바람직한 CSO(Chief Security Officer)의 역할 모델

본 기고는 기업에서 지난 6년 동안 정보보호 관련업무 실무책임자로서의 경험을 토대로 어떻게 하면 보다 더 효율적이고 안정적인 정보보호활동을 수행할 수 있을까 하는 관점에서 바람직한 CSO의 역할 모델을 정리해 본 글이다.

전혀 보안에 신경을 쓰지 않아도 보안사고가 발생하지 않으면 100점짜리 보안수준이 되는 것이고, 제아무리 보안교육과 점검을 실시하고 취약점을 개선하기 위한 다양한 보안투자를 시행하더라도 보안사고가 터지는 순간, 보안수준은 순식간에 빵점짜리로 전락한다. 때문에 필자는 종종 정보보호 책임자는 안전고리를 벗겨낸 폭탄을 가슴에 품고 언제 터질지 모르는 지뢰밭에 서있는 사람이라고 역설한 바 있다.

최근 급속한 IT기술의 발전과 극심한 개인주의 성향 등으로 그 어느 때보다 보안사고의 위험성과 피해규모가 크게 증대되고 있으며, 이에 따라 기업에서 정보보호 업무 수행부서의 역할과 책임범위 역시 과거와 달리 매우 광범위하게 확장되고 있는 실정이다. 특히 우리나라는 90년대 말 IMF 당시 구조조정의 여파로 중국을 비롯한 해외 경쟁회사로 국내 기술자들이 이직함으로써 핵심 산업기술의 유출이라는 피해를 경험한 바 있다. 그런데 최근 미국에서 시작된 세계경기의 위축으로 또 한 차례의 보안사고 위험성에 크게 노출되어 있는 상황이다. 각 국의 문화 및 산업의 다양성만큼이나 수많은 위험성이 산재하고 있는 현대 사회에서 바람직한 CSO가 되기 위한 몇 가지 착안사항들에 대하여 논해 보고자 한다.

글 **이희명** | POSCO 정보보호그룹 그룹장_ hmlee@posco.com

※ 본 기고는 전적으로 필자의 개인 견해임을 밝혀두는 바이다.

내가 생각하는 CSO란

일반적으로 CSO(Chief Security Officer)란 기업이나 정부기관 등 조직체에서 관리적, 물리적, 기술적 보안의 모든 보안 영역을 포괄적으로 총괄하여 관리하거나, 특정 영역을 별도로 분리하여 총괄하는 책임을 부여 받은 임원을 의미한다. 그렇지만 CSO는 특정분야 또는 일정부문의 전문가가 아니라 자신이 관리하고 있는 정보보호 관련 조직과 비용을 효율적으로 활용해 최상위 경영진의 관점에서 업무의 효율성 증대와 동시에 보안의 안전성을 유지시켜나가야 하기 때문에 그 의미를 보다 명확하게 정의할 필요가 있다.

정보보호 영역을 축소해 IT 관점에서만 그 역할을 고려한다든지, 너무나 광의로 해석해 포괄적인 경영위기의 영역까지 확대하게 된다면 CSO는 자신이 수행해야 할 업무분야의 불균형으로 인해 최적의 정보보호체계를 유지해 나갈 수 없게 된다. 따라서 CSO는 먼저 숲을 보고 개별적인 나무를 살펴보면서, 전체적인 균형을 이뤄나가는 자세로 조직에서의 정보보호활동을 수행해야 한다. 또한 최근 등장하고 있는 거버넌스(Governance)의 관점에서 보안기획, 운영, 진단 등 전체영역에서 보다 빠르고 정확한 의사결정을 통해 다양한 경영환경 하에서 기업의 경영활동을 적기에 지원하는 것이 CSO가 해야 할 중요한 임무다.

