CISO

Chief
Information
Security
Officer

정보보호 최고책임자

길라잡이

기본편

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

본 책자는 정보보호 최고책임자(CISO)의 이해를 돕고자 2019년 진행된 정보보호 최고책임자(CISO) 대상 역량강화 교육 Basic 과정의 내용으로 재편집하여 배포하게 되었습니다. 본 책자의 내용은 집필진의 개인적인 견해가 포함되어 있을 수 있습니다.

CISO 길라잡이

기본편

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

집필진 소개

강은성

강은성 대표는 국내 최대 보안기업의 연구소장과 인터넷 포털회사의 최고보안책임자(CSO)를 역임한 국내 최고의 보안전문가다.
CISO Lab을 설립하여 개인정보보호 및 정보보호 컨설팅과 교육 사업을 하고 있다. 저서로 IT시큐리티(한울, 2009)와 CxO가 알아야 할 정보보안(한빛미디어, 2015)가 있다.

(現) CISO Lab 대표
(前) 블록체인OS CISO/CPO

홍성권

홍성권 위원은 개인정보 및 정보보호 체계 수립, OT보안, 글로벌 컴플라이언스(GDPR) 등과 관련된 기업 자문 및 컨설팅을 하고 있으며 한국CPO포럼, 국가공무원인재개발원, 기업체 등에서 강의하고 있다.

(現)법무법인 린/전문위원
(前) EY한영회계법인 Advisory본부 CS/이사
자격증 : ISMS-P 심사원, ISO27001 Auditor
메일 : sungkwon.hong@gmail.com

백제현 법학박사

(現) 성균관대학교 과학수사학과 겸임교수
(現) Security InSight LAB 대표
(現) 한국ISLA수상자협의회(KISLAA) 정회원
(前) (ISC)² KOREA Chapter 부회장
(前) (주)위드이노베이션 정보보호 최고책임자(CISO)
(前) (ISC)² CISSP Authorized Instructor
2012 Asia-Pacific ISLA 수상
CISSP | CISA | CCFP | EnCE

CONTENTS

CISO 정보보호 최고책임자 길라잡이
기본편

CISO
Chief
Information
Security
Officer

정보보호 최고책임자

길라잡이

기본편

I

CISO란 무엇인가

1. 도입 – 수비의 승리

러시아 월드컵 D조 경기에서 아르헨티나의 리오넬 메시가 크로아티아 선수들을 상대로 경기하고 있다. 아르헨티나는 이 경기에서 크로아티아에 0-3으로 완패했다. (오마이뉴스 2018.06.22.)

리오넬 메시는 자타가 공인하는 세계 최고의 공격수이다. 축구선수의 최대 명예 중 하나인 발롱도르상을 5회나 수상한 그의 경력만 봐도 그가 얼마나 대단한 선수인지를 알 수 있다. 하지만 메시는 월드컵 같은 국가대표 대항전에서 한 번도 우승하지 못했다. 축구는 혼자 잘한다고 되는 스포츠가 아니기 때문이다. 특히 아르헨티나는 종종 수비가 무너져서 큰 점수로 지곤 했는데, 2018년 러시아 월드컵에서도 크로아티아에 0-3, 프랑스에 3-4로 많은 실점을 하며 16강에서 탈락하고 말았다.

러시아 월드컵이 아르헨티나에게 악몽이었다면 대한민국에게는 큰 기쁨으로 기억된다. 직전 월드컵 우승팀이자 FIFA 랭킹 1위인 독일을 2-0으로 이긴 것이다. 비록 16강에는 오르지 못했지만, 세계 최강 독일을 상대로 2-0으로 이긴 것은 우리나라뿐 아니라 전 세계 축구팬들에게 엄청난 충격이었다. 그 때문에 독일은 월드컵 예선 탈락까지 했으니 말이다.

러시아 월드컵 F조 경기에서 대한민국이 독일을 2대 0으로 이겼다. 이 경기에서 탁월한 수비를 보여 준 수문장 조현우가 경기 최우수선수(Man of the Match)로 선정되었다. (더팩트 2018.06.27.)

독일전의 승리는 한마디로 하면 수비의 승리다. 이 경기에서 대한민국 대표팀은 전원 수비라는 극약처방을 써 가며 세계 최고의 독일 공격진을 막아냈고, 수문장 조현우는 골이 될 만한 슈팅을 막아내는 탁월한 역량을 보이며 이 경기 최우수선수로 선정되었다. 수비가 얼마나 중요한지를 그대로 보여준 경기라 할 수 있다. 세계 최고의 공격수를 갖고 있던 아르헨티나와 대조되는 경기였다.

기업에도 공격과 수비가 있다. 매출이나 영업이익, 트래픽, 고객 수 등 기업의 사업 목표를 달성해 나가는 조직이 공격수라고 한다면, 이 과정에서 발생할 수 있는 위험(리스크)을 관리해 나가는 조직은 수비수라고 할 수 있다. 영업, 마케팅, 상품이나 서비스 개발, 이들을 지원하는 IT운영 조직을 공격수라고 한다면, 법무(법규 위험), 재무(재무 위험), 홍보(언론 위험), 인사(인사 위험), 보안(보안 위험), 개인정보(개인정보 위험) 등 위험을 관리하는 조직은 수비수라고 할 수 있다.

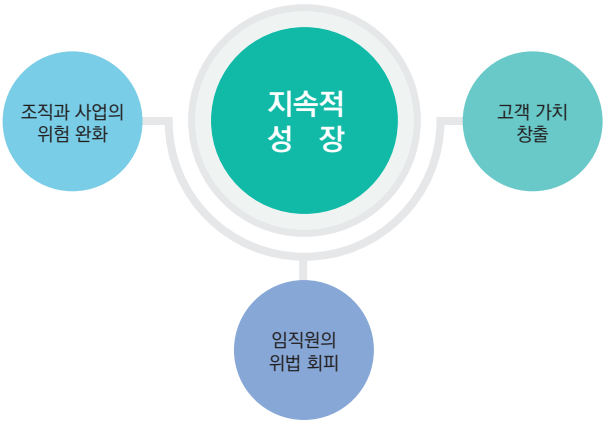
기업의 공격수가 기업의 단기적 성장에 집중하는 조직이라고 한다면, 수비수는 기업의 위험을 관리하여 중장기적으로도 튼튼하게 성장할 수 있도록 지원하는 조직이다. 1997년 외환위기, 2008년 글로벌 금융위기에서 단기적 성장에 치중하다가 큰 타격을 입은 기업이 적지 않다. 기업경영에서 위험 관리가 얼마나 중요한지 단적으로 보여주는 사례들이다.

2. 기업경영과 정보보호

(1) 정보보호의 목적

전통적으로 정보보호의 목적은 정보자산의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 보호하는 것이라고 설명해 왔다. 기술적으로 옳은 말이긴 하나, 기업경영에 정보보호가 어떤 기여를 하는지 설명하지 못한다. 정보보호가 여전히 기술과 기술전문가의 영역에 머물러 있다는 방증이기도 하다. 기업의 정보보호 최고책임자(CISO: Chief Information Security Officer)는 최고경영층에게 정보보호의 역할과 가치를 설명해야 한다. 당연히 기업경영의 측면에서 정보보호를 설명할 필요가 있다.

