Deloitte.

사이버 리스크 평가

이사회와 최고 경영진을 위한 핵심적인 질문

Risk powers performance

서언 – 리스크가 성과를 주도하는 시대 (Risk powers performance)

리스크는 전통적으로 최소화하거나 회피해야 할 것으로 간주되었고, 많은 기업들이 가치를 보존하기 위해 엄청난 노력을 기울여 왔습니다. 하지만 딜로이트는 리스크가 기회를 창출할 수 있고, 따라서 올바른 방법으로 관리한다면 리스크는 사업의 성과를 견인하는 고유한 역할을 할 수 있다고 믿습니다.

사이버 리스크를 예로 들어봅시다. 테크놀로지의 발전과 세계화는 사이버 리스크를 만들어내는 동인이지만, 동시에 경쟁우위를 확보하기 위한 핵심 원천이기도 합니다. 이러한 동인들에 소극적으로 대응해서 기존의 가치를 보호하고자 하는 조직은 뒤처질 것이고, 사이버 리스크를 더 잘 관리할 방안을 모색하는 조직은 테크놀로지의 발전과 세계화를 통해 탁월한 성과를 이루어낼 것입니다.

조직의 사이버 리스크 관리역량을 이해하는 것은 사이버 리스크를 관리하는 여정의 중요한 첫걸음이 됩니다. 본 자료는 실무적인 지침과 자가평가기법들을 통해 리더들이 조직의 성숙도를 측정하고, 새로운 사이버 리스크를 이해하며 아래의 중요한 질문들에 답할 수 있도록 할 것입니다;

- 적절한 리더와 조직적인 역량을 보유하고 있는가?
- 적절한 곳에 집중해서 투자하고 있는가?
- 사이버 리스크 프로그램의 효과성은 어느 정도인가?

현재는 리스크 관리를 통해 가치를 보호하는 조직들이 산업을 선도합니다. 미래에는 리스크에서 기회를 포착해서 가치를 창출해 내는 조직이 리더가 될 것입니다.

리스크 관리에 대한 책임

사이버 리스크는 기업 내 모든 구성원이 필수적으로 참여하고 관리해야 하는 사안이지만, 사이버 리스크를 감독해야 할 궁극적인 책임은 최고 경영자에게 있습니다.

그러나, 많은 이사회와 최고 경영진은 진화하는 사이버 리스크를 모니터링/탐지/대응하는 일상의 업무에서 너무 멀리 떨어져 있습니다. 사이버 리스크에 관한 조직의 현 상태를 깊이 있게 이해하고 있는 경영자만이 사업을 보다 잘 관리할 수 있습니다.

효과적인 사이버 리스크 관리는 이사회와 최고 경영진의 인식으로부터 시작됩니다. 사이버 리스크를 이해하고 성과를 관리하며 사이버 리스크 관리 성숙도를 높일 수 있는 역량을 향상시키는 것은 핵심적인 질문에 답변하는 것에서 출발하고, 결과적으로 사이버 보안 측면에서 사전 대응(secure)과 지속적 경계(vigilant) 및 신속한 복구(resilient)가 가능한 조직이 될 것입니다. 오늘날 세 가지 요소가 사이버 위협관리에서 매우 중요함에도 불구하고 전통적으로 "사전 대응"에 집중하여 "지속적 경계"와 "신속한 복구"에는 상대적으로 소홀했던 것이 사실입니다. 다음은 경영자들이 조직의 "secure, vigilant, resilient"에 대한 현황을 이해하는데 도움이 되는 10 가지 핵심 질문들입니다.

1. 사이버 리스크에 대해 주의 의무를 다하여 효과적으로 관리하고 있는가?
2. 적합한 책임자와 조직 역량을 보유하고 있는가?
3. 리스크 선호도와 보고 기준을 포함한 적절한 사이버 리스크 보고체계를 구축하였는가?
4. 필요한 곳에 집중하여 투자하는가 ? 그렇다면, 의사결정의 결과는 어떻게 평가 및 측정하는가?
5. 산업 표준 및 산업 내 경쟁사 대비 사이버 리스크 프로그램과 역량은 어느 정도인가?
6. 조직 전반에 걸쳐 사이버 리스크를 중시하는 사고 방식과 문화가 정착되어 있는가?
7. 협력업체 등 제 3 자에서 발생한 사이버 리스크로부터 조직을 보호하기 위한 장치가 마련되어 있는가?
8. 사이버 사고 발생 시 손실을 최소화하고 대응 자원을 신속하게 가동할 수 있는가?
9. 사이버 리스크 프로그램의 효과성을 어떻게 평가하는가?
10. 긴밀하게 연결된 산업 생태계 내에서 강력하고 안전한 관계를 확보하고 있는가?