CSO의 역할과 책임

일반적으로 조직원들은 가정에서 지키는 본능적인 보안준수 행동(문단속이나 귀중품 보관 등)과 달리, 회사에서는 엄격한 보안규정 때문에 업무에 방해를 받고 불편하다고 느끼고, 최소한의 수준에서만 지키면 된다는 의식이 매우 강하다. 또한, 한국적 문화의 특성으로 보안사고 징후자에 대한 내부 고발은 회사를 지키려는 선의로 평가받기보다는 인격적으로 폄하되곤 한다. 또 혈연, 지연, 학연 등의 개인적 유대관계를 중요시하는 풍토에 의해 중요한 정보를 불법적으로 과다하게 제공하는 등 보안활동에 매우 취약한 구조를 지니고 있다. CSO는 개인의 감정에 따라 좌지우지되는 이런 특성을 고려해 기업 내 구성원들에게 근원적인 보안의식의 차이점을 해소하는 것이 급선무이다.

최근 일정 규모 이상의 대기업이나, IT 관련 업체(HW/SW 제작 및 서비스 업체), 또 통신이나 포털 기업 등에서는 정보보호 담당 전문인력과 조직을 상설 운영하고 있다. 기업의 속성과 규모에 따라 정보보호 업무수행 조직 구성원의 숫자나 책임자의 경력이 다를 뿐이다. 하지만 보안의 영역이 점점 확대되고 있는 추세이기 때문에 CSO는 정책 및 제도, 인원 등에 대한 관리적 보안과 시설 및 사무실 출입을 통제하는 물리적 보안 그리고, 현대사회에서 업무수행의 근간을 이루고 있는 IT 중심의 기술보안에 이르기까지 모든 영역을 총괄적으로 관리하면서 보안사고 예방 및 취약점 개선활동을 효율적으로 수행해야만 한다. 또한 ISO 27001을 근간으로 한 정보보호 국제표준을 기반으로 지속적인 자체진단 및 취약점 개선활동을 하면서 핵심정보에 대한 Risk Management를 수행해야 한다. 더 나아가 기업을 둘러싸고 있는 다양한 이해관계자(경영진 및 조직원 등 내부자, 주주, 고객, 정부기관 등 외부 이해관계자)를 보호하기 위한 포괄적이고 효율적인 보안활동을 해 나가야만 한다.

단순히 기업만을 보호하는 것이 아니라 회사 직원 및 고객의 개인정보까지 동시에 보호를 해야 한다. 특히 보안사고는 회사 수익성을 저하시키는 직접적인 손실은 물론, 회사 이미지 훼손이나 주가하락 등 많은 영향을 끼치기 때문에 보안사고 예방 및 사후 관리에 만전을 기해야 한다. 또한, CSO는 단순히 임원으로서 경영층의 의사결정에 참여하는 것만이 아니라, 정보보호에 대한 전문적인 지식과 경영의식을 가지고 회사에 기여하는 구성원이 되어야 한다. 즉, CEO(Chief Executive Officer)를 보좌하며 기업의 수익성 창출과 보안사고 예방에 최선의 노력을 기울여야 한다. 정보보호 관련 제안이나 활동들이 실질적인 업무와 연계성을 지니고 회사의 경영목표 달성에 크게 기여한다는 점을 최고 경영진에게 제시하지 못한다면 그야말로 정보보호 활동 자체가 무용지물로 전락할 수 있다. 따라서 CSO는 항상 보안전문가와 보안관리자의 의견을 종합하고 분석하여 경영활동에 이바지할 수 있는 구체적이고, 실현가능한 대책을 모색해 나가야 한다.

CSO의 기본소양과 자기계발 항목

어느 조직에서나 관리자의 지위에 있는 사람이라면 자신의 말과 행동에 책임을 질 수 있어야 한다. 하지만 보안을 총괄하는 CSO는 여기에 추가적으로 갖춰야 할 기본 소양이 있다. 무엇보다도 중요한 것은 민감한 내부정보와 조직 구성원에 대한 모니터링 결과 등 중요한 자체 분석정보에 대해 비밀을 유지하고, 조직에 대한 로열티를 지녀야 한다. 또한, 조직의 목표를 달성하기 위한 정보보호 추진 방향을 결정할 때, 보안과 업무효율성 간의 충돌을 방지하기 위하여 비즈니스에 대한 충분한 이해력을 갖춰야 한다. 현업부서의 자발적인 참여를 유도하기 위하여 원만한 커뮤니케이션 능력도 보유해야 한다.

