를 취해야 하는지 질문하고 있습니다.

사이버보안 리스크 감독은 본 제안이 발표되기 전에도 이사회의 관심이 증대되는 분야가 되었습니다. 지난 1월 딜로이트와 감사품질센터(Center for Audit Quality)에서 감사위원 246명을 대상으로 진행한 서베이에 의하면 사이버보안에 대한 감독 책임이 있는 응답자의 3분의 2가 내년에도 이 주제에 더 많은 시간을 할애할 것으로 예상했습니다. 더불어, 응답자 중 62%는 사이버보안을 2022년에 집중해야 할 기업의 최대 리스크 중 하나로 꼽았습니다.

If adopted as proposed, the SEC's new rules would require prompt reporting of material cybersecurity incidents and disclosures in periodic filings focused on:

- Policies and procedures to identify and manage cybersecurity risks
- Management's role in implementing cybersecurity policies and procedures
- Corporate directors' cybersecurity expertise, if any, and the board's oversight of cybersecurity risk
- Updates about previously reported material cybersecurity incidents

The SEC received nearly 150 comment letters on the proposal and is expected to issue final requirements later in 2022.

Leading up to the proposal, cyber incidents have increased in recent years, both in frequency and magnitude. Cyberthreats have become more complex as threat actors use more sophisticated techniques. At the onset of the pandemic, the cyberattack surface expanded significantly, and risk persists for many companies that are maintaining hybrid work arrangements. Companies face threats related to the theft of information, disruption of functions, ransomware demands, destruction of hardware and software, and corruption of data.

The financial risks that can stem from loss of confidentiality, integrity, critical business processes, and information assets can be substantial. In addition to direct costs, operational impacts such as an inability to produce goods and services, system downtime, missed opportunities, and an outsized focus on incident or breach management impacts can be significant. A company's brand, one of its greatest assets, can be damaged significantly from the loss of customer trust that can occur with cyber incidents.

These and other impacts compound pressures within the cyberthreat landscape, making active board oversight essential to cyber risk management. These pressures can increase the need for more strategic dialogue among management and directors to help improve understanding of risk.

Revisit, intensify focus on governance

The importance of the board's role in promoting a cyber-focused mindset and a cyber-conscious culture throughout the organization cannot be overstated. The board's oversight role is a fundamental aspect of governance, which includes defined strategies, policies, and procedures to mitigate cyber risk. Many companies could benefit from an increased focus on cyber risk governance, with or without new disclosure requirements.

Boards can consider several measures to promote this increased focus, beginning with a cyber risk assessment, by business area, that includes the company's readiness for a cyber incident, the response plan, and the recovery plan. Evaluation of the organization's cyber incident response plan is also critical at the board level, with a focus on the controls surrounding business functions and what steps will be taken in the event of an incident.

Cyber expertise on the board

The SEC's recent cyber disclosure proposal says that cybersecurity is among the top priorities for many boards and that cyber incidents and other cyber risks are considered among the biggest threats for many companies.[3] "Accordingly, investors may find disclosure of whether any board members have cybersecurity expertise to be important as they consider their investment in the registrant as well as their votes on the election of directors of the registrant," the SEC wrote in its proposing release.[4]

This aspect of the SEC proposal has promoted discussion in some boardrooms about whether boards should have someone with cyber expertise as a member. Some corporate directors regard this aspect of the disclosure proposal as analogous to the current requirement for boards to disclose if they have a financial expert on their audit committee, and if they do not, to explain why. The audit committee financial expert disclosure requirement has prompted many boards to have financial experts on the audit committee.

