CSO, 역할과 과제

기업에서 정보보호의 역할이 중요해 지면서 이를 책임지는 CSO제도가 점차 도입되어 가고 있다. 특히, 최근 국내 정부기관에서는 정보보호를 위한 종합대책을 발표하면서 중앙행정기관 및 지자체와 일정 규모 이상의 기업들에게 CSO 제도 도입을 의무화 하고 있다. 이런 상황에서 CSO의 역할과 변화추세, 그리고 해결해야 할 과제를 살펴보는 것은 매우 시의 적절하다고 하겠다.

글 **김정덕** | 중앙대학교 정보시스템학과 교수
jdkimsac@cau.ac.kr

CSO, 누구인가?

* * CSO의 역할은 조직의 규모와 성격, 산업의 특성, 특히 규제 감독의 정도에 따라 매우 다양하다고 할 수 있다. 그러나 대부분의 조직에서 공통적으로 발견할 수 있는 CSO의 역할은 조직의 핵심 정보시스템과 정보자산 및 프로세스를 보호하며, 정보보호 정책을 개발, 유지하는 임무를 수행하는 것이다. 즉 정보보호를 위한 기획, 개발, 운영 및 통제라는 전체 수명주기에 걸쳐 책임을 지는 자리라고 할 수 있다. 대부분의 조직에서는 이 역할은 기술 중심적이어서 IT 부서에 보고하는 경우가 많으나 점차 CSO의 역할이 기술적, 운영적 측면에서 전략적이고 전사적 측면으로 변화되고 있는 현상을 발견할 수 있다.

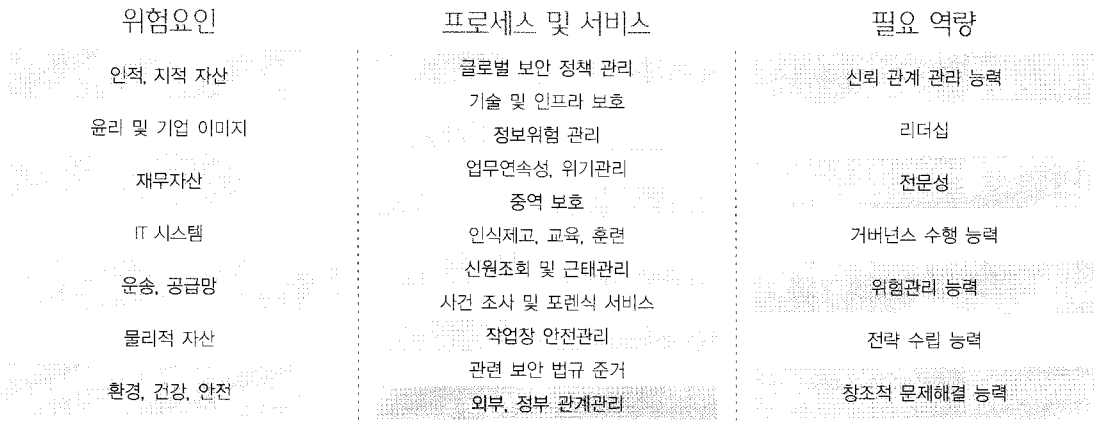
이러한 변화의 주요 원인은 정보보호 기능이 점차 분산화되고 있으며, IT 부서에서 벗어나서 수행되고 있기 때문이다. 정보보호에 대한 전략적 의사결정은 종종 상위 경영층에서 이루어지며, 보다 기본적인 정보보호 기능들은 점차 보편화/일상화 되고 있다. 이러한 경향은 현업 관리자가 일상적인 정보보호 의사결정을 내릴 수 있도록 권한위임이 되고 있다는 것을 의미하며, CSO로 하여금 보다 전략적이고 가시적인 역할을 수행할 수 있는 기회를 주고 있다는 점이다.

결과적으로, 조직에서 CSO 위상이 높아지고 있으며, 이는 CSO가 단순히 IT 전문가나 정보보호 전문가가 아닌 의사소통과 관계관리, 변화관리 등 조정 능력을 갖춘 비즈니스 관리자로서의 역할로 변화되고 있음을 보여주고 있다.

가트너의 조사에 의하면, 약 70%의 조직이 정보보호와 관련한 사안을 IT 부서장에게 보고하고 있지만, 30%의 조직은 IT 부서를 벗어나 전사위험관리 조직이나 심지어 이사회에 직접 보고하는 경우를 발견할 수 있다. 특히 법/규제 준수 책임이 큰 조직인 경우에는 위험관리부서나 준법부서와 같은 전사적 부서에 보고하는 사례를 많이 발견할 수 있다.