이와 함께 보안업무의 기반이라 할 수 있는 IT 인프라와 애플리케이션에 대한 전반적인 이해는 물론, 다양한 이해관계자들의 상호 충돌이나 보안사고 대응에 걸맞는 법률지식과 경영에 대한 지식도 폭 넓게 갖춰야 한다. 따라서 보안의 총괄책임자는 문제인식 및 분석 능력과 함께 통합 및 조정 능력을 보유하고 일관된 보안정책을 펼쳐 나갈 수 있는 적극성도 지녀야 한다고 본다.

CSO는 꾸준한 자기 계발 노력을 통해 가능하다면 보안전문 자격증(SIS, CISSP, CISA 등)을 취득하거나, 정보보호 관련 학을 추가로 배우는 것도 필요하다. 즉, 자신의 Career Path나 Career Plan을 만들어 자체적으로 업무의 영역을 넓혀나가야 한다. 이런 다양한 경험과 신기술에 대한 이해 및 정보보호 관련분야의 학업 등을 통해 가장 최적의 정보보호 정책과 보안 통제수단을 결정할 수가 있다. 또한 보안활동 특성 상, 중요하고 민감한 일을 신속하고 정확하게 처리해야 하는 업무적 부담감으로 인하여 스트레스가 강한 편이기 때문에 오히려 스트레스를 즐기는 자기 관리능력도 필요하다고 본다. 보안사고나 문제점이 발생하면 근본적인 원인파악 및 대응방안 수립과 함께 강력한 실행으로 발본색원하는 자세가 필요하다. 극도의 불안감에서 안정성을 유지하면서, 침착하게 합리적으로 문제점을 분석하고 대응해 나가는 자가 치유 능력을 보유해야만 한다.

CSO에 대한 편견

대부분의 기업에서 심지어 대기업에서조차 정보보호 전담 관리자를 두고 있지 않거나, 특정 업무에 정통한 보안 전문가에게 보안업무를 총괄하도록 하는 경우가 많다. 특히, IT 출신 관리자와 직원을 묶어서 보안부서를 구성하고, 몇몇 보안 툴을 설치하는 것으로 전반적인 정보보호관리체계를 갖췄다고 오판하는 사례는 지극히 위험하다.

현재까지는 일반 IT 부서의 전문인력을 정보보호업무의 총괄책임자로 임명하는 경우가 많고, 인력보안이나 물리보안을 관리해 본 경험이 있는 경찰이나 군 출신을 비상계획 업무와 연계해 책임을 부여하는 사례도 있다. 물론 다양한 분야로부터 실질적인 정보보호 업무의 총괄 책임자를 선정할 수 있다. 하지만 급변하는 경영환경과 쉴 틈 없이 진보하는 IT의 기술발전과 보안사고의 위험성이 고조되는 상황에서는 무엇보다도 전체적인 관점에서 보안사고의 위험성과 피해를 사전에 탐지하고 예방체제를 갖출 수 경영적 마인드와 사고를 갖춘 사람을 정보보호의 총괄적인 책임자로 선정하는 것이 타당하다고 본다.

보안업무를 관장하는 임원은 CIO(Chief Information Officer) 산하에 두는 사례가 많지만, 최근에는 CFO(Chief Financial Officer) 산하 또는 CEO(Chief Executive Officer) 직속으로 편성하는 사례가 늘고 있다. 최근 들어 가장 바람직한 형태인 별도의 보안담당 임원 CSO(Chief Security Officer)나 고객들의 개인정보보호를 최우선으로 하는 통신회사 및 포털업체의 경우 CPO(Chief Privacy Officer)를 두기도 한다. 이처럼 각 기업의 특성에 따라 보안총괄 책임자나 임원을 둘 수 있지만, 특정분야를 전공한 사람만이 전체 보안영역의 책임자로 적격할 것이라는 판단의 오류는 피해야 한다고 본다.