Boards can consider a variety of aspects of their operating model and culture to evaluate whether the company would benefit from having someone with cyber expertise on the board, including the extent to which the company believes investors will expect cyber expertise at the board level. Boards can also evaluate the extent to which they could benefit from increased education at the board level to promote an increased level of tech-savviness in the boardroom. Corporate directors can tap into several resources that may help them increase their understanding of cybersecurity issues. These may include:

- Participation in ongoing organizational cyber risk governance awareness programs and board education programs
- Presentations at board meetings by internal and external cyber risk experts
- Industry forums and resources offered by professional associations
- Interaction with peers serving on other boards
- Reviews of cyber incident responses at other companies to understand the lessons learned
- Cyber wargames and simulations
- Directors' colleges, which are executive-level programs at some universities intended for board directors and C-suite leaders

3. Securities and Exchange Commission, "*Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*," March 9, 2022.
4. Ibid.

본 제안이 채택될 경우, SEC가 발표한 새로운 규정은 다음의 영역에서 정기보고서에 중요한 사이버보안 사건 및 공시를 신속하게 보고하도록 요구할 것입니다.

- 사이버보안 리스크를 식별하고 관리하기 위한 규정 및 절차
- 사이버보안 규정 및 절차 실행에서 경영진의 역할
- (기업 이사진이 사이버보안에 대한 전문지식을 보유한 경우) 이사회의 사이버보안 리스크 감독
- 이전에 보고된 중요한 사이버보안 사고에서의 업데이트 사항

SEC는 이 제안에 대해 약 150건의 의견서를 받았고 올 해 말에 최종 요구사항을 발표할 예정입니다.

제안에 앞서, 최근 수 년 간 사이버 사고의 빈도와 규모가 증가하였습니다. 사이버위협은 위협 행위자들이 더욱 정교한 기술을 사용함에 따라 더욱 복잡해졌습니다. 팬데믹 발발 이후 사이버공격의 범위가 유의하게 확장되었고 하이브리드 업무 방식을 유지하는 많은 기업들에 대한 리스크 또한 지속되고 있습니다. 기업들은 정보 탈취, 기능 중단, 랜섬웨어 수요, 하드웨어 및 소프트웨어 파손, 데이터 손상 등의 위협에 직면해 있습니다.

기밀성, 무결성, 중대한 비즈니스 프로세스, 정보자산의 손실에서 발생할 수 있는 재무적인 리스크는 상당할 수 있습니다. 직접비용과 더불어 제품 및 서비스 생산 불능, 시스템 다운타임, 기회 상실, 사고 또는 침해 관리에 대한 과도한 집중과 같은 운영상의 영향이 상당할 수 있습니다. 기업의 가장 큰 자산 중 하나인 브랜드는 사이버 사고로 고객의 신뢰를 잃을 때 크게 손상될 수 있습니다.

이러한 영향은 이러한 영향과 기타 영향은 사이버위협 환경 내 압력을 가하므로 사이버 리스크관리에 있어 적극적인 이사회 감독은 필수적입니다. 이러한 압박은 리스크에 대한 이해도를 높이는 데 도움이 되는 경영진과 이사진 간에 보다 전략적인 대화의 필요성을 증가시킬 수 있습니다.

거버넌스에 대한 집중 강화 및 재논의

조직 전체에 사이버 중심 사고방식과 사이버에 민감한 문화를 촉진하는 이사회 역할의 중요성은 아무리 강조해도 지나치지 않습니다. 이사회의 감독 역할은 사이버 리스크를 완화하기 위해 정의된 전략, 규정, 절차를 포함하는 거버넌스의 근본적인 측면입니다. 많은 기업들은 새로운 공시 요구사항의 유무와 관계없이 사이버 리스크 거버넌스에 대한 집중도를 높임으로써 이익을 볼 수 있을 것입니다.

이사회는 사이버 사고에 대한 회사의 준비, 대응 및 복구계획을 포함하여, 사업영역별 사이버 리스크 평가 등 이러한 관심 향상을 촉진하기 위해 몇 가지 조치 등을 고려할 수 있습니다. 조직의 사이버 사고 대응 계획에 대한 평가도 이사회 차원에서 매우 중요한데, 사업 기능을 둘러싼 통제와 사고 발생 시 어떤 조치를 취할 것인지에 초점을 맞추고 있습니다.