CSO, 누가 되어야 하는가?

* * 최근 미국표준협회(ANSI)는 미국산업보안협회(ASIS)의 정보보호책임자 가이드라인을 미국 표준으로 채택했다. 이 표준은 여러 보안 위협으로부터 조직을 보호하기 위한 CSO의 리더십 개발 및 통합 위험전략을 제공하고 있다. 이 표준은 민간과 공공부문 모두에 적용 가능하며, CSO의 주요 책임과 핵심역량, 경험, 교육과 보상뿐만 아니라 직무 모델 등에 대한 설명을 포함하고 있다.



▲ CSO 역할을 위한 모델 프로파일

앞서 그림에서 본 것처럼, CSO의 중요 책임은 클라이언트 그룹과의 효과적인 관계 정립을 유지 개선하는 일이다. 이 표준에서는 비즈니스 보호의 궁극적 책임자는 각 단위부서의 부서장이며 CSO는 위험평가, 보안정책 수립 및 지원 인프라를 제공함으로써 각 부서간의 정보보호 노력을 조정하며, 협력체계를 유지 발전시키는 역할로 규명하고 있다.

따라서 "CSO가 **되기 위한 핵심성공요인**"으로 다음과 같은 사항들을 꼽을 수 있다.

* **실용적, 혁신적 보안 솔루션을 통해 지속 가능한 비교우위를 확보할 수 있는 능력**
* **내부, 외부의 압력하에서도 정보보호 정책 및 원칙을 유지할 수 있는 능력**
* **높은 수준의 분석 능력, 관리 경험, 우수한 관계관리 역량**
* **전략 계획 수립 또는 정책 개발 경험**
* **급변하는 변화를 빠르게 적응할 수 있는 예측 및 조정 능력**
* **바람직한 행동을 유도할 수 있는 의사소통 능력**

"CSO의 **주요 책임**"은 아래와 같다:

* 전략 개발 – 보안사고를 예방하고 대응할 수 있으며, 비즈니스 연속성 계획을 수립하고 이를 상위 경영층에 분명하게 전달해야 함
* 정보 수집 및 위험평가 – 다양한 소스로부터의 정보를 수집하여 위험을 식별, 평가할 수 있어야 하며 우선순위에 기초하여 적절한 예방 전략을 수립해야 함

* 조직의 보안사고 대응능력 제고 – 보안사고나 재난에 대비해서 훈련, 연습 프로그램을 개발하고 감독해야 하며, 더불어 대응능력에 대한 주기적 검토와 평가를 수행해야 함
* 인적 자원, 핵심 비즈니스, 기업 이미지 보호 – 물리적 자산이나 정보에 대한 보호도 중요하지만, 기업 이미지나 지적재산권, 영업비밀 등 관련 위험도 면밀하게 식별하여 보호해야 하며, 기업 내 주요 인적자원 뿐만 아니라 고객정보도 포함해서 보호해야 함
* 보안사고 대응, 관리, 복구 – 보안사고 시, 대내외 자원을 적극 활용하여 적절한 의료, 재정, 감정적 지원을 제공해야 함. 또한 관련 기관과의 연락과 협조체계를 구축 활용해야 함
* 조직 외부의 이해관계자와의 협력 – 투자자, 홍보, 정부와의 관계관리를 책임지는 부서와 밀접하게 협력해야 함.

특히 CSO의 핵심역량으로는 전략적 마인드를 가지고 있어야 하며, 높은 수준의 비즈니스 이해도와 대인관계 능력이 요구된다. 또한 위기상황에서도 침착하게 적절한 해결을 모색할 수 있는 감정적인 조절 능력도 요구된다. 무엇보다 중요한 것은 상위 경영층과 이사회 구성원이 관심을 가질 수 있도록 정보보호 프로그램이나 프로젝트의 가치를 제시할 수 있는 세일즈 능력도 매우 필요한 역량이라고 할 수 있다.

CSO가 해결해야 할 5대 이슈

가트너에서는 아래와 같이 CSO가 관심을 가지고 해결 또는 연구해야 할 5대 과제를 제시하고 있다. 이 문제는 지금 현재 시점뿐만 아니라 앞으로도 지속적인 관심과 노력 속에서 해결될 수 있을 것이다.

1 정보보호에 대한 거버넌스 체계를 어떻게 수립할 것인가?

