정보보호최고책임자의 자격요건과 역할론

Chief Information Security Officer Qualifications and Role theory

공 병 철[1]　국 경 완[2]　마 기 평[3]

◈ 목 차 ◈

1. 서　론

일상의 모든 제품이 네트워크에 연결되는 초연결 사회는 AI, IoT, 빅데이터, 클라우드 등 4차산업으로 급속하게 확대되면서, 글로벌 인터넷 환경은 지능화·고도화되는 사이버 공격의 지속적인 증가와 더불어 개인정보와 민감정보들의 반복적인 피해로 현업에서 활동하는 정보보호최고책임자(CISO)의 역할이 부각되고 있다.

정부부처와 공공 부문의 보안 전담조직(정보보호담당관)과 일선 현장에서 활동을 하고 있는 정보보호최고책임자(이하, CISO)는 조직의 임원진으로써 다른 조직의 임원들과의 원활한 소통과 협업을 통하여 조직內 정보보호관리체계(거버넌스) 구축과 관리적, 물리적, 기술적, 법률적 전문성 강화를 실현하는 중요한 역할을 담당하고 있다.

지난 2018년 6월 12일 정「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하, 정보통신망법)」이 개정되면서 사이버보험 가입 의무화(제32조의3)와 임원급의 정보보호최고책임자의 지정 및 겸직 금지(제45조의3제3항 및 제7항 신설 등)하고, 자격요건 등을 대통령령으로 정하는 내용이 통과가 되었으며, 중기업 이상의 정보통신서비스 제공자, 자본금 1억 원 이하의 부가통신사업자를 제외한 모든 전기통신사업자와 정보보호관리체계(ISMS) 인증을 받아야 하는 모든 정보통신서비스 제공자 등 4만1천 여 개 기업은 정보보호최고책임자를 의무지정하고 이를 과기정통부장관(중앙전파관리소장에게 위임)에게 신고하는 시행령을 지난 2019년 6월 25일 개정 하였다. 따라서, 조직의 C-level 임원으로 활동하기 위한 다양한 전문적 지식이 요구되는 CISO 자격요건과 업무를 원할하게 수행함에 있어서의 역할론을 살펴보고자 한다.

2. 정보보호최고책임자(CISO) 자격요건

2.1 정보보호최고책임자의 정의

2.1.1 용어의 정의

CISO는 기업에서 정보 보안을 위한 기술적 대책과 법률 대응까지 총괄 책임을 지는 최고 임원을 지칭한다. ※ 출처 KISA

조직의 비전과 미션을 수행하기 위하여 정보 자산을 안정적으로 운영하는 데 필요한 정보보호 전략 및 정책을 수립하고, 관련 법제도 준수, 보호관리 활동을 수행하며, 위험관리에 기반한 정보보호 대책을 도출하고 실행하는 일을 임무로 한다. ※ 출처 NCS

정보보호최고책임관리사는 정보시스템의 사이버 공격에 대한 예방과 신속한 대응을 위한 정보보안에 대한 전문지식과 운용 능력을 갖추고, 정보보호 관련 법률과 규제를 만족하는 조직의 정보보호관리체계 정책 기획수

1 (사)한국사이버감시단
2 국방통합데이터센터
3 정보보호인정협회

립 및 정보보호를 위한 자원 확보, 성과 검토, 주요 정보자산의 기밀성·무결성·가용성·관리 적정성을 점검 등의 거버넌스 구현하고 관리하는 업무 수행 능력을 가진 자를 말한다. ※ 출처 CISO-CQ

2.2 정보보호최고책임자 법률 관련 근거

2.2.1 관련 법률의 명시

관련 법률에서는 CISO의 자격요건으로 정보보호 또는 IT 분야의 학력 및 자격(경력)을 충족하도록 요구하고 있다. 특히, CEO를 비롯하여 타 임원들에게 정보보호의 중요성 설명하고 이해상충 시 이를 조정하기 위해서는 정보보호 및 실무적 지식을 겸비해야 하며, 정보보호 이슈에 대한 신속하고 정확한 의사결정을 내리고, 정보보호 조직을 효율적으로 운영하기 위한 리더십을 갖출 필요가 있다.

정보통신망법(제45조의3제3항 및 제7항 신설 등)에서는 예외 요건에 해당하지 않는 정보통신서비스제공자는 임원급의 CISO를 지정, 신고하여야 하며, 일정 요건에 해당하는 정보통신서비스제공자의 CISO는 제4항에서 지정된 업무 외의 다른 업무를 겸직할 수 없다. 라고 명시하고 있다.

정보통신망법 제45조의3 (정보보호 최고책임자의 지정 등)

① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하지 아니할 수 있다.

② 제1항에 따른 신고의 방법 및 절차 등에 대해서는 대통령령으로 정한다.

③ 제1항 본문에 따라 지정 및 신고된 정보보호 최고책임자 (자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우로 한정한다)는 제4항의 업무 외의 다른 업무를 겸직할 수 없다.

④ 정보보호 최고책임자는 다음 각 호의 업무를 총괄한다.