이사회의 사이버보안 전문성

최근 SEC 사이버 공시 제안에 의하면 사이버보안은 많은 이사회의 최우선 과제 중 하나이며 사이버 사고 및 기타 사이버 리스크는 많은 기업들의 가장 큰 위협으로 간주됩니다. SEC는 제안 발표문을 통해 다음과 같이 밝혔습니다. "따라서 투자자들은 공시 내용을 기반으로 이사회 내 사이버보안 전문성을 갖춘 사외이사가 존재하는지 뿐만 아니라 사외이사 선출 시에도 중요하게 고려할 수 있습니다".

이러한 SEC 제안은 이사회 내 사이버 전문가의 필요성에 대한 논의를 촉진했습니다. 일부 이사진은 이러한 공시 제안이 감사위원회에 재무전문가가 존재하는지 여부와 그렇지 않은 경우 이사회가 그 사유를 설명하도록 하는 현행 요구사항과 유사하다고 보고 있습니다. 감사위원회 내 재무전문가 공시 요구사항으로 인해 많은 이사회가 감사위원회에 재무전문가를 보유하게 되었습니다.

이사회는 투자자들이 이사회 수준에서 사이버 전문성을 기대한다고 믿는 정도를 포함하여, 회사가 이사회에 사이버 전문가를 보유하는 것으로부터 이익을 얻을 수 있는지 여부를 평가하기 위해 운영모델과 문화의 다양한 측면을 고려할 수 있습니다. 또한 이사회는 이사회 차원에서 교육을 강화하여 이사회의 기술지식 수준을 향상시킬 수 있는 정도를 평가할 수 있습니다. 사이버보안에 대한 이해를 돕기 위해 이사회는 다양한 자원을 참고할 수 있습니다. 여기에는 다음의 사항이 포함될 수 있습니다.

- 진행중인 조직의 사이버 리스크 거버넌스 인식 프로그램 및 이사회 교육 프로그램에 참여
- 내부 및 외부 사이버 리스크 전문가가 진행하는 이사회 회의 시 발표
- 전문 협회에서 제공하는 산업 포럼 및 자원
- 타 기업 이사회 동료들의 교류
- 타 기업의 사고 대응사례 검토를 통한 교훈 획득
- 사이버 가상 훈련 및 시뮬레이션
- 디렉터즈 칼리지 등 일부 대학에서 이사회 및 C-레벨 경영진을 대상으로 진행하는 임원급 관리자 양성 프로그램

The board can also set an expectation that the incident response plan has been practiced through scenario planning or wargaming exercises to improve the company's ability to respond and recover in the event of an attack. The teams for such a review should include senior management from each line of business and corporate function.

In many organizations, budgets for security are typically given lower priority than budgets for other IT or business priorities, often rendering companies that take this approach unprepared to deal with risks and attacks. An annual review of cybersecurity budgets by the board or a designated committee, such as the audit committee or a technology committee, can promote an increased focus on the importance of adequately resourcing the business to manage and mitigate cyber risk.

The board can also review top-level policies on cyber risk to create a culture of awareness and accountability. Companies often enhance their security position when they promote a culture of cyber risk consciousness as part of the overall enterprise risk management structure.

External reviews of cyber risk programs, including the governance structure for cyber risk and the strategy and implementation of mitigation controls, can also give the board an improved understanding of the company's level of resilience.

Boards can also request and review high-level reports on risk assessments at third parties—such as vendors and suppliers in cloud, mobile, hosting, and software-as-a-service arrangements—to confirm that those organizations are complying with the company's cyber risk program and standards.