그림 1-1 기업경영 측면에서 정보보호의 목적

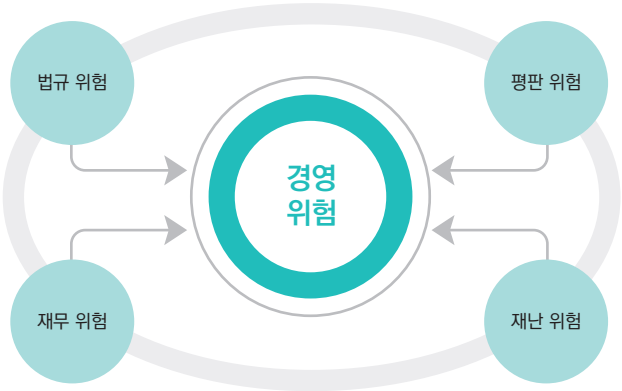


앞서 기업의 수비수에 관한 설명에서 언급했듯 정보보호는 기업의 보안 위험을 관리한다. 보안 위험은 크게 조직과 사업, 서비스에 내재하는 것도 있고, 임직원 개인에게 해당하는 위험도 있다. 이 두 가지 위험을 지속적으로 관리하고 최소화하여 기업이 지속적으로 성장하는 것을 지원하는 것이 정보보호 조직의 임무가 된다.

한발 더 나아가서 정보보호가 고객가치를 창출할 수도 있다. 고객가치가 보안인 보안제품을 제외하고 제품의 고객가치에 보안이 포함되는 경우는 많지 않았다. 국내에서는 2013년에 이미 팬택의 '베가 시크릿폰'이 지문인식기술을 이용하여 사진이나 동영상, 앱 등에서 사용자 인증을

통과해야 이용할 수 있도록 숨기는 기능을 제공하여 고객에게 사생활 보호의 가치를 제공한 바 있는데, 애플의 아이폰에서 휴대폰 자체의 사용자 인증과 결제에 지문인식기술을 활용하면서 보안이 전면적으로 안전하고 편리한 고객가치를 제공하는 사례가 되었다.

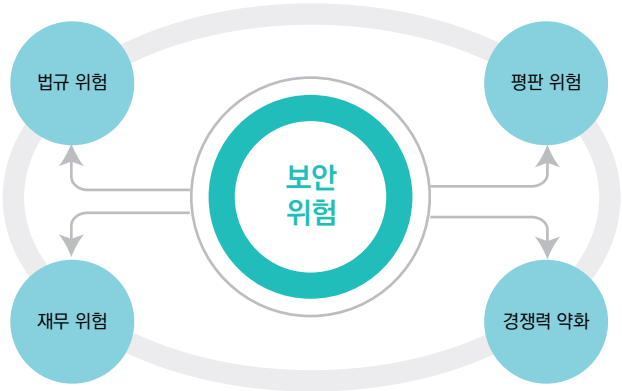
그림 1-2 기업차원의 위험의 예



(2) 기업차원의 보안 위험

기업은 사업목표 또는 경영목표를 정하면 그것을 추진하면서 지속적으로 위험 관리를 해나간다. 기업의 위험에 대한 국제표준이 있고, 분류 방법도 있다. 〈그림 1-2〉는 일반 기업에서 전사적으로 관리하여야 하는 위험의 예이다. 법규 위험이나 재무 위험은 전통적인 위험 관리 대상이었는데, 평판 위험은 최근에 큰 이슈가 되어있다. 평판에 문제가 생기면 사회적으로 여론이 들끓고 이에 관한 수사가 시작되어 법규 위험으로 확대되며, 불매운동이나 과징금 부과로 재무 위험까지 생기는 경우가 있기 때문이다. 재난 위험은 자연적인 재난도 있지만, 사회적 재난도 있어서 자주 발생하지는 않는다고 하더라도 중요하게 점검해야 할 조직이나 사업이 존재한다.

그림 1-3 기업차원의 위험인 보안 위험



보안은 강력한 규제가 있는 분야이다. 웬만한 오프라인 기업들도 사업을 위해 인터넷을 이용하고 있는데, 그런 기업들은 정보통신망법의 규제를 받고, 고객의 개인정보를 수집, 이용하면 정보통신망법의 개인정보보호 규정과 함께 개인정보 보호법의 규제를 받는다. 일정 이상의 개인정보를 보유하거나 정보통신서비스부문의 매출액이 발생하면 정보보호 및 개인정보보호 관리체계 인증을 취득해야 한다. 이를 준수하지 못했을 때 법규 위험이 발생하고, 보안이나 개인정보 문제가 사회적으로 드러나면 평판 위험이, 이를 통해 과징금이나 민사소송이 생기면 재무 위험이 발생한다. 경영 위험은 시장에서의 경쟁, 현금 흐름, 기술력 약화, 과도한 인수합병 등 여러 요인으로 발생하지만, 보안 위험 역시 경영 위험의 한 원인으로 떠올랐다.

(3) CISO 조직의 역할

이에 따라 보안 위험을 관리하는 정보보호 조직의 임무는 기업의 경영과 사업 측면에서 다음과 같이 정의하는 것이 적절하다고 할 수 있다.

그림 1-4 정보보호 조직의 임무

조직과 사업의 보안위험을 최소화함으로써
기업의 **지속적 성장**을 지원하는 조직

보안 관련 법규 위반으로 인한
동료의 보안 위험을 최소화하는 조직

CISO의 임무 역시 기업경영과 사업의 측면에서 보면 다음과 같이 정의할 수 있다.

그림 1-5 CISO의 임무

조직과 사업의 보안위험을 최소화함으로써
기업의 지속적 성장을 지원하는 **비즈니스 리더**

C×O의 보안 위험을 최소화하는 **경영의 동반자**

3. 정보보호 업무와 정보보호 거버넌스

(1) 정보보호 업무 vs. 정보보호 조직의 업무

CISO와 정보보호 조직이 수행하는 업무를 보통 정보보호 업무라고 부른다. 하지만 기업에서 발생하는 모든 정보보호 업무를 CISO조직에서 하는 것은 아니다. 기업의 인사평가 업무는 인사조직이 주관하긴 하지만, 각 조직의 부서장이나 임원들이 하는 것과 마찬가지다. 인사조직에서는 인사평가의 기준과 방법, 절차를 제시하고, 인사평가 과정에서 문제가 발생할 경우 이를 지원하며, 필요한 경우 경영진이 참고할 수 있도록 주요 조직의 장에 대한 인사평가 자료를 제공하기도 한다.

그림 1-6 정보보호 업무와 정보보호 조직

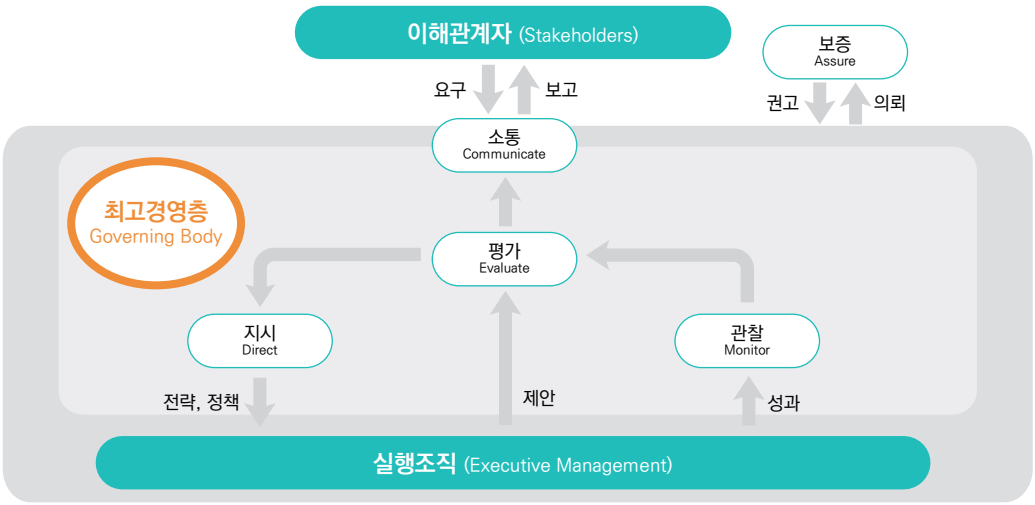
이와 마찬가지로 정보보호 업무 역시 정보보호 조직에서 하는 업무와 다른 조직에서 하는 업무가 있다. 〈그림 1-6〉에서 보듯 예를 들어 정보보호 관리체계의 수립과 운영, 보안기술의 검토와 확보, 수시로 발생하는 각종 보안 이슈에 대한 대응, 일부 보안솔루션의 운영과 분석 등은 정보보호 조직에서 수행하지만, IT 개발을 외주용역으로 수행하고 있다면, 해당 외주인력에 대한 보안서약서 작성이나 그들에게 PC 등 정보자산의 제공과 회수, 서버 계정의 관리 등은 외주를 관리하는 조직이나 IT 운영조직에서 수행할 일이다. 입사자가 있을 때도 보안서약서는 인사조직에서 받고, 보안교육은 정보보호 조직에서 수행한다. 이렇게 정보보호 업무는 정보보호 조직과 비(非)정보보호 조직이 협업하여 수행하는 전사 업무이다. 또한 정보보호 조직에서 전사적인 업무를 주도해 나가기 위해서 정보보호 인력에게 소통과 협업 역량이 필요하다는 점에 유의할 필요가 있다.