* * 대부분의 CSO는 전사적 보안을 위해 효과적 거버넌스가 매우 중요하다는 것을 인식하고 있다. 특히 정보보호에 대한 궁극적인 책임과 정보자산의 무결성은 결국 자산 소유자에게 있다는 점을 인식하여야 하고, 이는 과거의 전통적인 정보보호 모델, 즉 정보보호는 IT 조직이나 정보보호팀의 책임이라는 인식이 아니라, 자산 소유자에게 있다는 점이다. 많은 경우, 자산 소유자는 IT 조직에게 권한위임을 하는데 그 이유는 IT 조직이 IT 자산과 IT가 지원하는 비즈니스 프로세스의 보호자로서의 역할을 하기 때문이다. 이 경우, 궁극적 책임과 책임간의 분명한 구분이 있어야 한다.

2 정보보호 정책, 통제, 프로세스가 비즈니스 요구와 어떻게 연계될 수 있는가?

* * 정보보호 활동이 비즈니스 요구사항과 연계되어야 한다는 점은 어쩌면 매우 자명한 것일 수 있으나, 현실적으로 정확히 비즈니스 요구사항을 반영하고 있는 정보보호 정책, 통제, 프로세스를 개발하기 매우 어렵다. 두 영역간의 연계를 위해서는 지속적인 정보보호 정책 및 프로세스 관리과정을 구현하여야 한다. 이를 위해서는 CSO는 현업 관리자, 중역들과의 긴밀한 관계를 유지해 비즈니스의 요구사항을 식별할 수 있어야 하며, 유연하고 계층적인 정책 프레임워크를 개발할 필요가 있다.

3 정보보호에 대한 전사적인 인지/경각심을 어떻게 수립하고 유지할 것인가?

* * 전사적 정보보호에 대한 인식 또는 경각심을 어떻게 조직 내에 정착시킬 것인가 하는 문제는 지속적으로 해결해야 할 이슈이다. 이는 조직 문화의 근본적인 변화를 요구하며 그 성공을 위해서 보다 긍정적이고 비위협적인 방법으로 인식제고 노력을 기울어야 가능할 것이다. 정보보호 노력이 자신과 조직에 가치가 있는 활동이라는 점을 인식시키는 것도 중요하지만, 실제로 정보보호 수준 제고를 위해 수행해야만 하는 활동이 있으며 이를 기꺼이 실행에 옮길 수 있는 교육, 훈련 프로그램을 시행해야 한다.

4 정보보호 활동과 가치를 어떻게 효과적으로 측정하고 보고할 것인가?

* * CSO는 정보보호 활동을 측정하는 척도(Metrics) 개발과 보고(Reporting) 방법에 대해 지속적으로 고민하고 있다. 그러나 불행하게도 많은 경우 척도를 먼저 개발하고 측정 대상인 정보보호 프로그램을 차후에 수립하고자 하는 실수를 범하고 있다. 우선적으로 비즈니스 요구사항을 반영한 위험관리를 통해 필요한 보안통제수단을 구현한다면 비교적 용이하게 적절한 척도를 개발하여 정보보호 활동 및 결과에 대한 성과를 측정할 수 있을 것이다. 또한 모든 환경에 적용할 수 있는 척도나 보고방식을 규정한 표준은 없다. 가트너에서 조사한 바로는 성공적인 측정 프로그램을 구현한 조직은 전사적 보고체계와 매우 밀접하게 연계된 것을 알 수 있다. 즉, 기존의 척도를 재사용하고 보고양식도 거의 유사한 형태로 제시하고 있음을 파악하였다. 또한 효과적인 척도를 개발하고 개선시키는 것은 장기간에 걸쳐 수행된다는 사실을 간과하지 말아야 할 것이다.

5 현존 또는 미래의 기술과 비즈니스 시나리오를 지원하기 위해 정보보호 아키텍처를 어떻게 개발하고 사용할 것인가?

* * 기업환경이 점차 서비스 지향, 가상화, 소비자 지향 추세로 변화됨에 따라, 네트워크나 데이터 센터의 보안통제에서 특정 정보자산의 보안 요구사항을 만족시키는 보안통제로 변화하고 있다. 그러나 이러한 변화를 가능하게 하는 기술/방법은 아직 존재하지 않거나 미완성단계라는 점이 문제이다. 현재 특정 시점에서의 데이터나 서비스를 보호하기 위한 개념적 아키텍처를 개발하기 시작했으며, 더욱이 전사적 아키텍처와의 결합은 아직 희망사항에 머물고 있는 실정이다.

이상과 같이 CSO의 역할이 과거의 기술적 관점에서의 전문성을 요구하는 위치에서 전사적이며 전략적 관점에서 관리 능력을 요구하는 위상으로 변화함에 따라 앞으로 CSO는 새로운 과제를 해결해야 하고 이를 위한 다방면의 역량이 요구되고 있다고 할 수 있다. **S**