The National Association of Corporate Directors (NACD) suggests that boards consider five cybersecurity principles to improve their oversight of cyber risk.[5] These principles are:

1. Boards should understand and approach cybersecurity as a risk management issue for the entire enterprise and not just a technology or IT issue. Cybersecurity may have begun as primarily a technology-centric risk, but it has evolved to become a multifaceted business issue. The ability to manage cyber risk is integral to every aspect of business operations.
2. Boards should understand the legal aspects of cyber risks that are relevant to the company's own facts and circumstances. In addition to the business impacts of a breach, companies and directors may also face legal consequences that boards should consider as they set strategy and define risk appetite.
3. Boards should have appropriate access to cybersecurity expertise and discuss cyber risk management regularly in board meetings. Boards should expect cyber risks to be communicated to the board frequently, with adequate discussion about the company's threat landscape and risk mitigation strategies. Boards can seek input from both internal and external experts.
4. Boards should set an expectation for management to establish an enterprise-wide risk management framework that is adequately resourced. The board can ask questions to confirm that the framework is implemented across the organization at all levels and that it had adequate staffing and budget.
5. Boards should discuss identified risks with management, including risk prioritization, appetite, and mitigation strategies. This discussion may include a review of options to transfer risks that cannot be practically mitigated using cyber risk insurance.

The benefits of a framework approach

Boards can evaluate the extent to which the organization's cyber risk strategy aligns with a commonly accepted framework, such as the National Institute of Standards and Technology (NIST) cybersecurity framework.[6] A framework approach guides how companies can assess and improve their ability to prevent, detect, and respond to cyber incidents.

A framework also provides a common language that enables companies—boards, management, and other critical stakeholders—to develop a shared understanding of cyber risks, and it enables a means for benchmarking the company's approach against those of other companies. Under the NIST framework, the strategy would focus on five critical functions.

5. National Association of Corporate Directors, "*NACD Director's Handbook on Cyber-Risk Oversight*," February 24, 2020.
6. National Institute of Standards and Technology, "*Framework for improving critical infrastructure cybersecurity version 1.1*," April 16, 2018.

이사회는 또한 공격 발생 시 회사의 대응 및 복구역량 향상을 위해 시나리오 계획 또는 전쟁게임 연습을 통해 사고 대응 계획을 실행하도록 할 수 있습니다. 검토 수행팀에는 각 사업부 및 기능별 고위 경영진이 포함되어야 합니다.

많은 조직에서 보안 예산은 일반적으로 다른 IT 또는 사업부에 비해 낮은 우선순위가 부여되므로, 기업들이 리스크 및 공격에 대처할 준비가 되어 있지 않은 경우가 많습니다. 감사위원회 및 기술위원회와 같은 지정된 위원회나 이사회에서 매년 사이버 보안 예산을 검토한다면, 사이버 리스크를 관리하고 완화하기 위한 사업의 적절한 자원 조달의 중요성을 강조할 수 있습니다.

또한 이사회는 사이버 리스크에 대한 최고 수준의 규정을 검토하여 인식 및 책임해명성의 문화를 조성할 수 있습니다. 기업은 전사적 리스크 관리 구조의 일부로서 사이버 리스크 인식 문화를 장려할 때 보안을 강화하는 경우가 많습니다.

이사회는 사이버 리스크 프로그램(사이버 리스크에 대한 거버넌스 구조와 경감 통제 전략 및 구현을 포함)에 대한 외부 검토를 통해 기업의 복원력 수준을 이해할 수 있습니다.

또한 이사회는 클라우드, 모바일, 호스팅 및 서비스형 소프트웨어(SaaS) 계약의 공급업체 및 제3자 리스크 평가에 대한 높은 수준의 보고서를 요청하고 검토하여 해당 조직이 회사의 사이버 리스크 프로그램 및 기준을 준수하고 있는지 확인할 수 있습니다.

미국기업이사협회(The National Association of Corporate Directors; 이하 NACD)는 이사회가 사이버 리스크에 대한 감독을 개선하기 위해 다음과 같은 5가지 사이버 보안 원칙을 고려할 것을 제안합니다.