이사회와 최고 경영진은 조직이 지속적으로 고도화되는 사이버 위협에 대응하는데 핵심적인 역할을 합니다.

비즈니스 세계가 디지털화되고 상호 연결됨에 따라 사이버 위협과 사이버 공격의 빈도와 복잡성이 지속적으로 증가하고 있습니다. 이런 새로운 환경 속에서 사이버 리스크 관리는 사업전략의 핵심으로 자리잡게 되었습니다. 최근 사이버 범죄는 단순한 부정이나 데이터 탈취의 수준을 넘어섭니다. 방대한 범죄조직이나 외국 정부가 지원하는 해커집단, 사이버 테러리스트 등으로 인해 사이버 범죄는 서비스 중단, 데이터 손상 및 파괴, "랜섬웨어"를 통한 자금이나 접근권한, 기업기밀 탈취에 이르기까지 그 범위가 크게 확대되었습니다.

오늘날 사이버 리스크와 조직의 성과는 긴밀하게 관련되어 있습니다. 사이버 범죄에 따른 유형의 비용은 자금 도난이나 시스템의 손상에서부터 벌금, 법적 및 피해자에 대한 보상 등을 들 수 있습니다. 무형의 비용에는 지적재산의 도난에 따른 경쟁우위 상실, 고객 상실 또는 사업 파트너로부터의 신인도 하락 및 조직의 명성과 브랜드 이미지에 대한 전반적인 손상 등이 포함됩니다. 최근의 사이버 공격 범주는 개별 조직에의 피해를 넘어, 대규모 인프라의 붕괴를 초래하거나 금융시스템 전체의 신뢰성이나 경제의 안정성에까지 영향을 미칠 수도 있습니다.

가장 중요한 이슈

사이버 리스크의 중요성이 워낙 크기 때문에 이를 기업 문화에 깊이 내재되어야 할, 가장 중요한 사업리스크로 다루어야 한다고 인식하는 이사회와 최고 경영진이 증가하고 있습니다. 오늘날 모든 사업 영역에 디지털적 요소가 포함됨에 따라, 사이버 리스크에 대한 관심과 우려는 IT 는 물론 한 조직을 뛰어 넘어 모든 파트너사, 고객, 임직원 및 비즈니스 프로세스까지 확장되고 있습니다.

언젠가 침해 사고가 발생할 것이라는 것을 깨닫게 되면 경영자는 가장 중대한 위협이 무엇이고 조직 운영에 필수적인 자산에 어떤 위협을 줄 것인지를 파악해야 합니다. 이사회와 최고 경영진이 사이버 위협으로부터 적극적으로 조직을 보호하는 데 앞장서면, 많은 임직원들은 그 노력이 헛되지 않도록 노력하게 될 것 입니다. 그렇다면, 이사회와 경영진의 책임은 무엇일까요? 그들은 어떤 역량을 배양하여야 하고, 어떤 바람직한 질문을 던져야 할까요? 이런 질문들과 진화하는 사이버 위협에 직면해서, 모든 가능성을 염두에 두고 준비를 하는 것은 어려운 일입니다. 따라서, 단순히 발생 가능성이 있는 위협이 아닌 발생 가능성이 높은 위협에 대비하는 것이 경영자가 취해야 할 바람직한 방향입니다.

모든 사이버 위협에 대응할 수 있는 완벽한 대비책은 없지만 이사회와 최고 경영진이 새로운 보안 프로그램을 개발하거나, 기존 프로그램을 보완함으로써 그 준비를 시작할 수 있습니다. 이후에 소개될 10 개의 핵심 질문들은 진화하는 사이버 리스크에 대한 경영진의 전략, 효과적인 대응 방안과 완화 방안 및 예측 방안의 수립과 관련해서 이사회에서 논의하는데 도움이 될 것입니다.

