Deloitte.

Where insights lead

사이버보안과 내부감사의 역할

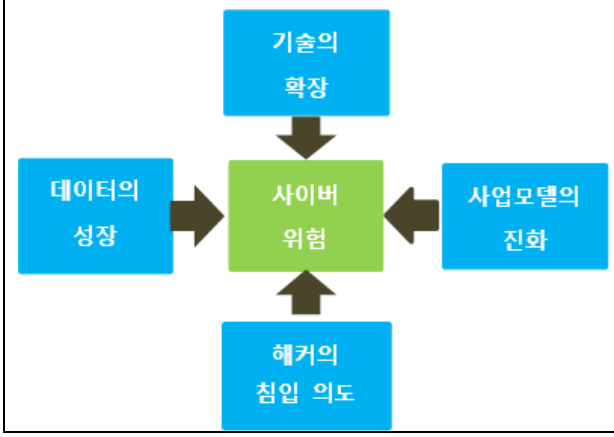
(Cybersecurity and the role of internal audit: An urgent call to action)

사이버공격에 의한 위협은 매우 심각하며, 지속적으로 진화하고 있습니다. 2015년 5월의 조사에 따르면 사이버 범죄로 인해 기업이 부담해야 할 비용은 2019년까지 US$ 2조를 넘어설 것으로 전망되며, 이는 2015년 예상치의 4배에 이르는 금액입니다[i]. 다수 기업의 감사위원회와 이사회는 내부감사 조직이 정보보안위험을 관리하는 조직의 역량을 평가할 것을 기대합니다. 우리의 경험에 의하면, 내부감사의 효과적인 첫 번째 단계는 사이버 위험을 평가하고 이에 대한 결과들을 간결하게 요약하여 감사위원회 및 이사회에 전달하는 것이며, 감사위원회 및 이사회는 이를 통해 리스크에 기반한 장기 사이버보안 내부감사계획을 주도하게 됩니다.

사이버 위협에 대한 관심 증가

사업의 성장과 효율성을 견인하는 영향요인은 동시에 사이버 공격의 범위를 확장시킵니다 (그림1). 오늘날 대중적으로 사용되고 있는 인터넷, 클라우드 컴퓨팅, 모바일, 소셜 네트워크 서비스 등의 플랫폼은 본질적으로 “공유”를 목적으로 합니다. 아웃소싱이나 계약, 원격지의 사업장으로 인해 통제와 관리의 방식이 전환되고 있습니다. 데이터의 지속적인 확장과 더불어 데이터 보안의 필요성도 함께 증가하고 있습니다. 또한, 사이버 공격의 주체는 개인 해커에서부터 국가 차원의 해커에 이르기까지 다양하며, 지속적으로 혁신하여 일반적인 통제를 무력화시키고, 때로는 법으로 관리할 수 있는 범위를 넘어서고 있습니다.

[그림1. 사이버 취약점의 영향요인]



언론에 주요 기사로 등장하는 대형 정보보안 사고들은, 사이버 위협에 대한 정부 차원에서도 강조하면서 감사위원회와 이사회의 관심도 증가하고 있습니다. 미국 증권거래위원회(US SEC)의 지침에 따라 미국 증권시장에 상장한 기업들은 사업보고서에 중요한 사이버보안 위험과 정보보안 사고를 언급하여야 합니다. 국가의 핵심 인프라에 영향을 미칠 수 있는 사이버공격에 대한 우려가 높아지고 있는 가운데, 오바마 미국 대통령의 행정명령["Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity (행정명령 13636, 인프라 사이버보안의 향상)]에서는 국가의 사이버보안 체계를 개선함에 있어 기업부문의 역할과, 빠르게 변화하고 있는 규제기관의 요구사항을 적용하는 것의 필요성을 강조한 바 있습니다.