1. 이사회는 사이버 보안을 단순한 기술 혹은 IT 문제가 아닌 기업 전체의 리스크 관리 문제로 이해하고 접근해야 합니다. 사이버 보안은 주로 기술 중심의 리스크에서 시작되었을 수 있으나, 그것은 다면적인 사업상의 문제로 발전했습니다. 사이버 리스크를 관리하는 능력은 비즈니스 운영의 모든 측면에서 필수적입니다.
2. 이사회는 기업이 직면한 상황과 관련된 사이버 리스크의 법적 측면을 이해해야 합니다. 위반으로 인한 사업상의 영향 외에도, 기업과 이사회는 전략을 수립하고 리스크 선호도를 정의할 때 고려해야 하는 법적 결과에 직면할 수도 있습니다.
3. 이사회는 사이버 보안 전문지식에 대한 적절한 접근권한을 보유해야 하며 회의에서 정기적으로 사이버 리스크관리에 대해 논의해야 합니다. 이사회는 기업의 위협 범위 및 리스크 완화 전략에 대한 적절한 논의를 통해 사이버 리스크가 이사회에서 자주 다뤄지도록 해야 합니다. 또한, 이사회는 내부 및 외부 전문가로부터 자문을 구할 수 있습니다.
4. 이사회는 경영진이 적절한 자원을 갖춘 전사적 리스크관리 프레임워크를 수립할 수 있도록 기대치를 설정해야 합니다. 이사회는 모든 수준에서 조직 전체에 걸쳐 프레임워크가 구현되고 있으며, 적절한 인력 및 예산이 확보되어 있는지를 확인하기 위해 질문할 수 있습니다.
5. 이사회는 리스크 우선순위 지정, 선호도 및 완화전략을 포함하여 식별된 리스크에 대해 경영진과 논의해야 합니다. 이러한 논의에서 사이버 리스크 보험을 사용하여 실질적으로 완화될 수 없는 리스크를 이전하기 위한 선택지를 검토할 수 있습니다.

프레임워크 접근 방식의 이점

이사회는 조직의 사이버 리스크 전략이 미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)의 사이버 보안 프레임워크와 같이 일반적으로 수용되는 프레임워크와 일치하는 정도를 평가할 수 있습니다. 프레임워크 접근 방식은 기업이 사이버 사고를 예방, 탐지 및 대응하는 능력을 평가하고 개선할 수 있는 방법을 안내합니다.

또한 프레임워크는 기업(이사회, 경영진 및 기타 주요 이해관계자)이 사이버 리스크에 대한 공유된 이해를 개발할 수 있는 공통 언어를 제공하며, 타기업의 접근 방식에 자사 접근 방식을 벤치마킹할 수 있는 수단을 제공합니다. NIST 프레임워크에 따르면, 전략은 5가지 중요한 기능에 초점을 맞춥니다.

- **Identify.** An effective approach begins with identifying cybersecurity risk to systems, people, assets, data, and capabilities. This might include a focus on critical assets of the company and the degree of exposure in the environment, threats and threat actors, and possible business impacts. It could also include an understanding of regulatory requirements, governance, risk assessments (including risks arising from third parties), and risk management strategy.
- **Protect.** Appropriate safeguards to limit or contain potential impact of a cyber incident can be established to protect critical infrastructure. Here, the organization would focus on developing a cyber risk management framework with appropriate controls and asset management tactics that would be integrated into the overall ERM and crisis management programs to provide mobile and endpoint security.
- **Detect.** It's not always immediately evident that a breach has occurred. Companies need to define how they will identify the occurrence of a cyber incident. Metrics for monitoring cyber key performance indicators and controls testing can help detect incidents. Security information and event management technologies as well as audits of third parties are also helpful.
- **Respond.** Companies need to define what actions they will take to effectively minimize the impact or negative effects of a cyber incident. Crisis response planning is critical, as is practicing the response through exercises such as scenario planning or wargaming, to promote resilience. Companies can also consider when and how to engage local, national, and global law enforcement resources.
- **Recover.** Timely recovery from a cyber incident and restoration of capabilities or services that were impaired is critical. Companies should understand leading practices at peer companies in their industry for activating crisis response plans and promoting technical resilience.