조직 성숙도 평가

주요 사이버 리스크에 질문과 답변을 통해 현재 조직의 사이버 리스크 대응 수준을 평가하고, 정보보안팀에 적합한 의문을 제기하고 중요한 정보를 제공하며, 향후 사이버 보안에 대한 복구능력을 일관성 있게 모니터링하고 개선할 수 있도록 할 것입니다.

이 질문서는 강점과 약점뿐만 아니라 개선 방향도 식별할 수 있도록 구성되어 있습니다. 다음 질문서에 대한 답변을 통해 조직의 사이버 성숙도 수준을 확인해 보십시오.

사이버 보안 성숙도

높음(High)
조직 내 강력한 사이버 보안 대비책이 마련된 상태

보통(Moderate)
사이버 리스크 대비책이 마련되어 있으나 일부 개선이 필요한 상태

낮음(Low)
사이버 리스크 대비책이 거의 없어 상당한 개선이 필요한 상태

사전 대응, 지속적 경계, 신속한 복구의 정의

사전 대응 (Secure)

정보보안에 관한 근본역량을 개발하고 지속적으로 유지 - 산업 내 사이버 리스크 표준과 규제를 준수하면서, 기존에 알려진 위협과 신규 위협으로부터 조직을 보호할 수 있는 위험중심의 접근법을 활용

지속적 경계(Vigilant)

침해사고와 이상 징후 감지 - 생태계 내의 모든 영역에서 상황에 대한 인지역량 제고

신속한 복구 (Resilient)

불가피한 사이버 공격으로 인한 피해를 복구하고 신속히 정상화 할 수 있는 역량 개발

1 사이버 리스크에 대해 주의 의무를 다하여 효과적으로 관리하고 있는가?

경영자 수준에서의 적정한 책임의 정도를 결정하는 것이 중요합니다. 경영진이 감독하는 수준이 사이버 이벤트에 대해 비정규적인 짧은 보고 정도에 그친다면, 리스크를 효과적으로 관리하기에는 부족합니다.

높은 성숙도

- 이사회와 최고 경영진이 사이버 리스크 관리에 대한 책임, 즉 사이버 리스크 관리 프로그램의 개발과 실행을 감독하는 책임을 부담함
- 이사회와 최고 경영진이 사이버 위협과 이에 따른 잠재적 영향에 대한 정보를 지속적으로 제공받음
- 이사회 내에 IT 와 사이버 리스크를 이해하는 1 명 이상의 이사가 포함됨 (또는 외부 전략적 자문기관을 적절히 활용함)
- 사이버 리스크와 관련된 이슈를 전담하는 최고 경영진 수준의 위원회나, 경영진과 이사회 멤버가 함께 참여하는 위원회(또는 전반적인 사이버 프로그램에 대해 상당한 시간을 할애할 수 있는 대체적인 고위 경영진 수준의 위원회)가 구성됨
- 이사회가 사이버 보안에 대해 정기적으로 보고를 받고, 예산 분석, 경영진에 도전적인 질문 등 정당한 주의의무를 다함

보통 성숙도

- 이사회가 경영진이 사이버 이슈를 감독하고 있으나, 이해관계자와의 의사소통이나 특정 영역에 대한 감독은 대체로 일반적인 수준으로 국한됨
- 이사회가 IT 및 사이버 리스크에 대한 실무지식을 보유함
- 사이버 리스크에 대한 적절한 수준의 감독이나 경영진에 도전적인 질문을 제기할 수 있는 이사회의 역량이 부족
- 이사회가 사이버 리스크 프레임워크 및 전략적 요구사항을 비정기적으로 평가

낮은 성숙도

- 사이버 리스크와 전략적 이슈에 대한 최고 경영진의 의지 부족
- IT 보안 관련 이슈에 대한 대한 경영진의 참여 부족
- IT 및 사이버 리스크에 대한 이사회의 경험이 부족하고, 사이버 이슈를 IT 선에서 해결해야 할 사안으로 취급
- 사이버 리스크의 감독과 관련 예산의 적합성 평가가 형식적인 수준에 그침

2

적합한 책임자와 조직 역량을 보유하고 있는가?

조직 내 모든 구성원은 사이버 리스크에 대해 일정한 정도의 책임을 부담합니다. 모든 사람의 책임이고, 리더들이 전통적으로 해 오던 업무들로 바쁜 상황에서, 자칫 사이버 리스크 대해 궁극적인 책임을 담당할 적임자("right leader")를 선정하는 것을 놓칠 수 있습니다.