3단계 방어선

사업부문과 IT기능은 일상적인 업무 의사결정 및 운영과정에서 사이버 리스크를 관리하는데 이것이 1차 방어선을 구성합니다. 2차 방어선은 사이버 리스크를 관리·감독하고, 정보보안 운영을 모니터링하여 필요 시에 적절한 조치를 취하는 정보위험관리자들이 주된 역할을 합니다. 2차 방어선은 최고정보보안책임자(CISO)의 지휘 하에 이루어지는 경우가 많습니다.

많은 기업에서 사이버 리스크의 3차 방어선, 즉 내부감사에 의한 정보보안관리의 독립적인 검토와 확인이 필요하다는 인식이 증가하고 있습니다. 내부감사는 조직의 정보보안체계를 평가하고 개선기회를 식별하는데 핵심적인 역할을 담당하여야 합니다. 동시에, 법적, 재무적 책임을 부담하는 이사회에서 정보보안에 대한 관심이 높아짐에 따라, 내부감사는 관련된 내부통제가 제대로 설계되고 작동하고 있는지를 감사위원회와 이사회에 보고할 의무가 있습니다.

사이버 위험평가의 필요성과 방법

기업의 사이버 위험에 대한 평가는 아래의 세 가지 질문에서 시작합니다.

1. **사이버 위협의 주체가 누구인가?**
   범죄자, 경쟁자, 외부 공급업체, 불만을 품은 내부자, 특정한 목표를 지닌 해커 등 다양한 주체가 될 수 있음.
2. **사이버 공격의 목적은 무엇이며, 어떤 사업위험이 완화되어야 하는가?**
   돈이나 지적재산권을 노릴 수도 있고, 회사 운영을 중단시키거나 평판을 훼손하려는 의도일 수도 있으며, 보건 및 안전의 위험을 초래할 수도 있음
3. **어떤 경로로 공격할 수 있는가?**
   피싱, 시스템의 취약성, 탈취한 자격증명(ID와 패스워드)을 사용하거나, 취약한 제3자의 네트워크를 통해 회사의 시스템에 접근할 수 있음

위 질문을 통해 파악된 위험을 관리하기 위해 딜로이트는 아래의 세 가지 차원의 접근방식을 제시합니다;

1. **사전 방어(Secure)**. 대부분의 기업에서 기존에 알려졌거나 새롭게 등장하는 정보보안위협을 관리하기 위해 경계선 방어(perimeter defenses), 계정 관리(Identity Management), 데이터 보호 등의 통제를 적용하고 있습니다. 위험기반의 프로그램에 따라 사업위험이 높은 영역들을 우선적으로 통제합니다.
2. **지속적인 경계(Vigilant):** 응용프로그램 설정의 변경이나 비정상적인 데이터 이동 등 악의적이거나 승인 받지 않은 활동을 적발하고 지속적으로 변화하고 진화하는 위협에 효과적으로 대응할 수 있도록 정보보안위험 징후 포착, 보안성 모니터링, 행동 및 위험분석 등을 수행합니다.
3. **신속한 복구(Resilient):** 보안사고로부터 최대한 빨리 복구하고 영향을 최소화하기 위해 사고 대응 프로토콜, 포렌식 기법, 사업연속성계획 및 재해복구계획 등을 활용합니다.

누가, 왜, 어떻게 사이버 공격을 감행할 것인가를 사전 방어, 지속적 경계 및 신속한 복구의 세 가지 관점에서 분석하는 것은 내부감사가 사이버보안 평가 프레임워크의 기본 토대가 되고, 나아가 조직의 사이버 리스크 관리의 핵심적인 구성요소가 될 것입니다.