Leading practices for boards that are highly effective in overseeing cyber risk begin with driving cyber awareness with a strong tone at the top. Proactive boards often participate in organizational awareness programs and demonstrate due diligence, ownership, and effective governance of cyber risk.

These boards hold regular board and committee briefs to understand the threat landscape, the business-critical risks, and the metrics that describe the state of the control environment and mitigation efforts. Metrics can be developed with respect to many aspects of cyber risk management and mitigation, such as overdue security assessments, third-party incidents and recovery testing, overdue access reviews, deficient password requirements, asset threats, and many more.

Leading practices for highly effective boards also often include evaluation of the impact of an incident and the company's existing cyber incident response plan with a focus on the controls surrounding business functions and what steps will be taken in the event of an incident. These boards often review policies and the company's cyber risk framework to create a culture of awareness and accountability, and they meet with the CISO and CIO or other appropriate members of management to discuss cybersecurity risk, cyber talent, control activities, and improvement initiatives.

Questions for the board to consider asking:

Boards can ask management many questions about the company's approach to cyber risk management, but the list of relevant questions is growing and becoming more specific over time. In addition to many common questions boards can ask related to risk assessments, threat intelligence, monitoring and mitigation strategies, talent, culture, oversight, reporting, and metrics, boards can consider some newer questions that may spark discussion on emerging issues. Such questions might include:

1. What is the company's approach to access management throughout the business? Who is responsible for determining access in each of the company's functional areas? Which function is requesting and granting the highest number of exceptions?
2. What is the approach to incident response in the event of a ransomware attack? What is the recovery time for the company's most important business operations? How has the company prioritized business operations based on possible impact? Has the response plan been practiced throughout the company up to the C-suite level?
3. When was the most recent cyber risk assessment performed, and what has changed since that time?
4. To what extent has the risk assessment considered risks related to operational technology, not just information technology?
5. To what extent does cyber risk governance mitigate risks related to third parties, contracts, and the potential for peripheral devices?
6. What is the cyber assessment process for mergers and acquisitions? How has the company considered cyber risk with respect to integrating an acquired business?
7. What is the company's cyber risk mitigation strategy, and how robust is the review of the strategy?

In addition, boards observing leading practices often conduct ongoing board education programs focused on enhancing the understanding of cyber risk and mitigation strategies. They request high-level reports on third-party risk assessments and ask questions about requirements for vendors and suppliers.

Like all risks that organizations face, cyber risk requires established and mature governance, oversight by the board, and inclusion into the overall enterprise risk management program. When the board works with management, each fulfilling its unique role, each can complement the other to drive an effective cyber-conscious culture, resulting in a high level of resilience to cyberthreats.