높은 성숙도

- 사이버 리스크 리더가 정보기술과 비즈니스 양쪽 모두에서 경험을 보유하여 조직의 운영 방식을 이해하고, 사이버 리스크 관리에 현업의 참여를 이끌어 내며, 사이버 리스크 관리의 우선순위가 무엇인지 파악할 수 있음.
- 사이버 관리 팀원들은 열정적이고, 사이버 리스크의 최신 동향이나 위협, 조직에 미치는 영향 등을 인지하고 있음.
- 사이버 리스크가 이사회와 최고 경영진 수준에서 논의됨.
- 필요한 영역에 대해 관련 산업의 숙련된 유경험자를 조직 내에 충분히 보유하고 있음.
- 리스크의 내용이나 조직에 미치는 중요성과 연계되어 보상 프로그램이 운영됨.

보통 성숙도

- 사이버 리스크 리더가 지정되어 있으나, 사이버 보안과 관련된 기술적 리스크에 편중됨.
- 사이버 리스크 리더가 정보보안에 대한 실무 지식은 있으나, 조직 운영 방식은 완전히 이해하지 못함.
- 사이버 리스크가 중요하게 다루어지고 있으나 실무적인 접근이 상대적으로 취약함.
- 주로 IT 나 경영진 수준에서만 사이버 리스크에 관심.
- IT 와 일정한 비즈니스 영역에 대한 실무경험자가 있으나, 산업에 고유한 사이버 위협에 대한 지식이 부족.

낮은 성숙도

- 사이버 리스크에 대한 경영진의 관심이 낮음.
- 사이버 리스크 지식 및 역량이 IT 만의 책임으로 국한됨.
- 교육 훈련 프로그램이 특정한 신기술에 대해서 임시적으로만 개발됨.
- 인재확보를 위한 투자 부족으로 이직률이 높음.

3

리스크 선호도와 보고 기준을 포함한 적절한 사이버 리스크 대응 체계를 구축하였는가?

사이버 리스크와 관련하여 의미있는 메시지를 조직에 전파하는 것은 사고 발생 시 정보의 흐름을 원활하게 합니다. 그러나, 정보를 경영진에까지 전달하는 프로세스뿐만 아니라, 보고 대상이 되는 정보나 사건을 명확하게 정의하는 것이 중요합니다.

높은 성숙도

- 사이버 리스크의 수용 한계가 명확하게 정의되어 기존 리스크 관리프로세스에 녹아있음.
- 이사회가 전사적인 사이버 리스크 정책을 면밀하게 검토하고 승인함.
- 사이버 리스크 프로그램 전반에 걸쳐 역할과 책임이 명확하게 정의되고 작동함.
- 핵심 리스크지표(KRI)와 핵심 성과지표(KPI)가 존재하며, 경영진에게 보고해야 할 중요하거나 치명적인 사이버 사고의 기준이 마련되어 있음.
- 사고 관리 프레임워크에 사이버 리스크 프로그램과 연계된 보고기준이 포함됨.
- 사이버 리스크에 대한 보험의 가치를 평가 및 모니터링.

보통 성숙도

- 사이버 리스크 정책이 IT 를 제외한 영역에서는 완전히 적용되지 않음.
- 사이버 리스크가 전반적인 리스크 관리 프로세스에서 일반적인 수준으로 언급됨.
- 리스크 수용 한계가 사이버 리스크 프레임워크와 통합되지 않음.
- 선도적이기보다 사후 대응적인 사이버 리스크 관리 경향.
- (이사회가 아닌) 경영진으로 구성된 위원회에서 사이버 리스크에 대해 적절한 시간을 투자.

낮은 성숙도

- 정형화된 사이버 리스크 대응체계가 존재하지 않음.
- 사이버 리스크에 대해 주기적으로 경영진에 보고하는 절차가 없거나 사고 발생 시에만 보고됨.

4

필요한 곳에 집중하여 투자하는가? 그렇다면, 의사결정의 결과는 어떻게 평가 및 측정하는가?

리스크는 성과와 긴밀하게 관련되어 있기 때문에 리더는 사이버 리스크를 관리하기 위해 어떤 자원을 사용하고 있는지, 나아가 적절한 자원을 동원하고 있는지를 알고 있어야 합니다. 적절한 인력을 유지하지 못하거나, 외부 서비스에 대해 과도한 대가를 지급하거나, 운영비용이 증가하는 등 모두가 실제 일어나는 리스크입니다.