앞서 살펴본 것처럼 정보보호 위험은 기업 차원의 위험으로써, 이를 관리하는 정보보호 업무 역시 최고경영층이 관심을 갖고 전사적으로 지휘, 통제해 나가야 하는 업무임에 틀림없다.

(2) 정보보호 거버넌스

이미 기업에서는 각종 전사적인 위험을 관리하는 기제가 있다. 처음 영국이 유럽연합을 탈퇴하는 브렉시트(Brexit)[1] 이슈가 불거졌을 때 유럽연합에 사업의 이해관계가 있거나 환율이 중요한 기업에서는 브렉시트의 여러 시나리오가 기업에 어떤 영향을 미칠지 점검했을 것이다. 보안 위험 역시 그러한 기제를 통해 검토하면 된다.

그림 1-7 정보보호 거버넌스 프로세스



출처: ISO 27014

정보보호 거버넌스는 기업 거버넌스를 토대로 정보보호에 관한 경영적 의사결정을 내리는 구조이다. 정보보호 거버넌스 국제표준인 ISO 27014에서는 정보보호 거버넌스 프로세스를 〈그림 1-7〉과

1 영국(Britain)과 탈퇴(exit)를 합쳐서 만든 혼성어

같이 규정하고 있다. 이와 관련된 프로세스는 다음과 같다.

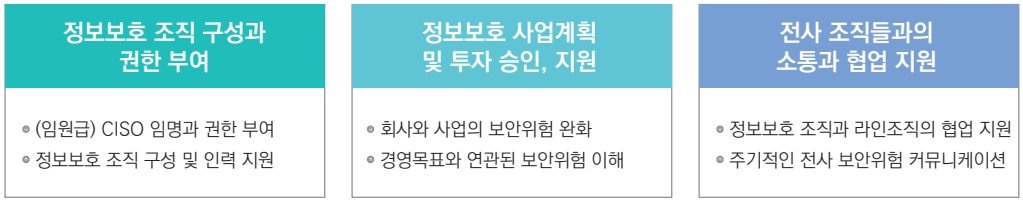
- 정보보호 조직과 비(非)정보보호 조직을 포함하여 실행 조직에서 정보보호 관련된 정책, 사업, 조직 등에 관하여 제안(보고)한다.
- 최고경영층[2]은 실행조직의 보고 내용을 검토, 평가한다.
- 최고경영층은 보고 내용을 시행할 필요가 있다고 판단하면, 이에 관한 전략, 정책을 실행조직에 지시한다.
- 최고경영층은 실행조직이 수행한 결과를 관찰하여 평가한다.
- 최고경영층은 보안 과제 또는 그것을 수행한 결과를 이해관계자와 소통한다.
- 최고경영층은 보안 활동이 잘 되고 있는지 객관적이고 전문적인 기관에 검토를 의뢰하고, 그 결과를 받아 검토한다.
- 실행조직은 최고경영층과의 소통과 보안업무를 수행하는 다른 조직의 협업을 통해 업무를 수행한다.

과연 기업의 최고경영층이 이러한 과정을 주도할 수 있을 것인가, 하는 질문을 던질 수 있다. 하지만 그 질문은 일반적으로 최고경영층의 역할로 여겨진 대규모 신규 사업 결정, 신규 투자 확보, 대형 고객사 확보, 연구, 개발 투자 등을 하는 데 최고경영층이 전문성이 있느냐는 질문과 같은 맥락에 있다. 최고경영층이 해당 분야에 전문성이 있어 추진하는 일도 있지만, 좋은 스태프들의 보고와 조언을 통해 경영적 판단을 내리는 경우도 많이 있기 때문이다. 〈그림 1-7〉에서 보듯 보안 위험 역시 좋은 스태프의 보고와 조언을 받아 기업의 위험 관리 영역에서 최고경영층이 의사결정을 내려야 할 사안이다. 국내 기업 거버넌스에서 CISO가 최고경영층에 포함되는 경우는 별로 없다. 따라서 최고경영층이 정보보호 거버넌스에서 어떤 역할을 하는지가 매우 중요하다.

---

2 ISO 27014에서는 Governing Body라고 되어 있어서 이사회라고 보는 것이 맞으나 국내 환경에 적합하지 않다고 봐서 주로 최고경영층이라고 번역하여 사용한다.

그림 1-8 최고경영층의 정보보호 역할



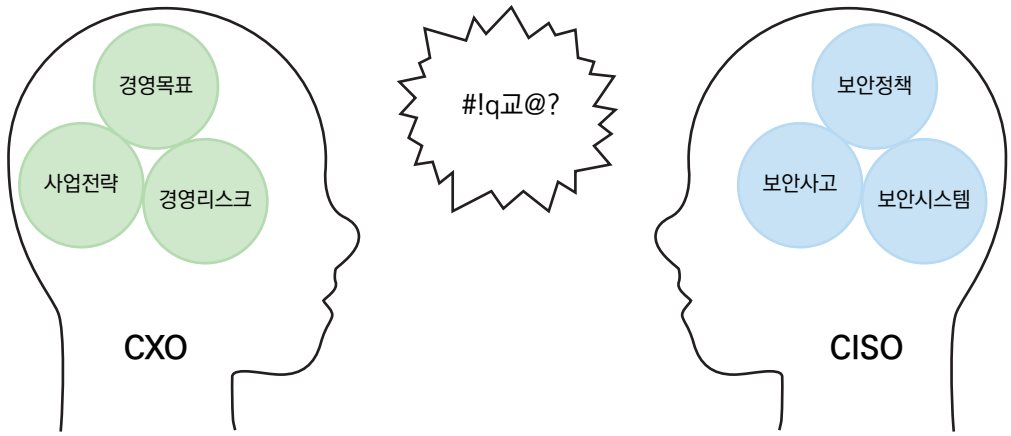
최고경영층은 조직과 인력, 예산에서 최종 의사결정자이다. 정보보호와 관련해서도 마찬가지다. 특히 경영진의 일원으로서 전사 보안 위험을 관리할 임원급 CISO의 임명과 적절한 권한을 부여하는 일은 무엇보다도 중요하다. 기업은 직위와 직책에 부여된 권한과 책임을 행사하는 계층 구조의 조직이기 때문이다. CISO조직의 업무에 걸맞은 조직과 인력을 구성해 주는 일 또한 최고경영층이 해야 할 중요한 정보보호 업무이다.

또한, 최고경영층은 정보보호 사업계획 및 투자에 대한 승인 여부를 판단해야 하고, 이를 위해서는 사업 목표를 추진해 나가는 데 존재하는 다양한 경영 위험과 함께 보안 위험 역시 파악하고 있어야 한다. 그리고 정보보호 조직과 다른 조직 사이의 소통과 협업에 일정한 역할을 담당해야 한다. 기업에서의 협업은 최고경영층의 확고한 의지와 전사 커뮤니케이션을 기반으로 이뤄지는 것이 일반적이기 때문이다. 이러한 최고경영층의 역할을 끌어내는 일이 CISO의 중요한 역할이기도 하다.