CSO 양성방안

기업에서 최적의 CSO를 양성하고 임명하기 위해서는 보다 더 계획적이고 실질적인 육성방안이 필요하다고 본다. 먼저 각 분야(IT, 경영기획, 인사 등)에서 일정수준을 갖춘 후보군을 선정하는 것이 필요하다고 본다. 즉, 조직에 대한 로열티와 윤리의식이 강한 직원 중에서 경영 마인드와 관리능력(문제의식과 분석능력, 통합 및 조정 능력, 적극적인 사고력 등)을 갖춘 사람을 선발해야 한다. 다음은 정보보호와 관련된 별도의 교육 및 훈련, 그리고 실질적인 업무수행과정을 살펴보면서 가장 적합한 인물을 선정하는 것이 효과적이다. 무엇보다도 경영적인 마인드를 지니고 기업의 정상적인 수익창출과 핵심정보의 보호 및 업무의 원활한 수행을 지원할 수 있는 인물을 후보로 선정하여 지속적으로 양성해 나가야 하는 것이 필요하다.

바람직한 CSO가 되기 위하여

CSO는 경영진의 일원으로서 기업의 경영성과 달성에 기여할 수 있어야 한다. 즉, 생산이나 마케팅 부서의 임원처럼 직접적인 수익창출의 역할수행자는 아니지만, 기업의 핵심기술 유출이나, 해킹이나 바이러스 침투로 인한 시스템 마비, 외부세력의 불법적인 시설물 점거 등 예기치 않은 보안사고가 발생할 경우, 기업의 이미지 훼손이나 주가하락 등으로 회사의 피해는 물론, 심지어 존폐위기까지 내몰릴 수 있는 상황을 고려하여 항상 철저한 정보보호 관리체계를 유지 관리해야만 한다.

또한, 단순히 기업의 정보자산 보호활동에서 벗어나 천재지변이나 세계적인 경제환경의 변화로 직접적인 영향을 받는 글로벌 경쟁시대에 걸맞는 리스크 매니지먼트를 통해 다양한 위협에 효율적으로 대응할 수 있는 능력을 갖춰야 한다. 지속적으로 변화하는 경영환경 속에서 보안의 발전 트렌드와 이슈사항을 적기에 대비해 해결하고 최적의 정보보호 관리체제(업무효율성과 보안 안전성 동시 유지)를 운영함으로써 사전예방체제를 구축할 수 있는 역량을 키워야 한다. 더불어 CSO 본인뿐만 아니라 조직원 모두가 비즈니스와 직결된 보안체제를 갖추기 위하여 전문적인 보안지식을 쌓아야 한다. 이런 실질적이고 광범위한 영역에서의 역할모델을 통하여 무엇보다도 CEO의 강한 신뢰를 확보함으로써 단순한 실무형 임원에서 벗어나 경영과 연계한 의사결정형 임원의 자리로 나아가야 한다.

사전에 주기적으로 정기검진을 받고 응급상황 발생시 별도의 세부진단을 통해 질병의 원인을 파악하고 적절한 치료와 수술을 통해 다시 건강을 회복하는 것처럼, 정보보호 영역은 항상 IT 체계 구조도를 기반으로 시설 출입관리와 보안 거버넌스 체계상의 문제점을 사전에 인지하고 사고를 예방할 수 있는 능력을 충분히 키워 나가야 한다. 바람직한 CSO의 모습은 그런 것이다.

마지막으로, 보안활동의 핵심과 최종목표는 바로 사람을 관리하는 것임을 깨닫고, 조직원의 자발적인 정보보호실천문화를 가정에서 지키는 본능적인 보안수준으로까지 끌어올릴 수 있도록 최선의 노력을 기울여야 한다. **S**