사이버 리스크 평가 프레임워크 – 포괄적인 접근방식

많은 내부감사기능들이 조직의 사이버 리스크 관리수준을 평가해 왔습니다. 이러한 내부감사 활동들은 사이버 공격이나 침입탐지 등 특정한 목적으로 수행한 감사에서는 의미가 있지만, 사이버 리스크 전반에 대해서는 확신을 제공하지 못합니다. 내부감사가 사이버 리스크에 대해 포괄적인 관점을 제공하고, 특정한 영역에 대한 감사만 수행함으로써 발생한 보안에 대한 잘못된 인식에서 탈피하기 위해서는, 포괄적인 접근방식을 적용하여야 합니다. [그림2]는 딜로이트가 권고한 사전 대응(Secure), 지속적 경계(Vigilant), 신속한 복구(Resilient)에 기반한 사이버 리스크 평가 프레임워크를 제시하고 있습니다. 복수의 사이버 도메인들이 세 가지 주제를 각각 지원하고 있습니다. 사이버 리스크 관리를 평가할 때 내부감사는 12개의 도메인 각각에 있는 각 역량과, 현재 관리하고 있는 방식 및 개선이 필요한 영역을 이해하는 방식으로 이 프레임워크를 활용할 수 있습니다.

무엇보다도, 사이버보안 프레임워크 내에서의 역할과 책임은 IT조직에만 한정된 것이 아니라, 조직 전체에 있습니다. 예를 들어, [그림2]에 지속적 경계(Vigilant)의 요소 중 하나로 표시된 데이터관리 및 보호와 관련해서, 관리하는 데이터는 각 사업부문의 관리자와 직원이 정의하여야 합니다. 이러한 책임은 조직 내에서 모든 직급에 해당하며, CEO도 자신의 메모나 기타 의사소통에서 노출된 위험을 평가할 임무가 있습니다.

또한 기존 IT감사의 범위가 제한적이라는 것도 중요하게 고려하여야 합니다. 프레임워크에서 색상으로 표시한 부분은 내부회계관리제도의 평가, 침투 및 취약성 테스트와 사업연속성 및 재해 복구테스트가 각각 다루는 사전 대응 (Secure), 지속적 경계(Vigilant), 신속한 복구(Resilient)의 특정한 요소들을 표시하고 있습니다. 그러나, 지속적 경계(Vigilant) 중의 위협모델링과 보안 이벤트 모니터링, 신속한 복구(Resilient) 중의 복구 테스트와 모의훈련 등 색상으로 표시되지 않은 부분 등 많은 기타의 위험들이 IT와 관련된 IT 일반통제 테스트에서 누락될 수 있습니다. 내부감사의 사이버 위험평가를 통해 점검대상에서 누락된 사항들을 식별해서 위기대응 모의훈련을 수행할 때 중요한 질문으로 이어질 수 있습니다. 감지한 위협을 누구에게 알려주어야 합니까? 조직이 어떻게 대응합니까? 돈을 요구하는 경우 지급해야 합니까?

(다음 페이지에 계속)

[그림2. 대표적인 사이버보안 프레임워크]

사전 방어 (Secure)

사이버 리스크 관리와 법규 준수	개발보안 생명주기	보안 프로그램과 인력관리
▪ 법규준수 모니터링 ▪ 이슈 및 시정조치 계획 ▪ 조사 대응 ▪ 정보보안 및 법규준수 위험평가 ▪ 법규 요구사항과 통제절차의 통합관리	▪ 개발보안지침 ▪ 응용시스템 역할 설계 및 접근권한 관리 ▪ 정보보안 설계/아키텍처 ▪ 정보보안 측면의 요구사항 관리	▪ 정보보안 방향성과 전략 ▪ 정보보안 예산관리 ▪ 정보보안지침 관리 ▪ 예외사항 관리 ▪ 인력관리 전략

외주업체 관리	정보자산 관리	접근권한 관리
▪ 업체 평가 및 선정 ▪ 계약 및 서비스 시작 ▪ 지속적인 모니터링 ▪ 서비스 종료	▪ 정보자산 분류 및 목록 작성 ▪ 정보기록 관리 ▪ 물리적 보안 및 환경보안 ▪ 물리적 장치 처리	▪ 계정 부여 ▪ 슈퍼유저 관리 ▪ 접근권한 인증 ▪ 접근권한 관리

지속적 경계 (Vigilant)