(3) 최고경영층과의 의사소통

기업에서의 소통과 협업은 다른 영역에서와 마찬가지로 개인과 개인 사이의 역량과 노력에도 영향을 받지만, 거버넌스와 그에 기초한 조직 간의 관계에 훨씬 더 큰 영향을 받는다. 기업은 전사 각 조직의 힘을 집중해 경영목표를 달성해 나가는 조직이기 때문이다.

그림 1-9 최고경영층과의 의사소통



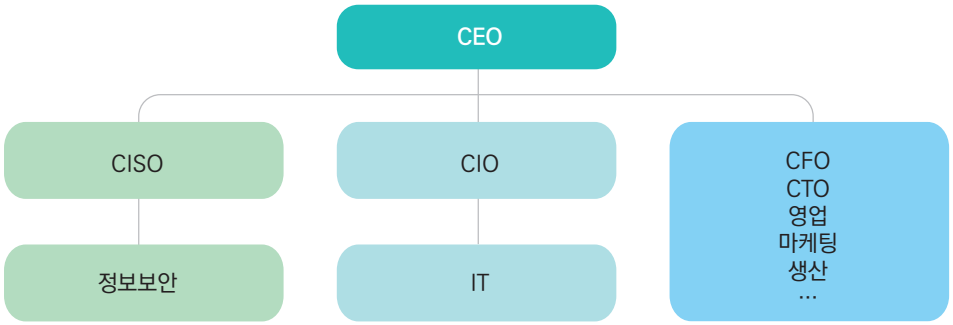
먼저 CISO가 최고경영층과의 의사소통에 노력해야 한다. 최고경영층은 경영목표와 그것을 달성하기 위한 사업전략, 그리고 그에 따른 경영 위험을 주요 어젠더로 갖고 있다. 정보보호 역시 그러한 틀에서 경영판단을 하게 되는데, 정보보호 영역의 보고서가 기술적인 사안으로 올라오는 경우가 적지 않다. 전사적으로 새로운 보안 정책이나 보안시스템을 도입하려고 할 때 이를 매출, 영업이익, 법률, 고객, 트래픽 등 경영적 판단을 내릴 수 있는 방식으로 보고하지 않으면, 최고경영층을 이해시키기 어렵다.

또한 CISO 입장에서는 모든 보안 이슈가 다 중요하다고 판단할 수 있지만, 한정된 자원을 가지고 경영목표를 달성해 나가는 최고경영층 입장에서는 우선순위가 있어야 한다. 그래야 CISO들이 최고경영층과의 의사소통이 원활해질 수 있다.

(4) 정보보호 거버넌스와 정보보호 조직체계

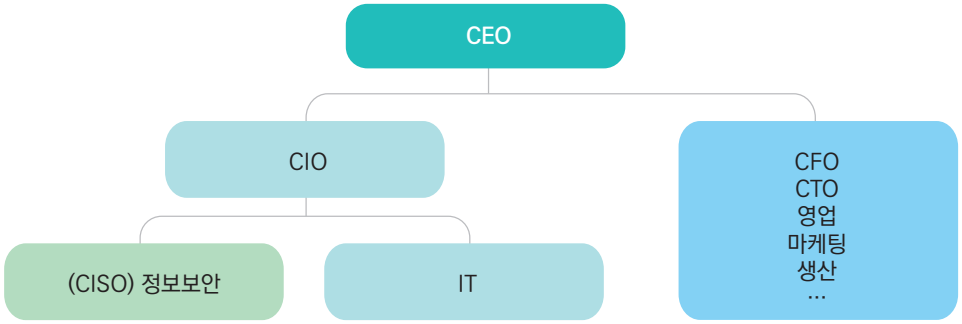
거버넌스에서 내린 결정사항은 조직체계를 통해 기업에서 구현된다. 정보보호 거버넌스에서 정보보호 조직체계가 중요한 이유다. 정보보호 거버넌스와 정보보호 조직체계의 핵심 고리는 조직체계상 CISO조직의 위치와 부여된 권한이다. CISO조직을 중심으로 한 정보보호 조직체계가 전사적 정보보호 업무를 잘 수행할 수 있도록 구성되지 않으면, 정보보호 실무자들이 열심히 일을 하더라도 성과를 내기 어렵고, 보안 문제가 발생할 경우 권한도 없는데 책임만 지는 결과가 나오기도 한다.

그림 1-10 정보보호 조직체계 – CEO 직속 CISO



정보보호 거버넌스 측면에서 가장 바람직한 정보보호 조직체계는 〈그림 1-10〉과 같은 형태이다. CISO가 CEO 직속으로 실질적인 C레벨 임원이기 때문에 전사 정보보호를 위한 권한을 행사할 수 있고, 예산과 인력의 확보, 전사 보안 위험에 대한 가시성(visibility)의 확보, 전사 보안을 위한 협업을 하는 데에도 수월하다. 하지만, CISO가 CEO 직속이면서도 C레벨 임원도 아니고 심지어 임원도 아니라면 CEO 직속의 구조가 오히려 전사 업무를 수행할 때 어려움이 될 수도 있다. CEO가 가지고 있는 경영 의제가 많기 때문에 일상적으로는 CISO가 정보보호 업무를 챙겨야 하는데, 그에 적합한 직위와 권한이 주어지지 않았기 때문이다.

그림 1-11 정보보호 조직체계 – CIO 산하 CISO

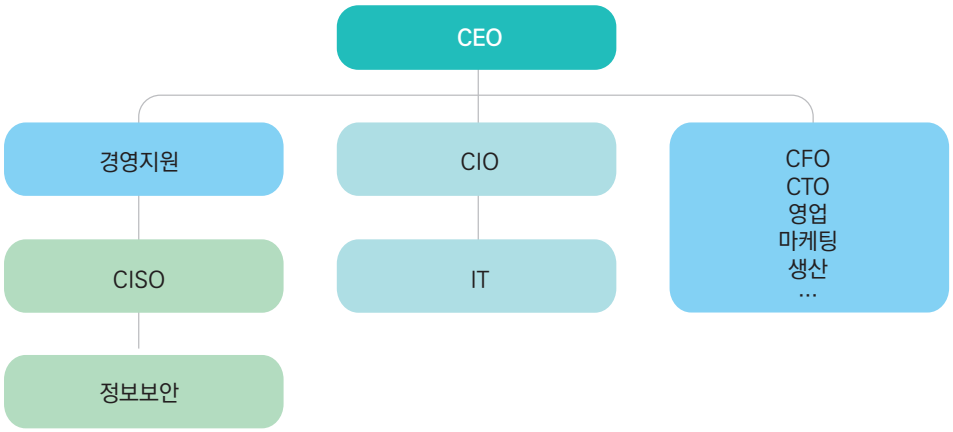


〈그림 1-11〉은 기업에서 정보보호 조직을 처음 만들 때 쉽게 생각할 수 있는 구조이다. 정보보호 업무의 50% 이상은 IT 보안업무이기 때문에 최고 IT 책임자(CIO: Chief Information Officer) 산하에 CISO(또는 정보보안 조직)를 두거나 CIO가 CISO를 겸임하기도 한다. 팀을 만들 만한 규모가 되지 않는다고 판단하면 IT 운영팀 내에 정보보호 실무자를 두는 경우도 있다. CIO나 IT 운영 조직이 보안 위험에 대한 인식이 어느 정도 있다면, 이러한 조직 구조는 효율적으로 IT 보안업무를 수행하는 데 도움이 된다.