높은 성숙도

- 조직 내 모든 부문에서, 전략수립에서부터 일상 업무에 이르는 모든 활동에서 사이버 리스크가 고려됨.
- 대부분의 사이버 위협을 통제할 수 있는 기본적인 보안 체계에 투자를 집중하고, 조직의 가장 핵심적인 프로세스와 정보에 대한 리스크를 관리하기 위해 전략적인 관점에서 선별적인 투자가 이루어짐.
- 발생가능성은 희박하지만 치명적인 영향을 미치는 위협(블랙스완)을 식별하고 예측하며 회피하기 위한 전문 프로그램을 보유.
- 리스크와 연계하여 조직의 투자 및 예산이 수립(투자에 대한 명확한 근거가 존재)되고 사이버 전략 내에 반영됨.
- 조직의 사이버 리스크 관리체계를 이행하기 위해 경영진이 적합한 자금과 충분한 자원을 제공.
- 기존 사이버 리스크 관리체계의 한계와 개선점을 제시할 수 있는 메커니즘이 존재.

보통 성숙도

- 사이버 리스크 관리체계가 산업의 특성을 반영하지 않고 내부적으로만 집중됨.
- 사이버 리스크 전략이 투자와 일관되지 않음.
- 기본적인 보안체계와 고도화된 사이버 공격 대응에 필요한 투자간의 적절한 균형이 이루어지지 않음.
- 강력한 위협 인지 체계가 IT 인프라와 응용 프로그램 보호에 집중.
- 식별된 보호대상 정보에 대한 보호체계가 구축됨.
- 자동화된 IT 자산 취약점 모니터링 체계가 구축됨.
- "블랙스완"을 예측할 수 있는 유의한 메커니즘이 존재하지 않음.

낮은 성숙도

- 사이버 리스크 전략, 추진 방향성 및 투자 계획 부족.

- 기본적인 네트워크 보호나 고전적인 바이러스 기반의 정보보안 통제만 존재하고 새로운 기술이나 방법론에 대한 대비가 부족.
- IT 자산 취약점 모니터링이 비정규적으로 수행.
- 사이버 투자에 대한 사업성 검토가 거의 이루어지지 않음.

5

산업 표준 및 산업 내 경쟁사 대비 사이버 리스크 프로그램과 역량은 어느 정도인가?

조직의 수준이 사이버 리스크를 효과적으로 다루고 있는 사례에 대비하여 뒤쳐져 있지 않은지 확인하는 것이 중요합니다. 그러나, 뒤쳐져 있다는 것을 파악했을 때는 어떻게 해야 할까요? 이러한 상황은 이사회와 경영진이 주도적으로 극복해 나가야 합니다.

높은 성숙도

- 포괄적인 사이버 프로그램이 산업 표준과 모범 사례를 활용하고 있으며, 이를 통해 기존의 위협으로부터 조직을 보호하고, 새로이 등장하는 위협에 대한 정보를 지속적으로 수집하며, 사고 발생 시 적시 대응 및 복구가 가능함.
- 사이버 프로그램을 수립, 운영, 유지 및 개선하는데 있어 산업 표준을 도입.
- 외부와의 벤치마킹을 통한 사이버 프로그램의 성숙도 진단.
- 내부 정책, 산업표준 및 규제의 준수여부를 주기적으로 확인.
- 사업의 핵심 영역에 대해 공식적인 인증을 획득. (예: ISO 27001:2013 인증)

보통 성숙도

- 산업 내 다양한 모범사례와 역량이 구현됨 (예: 기본적인 온라인 브랜드 모니터링, 자동화된 악성코드 포렌식, 수작업 e-Discovery, 범죄자/해커의 활동 감시, 작업자/고객 행동 프로파일링, 내부 사용자에 대한 모니터링 등)
- 컴플라이언스 등 내부 검토가 시행되나 일관적으로 적용되지는 않음.

낮은 성숙도

- 사이버 리스크 대응을 위한 장치들이 산업 표준이나 모범 사례를 고려하지 않고 임시 방편적으로 운영됨.
- 사이버 관리체계의 검토가 법규의 요구사항을 지원하는 수준에서의 간헐적으로 이루어짐 .