1. 정보보호관리체계의 수립 및 관리·운영
2. 정보보호 취약점 분석·평가 및 개선
3. 침해사고의 예방 및 대응
4. 사전 정보보호대책 마련 및 보안조치 설계·구현 등
5. 정보보호 사전 보안성 검토
6. 중요 정보의 암호화 및 보안서버 적합성 검토
7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

⑤ 정보통신서비스 제공자는 침해사고에 대한 공동 예방 및 대응, 필요한 정보의 교류, 그 밖에 대통령령으로 정하는 공동의 사업을 수행하기 위하여 제1항에 따른 정보보호 최고책임자를 구성원으로 하는 정보보호 최고책임자 협의회를 구성·운영할 수 있다.

⑦ 정보보호 최고책임자의 자격요건 등에 필요한 사항은 대통령령으로 정한다. 〔시행일 : 2019.6.13.〕

정보통신망법 시행령 제1항에 대해 소기업과 소상공인을 예외로 인정하였으며, 겸직금지 요건으로는 자산총액 5조 원 이상인 자와 정보보호 관리체계 인증 의무대상자 중 자산총액 5천억 원 이상인 자로 하였으며, 직무 수행에 필요한 정보보호 또는 정보기술 관련 전문지식이나 실무 경험이 풍부한 자를 지정하도록 자격요건을 명시하였다.

제36조의6 (정보보호 최고책임자의 지정 및 겸직금지 등)

② 법 제45조의3제1항 및 제7항에 따라 정보통신서비스 제공자가 지정·신고해야 하는 정보보호 최고책임자는 다음 각 호의 어느 하나에 해당하는 자격을 갖추어야 한다. 이 경우 정보보호 또는 정보기술 분야의 학위는 「고등교육법」 제2조 각 호의 학교에서 「전자금융거래법 시행령」 별표 1 비고 제1호 각 목에 따른 학과의 과정을 이수하고 졸업하거나 그 밖의 관계법령에 따라 이와 같은 수준 이상으로 인정되는 학위를, 정보보호 또는 정보기술 분야의 업무는 같은 비고 제3호 및 제4호에 따른 업무를 말한다.

1. 정보보호 또는 정보기술 분야의 국내 또는 외국의 석사학위 이상 학위를 취득한 사람
2. 정보보호 또는 정보기술 분야의 국내 또는 외국의 학사 학위를 취득한 사람으로서 정보보호 또는 정보기술 분야의 업무를 3년 이상 수행한 경력이 있는 사람
3. 정보보호 또는 정보기술 분야의 국내 또는 외국의 전문학사 학위를 취득한 사람으로서 정보보호 또는 정보기술 분야의 업무를 5년 이상 수행한 경력이 있는 사람
4. 정보보호 또는 정보기술 분야의 업무를 10년 이상 수행한 경력이 있는 사람
5. 법 제47조 제6항 제5호에 따른 정보보호 관리체계 인증 심사원의 자격을 취득한 사람
6. 해당 정보통신서비스 제공자의 소속인 정보보호 관련 업무를 담당하는 부서의 장으로 1년 이상 근무한 경력이 있는 사람

③ 법 제45조의3제3항에서 "자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자"란 정보통신서비스 제공자로서 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 직전 사업연도 말 기준 자산총액이 5조원 이상인 자
2. 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 직전 사업연도 말 기준 자산총액 5천억원 이상인 자

④ 제3항에 따른 정보통신서비스 제공자가 지정·신고해야 하는 정보보호 최고책임자는 제2항에 따른 자격 요건을 충족하고, 상근하는 자로서 다음 각 호의 어느 하나에 해당하는 자격을 갖추어야 한다. 이 경우 정보보호 또는 정보기술 분야의 업무는 「전자금융거래법 시행령」 별표 1 비고 제3호 및 제4호에 따른 업무를 말한다.

1. 정보보호 분야의 업무를 4년 이상 수행한 경력이 있는 사람
2. 정보보호 분야의 업무를 수행한 경력과 정보기술 분야의 업무를 수행한 경력을 합산한 기간이 5년(그 중 2년 이상은 정보보호 분야의 업무를 수행한 경력이어야 한다) 이상인 사람 〔전문개정 2019. 6. 11.〕

○ 「전자금융거래법」 제21조의2(정보보호최고책임자 지정) 제1항에 의거 금융회사 또는 전자금융업자는 전자금융업무 및 그 기반이 되는 정보기술부문 보안을 총괄하여 책임질 정보보호최고책임자를 지정하며, 제3항에 의거 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 금융회사 또는 전자금융업자의 정보보호최고책임자는 다른 정보기술부문 업무를 겸직할 수 없도록 명시하고 있다.

전자금융거래법 제21조의2 (정보보호최고책임자 지정)

① 금융회사 또는 전자금융업자는 전자금융업무 및 그 기반이 되는 정보기술부문 보안을 총괄하여 책임질 정보보호최고책임자를 지정하여야 한다.

② 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 금융회사 또는 전자금융업자는 정보보호최고책임자를 임원(「상법」 제401조의2제1항제3호에 따른 자를 포함한다)으로 지정하여야 한다.

③ 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 금융회사 또는 전자금융업자의 정보보호최고책임자는 제4항의 업무 외의 다른 정보기술부문 업무를 겸직할 수 없다.

④ 제1항에 따른 정보보호최고책임자는 다음 각 호의 업무를 수행한다.