하지만 일부 회사에서 CIO는 권한이 많은 조직이 아니다. CIO 산하에 CISO가 있는 경우 CISO의 전사 보안 위험에 대한 가시성의 확보나 CISO의 전사 통제 업무에 어려움이 있을 수 있다. 더욱이 정보보호 조직과 IT 운영조직이 업무에서 종종 부딪힐 때도 있다. IT 운영조직의 임무가 영업, 개발 등 전사 조직이 효율적이고 편리하게 IT 인프라를 이용할 수 있도록 지원하는 것이라고 한다면, 정보보호 조직은 효율과 편리를 조금은 희생한다고 하더라도 보안 위험을 최소화하기 위해 전사 조직을 지원하면서 통제하기도 해야 하는 조직이기 때문이다. 근본적으로 임무의 성격이 상충하는 측면이 있다.

서로 역할이 다른 조직이 서로 다른 관점으로 사안을 살펴보면서 문제를 찾아내고 해결해 나가는 것은 매우 정상적인 기업 내 활동이다. 문제는 이러한 조직 구조가 보안 위험을 관리하는 데 적절하지 않을 수 있다는 점이다. 예를 들어 IT 인프라에서 전사적 보안 위험이 발견되었을 때 CIO가 CEO에게 보고하지 않고, IT 중심의 의사결정을 하거나, IT 입장에서 보고하여 CEO가 그에 관해 잘못된 판단을 내린다면 IT 부문의 위험이 전사 위험으로 비화 될 수도 있다. 심지어 정보보호 담당자가 IT 운영팀 내에 있다면 아예 팀 이상으로 문제 제기를 하는 일이 어려워질 수 있다.

그림 1-12 정보보호 조직체계 – 경영지원 산하 CISO



〈그림 1-12〉에서와 같이 CISO 조직을 CFO나 경영지원, HR 등 경영지원조직 산하에 둘 수도 있다. 어느 회사에서는 준법감시인이나 감사 밑에 두기도 한다. 이러한 조직 구조는 일견 〈그림 1-11〉과 거의 같이 보이지만, 경영지원조직은 전사 가시성이나 협업, 일정하게 내부통제 역할도 갖고 있다는 측면에서 CISO 조직이 업무를 수행하기에는 CIO 산하에 있는 것보다 좋은 환경이다. 따라서 CISO 조직이 일정하게 커지고 전사 역할이 중요한 시점이 되면, 〈그림 1-11〉보다는 〈그림 1-12〉의 조직 구조를 갖는 것이 바람직하다.

CISO가 정보보호 거버넌스를 바꾸기는 쉽지 않다. 하지만 기업에서 업무를 성과 있게 수행하기 위해서는 거버넌스와 조직체계가 무엇보다도 중요하다. 업무를 추진하기 위해 적절한 구조가 되어 있지 않다고 한다면 CISO가 이를 바꾸기 위해 계획을 세우고 추진할 필요가 있다.

4. CISO의 업무

(1) 법률에서의 CISO 업무

CISO의 업무를 규정하는 것은 그리 간단하지 않다. 먼저 CISO 지정을 의무화하고 있는 전자금융거래법과 정보통신망법을 살펴보자. 전자금융거래법에서는 CISO의 업무를 다음과 같이 정의하였다.

표 1-1 전자금융거래법 제21조의2 제4항

CISO의 업무 (전자금융거래법 제21조의2 제4항)
1. 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립
2. 정보기술부문의 보호
3. 정보기술부문의 보안에 필요한 인력관리 및 예산 편성
4. 전자금융거래의 사고 예방 및 조치

전자금융거래법은 법률의 목적에 따라 CISO의 업무가 전자금융거래의 보호와 전자금융거래를 구현한 IT 부문의 보안에 집중하고 있는 것을 알 수 있다. 전자금융거래법에서의 보안은 한 마디로 IT 보안이다. 정보통신망법 제45조의3 제4항에서는 CISO의 업무를 다음과 같이 정의하였다.

표 1-2 정보통신망법 제45조의3 제4항

CISO의 업무 (정보통신망법 제45조의3 제4항)
1. 정보보호 관리체계의 수립 및 관리·운영
2. 정보보호 취약점 분석·평가 및 개선
3. 침해사고의 예방 및 대응
4. 사전 정보보호 대책 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

'사전 정보보호 대책 마련 및 보안 조치 설계·구현'(제4호)와 '정보보호 사전 보안성 검토'(제5호)는 새로운 사업이나 서비스를 추진할 때 또는 네트워크나 서버, 소프트웨어 등 새로운 정보시스템을 도입하거나 개발할 때 각 단계별로 적절한 보안 활동을 통해 보안취약점을 제거하는 업무를 말한다. 기존 시스템을 개선할 때에도 적용할 수 있다. 세밀하게 보면 조금 다른 이름과 내용을 갖고 있지만 이와 유사한 활동이 여럿 있는데, 세부적인 가이드가 나와 있는 '정보보호 사전점검'을 살펴보면 다음과 같다.

「정보보호 사전점검 안내서」에서는 정보보호 사전점검을 〈그림 1-13〉과 같이 설명하고 있다.

그림 1-13 정보보호 사전점검

출처: 과학기술정보통신부, 한국인터넷진흥원, 「정보보호 사전점검 안내서」, 2018.3.

즉 계획, 분석/설계, 구현, 시험 등 정보시스템 구축 단계에서 필요한 보안 활동을 함으로써 시스템의 보안 위험을 최소화하자는 것이다. 이에 대비하여 정보보호 관리체계(ISMS)는 정보시스템의 출시 이후에 운영 및 유지보수 단계에서 보안 위험을 관리하는 활동이다. 소프트웨어 개발 관점에서 이와 비슷한 것으로는 Security by Design, 개발 보안, 이에 관한 마이크로소프트의 방법론인 Security Development Lifecycle 등이 있다.

소프트웨어 개발 분야로 가면 CISO들이 시험 단계에서 모의해킹 이상을 하기 어려운 것이 현실이다. 소프트웨어 개발 프로세스, 개발 프로세스 안에 녹아든 보안 활동, 소프트웨어 보안기술 등 현 CISO조직의 업무나 역량 상 모두 쉽지 않은 일이기 때문이다. 다만 계획 단계나 분석/설계 단계에서 보안 요구사항을 잘 정리하여 시험 단계나 출시 후 운영 단계까지 관리하면 많은 부분을 해결할 수 있다.

(2) 기업에서의 CISO 업무

현업 측면에서 CISO의 업무를 다음과 같이 정의할 수 있다.

그림 1-14 CISO의 정보보호 업무의 예

출처: 강은성, 「CxO가 알아야 할 정보보안」, 한빛미디어, 2015.

여기에서 정의한 CISO의 업무가 관련 법률에서 정의한 것들과 가장 큰 차이가 나는 부분은 정보보호 거버넌스와 규제 대응을 CISO의 업무로 명시했다는 점이다. 상당수의 CISO가 정보보호 관련된 법과 규제에 대한 대응 업무를 수행하고 있다. 특히 고객의 개인정보를 보유한 기업에서는 '개인정보의 기술적·관리적 보호조치'의 많은 부분을 수행하고 있는 CISO가 관련 법령이나 고시를 충분히 이해할 필요가 있다.

이미 어느 정도 수행하고 있지만, 충분히 인식하지 못하고 있기 때문에 업무로 정의하지 못한 업무가 바로 거버넌스 영역의 업무이다. 기업 거버넌스가 있고, 정보보호 활동이 있다면 어떤 식으로든 정보보호 거버넌스가 존재하여 주요 정보보호 정책과 조직 등에 관해 최고경영층이 경영적 의사결정을 내리고 있을 것이다. 거버넌스 영역의 정보보호 업무의 예는 다음과 같다.