6 조직 전반에 걸쳐 사이버 리스크를 중시하는 사고방식과 문화가 정착되어 있는가?

사전 대응(secure), 지속적 경계(Vigilant) 및 신속한 복구(Resilient)에 대한 역량을 강화하기 위해 많은 조직이 교육과 인식수준 제고에 많은 노력을 기울이고 있습니다. 그러나, 이것만으로는 부족합니다. 어떻게 하면 행동을 바꿀 수 있을까요? 이사회와 최고 경영진이 그 해답에 대한 방향성을 제시하여야 합니다.

높은 성숙도

- 강력한 경영진의 의지(tone at the top); 이사회와 최고 경영진이 강력한 리스크 문화와, 리스크와 수익의 상호관계에 대한 사고를 강조.
- 개인의 관심, 가치 및 윤리관이 사이버 리스크 전략, 허용수준 및 접근방식과 연계됨.
- 사이버 리스크에 대해 공개적으로 솔직하게 논의하는 것에 대한 부담이 없음.
- 사이버 리스크에 대한 전사적인 교육과 인식 개선 캠페인을 시행 (모든 임직원, 외부 거래업체 등 포함).
- 사이버 리스크에 대한 개개인의 역할 및 책임을 이해할 수 있도록 개인의 업무에 따른 맞춤형 교육을 제공.
- 임직원이 리스크 관리에 개인적인 책임을 인식하고 필요 시 적극적으로 다른 임직원의 참여를 유도.

보통 성숙도

- 일반적인 정보보안 교육 시행.
- 자산의 리스크와 및 위협의 유형에 집중된 정보기반의 사이버 인식 교육 시행.

낮은 성숙도

- 허용 가능한 (데이터) 사용정책이 존재
- IT 이외의 영역에서 사이버 리스크에 대한 강조 부족.
- 사후 대응차원에서 인식과 교육을 접근하여 정보유출이나 위반사항이 발견한 후에만, 제한적인 임직원에 대해 교육이 제공됨.

7

협력업체 등 제 3 자에서 발생한 사이버 리스크로부터 조직을 보호하기 위한 장치가 마련되어 있는가

많은 사이버 침해 사고가 협력업체나 벤더사 등의 사업 파트너로부터 발생합니다. 사이버 리스크는 조직의 업무 울타리를 크게 넘어선 범위에서 발생하기 때문에, 협력업체들이 어떤 활동을 하고 있는지를 이해하고, 이러한 제 3 자와의 사업관계에서 발생하는 리스크 요인들이 수용 가능한 수준인지를 확인하여야 합니다.

높은 성숙도

- 사이버 리스크가 중요한 아웃소싱 계약이나 하청업체 선정 시 사전에 검토해야 할 항목의 일부로 고려됨.
- 모든 협력업체가 일관된 프로세스를 준수하며, 조직의 기대수준과 리스크 수용한계와 연계된 정책과 통제(예: 협력업체의 관리실태에 대한 감사 권한)가 수립됨.
- 협력업체의 필요성이나 리스크에 따른 맞춤형 사이버 리스크 교육을 제공.
- 모든 제 3 자와의 중요한 협력관계와 정보의 흐름을 식별하고 평가하는 활동이 리스크 관리 프로그램에 포함되어 있음.
- 협력업체의 사이버 사고 발생 시 신속한 보고 체계가 운영됨.
- 협력업체에 대한 리스크 식별 및 평가결과를 기반으로, 아웃소싱 계약의 잠재적 리스크를 줄이기 위한 절차를 수행.

보통 성숙도

- 아웃소싱 계약으로부터의 잠재적인 사이버 리스크를 줄이기 위한 절차를 수행.
- 아웃소싱 및 하청업체에 대한 사전 조사(due diligence)가 권장되나, 일관되게 실행되지는 않음.
- 사이버 사고에 대한 협력업체 보고 절차가 계약사항에 명시되어 있지 않음.
- 사이버 위협 관련 정보 수집을 내부 및 외부 협업 체계가 일부 존재.

낮은 성숙도

- 기본적인 네트워크 보안기능만 존재.
- 협력업체에 대한 조사 및 사이버 리스크 보호 대책이 존재하지 않음.

8

사이버 사고 발생 시 손실을 최소화하고 대응자원을 신속하게 가동할 수 있는가?