1. 제21조제2항에 따른 전자금융거래의 안정성확보 및 이용자보호를 위한 전략 및 계획의 수립
2. 정보기술부문의 보호
3. 정보기술부문의 보안에 필요한 인력관리 및 예산편성
4. 전자금융거래의 사고 예방 및 조치
5. 그 밖에 전자금융거래의 안정성 확보를 위하여 대통령령으로 정하는 사항

- 시행령에서는 직전 사업연도 말을 기준으로 총자산이 2조원 이상이고, 상시 종업원 수가 300명 이상인 금융회사 또는 전자금융업자는 정보보호최고책임자를 임원으로 지정하고 자격요건에 대하여 명시하고 있다.

제11조의3(정보보호최고책임자 지정대상 금융회사 등)

④ 법 제21조의2제5항에 따른 정보보호최고책임자의 자격요건은 별표 1과 같다.

〔별표 1〕 정보보호 또는 정보기술(IT) 분야의 학력 또는 기술자격을 가진 사람으로서 다음 각 목의 어느 하나에 해당하는 사람은 정보보호최고책임자의 자격을 가진다.

가. 정보보호 또는 정보기술(IT) 분야의 전문학사학위를 취득한 후 4년 이상 정보보호 분야 업무 또는 5년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람

나. 정보보호 또는 정보기술(IT) 분야의 학사학위 또는 다음 전문자격을 취득한 후 2년 이상 정보보호 분야 또는 3년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람

2.3 정보보호최고책임자 지정 현황

2.3.1 일반 현황

구분	정보관리책임자 CIO	정보보호최고책임자 CISO	개인정보관리책임자 CPO
전체	8.7%	8.8%	8.4%
농림수산업	17.8	17.7	9.4
제조업	8.5	8.0	7.2
건설업	3.9	6.4	3.9
도·소매업	6.7	5.4	1.9
운수업	2.5	4.1	3.6
숙박 및 음식점업	2.2	1.9	1.9
정보서비스업	41.3	28.2	28.3
금융보험업	52.5	63.6	64.7
부동산 및 임대업	4.9	2.9	3.7
기술서비스업	16.0	12.7	12.9
시설/사업 지원	16.9	16.1	13.4
협회·단체·수리 및 개인 서비스업	4.3	4.1	3.9
기타 서비스업	12.1	15.4	13.4

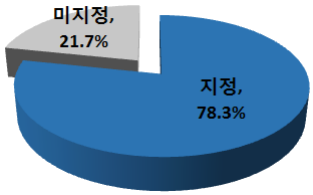
※ 출처 : 과기정통부, 2018년 정보보호실태조사

2.3.2 금융권 CISO 지정현황

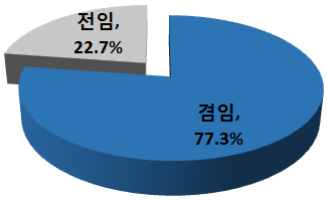
금융권 보안 강화를 위해 도입된 정보보호최고책임자 지정 현황을 살펴보면 총 152개 응답기관 중 78.3%(119개 기관)가 임원급 CISO를 지정하여 운영하고 있는 것으로 조사되었다.

업종별로는 국내 은행의 경우 전체 은행이 임원급 CISO를 지정하고 있으며 전임 비중은 21.1%로 작년

금융기관 CISO 임원 지정 현황

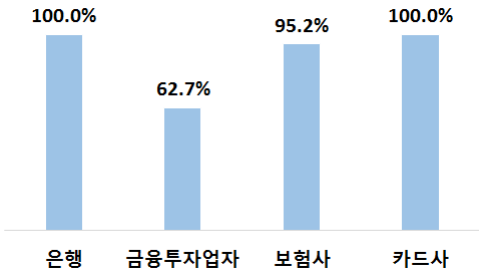


CISO 임원 전임 현황

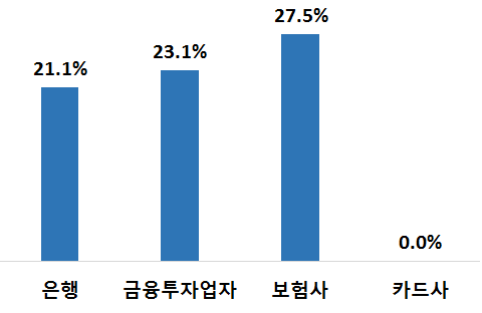


(17.6%)보다 증가하였다. 증권사의 경우 임원급 CISO를 지정하는 비중은 62.7%이며 전임 비중은 23.1%로 나타났고, 보험사의 임원급 CISO 지정 비중은 95.2%, 전임 비중은 27.5%로 나타났다. 한편 카드사는 전체가 임원급 CISO를 지정하고 있으나 전임 비중은 0%이었다.