표 1-3 거버넌스 영역의 정보보호 업무(예)

업무	세부 내역
1. 최고경영층 주도 체계 구축	• CEO를 비롯한 최고경영층이 보안 위험을 책임지고 주도하는 체계 구축과 전사적인 커뮤니케이션 시행 • 임원급 (전담) 정보보호 책임자 선임과 위상 부여
2. 최고경영층 및 타 임원 소통 체계 구축	• 주요 임원이 정보보안 정책 등 정보보호 관련 의사결정, 전략 및 정책 공유, 전사적인 추진과 협업할 수 있는 체계 구축 • 임원회의, 정보보호 경영위원회에서 정보보호의제 처리와 소통
3. 정보보호 조직·인력·예산 확보	• 정보보호 조직의 구축과 위상 확보 • 적절한 규모의 보안 인력 및 보안전문가 확보 • 정보보호 예산 확보
4. 정보보호 계획의 수립과 추진	• 회사 경영목표와 연계된 정보보호 전략 및 사업계획 수립. 전사 관련 조직의 정보보호 활동이 각 조직의 사업계획에 포함되도록 협업 • 회사 경영목표 달성에 잠재한 정보보안 위험의 최소화
5. 정보보호 경영 지원	• CEO의 정보보호 어젠더 지원 • CISO의 정보보호 어젠더 수립과 추진 • 타 임원의 정보보호 업무 및 활동 지원

출처: 강은성, 「CxO가 알아야 할 정보보안」, 한빛미디어, 2015.

(3) 정보보호 경영위원회, 전사 협업의 근간

거버넌스 영역의 업무 중 전사적으로 정보보호 업무를 추진하기 위해 필요한 것이 최고경영층 및 타 임원 소통체계 구축이다. 앞에서 설명한 정보보호 거버넌스와 정보보호 조직체계는 전사 정보보호 협업을 위한 토대가 되고, '정보보호 경영위원회'는 이것의 골격이 된다.

먼저 전자금융감독규정이나 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증에서 규정하고 있는 정보보호 위원회에 관해 살펴본다.

표 1-4 전자금융감독규정 상의 정보보호 위원회

정보보호 위원회 (전자금융감독규정 제8조의2)	
구성	• 위원장: 정보보호 최고책임자(CISO) • 위원: 정보보호 업무 관련 부서장, 전산 운영 및 개발 관련 부서장, 준법 업무 관련 부서의 장
역할	• 중요 정보보호에 관한 사항을 심의·의결
업무	• 정보기술부문 계획서에 관한 사항 • 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립 • 취약점 분석·평가 결과 및 보완 조치의 이행계획에 관한 사항 • 전산보안사고 및 전산보안관련 규정 위반자의 처리에 관한 사항 • 기타 정보보호 위원회의 장이 정보보안업무 수행에 필요하다고 정한 사항

ISMS-P에서는 정보보호 위원회의 구성에 대한 규정을 담고 있지 않다. 다만 "1.1 관리체계 기반 마련 - 1.1.3 조직 구성"의 '세부 설명'에서 기술한 내용을 정리하면 다음과 같다.

표 1-5 ISMS-P 상의 정보보호 위원회

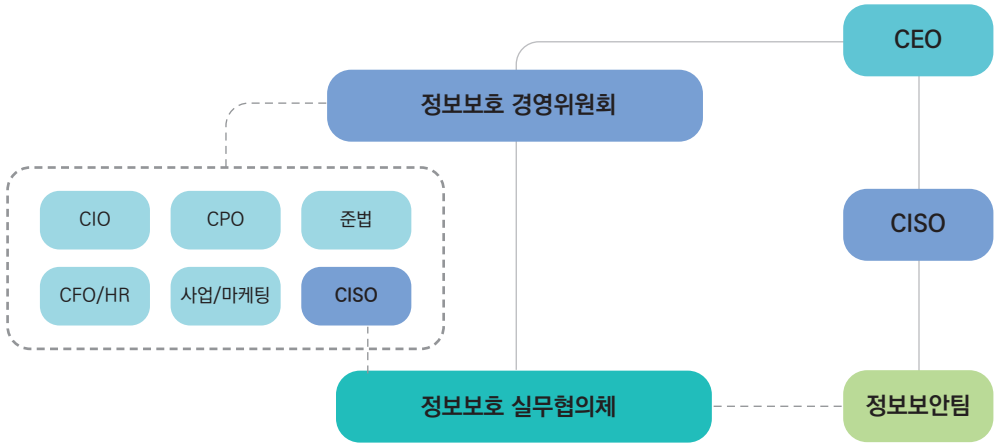
정보보호 위원회 (ISMS-P)	
구성	• 위원: 경영진, 임원, 정보보호 최고책임자, 개인정보 보호책임자
역할	• 조직 전반에 걸친 중요한 정보보호 관련 사항에 대하여 검토, 승인 및 의사결정
업무	• 정보보호 및 개인정보보호 정책·지침의 제·개정 • 위험평가 결과 • 정보보호 및 개인정보보호 예산 및 자원 할당 • 내부 보안사고 및 주요 위반사항에 대한 조치 • 내부감사 결과 등

정보보호 위원회에 관한 전자금융감독규정과 ISMS-P의 가장 큰 차이는 위원회의 구성에 있다. 전자금융감독규정에서 정보보호 위원회는 임원이 아닌 정보보호 관련 부서장으로 구성되어 있다. 회의 참석자들이 임원이 아니면 그 회의에서의 결정사항이 전사에 의미 있는 영향을 주긴 어렵다. 아예 그 회의에서 전사에 영향을 미칠 만한 의사결정을 하지 않으려고 할 수도 있다. 반면, ISMS-P에서는 경영진, 임원이 들어가 있고, 결함의 사례로 "정보보호 및 개인정보보호 위원회를

구성하였으나, 임원 등 경영진이 포함되어 있지 않고 실무부서의 장으로 구성되어 있어 조직의 중요 정보 및 개인정보보호에 관한 사항을 결정할 수 없는 경우"라고 명시하여 임원의 참여를 중시하였다.

회사에서 정보보호 위원회를 운영할 때 크게 2가지 점에 유의하여야 한다. 하나는 위원회의 구성이고 다른 하나는 의제이다. 일반적으로 기업에서 전사적으로 중요한 의사결정은 CEO까지 올라가는 결재 절차나 CEO가 참석하는 임원회의에서 결정한다. 위원회를 전사적인 의사결정 구조로 만들려면 CEO가 위원장을 맡는 것이 바람직하다. "정보보호 경영위원회"라고 위원회 이름에 굳이 '경영'을 넣은 이유다.

그림 1-15 정보보호 경영위원회의 구성과 운영



의제도 정보보호 법규나 사내 중요한 보안사고 또는 동종 업계의 보안사고, 전사에 영향을 미칠 주요 보안 정책 등 임원들이 참석하여 토론하고 의사결정에 참여할 수 있는 의제를 선택해야 한다. 기술적인 내용은 가능한 한 제외하는 것이 좋다. 위원회를 만들지 않고, 분기에 한 번씩 임원 회의를 위원회 회의로 갈음할 수도 있다. 중요한 건 CEO와 주요 임원들이 참석하여 정보보호 주요 사안에 관해 토론하고 결정하는 회의를 개최하는 것이다. 그리고 그 회의를 열기 전에 정보보호 실무협의체가 가동하여 의제를 협의하고, 이전 회의에서 결정한 사안의 후속 조치 진행사항을 점검하며, 회의 뒤에는 회의의 결정사항을 전사 관련 조직이 수행할 수 있도록 구체화하여 전달하고

후속 조치를 관리해야 회의체가 제대로 작동한다.

이렇게 정보보호 경영위원회에서 전사 업무에 영향을 미칠 수 있는 주요 의제들을 다룸으로써 전사 정보보호 업무 수행과정에서 필요한 협업 의제가 논의, 결정될 수 있고, 정보보호 업무 수행과정에서 발생할 수 있는 조직간 갈등 요인도 회의에서 정리될 수 있다. 그러면 정보보호 경영위원회가 전사 정보보호 협업의 근간으로 작동하게 된다.