사이버 보안이 철저한 기업조차도 침해사실을 발견하는데 수일 또는 수주가 소요될 수 있습니다. 실제 사이버 위협이 발견되었을 때 대응 프로세스를 가동하는 역량을 보유하는 것이 중요합니다. 경영자의 관점에서, 대형 사고에 대응하는 역량에는 명확한 지휘계통, 확실한 의사소통계획(비상연락 포함), 법적 이슈에 대한 폭넓은 시야, 대외 홍보 필요성, 브랜드나 사업 운영에 미치는 영향 등이 포함됩니다.

높은 성숙도

- 정보보안 사고 발생 시의 대응 행동 및 의사소통을 위한 명확한 보고 및 의사결정 절차가 존재.
- 사이버 사고 대응 정책과 절차가 기존의 사업연속성 관리(Business Continuity management) 및 재해복구계획(Disaster Recovery Plan)과 통합.
- 위기관리 및 사이버 사고 대응 계획과 절차의 문서화 및 시뮬레이션기법 등을 통한 모의훈련의 실시.
- 사이버 사고 발생 시 내부 및 외부 주요 이해관계자 대상의 의사소통계획 존재.
- 업계의 전문업체가 주도하는 시뮬레이션 및 교육훈련에의 적극적 참여.

보통 성숙도

- 기본적인 사이버 사고 대응 정책 및 절차가 정비되어 있으나, 기존의 사업연속성 관리나 재해복구계획과 효과적으로 통합되지 않음.
- IT 사이버 공격에 대한 모의 훈련을 정기적으로 수행.
- 조직 전반에 걸친 사이버 공격 대응훈련은 비정기적으로 수행.

낮은 성숙도

- IT 사업연속성 및 재해복구 훈련을 제한적으로 실시.
- 사이버 사고 정책, 대응 계획 및 의사소통 절차가 미흡하거나 존재하지 않음.

9 사이버 리스크 프로그램의 효과성을 어떻게 평가하는가?

이 질문에 대한 답은 간단합니다. 처음부터 끝까지 평가하면 됩니다. 하지만, 실행하는 것은 말처럼 쉽지 않습니다. 또 다른 과제는 시스템을 넘어서서 사업 전반에 미치는 광범위한 함의를 이해하고, 비판적 시각을 통해 IT 뿐만 아니라 업무 프로세스를 검토하는 것입니다. 사이버 리스크 프로그램을 실행하고 관련 도전과제들을 극복하기 위해서는 이사회 및 최고 경영진의 참여를 필요로 합니다.

높은 성숙도

- 사이버 보안 프로그램의 효과성이 검토되었고, 식별된 취약점이 리스크 허용한도 내에서 관리되고 있는지를 이사회와 최고 경영진이 확인.
- 이사회 또는 이사회 내의 위원회가 기존 통제의 적정성을 포함한 사이버 보안 프레임워크와 이행계획의 이행상황을 주기적으로 검토하고 논의.
- 사이버 보안 관련 통제 상의 결함이 존재하는지를 확인하기 위한 주기적인 내/외부 취약점 평가(health checks, penetration test 등) 수행.
- 주기적인 감독 활동 (사이버 보안 예산 평가, 서비스 아웃소싱, 사고 보고, 평가 결과, 정책의 검토 및 승인 등)
- 내부감사의 분기별 검토 과정에서 사이버 리스크 관리의 효과성을 평가.
- 사고 이전보다 더 강력한 시스템으로 거듭나기 위해, 사고를 통해 학습하고 기존의 사전 대응(secure)과 지속적 경계(vigilant) 측면에서 사이버 리스크 프로그램을 수정 및 보완함.

보통 성숙도

- 기본적인 사이버 리스크 평가가 고정된 일정으로 수행되며 산업별 특성을 고려하지 않음.
- 내부감사가 연 1 회 이상 사이버 리스크 관리의 효과성을 평가.
- 사고를 통한 교훈을 사이버 리스크 관리 개선에 활용하나 일관되게 적용되지는 않음.

낮은 성숙도

- 내부감사에 의한 사이버 리스크 관리체계 평가가 간헐적으로 수행 또는 수행되지 않음.
- 사이버 리스크 대응방안이 현장 경험을 반영하여 적시에 개선되지 않음.

10

긴밀하게 연결된 산업 생태계 내에서 강력하고 안전한 관계를 확보하고 있는가?