위협 및 취약점 관리	데이터 관리 및 보호	리스크 분석
▪ 사고 대응 및 포렌식 ▪ 응용시스템 보안 테스트 ▪ 위협 모델링과 sensing ▪ 보안 이벤트 모니터링과 로그 ▪ 침투 테스트 ▪ 취약점 관리	▪ 데이터 분류 및 목록 작성 ▪ 보안 이벤트 통지 및 관리 ▪ 데이터 손실 방지 ▪ 데이터 보안 전략 ▪ 데이터 암호화 및 난독화 ▪ 모바일 장치 관리	▪ 정보 수집 및 분석 - 사용자, 계정, 조직 - 사건/사고 - 부정 및 자금세탁방지 - 운영 상의 손실

신속한 복구 (Resilient)

위기관리 및 탄력성	보안 운영	보안 인식 및 교육
▪ 복구 전략, 계획, 절차 ▪ 모의훈련 ▪ 사업영향분석 ▪ 사업연속성계획 ▪ 재해복구계획	▪ 변경 관리 ▪ 설정 관리 ▪ 네트워크 보안 ▪ 보안 운영관리 ▪ 보안 아키텍처	▪ 보안교육 훈련 ▪ 보안인식 제고 ▪ 제3자 책임

내부회계관리제도 (재무 시스템만)	침투 및 취약성 테스트	BCP/DRP 테스트

내부감사전문가들이 사이버보안평가를 수행할 때 고려해야 할 요소들은 아래와 같습니다.

먼저, 필요한 경험과 역량을 보유한 사람들을 포함시키는 것이 가장 중요합니다. 내부감사는 위험평가에 대한 노하우를 가지고 있지만 IT부서나 CISO가 수행하는 위협 모델링업무를 이해하기 위해서는 이에 대해 보다 효과적인 질문을 할 수 있는 전문가가 필요합니다. 사이버 보안에 정통한 IT감사 전문가는 필수적인 자원입니다.

특정한 항목에 한정되지 않고 사이버보안 프레임워크 전체를 평가하는 것도 중요합니다. 이러한 평가에는 프레임워크 대비 현재 상태, 조직이 지향하는 방향, 그리고 동종 산업에서 시행 중인 최소한의 사이버보안 practice를 이해하는 것을 포함합니다.

마지막으로, 초기 평가는 광범위한 것이어야 합니다. 이는 광범위한 테스트를 필요로 하는 빠짐없는 분석을 의미하는 것은 아니며, 추가적으로 위험에 기반한 사이버보안에 대한 심층적인 검토를 이끌어 낼 수 있어야 합니다.

사이버 위험 평가 - 중요한 출발점

정보보안에 관한 역량을 유지하고 강화하는 것은 사이버 위협을 완화시켜 사이버보안의 성숙도를 조직이 원하는 수준에 도달할 수 있도록 합니다. 포괄적인 사이버 위험 평가를 통해 내부감사는 감사위원회와 이사회에 보다 객관적인 관점과 이슈들을 제시하고, 이들 이슈들을 사용해서 사이버 리스크를 다룰 한 해 또는 다년도 내부감사 계획을 수립할 수 있습니다. 위험평가를 수행하는 것이 하나의 전략이 될 수 있고, 아니면 성숙도 분석의 방법으로 접근할 수도 있습니다. 성숙도 분석방법은 보완이 필요한 영역에 대해 명확한 신호를 시각적인 효과로 전달함으로써 경영진이나 이사회 기타 기업의 감독기구에 추가적인 가치를 제공할 수 있습니다. 사이버보안 분야에 대한 전문가의 참여를 바탕으로, 사이버 위험평가는 사이버 보안을 강화하기 위한 개선사항을 파악하고, 개선활동에 대한 장단기 실행계획을 제공 수 있습니다.