업종별 CISO 임원 지정 비중



업종별 CISO 임원 전임 비중



※ 출처: 한국은행, 금융결제국 2017년도 금융정보화 추진현황

3. 정보보호최고책임자(CISO) 역할

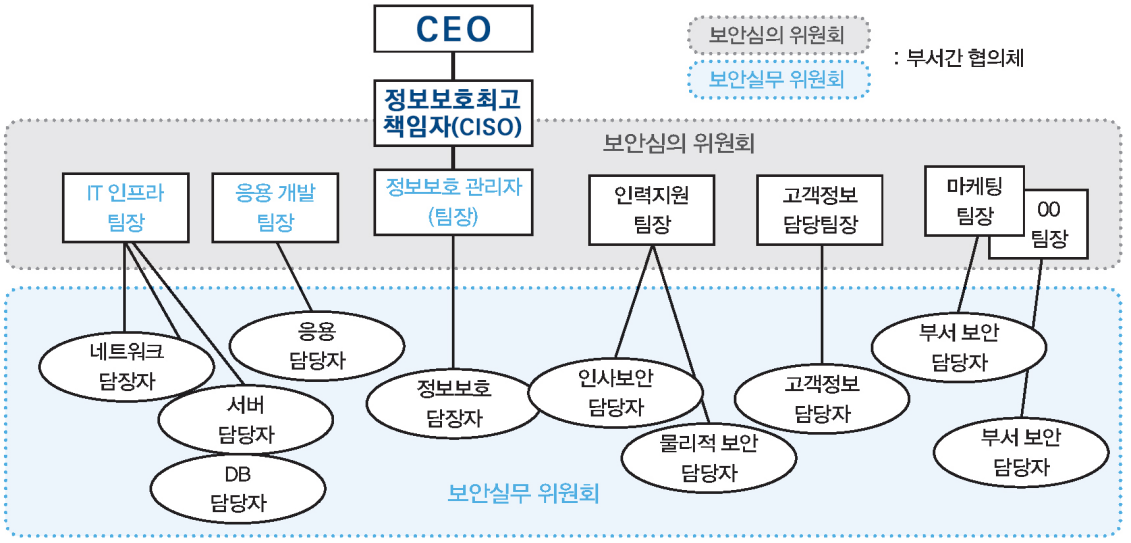
3.1 정보보호 조직의 구성

3.1.1 조직구성의 개요

공공기관과 기업의 정보보호거버넌스 구현을 위하여 정보보호관리체계 수립과 시행을 위한 전담조직을 구성하여야 한다. 단, 조직의 규모에 따라 구성시 차이가 있을 수 있다.

1) 일반적인 거버넌스는 통치, 관리, 통치 방식을 의미하며, 어떤 목적을 이루어 나가는 과정을 관리하기 위해서는 계획(Planning), 통제(Control), 조직화(Systematization), 감시(관찰; Monitor), 지휘(Command), 평가, 개선 등 일련의 활동을 의미한다.
2) 공공 거버넌스는 사회 내 다양한 기관(중앙정부, 지방정부, 사회단체, NGO 등)이 자율성을 지니면서 함께 국정운영에 참여하는 변화 통치방식을 말하며, 다양한 행위자가 통치에 참여·협력하는 점을 강조해 '협치'라고도 한다.
3) 기업 거버넌스는 조직의 목적 달성을 지향하도록 조직 내 활동들을 통지, 지휘, 관리, 감시하기 위해 최고경영진 및 이사회가 구현한 프로세스 및 구조의 집합으로써 효과성, 책임성, 투명성을 바탕으로 기업목표를 가지고 경영활동을 수행하도록 하는 것을 말한다.
4) IT 거버넌스는 조직의 목표와 IT와 연계, 이익 창출, 위험 관리, 자원 최적화 관리, IT 성능을 측정 등 거버넌스의 일부분이다.
5) 정보보호 거버넌스는 IT 거버넌스, 기업 거버넌스의 하위에서 정보보호 분야를 특화하는 전사적 정보보호 관리체계를 통칭하며, ISO/IEC 27014:2013(Information Technology－Security Techniques－Governance of Information Security)에 의하여 국제 표준으로 그 개념과 원칙이 지정되어 있다. 또한 핵심 활동으로 평가(Evaluate), 지시(Direct), 감시(Monitor)를 중심으로 이사회와 임원의 역할 및 책임을 정의한다.

정보보호 조직은 정보보호 활동을 수행하기 위하여 책임, 권한, 관계가 정의된 조직, 인원 등을 말하며, 정보보호 전담조직은 정보보호 업무를 체계적이며 책임성 있게 수행하기 위해서 정보보호 전문지식을 가지고 정



보보호관리체계를 운영하는 조직으로 정보보호팀, 개인정보보호팀, 침해사고&재해복구 대응팀, 보안 감사팀 등을 구성하는게 일반적이다.

정보보호 조직 구성원은 정보보호최고책임자, 정보보호 관리자, 부서별 정보보호 담당자, 정보통신 분야별 담당자, 비정보통신 업무부서 담당자 등으로 나눌수 있으며 조직의 규모와 특성에 따라 역할이 변경될 수 있다.

3.2 CISO의 전담조직 구성

3.2.1 CISO 전담조직 구성의 개요

CISO가 정보보호 업무에 대한 의사결정 권한을 갖고 CIO 등 타 임원들과 협업하기 위해서는 C-Laver의 임원으로 지정되는 것이 바람직하며, CISO의 조직은 같이 다른 조직에 속하지 않고 CEO에게 직접 보고하는 별도의 조직으로 구성하는 것이 효과적이다.