사업 파트너들의 사이버 리스크 준비 상황이 조직의 대응체계에도 영향을 미칩니다. 사이버 리스크는 상호보완적입니다. 우리 조직이 산업 생태계 내에서 사이버 리스크 취약지점 혹은 리더입니까? 우리 조직이 사이버 리스크와 전체 산업환경에 대해 긍정적인 영향을 미칩니까? 타 조직 및 사업 파트너와 협력하여 사이버 위협에 대한 정보를 공유함으로써 보다 유기적이고 종합적인 접근방식을 마련할 수 있습니다.

높은 성숙도

- 내부 이해관계자, 외부 사업 파트너, 사법기관, 규제기관 등과 긴밀한 관계를 유지.
- 정보보안과 개인정보보호를 훼손하지 않는 범위에서 혁신적인 정보공유 활동을 적극 지원.
- 산업 내, 독립적인 사이버 정보분석센터, 정부, 정보기관, 학계 및 연구기관과 지식 및 정보를 공유.
- 정보 공유의 대상을 사업 파트너, 고객 및 최종 소비자까지 확장.
- 산업표준을 준수하거나 보안체계가 잘 갖추어진 협력사를 우선적으로 선정.
- 산업 생태계 내에서 사이버 리스크 취약지점(weak link)이 되지 않도록 성숙단계의 프로그램을 독립적으로 유지.

보통 성숙도

- 동종 산업 내 기업들과 비정기적인 사이버 위협 정보를 공유하거나, 사이버 위협 정보와 관련한 정부 및 민간기관과 활발한 협업 관계를 유지.

낮은 성숙도

- 외부 기관과 최소한의 협업 관계만 형성되어 동종 산업 내 기업이나 정부 혹은 외부 그룹과 정보나 지식 공유가 거의 이루어지지 않음.

더 높은 목표, 전략적 목표 설정

사이버 리스크 프로그램을 구축하거나 고도화할 때, 조직의 리스크 리더들이 성숙도 목표수준을 설정하는 것이 중요합니다. 이러한 목표수준을 효과적으로 설정하기 위해서는 사이버 리더들과 조직 내 다른 영역의 의사결정자간의 논의를 통해 사업에 미치는 영향과 그 결과에 따른 우선순위를 결정하여야 합니다. 모든 조직이 사이버 리스크 관리 성숙도의 모든 분야에서 최고의 수준을 달성할 필요는 없지만, 비용과 시간을 고려하면서 조직의 전략적 목표(strategic goals) 달성을 지원할 수 있는 수준이어야 합니다. 많은 경우 이러한 접근방식을 통해 사이버 리스크 중요도가 높은 영역에 보다 높은 수준의 관리체계를 구축할 수 있습니다. 성숙도가 높은 사이버 리스크 프로그램을 구축하는 것은 단순히 대규모로 투자하는 것만은 아닙니다. 이는 조직의 고유한 필요에 따라 사전 예방(secure), 지속적 경계(vigilant) 및 신속한 복구(resilient) 역량간에 균형있게 투자할 수 있는 차별적인 접근방식을 취하는 것이 필요합니다.

현재의 성숙도는 어느 정도입니까?

평가 결과, 현재의 성숙도 수준이 조직의 전략과 미션을 지원합니까? 혹은 전략과 미션의 달성을 방해하지는 않습니까? 현재의 성숙도 수준이 목표수준에 미치지 못하거나, 아직까지 적절한 목표수준을 설정하지 않았다면, 지금이 바로 사이버 리스크 대응방향을 개선해야 할 시점입니다.

사이버 리스크로부터 조직을 100% 보호하기는 불가능합니다. 하지만, 정보유출, 과태료, 손해배상, 평판훼손 등 사이버 위협에 따른 영향을 관리하고 크게 감축하는 것은 분명 가능합니다. 조직 내부에서,그리고 외부 기관과의 협력을 통해 지속적으로 증가하는 전국적 또는 전세계적 차원의 초대형 IT 서비스 중단이나 사업 중단 위협을 최소화 할 수 있습니다.

딜로이트 안진회계법인 사이버 리스크 서비스 (CRS: Cyber Risk Services)

서 영수
Partner
(02) 6676-1929
youngseo@deloitte.com

이상훈
Director
(02) 6676-2937
sanghunlee@deloitte.com