- **식별.** 효과적인 접근 방식은 시스템, 인력, 자산, 데이터 및 기능에 대한 사이버 보안 리스크를 식별하는 것에서 시작됩니다. 이는 회사의 중요한 자산과 환경 노출의 정도, 위협 및 위협 요인, 기업에 미칠 수 있는 영향에 주력하는 것이 될 수 있습니다. 또한 규제 요구사항, 거버넌스, 리스크 평가(제3자로부터 발생하는 리스크 포함) 및 리스크 관리 전략에 대한 이해도 포함될 수 있습니다.
- **보호.** 중요한 인프라를 보호하기 위해 사이버 사고의 잠재적 영향을 제한하거나 억제하기 위한 적절한 안전장치를 설정할 수 있습니다. 여기서 조직은 모바일 및 엔드포인트 보안을 제공하기 위해 전체 ERM 및 위기 관리 프로그램에 통합되는 적절한 통제 및 자산 관리 전술을 갖춘 사이버 리스크 관리 프레임워크를 개발하는 데 중점을 둘 것입니다.
- **탐지.** 위반 사실을 항상 즉시 알아차릴 수 있는 것은 아닙니다. 기업은 사이버 사고의 발생을 식별하는 방법을 정의해야 합니다. 사이버 핵심 성능 지표 및 통제 테스트를 모니터링하기 위한 지표는 사고를 탐지하는 데 도움이 될 수 있습니다. 보안 정보 및 사고 관리 기술 뿐만 아니라 제3자에 대한 감사도 도움이 됩니다.
- **대응.** 기업은 사이버 사고의 영향이나 부정적인 영향을 효과적으로 최소화하기 위해 어떤 조치를 취할 것인지 정의해야 합니다. 위기 대응계획은 복원력 증진을 위해 시나리오 계획이나 가상훈련 등을 통해 대응을 연습하는 것만큼 중요합니다. 또한 기업은 현지, 국가 및 글로벌 법 집행 자원을 언제 어떻게 활용할 것인지도 고려할 수 있습니다.
- **복원.** 사이버 사고 발생 시 적시에 복구하고 손상된 기능 및 서비스를 복원하는 것은 중요합니다. 기업은 위기 대응계획을 활성화하고 기술적 복원력을 촉진하기 위해 업계 내 동종기업의 선도사례를 이해해야 합니다.

사이버 리스크 감독에 능숙한 이사회를 위한 선도사례는 사이버 인식에 대한 경영진의 의지에서 시작됩니다. 선제적인 이사회는 종종 기업 인식 프로그램에 참여하여 사이버 리스크에 대한 실사, 소유권 및 효과적인 거버넌스를 보여줍니다.

이러한 사전예방적인 이사회는 위협환경, 사업에 치명적인 리스크와, 통제환경 및 경감 노력을 보여주는 지표에 대해 파악하기 위해 정기적인 이사회 및 위원회 브리핑을 개최합니다. 그러한 지표는 지연된 보안평가, 제3자 사고 및 복구 테스트, 지연된 접근검토, 암호 요구사항 부족, 자산위협 등 사이버 리스크 관리 및 완화와 관련하여 개발할 수 있습니다.

매우 효과적인 이사회를 위한 선도적인 관행에는 사건의 영향 평가와 사업 기능을 둘러싼 통제와 사고 발생 시 조치에 초점을 맞춘 회사의 기존 사이버 사고 대응계획도 포함됩니다. 정책 및 회사의 사이버 리스크 프레임워크를 검토하여 인식 및 책임해명성의 문화를 조성하고, CISO 및 CIO 또는 기타 적절한 경영진과 만나 사이버 보안 리스크, 사이버 인재, 통제 활동 및 개선 이니셔티브에 대해 논의합니다.

이사회에서 고려해야 할 질문은 다음과 같습니다

이사회는 사이버보안 리스크관리에 대한 회사의 접근 방식에 대해 경영진에게 많은 질문을 할 수 있지만, 관련 질문들은 시간이 지남에 따라 점점 커지며 구체화되고 있습니다. 이사회는 리스크평가, 위협인텔리전스, 모니터링 및 완화 전략, 인재, 문화, 감독, 보고 및 지표와 관련된 다양한 일반적인 질문 외에도 새로운 문제에 대한 논의를 촉발할 수 있는 새로운 질문을 고려할 수 있습니다. 이러한 질문에는 다음 사항들이 포함될 수 있습니다.