3.2.2 CISO 전담조직 구성시 고려사항

CISO는 CIO와 정보보호 대책구현 및 운영 업무에 대한 최종 책임 또는 수행 책임을 공유하므로, IT 조직과의 갈등을 최소화하기 위해서는 정보보호 업무와 IT업무를 명확히 구분 할 필요가 있다.

1) 정보보호 업무의 우선순위가 IT업무의 우선순위보다 낮아질 수 있으므로, CEO 및 CFO는 정보보호 위협, 취약점, 위험 등을 고려하여 요구되는 정보보호 대책과 예산의 적절성을 객관적으로 검토하여 전략수립과 이행 계획을 수립 할 필요가 있다.
2) 정보보호 전략, 계획 및 정책 수립, 취약점 진단 및 위험평가 결과와 대책 선정, 침해 사고 대응 등의 업무는 CIO가 CEO에게 보고하는 체계 보다는 CISO가 CIO와 검토 후 CISO가 CEO에게 직접 보고할 수 있는 체계를 구축한 것이 바람직하다.
3) IT 운영 업무에 대한 점검 또는 감사가 제한되면, 발견된 문제의 축소 또는 은폐가 가능하므로, 감사조직은 주기적으로(연 1회 이상) 정보보호 및 IT업무에 대한 감사를 수행하여 투명성을 보증할 필요가 있다.
4) CISO는 조직의 정보보호 위험 대비 구현된 대책 수준을 검토하여 전담조직 구성 및 CIO 조직과의 분리를 위한 객관적인 평가 보고서를 제출할 필요가 있다.
5) CISO가 CPO 겸직 시 개인정보보호 정책 및 대책은 타 임원 및 조직과 협의하여 수립하고, 통제의 운영은 관련 부서에서 수행되도록 역할을 구분 할 필요가 있다.

3.2.3 CISO 전담조직의 역할

CISO는 정보보호 전략수립, 조직 구성 및 운영, 위험관리 등 거버넌스 업무 대부분의 최종 책임과 수행 책임

이 있으므로, CEO의 전폭적인 지지 및 타 임원들과의 원활한 의사소통을 통해 해당 업무 수행의 효과성을 극대화하기 위한 것이다.

1) CISO는 중복투자 및 타 조직과의 갈등을 최소화하기 위하여 정보보호 전략 및 계획, 정책수립, 취약점 진단 및 위험평가 결과와 대책 수립, 정보보호 사고 대응 시 CEO에게 보고 전에 타 임원들과의 사전 협의를 통해 보고 내용을 조정해야 한다.
2) CISO는 정보보호 예산 확보, 정보보호 감사(관리체계 점검 및 개선), 정보보호 대책 구현 등 업무 전반에 대하여 타 임원과의 원활한 소통 및 협업을 통해 신속하게 전달하여 조직의 수행 책임을 공유하여야 한다.
3) CEO 및 C레벨 임원들과의 소통 시에는 단순히 법규 준수를 위한 정보보호 활동이 아닌 정보보호 대책이 미흡할 시 회사에 재무적, 운영적, 법률적으로 어떠한 위험이 존재하며, 어느 정도의 부정적인 영향을 미치는지 설명할 수 있는 위험 관리 기반의 소통 역량이 필요하다.
4) 조직의 비즈니스 환경을 고려한 전사적 정보보호 위험식별 및 평가를 기반으로 정보보호 대책을 선정하고 취약점 분석평가를 통해 위험관리 업무를 총괄해야 한다.
5) 정보보호 정책 수립, 정보보호 위험관리, 정보보호 대책구현 시 정보보호 업무와 개인정보보호 업무 중 중복되는 업무를 식별하여 비용 효과적으로 대책을 수립하고 운영하여야 한다.

3.2.4 CISO 전담조직 인력의 관리

사람에 의한 실수, 도난, 사기, 오용 등을 줄이기 위해서는 직원 채용 단계에서부터 당사자의 정보보호 책임이 언급되어야 하며 이는 계약서에 포함되어야 하며 그 직원이 근무하는 동안 지속적으로 관찰하기 위한 것이다.

1) 민감한 직책에 대해서는 특히 직원을 적절히 선정하여야 한다.
2) 정보처리시설을 사용하는 모든 내부 사용자와 제3자 사용자(외부 하청업자, 서비스 제공자)들은 정보보호 동의서에 서명하여야 한다.
3) 신규 채용시 비밀유지 동의를 이용하여 정보가 비밀사항이라는 점을 인식시켜야 한다.
4) 직원의 고용이 끝나는 경우 해고 통보와 동시에 적절한 종료절차를 처리해야 한다.
5) 정보보호에 대한 인식을 높이기 위한 교육을 수행해야 한다.
6) 조직의 정보보호 정책에 따라 각 직원의 정보보호 역할 및 책임은 필요한 경우 문서화(직무기술서) 되어야 한다.
7) 임직원과의 계약서에는 만일 이들이 불법적인 접속을 시도하는 경우의 처벌 내용을 명시하는 문구를 포함해야 한다.

정보보안에 적극적인 활동이나 규정 준수, 사이버 대응 훈련 우수 등 타의 모범이 되는 경우에는 적절한 포상 수여 및 관련한 내용이 지침이나 규정에 명시되어야 한다.

3.3 CISO의 업무와 문제점

3.3.1 CISO의 업무와 역할

비즈니스 요구사항의 반영 및 사업전략과 정보보호 전략의 연계 역할 수행 업무를 수행하기 위한 것이다.