정보보호 경영위원회와 정보보호 실무협의체의 구성과 역할은 다음과 같다.

표 1-6 정보보호 경영위원회

정보보호 경영위원회	
구성	• 위원장: CEO • 위원: 전사 정보보호 정책의 수립, 집행에 관련된 주요 임원
역할	• 전사 주요 정보보호의제를 경영적 측면에서 심의하고 결정
업무	• 전사 주요 정보보호의제 의사 결정 • 전사 정보보호 협업 사안 처리 • 경영적 측면에서 판단

표 1-7 정보보호 실무협의체

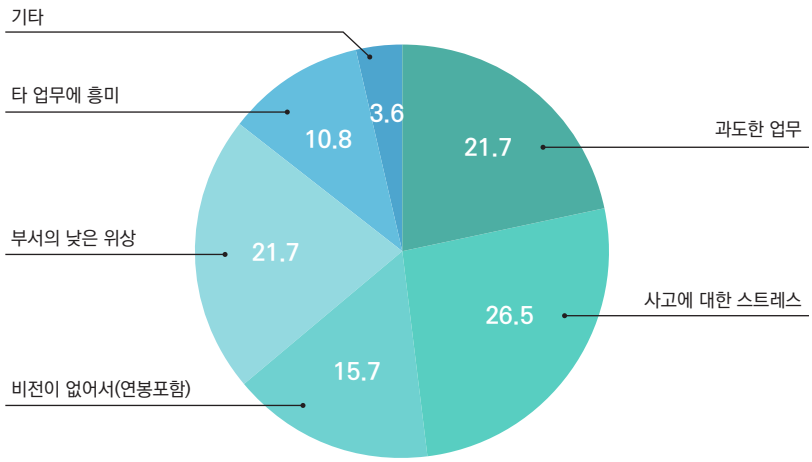
정보보호 실무협의체	
구성	• 위원장: CISO • 위원: 전사 정보보호 업무 또는 보안 이슈 대응에 관련된 팀의 리더(팀장 또는 시니어 실무자)
역할	• 정보보호 경영위원회를 보좌하고 전사 보안 이슈에 대응
업무	• 정보보호 경영위원회의 의제 검토, 결정사항의 후속 조치 등 실무 처리 • 정보보호 정책에 관한 실무책임자급의 협업 • 대내외 주요 보안 이슈에 대한 신속한 대응

(4) 정보보호 실무조직

정보보호 실무조직은 가능하면 실무적 의사결정의 기본 단위인 "팀"으로 만들어야 한다. 정보보안팀이 별도로 만들어져 있지 않고, 보안담당자가 다른 조직에 포함되어 있다면 전사 보안 위험을 실무적으로 관리하기 어렵기 때문이다. 특히 정보보호 실무자가 IT 통제의 대상이 되는 IT 운영팀에 소속되어 있다면 더욱 좋지 않다. 따라서 인원이 2명 이상이 되면 팀으로 만드는 것이 좋다. 또한, 팀으로 만들기 어려운 환경에서는 CISO와 직보 통로를 만들어서 CISO가 왜곡되지 않은 정보를 바탕으로 전사 보안 위험 관리를 해나갈 수 있도록 해야 한다. 그래야 긴급한 보안 이슈가 발생했을 때도 CISO가 관리할 수 있다.

이미 예상할 수 있다시피 각 회사의 정보보호 실무자의 사기가 그리 좋은 편이 아니다. 2018년 국내 300여 개 기업의 정보보안팀 내지 파트의 참여 협의체인 침해사고대응팀협의회(CONCERT)의 설문 조사에 따르면, 업무 변경을 희망하는 실무자들의 비율이 49%에 이르렀다.

그림 1-16 업무 변경을 희망하는 이유



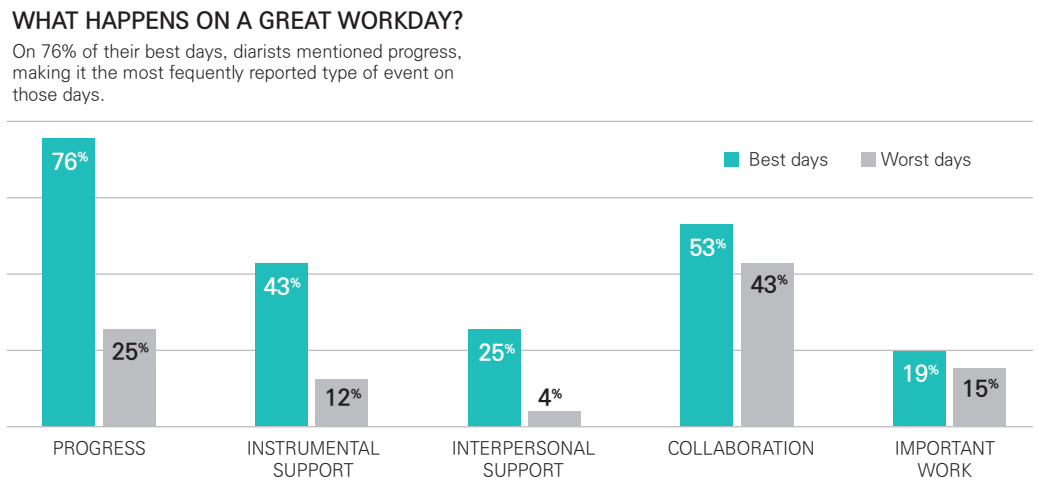
출처: 한국침해사고대응팀협의회, 2018년 기업 정보보호 담당자 의식조사 분석보고서

〈그림 1-16〉에서 업무 변경을 희망하는 이유 중 "부서의 낮은 위상"과 "비전이 없어서"를 합치면 37.4%이다. 이 두 요인은 주로 거버넌스의 문제로 발생한다. 사고에 대한 스트레스 또한 거버넌스와 연관이 있다. 정보보안 사고의 책임이 정보보호 담당자에게 돌아가는 구조이기 때문이다. 정보보호 담당자에게 그 책임이 있는 경우도 있지만, 책임을 질 만한 상황이 아닌 경우도 많다. CISO조직의 위상과 권한, 역할이 정립되어 있으면, 사고에 대한 스트레스가 있다 하더라도 그것이 업무를 변경할 수준까지 가지는 않았을 것이다.

(5) 최고의 날 vs. 최악의 날

Harvard Business Review(HBR)가 2010년에 흥미로운 조사 결과를 내 놓은 적이 있다. 이전에 HBR이 600명의 관리자에게 설문을 통해 동기부여에 관해 조사한 결과에서는 '1. 일에 대한 인정, 2. 인센티브, 3. 대인관계 지원, 4. 업무진행을 위한 지원, 5. 명확한 목표' 순이었는데, 실무자들에 대한 직접 조사에서 이와는 거리가 있는 결과가 나온 것이다. (269명 응답)

그림 1-17 무엇이 정말로 노동자에게 동기를 부여하나?