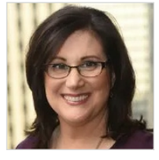
1. 사업 전반에 걸쳐 접근관리에 대한 회사의 접근방식은 무엇입니까? 회사의 각 기능 영역에서 접근 권한을 결정하는 책임은 누구에게 있습니까? 예외상황을 가장 많이 요청 및 부여하는 기능은 무엇입니까?
2. 랜섬웨어 공격 시 사고 대응방법은 무엇입니까? 회사에게 있어 가장 중요한 사업 운영의 복구 시간은 얼마나 걸립니까? 회사는 가능한 영향을 기반으로 사업 운영의 우선순위를 어떻게 정했습니까? 대응계획은 C-레벨 경영진의 수준까지 전사적으로 실행되었습니까?
3. 가장 최근의 사이버보안 리스크 평가는 언제 수행되었고, 그 이후 무엇이 변화되었습니까?
4. 리스크 평가는 정보기술 뿐만 아니라 운영기술과 관련된 리스크를 어느 정도까지 고려했습니까?
5. 사이버보안 리스크 거버넌스가 제3자, 계약 및 주변 장치에서 잠재적으로 발생할 수 있는 것들과 관련된 리스크를 어느 정도까지 완화합니까?
6. M&A에 대한 사이버보안 평가 프로세스는 무엇입니까? 회사가 인수한 사업을 통합하는 데 있어 사이버 리스크를 어떻게 고려했습니까?
7. 회사의 사이버보안 리스크 완화 전략은 무엇이며, 그 전략의 검토는 얼마나 강력합니까?

또한 선도적인 관행을 따르는 이사회는 사이버 리스크 및 완화 전략에 대한 이해를 높이는 데 중점을 둔 지속적인 이사회 교육 프로그램을 수행하는 경우가 많습니다. 이러한 이사회는 종종 제3자 리스크 평가에 대해 높은 수준의 보고서를 요청하며 공급업체와 공급업체의 요구사항에 대해 질문합니다.

조직이 직면하는 모든 리스크와 마찬가지로 사이버 리스크에는 확립되고 성숙한 거버넌스, 이사회의 감독 및 전체 기업 리스크관리 프로그램이 포함되어야 합니다. 이사회가 경영진과 협력하여 각각 고유한 역할을 수행할 경우, 서로 보완하여 효과적인 사이버에 민감한 문화를 주도할 수 있으므로 사이버 위협에 대한 높은 수준의 복원력을 얻을 수 있습니다.

On the board's agenda | US

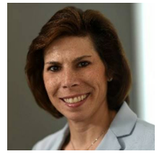
저자



Mary Galligan
Managing Director
Deloitte & Touche LLP
mgalligan@deloitte.com

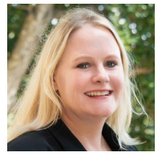
Carey Oven
National Managing Partner
Center for Board Effectiveness
Chief Talent Officer, Risk & Financial Advisory
Deloitte & Touche LLP
coven@deloitte.com

문의



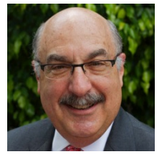
Maureen Bujno
Managing Director and
Audit & Assurance Governance Leader
Center for Board Effectiveness
Deloitte & Touche LLP
mbujno@deloitte.com

Audrey Hitchings
Managing Director
Executive Networking
Deloitte Services LP
ahitchings@deloitte.com



Krista Parsons
Managing Director
Center for Board Effectiveness
Deloitte & Touche LLP
kparsons@deloitte.com

Caroline Schoenecker
Experience Director
Center for Board Effectiveness
Deloitte LLP
cschoenecker@deloitte.com



Bob Lamm
Independent Senior Advisor
Center for Board Effectiveness
Deloitte LLP
rlamm@deloitte.com

기업지배기구발전센터 Contact

김한석 센터장
Partner / Audit & Assurance,
Center for Corporate Governance Leader

김학범 파트너
Partner / Risk Advisory

황현지 사원
Staff / Center for Corporate Governance

Tel: +82 2 6138 6815
E-mail: hyunjihwang@deloitte.com

정 현 파트너
Partner / Audit & Assurance

오정훈 파트너
Partner / Audit & Assurance