1) 조직 전반의 정보보호 정책 및 규정(정책, 지침, 매뉴얼, 직무기술서 등) 수립한다.
2) 정보보호 전략, 계획 및 정책 수립, 위험관리, 감사 등 예산 확보 및 집행 업무를 수행한다.
3) 중장기 정보보호 전략 및 계획수립, 취약점진단 및 위험평가 결과와 대책 선정 업무를 수행한다.
4) 정보보호 전략이 비즈니스 전략에 포함될 수 있도록 전략 및 기획, 홍보 부서 등과의 유기적인 협업체계 구축 (CIO와의 충분한 협의를 통해 정책 이행 계획 수립) 업무를 수행한다.
5) 서버, 네트워크, 정보보호시스템, 웹, 모바일, 단말기, 인프라 등 관련된 기술적 정보보호 대책과 침해사고 대응 수립 업무를 수행한다.
6) 임직원의 정보보호에 대한 부정적 인식을 전환하기 위하여 긍정적인 정보보호 문화 형성 및 유지와 정보보호 교육계획 수립 업무를 수행한다.
7) 정보보호 관련 법규 및 정책 위반자에 대한 징계 요구를 위하여 위반의 고의성, 파급효과 등 객관적인

기준 수립 업무를 수행한다.
8) 비즈니스의 복잡성 증가, 새로운 기술의 등장 등 비즈니스 및 정보보호 환경 변화에 따른 전사적 정보보호 활동시 조직 또는 부서 간 갈등을 조정하는 역할이다.

3.3.2 CISO의 일반적인 업무

CEO와의 원활한 의사소통을 통해 신속한 의사결정 및 실행권한 확보하기 위한 것이다.

1) 원활한 의사 결정을 위한 정보보호위원회 구성과 실무협의체의 운영 업무를 수행한다.
2) IT조직 및 비IT조직과의 원활한 소통 및 협업을 통한 전사적 정보보호 업무를 수행한다.
3) 정보보호 감사 등 내부통제 관련 이행과 정보보호 규정 위반자에 대한 징계조치 업무를 수행한다.
4) 법률적 문제 발생시 신속한 대응 업무를 수행한다.
5) 기술적 침해사고(디도스, 악성코드 감염, 해킹 등) 대응 등 비상대응 신속한 처리업무를 이행한다.
6) 침해사고 & 재해복구 조직 구성 및 대응 훈련 시행 업무를 수행한다.
7) 인적보안, 출입통제 등 비IT 정보보호 통제의 운영 업무를 수행한다.

3.3.3 CISO의 활동과 역할이 원활하지 못할 경우 발생가능한 문제점

1) 정보보호 업무가 IT 업무보다 우선 순위에 밀려 정보보호 활동 제한이 될수 있다.
2) 기술적 대책 중심의 정보보호 대책 수립으로 관리적, 물리적 대책 수립 및 운영에 제약이 따른다.
3) CISO의 역량이 부족할 경우 IT조직 및 비IT조직과의 갈등을 유발한다.
4) CISO의 직급이 낮을 경우 타 임원들의 견제를 받아 신속한 의사결정에 제약이 발생된다.
5) 인프라, PC 보안 등 정보보호 대책구현 및 운영 업무의 원만한 수행이 어려워진다.
6) IT운영 업무에 대한 점검 또는 감사가 제한되면, 발견된 문제의 축소 또는 은폐가 발생 될수 있다.
7) CEO에게 보고 시 정보보호 이슈 중 일부 사안이 누락될 수 있다.
8) 정보보호 업무가 단순 지원업무에 그칠 수 있다.

4. 바람직한 발전 방안

4.1 대내외 환경분석

4.1.1 인터넷 이용자의 불감증 증대

인터넷이 생활 필수요소로 작용하는 시대에 살아가는 국민들은 정보보안에 대한 인식부족과 인터넷 공간에서의 위기·위험에 대한 높은 불감증을 호소하고 있다.

1) 지난 1998년 국민의 정부인 김대중 대통령 시절 IMF 사태로 침체에 빠진 경제에 활력을 불어넣기 위하여 정보기술(IT) 관련 벤처기업을 육성을 최우선 국정과제 추진하였다.
2) 이러한 정책의 효과로, 경제 환란의 여파에도 불구하고 중소벤처기업의 성장기여율은 대기업에 비해 높았으며, 초고속 인터넷 보급과 콘텐츠 산업의 성장을 통하여 인터넷 산업이 오늘날 한국 경제의 한 축이 되는 기틀을 다질 수 있었다.

정부의 정보화 촉진과 정보산업 진흥으로 다음, 네이버, 인터파크, 리니지 등이 IT기업이 성장하였으며, 이들 기업이 제공하는 무료 콘텐츠가 늘어나면서 이용자의 개인정보 DB가 대량화되어지고(일부 소규모 기업들로부터 무분별하게 수집), 활용되면서 정보화의 역기능 또한 자연스럽게 나오기 시작되었다.