[그림3]에서 사전 방어(Secure), 지속적 경계(Vigilant), 신속한 복구(Resilient) 세 가지 주제와 12개 사이버보안 도메인을 연결한 성숙도 분석을 살펴 봤습니다. 초기단계, 관리단계, 정의단계, 예측단계, 및 최적화단계 등 다섯 개의 성숙단계는 사이버위협을 완화시켜 조직이 원하는 성숙도 수준을 달성하기 위해, 정보보안 역량을 유지하고 강화해 나가는 진행상황을 반영하고 있습니다. 그림에서 녹색 점선의 우측 끝부분은 조직이 목표로 하는 성숙도의 수준으로, 이는 로드맵을 작성하는 과정에서 식별할 수도 있습니다. 개선사항들을 이행해 나간 결과는 녹색 점선의 위치로 반영됩니다. 목표로 설정한 성숙도 수준에 이사회는 동의할 수 있어야 하며, 내부감사는 그 시점에서 다시 한번 테스트를 수행해서 목표수준에 도달했는지를 이사회에 보고하여야 합니다.

[그림3. 성숙도평가 예시]

초기단계 (initial)	관리단계 (Managed)	정의단계 (defined)	예측가능단계 (Predicatble)	최적화 단계 (Optimal)
▪ 문제점 인지 ▪ 임시 방편 / 사건별 접근 ▪ 부분적인 목표달성 ▪ 교육, 의사소통 부재, 비표준화	▪ 프로세스로 관리 ▪ 책임의 정의 ▪ 정의된 프로세스의 위반 사례 ▪ 프로세스 검토	▪ 정의된 프로세스 ▪ 업무절차의 공유 ▪ 성과 데이터 수집 ▪ 타 프로세스와의 통합 운영 ▪ 규정준수에 대한 감독	▪ 정량적인 성과지표와 통제의 한계 정의 ▪ 지속적인 개선 ▪ 자동화 및 도구의 활용 ▪ 사업목표와의 연계	▪ 지속적인 개선 ▪ 개선목표의 정의 ▪ IT와의 통합 ▪ 자동화된 업무흐름 ▪ 새로운 기술을 활용한 개선

성숙도 분석

* 일반적으로 알려진 Capability maturity Model Integration (CMMI)을 평가를 위한 모델로 사용할 수 있습니다. 각 도메인은 개별 역량들로 구성되어 있으며, 개별 역량 평가의 평균으로 전체 도메인의 성숙도를 계산합니다.

인력, 프로세스, 기술을 둘러싼 사이버 리스크를 세부적으로 기술한 별도의 평가표를 통해 성숙도 평가를 설명할 수 있어야 합니다. 발견사항을 문서화하고, 개선사항을 이행하기 위한 권고사항이 제시되어야 합니다.

사이버 보안에 대한 내부감사 계획의 기초

앞에서 언급한 것과 같이, 사이버 리스크 평가는 감사위원회와 이사회에 제공되는 성숙도 분석과, 사이버 보안 위험에 기반한 다년도 내부감사 계획을 수립하는데 활용할 수 있습니다. 다년도 감사계획 속에서, 일부 영역에 대해서는 그 시급성과 조직 내에서 진행된 다른 테스트 및 평가활동의 결과를 고려해서 보다 자주 감사를 진행할 수도 있습니다. 사이버보안에 대한 내부감사계획은 새로운 위험의 등장이나, 기존 위협의 상대적인 강도와 중요도 변화 혹은 조직의 성장과정에서 변경될 수 있습니다.

사이버 보안 강화를 위한 내부감사의 역할

사이버 위험은 발생빈도나 사건의 다양성, 해당 기업이나 거래 상대방, 고객에게 미치는 잠재적인 영향 등의 측면에서 지속적으로 증가하고 있습니다. 대부분의 기업들이 사이버 리스크를 심각한 것으로 인지하고 있지만, 사이버 리스크에 대처하고 경영진들이 회사의 대응상황을 지속적으로 평가하는 측면에서 해야 할 일들이 더 있습니다. 내부감사는 기존의 통제나 추가로 필요한 통제를 독립적으로 평가하고, 감사위원회와 이사회가 디지털 세계에서의 다양한 위험성을 이해하도록 지원함으로써, 조직이 사이버 위협을 지속적으로 관리하는데 핵심적인 역할을 맡고 있습니다.

---

[i] "Cybercrime will Cost Businesses Over $2 Trillion by 2019," Juniper Research, May 12, 2015, http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.