1) 대표적인 사이버 공격은 1999년 4.26 CIH 바이러스 대란, 2003년 1.25 인터넷 대란, 2009년 7.7 DDoS 공격 이였으며 이러한 공격으로 주요 인터넷 사이트의 접속 불가 사태가 발생하여 사회적 혼란을 경험했다.
2) 개인정보 유출사태는 2008년 옥션 1000만건, 2010년 25개 업체 2000만여건, 2011년 네이트닷컴 3500만건과 넥슨코리아 1320만, 2012년 KT 휴대전화 가입자 870만건, 2014년 국민/NH농협/롯데 카드3사 약 1억건 네이버 20만건 티몬 115만건, 2015년 아이핀 75만건 부정 발급, 2017년 알툴즈 13만여건 등 최근까지도 지속적으로 발생하고 있다.

4.1.2 외부환경 변화

이제는 일상의 모든 제품이 네트워크에 연결되는 초

연결 사회와 4차산업혁명 시대를 맞이하고 있으며 AI, IoT, 빅데이터, 클라우드, 5G 등의 최신 ICT기술들이 급속하게 확대되면서, 글로벌 인터넷 환경은 지능화·고도화되는 사이버 공격의 지속적인 증가와 개인정보와 민감정보들의 반복적인 피해로 현업에서 활동하는 CISO의 역할이 부각되고 있다.

4.1.3 내부환경 변화

정부는 CISO를 의무지정하여 신고하는 제도를 전자금융거래법에 근거하여서는 2011년부터, 정보통신망법에 근거하여 2014년부터 운영하고 있으며, 임원급의 CISO지정과 겸직금지 규정은 전자금융거래법에서는 2013년부터, 정보통신망법에서는 2019년 6월 25일 시행령 개정하였다.

4.2 정보통신망법 시행령 CISO 규정에 대한 정책적 제언

4.2.1 CISO 자격요건을 산업현장 수요에 맞는 경력요건으로 높일 필요가 있다.

1) 시행령에는 자격요건을 직무 수행에 필요한 정보보호 또는 정보기술 관련 전문지식이나 실무 경험이 풍부한 자로써 4년 이상의 정보보호 분야 또는 5년 이상 정보기술 분야(정보보호 2년 포함)의 경력을 구비하도록 명시하고 있으나 4년의 경험치는 글로벌 인터넷 산업환경에 대응할 능력이 부족할 수 있다.
2) 기업 및 기관들은 CISO 선정시 자체적으로 평가기준을 마련하여 현장 전문가를 확보할 수 있는 구체적인 가이드라인을 제시가 필요하다.

4.2.2 CISO의 권한의 범위를 구체적으로 명시할 필요가 있다.

1) CISO는 정보보호 전략수립, 조직 구성 및 운영, 위험관리 등 거버넌스 업무 대부분의 최종 책임과 수행책임이 있으므로, CEO의 전폭적인 지지 및 타 임원들과의 원활한 의사소통을 통해 해당 업무 수행의 효과성을 극대화하는 역할을 수행해야 하므로써 적절한 권한의 보장이 필요함.
2) CISO는 정보보호 예산 확보, 정보보호 감사(관리체계 점검 및 개선), 정보보호 대책 구현 등 업무 전반에 대하여 타 임원과의 원활한 소통 및 협업을 통해 신속하게 전달하여 조직의 수행 책임을 공유해야 하므로 적절한 권한 보장이 필요하다.
3) CISO 전담조직과 역량있는 전문인력을 선발하고 배치할 수 있는 재량권과 예산을 집행할 수 있는 권한 부여가 필요하다.

4.2.3 법률에서 CISO를 '임원급'으로 지정하도록 명시하고 있으나 '급'의 명시는 악용될 소지가 있다.

1) 일부 기업에서는 부장이나 팀장급을 '임원급'으로 보임하여(예: 상무보) 권한은 없으면서 책임만 지는 CISO를 지정하는 경우가 있을 수 있다.
2) 전자금융거래법에는 '임원'으로 명시
CISO 지정신고서 양식의 작성란에 직급/직책은 인사발령을 통한 정식 임원임을 입증하는 서류를 제출이 필요하다.
3) 매년 년초에 'CISO 지정신고서'를 새로이 받아서 운영관리의 실효성이 필요하다.
4) 규모가 작은 조직에서 CISO를 지정할 만한 임원이 없을 경우 CEO가 직접 CISO를 겸직해야 한다는 점을 명확히 할 필요가 있으며, 규모가 작은 조직은 CEO가 직접 CISO 역할을 수행해야 효과적인 정보보호 전략 수립과 예산집행 및 실효적인 이행 점검이 가능하다.

4.2.4 CIO가 CISO를 겸직해서는 안된다는 규정을 명확히 할 필요가 있다.

1) 기업의 효율성, 경영혁신과 비즈니스 지원을 목표로 하는 CIO는 정보보안 리스크의 최소화를 위해 기업의 미션과 목표를 수립하는 CISO 역할과 상충할 수 있어 CIO가 CISO를 겸직할 경우 보안리스크 관리 기능이 약화될 수 있다.

4.2.5 CISO가 CPO 및 DPO를 겸직할 수 있는 근거를 마련해 주어여야 한다.

1) 개인정보의 처리에 관한 총괄 업무를 담당하는 CPO의 업무는 본질적으로 보안리스크를 관리하는 CISO의 업무범위에 속하며 이용자의 개인정보를 보호해야 하는 CPO의 업무는 법률적(보호조치 기준 제6호)으로 중요 정보의 암호화를 관리해야 하는 CISO의

업무이기도 하다.

2) 정보통신망법(제28조 제1항 제4호, 시행령 제15조 제4항)에서는 개인정보를 안전하게 저장・전송할 수 있는 암호화기술 등을 이용한 보안조치를 위하여 기술적・관리적 조치를 하여야 한다라고 명시하고 있다.
3) EU GDPR의 규정에는 관련 분야 전문지식과 임무수행 능력을 가진 독립성을 지닌 데이터보호책임자(DPO)를 지정하도록 명시하고 있어 이 또한 CISO의 업무에 속한다.

5. 결 론

대한민국은 세계 최고수준의 정보통신기술과 관련 인프라를 보유하고 있으며, 국민은 일상생활에서 다양하고 편리한 사이버 공간을 통해 삶의 지평을 넓혀왔다.

사이버공간은 기업의 경제활동과 정부의 행정 서비스 등 국가 운영의 핵심기반으로 자리매김하고 있으며, 다가오는 4차산업혁명시대는 일상의 모든 제품이 인공지능(AI)·사물인터넷(IoT)·빅데이터 기반의 첨단 사이버 기술 개발과 아울러 5G 네트워크로 연결되는 초연결 사회가 될 것이다.

최근 개인이나 해커그룹이 주도하던 사이버공격이 범죄·테러 단체로 확산되고 국가가 개입·지원하는 등 조직화·대규모화 되는 사이버범죄와 테러가 급증하면서, 국민의 일상과 기업의 경제활동이 위협받고 있다.

정부는 사이버위협을 안보위협으로 인식하여 모든 역량을 결집·대응할 수 있도록 「국가안보전략」에 따라 「국가사이버안보전략」을 최초로 수립하고, 사이버위협으로부터 우리의 사이버공간을 보호하여 국민 모두가 사이버공간을 더 안심하고 향유할 수 있도록 노력하고 있다.

CISO는 조직의 정보자산을 안정적으로 운영하는 데 필요한 정보보호 전략 및 정책을 수립하고, 관련 법제도 준수, 보호관리 활동 수행, 위험관리에 기반한 정보보호 대책을 도출하고 실행하는 등 정보보안을 위한 기술적 대책과 법률 대응까지 총괄 책임을 지는 최고 임원을 지칭한다.

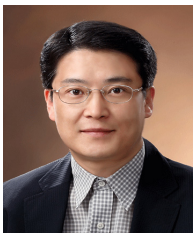
정부는 사이버안보 전문인력을 지속 확충하고 관련 예산을 별도 항목으로 편성·확대하고 있으나, 정보보안 산업의 지속적인 성장과 수요의 급증으로 전문 인력의 질적·양적 부족 현상도 심각하게 발생하고 있다.

공공기관과 기업 현장에서 활동하는 정보보호최고책임자의 역할과 현장 전문가 인력 양성이 그 무엇보다 중요한 시점으로써 정부의 CISO제도가 산업현장에서 실효성 있게 운영되어 국민으로부터 안전하고 신뢰할 수 있는 인터넷 환경과 정보보안에 대한 인식향상 및 대중적인 정보보호 마인드 활성화를 위한 다양한 방안들이 추가적으로 연구하는 것도 가능할 것으로 판단된다.

참 고 문 헌

[1] KISA www.boho.or.kr/ciso/
[2] NCS, 정보보호관리·운영 직무 정의 (직능수준8, 직무경험 16년 이상 www.ncs.go.kr
[3] 정보보호최고책임관리사, www.ciso-cq.com
[4] 과기정통부, 2018년 정보보호실태조사, 2019.4.16.
[5] 한국은행, 금융결제국 2017년도 금융정보화 추진현황
[6] 한국정보보호산업협회, 2017 국내 정보보호산업 실태조사, 2017. 12

◐ 저 자 소 개 ◑



공 병 철

1999년~현재 (사)한국사이버감시단 대표이사
2002년~현재 (사)한국인터넷정보학회 부회장
2015년~현재 정보보호인정협회(ISA) 회장
2015년~현재 (주)에스링크(S-LINK) 대표이사
관심분야 : 정보보호, 정보보안, 개인정보, 인공지능, 클라우드 컴퓨팅, IoT, NCS, ISO국제표준, ISMS(Information Security Management System)

국 경 완

2002년 국방대학교 전산정보 졸업(석사)
2014년~2016년 육군본부 정보화발전장교
2016년~2018년 육군본부 SW정책장교
2019년~현재 국방통합데이터센터 경영혁신실장
관심분야 : 빅데이터, 인공지능, ISMS, 정보보호, 정보보안, 클라우드, IoT, 블록체인
주요저서 : 리눅스 마스터, 자바 프로그래밍 등 다수

마 기 평

2015년 전남대학교 정보보안협동과정 졸업(석사)
2017년 전남대학교 정보보안협동과종 수료(박사)
2018년~현재 정보보호인정협회(ISA) 부회장
2018년~현재 CISSP KOREA 챕터 이사
관심분야 : ISMS(Information Security Management System), PIMS(Personal Information Management System), IoT, ISO국제표준, NCS, 보안