출처: The HBR List: Breakthrough Ideas for 2010, https://hbr.org/2010/01/the-hbr-list-breakthrough-ideas-for-2010, 2019.11.30. 검색

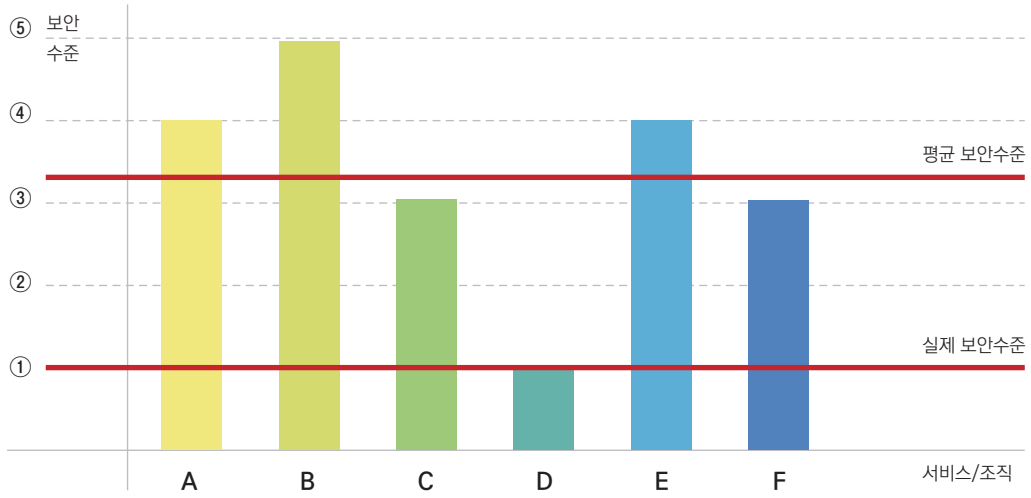
수백 명의 지식노동자들이 매일 하루의 일과가 끝났을 때 그들의 동기부여(motivation)와 감정(emotion)을 보내온 12,000개의 이메일을 분석한 결과가 〈그림 1-17〉처럼 나왔다. 좋은 날이 가장 많았던 최고의 날(Best days)의 동기부여는 일의 진도가 잘 나갔을 경우(progress, 76%)였고, 최악의 날(Worst days)의 동기부여는 협업(collaboration)이 잘되지 않은 경우였다. 협업은 최고의 날의 두 번째 이유를 차지하기도 했다. 즉 최고의 날은 일이 잘된 날(일의 진행이 잘된 날)이고, 최악의 날은 일이 잘되지 않은 날(협업이 잘되지 않은 날)이었다. 일이 잘되거나 잘되지 않은 것이 지식노동자들에게 매우 중요하다는 것을 밝힌 것인데, 이 조사는 HBR의 이전 조사나 노동자들의 동기부여에 관한 '상식'과도 차이가 있었다. 비록 이 조사가 인과관계를 조사한 것이 아니기 때문에 동기부여로 인해 기분이 좋은 날이었다고 추론할 수는 없지만, 이 둘 사이에 상관관계가 있다는 것은 입증된 것이다.

협업의 특성은 나 혼자 열심히 한다고 해서 일이 진행되는 것이 아니라 협업하는 상대방이 지원해 주고 함께 열심히 해야 일이 진행된다는 것이다. 보통 협업은 실무자들 개인의 역량으로는 한계가 있고, 거버넌스와 조직체계, 협업체계에서 주요 직책을 담당하고 있는 CEO, 임원, 부서장 등에 의해 규정되는 측면이 크다. 정보보호 협업에서는 무엇보다도 CISO의 역할이 중요하다. 앞에서 서술한 조직체계를 갖추는 일 못지않게, CISO가 협업 관리를 자신의 업무로 규정하고 수행하는 일 또한 중요하다. 조직원들의 일도 잘되고 동기부여에도 도움이 된다.

5. 결론

한 기업의 보안수준을 산정할 때 여러 방법이 있는데, 그중 여러 분야의 점수를 매기고 그것의 평균을 계산하는 방법을 쓰기도 한다.

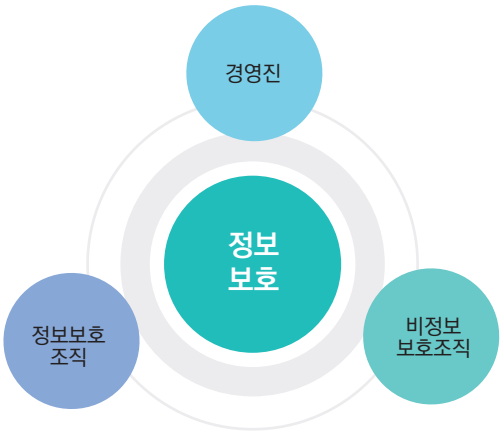
그림 1-18 기업의 보안수준



예를 들어, 정보보호 정책(A) 4점, 외부자 보안(B) 5점, 임직원 보안(C) 3점, 서버 보안(D) 1점, 네트워크 보안(E) 4점, 웹 사이트 보안(F) 3점이라고 할 때 이 회사의 평균 보안점수는 3.3점이라고 하는 방식이다. 이러한 방법은 회사의 전반적인 보안수준을 이해하는 데에는 도움이 되나, 보안사고가 날 만한 곳을 찾아내어 예방하는 데에는 별 도움이 되지 않는다. 보통 사고는 평균에 크게 못 미치는 D 영역에서 발생하기 때문이다. 따라서 CISO 입장에서는 이 기업의 실제 보안수준은 1점이라고 보는 것이 타당하다. CISO가 가장 시급하게 해야 할 일은 D 영역과 같이 보안수준이 많이 떨어지는 영역을 찾아내 최소한 평균 수준으로 높이는 일이다.

이렇게 보안수준이 낮은 영역을 찾아내는 손쉬운 방법이 있다. 이미 많은 부분은 실무자들이 알고 있기 때문이다. 보안실무자, IT 운영자, 개발자 등 이미 회사의 정보보호 정책, 솔루션을 꿰뚫고 있는 인력들과 허심탄회하게 이야기만 해도 많은 것을 파악할 수 있다. 또한, 회사에서 보호해야 할 중요한 자산은 무엇인지, 범행자의 입장에서 무엇을 가져갈 것인지를 살펴볼 수도 있다.

그림 1-19 기업 정보보호의 세 주체



이제까지 본 바와 같이 정보보호를 체계적으로 수행하기 위해서는 최고경영층이 주도하는 정보보호 거버넌스를 토대로 정보보호 조직과 비정보보호 조직이 협업을 해야 한다. CISO와 정보보호 조직 역시 이를 위해 소통과 협업에 적극적으로 나서야 한다.

CISO
Chief
Information
Security
Officer

정보보호 최고책임자

길라잡이

기본편

II

CISO의 Awareness

1. CISO가 꼭 알아야 할 법률
2. CISO가 꼭 알아야 할 보안

1. CISO가 꼭 알아야 할 법률

회원 가입을 받지 않고 홈페이지를 통해 제품을 홍보하는 기업이 있다면, 이 기업에는 정보보호와 관련하여 어떤 법률이 적용될까? 홈페이지에서 침해사고가 발생했을 때 신고 없이 자체적으로 해결한 기업은 법적 의무가 없을까? 홈페이지도 없고 회원가입도 없는 홍보 목적의 단순 블로그를 유지하는 스타트업은 지켜야 할 정보보호 관련 법률이 없을까? 정보보호 최고책임자는 이러한 질문에 명확하게 답변하기 쉽지 않다.

기업에 적용되는 정보보호 및 개인정보보호 관련 대표적인 법률은 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'과 '개인정보 보호법'이 있다. 일부 정보보호 최고책임자는 홈페이지를 통해 개인정보를 수집하지 않으면 정보통신망법은 준수하지 않아도 된다고 생각할 수 있다. 그런데, 정보통신망법의 제정 목적은 '정보통신망의 안전한 이용'과 '정보통신 서비스를 이용하는 자(이용자)의 개인정보를 안전하게 보호하는 것'이다. 단순 홈페이지를 운영한다고 하더라도 정보통신망의 안전한 이용에 영향을 줄 수 있으므로 정보통신망법을 준수해야하는 것이다.

2018년 국회는 정보보호 최고책임자의 겸직을 금지하고, 자격요건 등을 대통령령으로 정하는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 개정안을 통과시켰으며, 이에 따라 중기업 이상의 정보통신서비스 제공자, 자본금 1억원 이하의 부가통신사업자를 제외한 모든 전기통신사업자와 정보보호 관리체계(ISMS) 인증을 받아야 하는 정보통신서비스제공자 등 3만 4천여 개 기업은 정보보호 최고책임자(CISO)를 의무적으로 지정하고 과학기술정보통신부장관에게 신고하도록 되었다.

법적 요건에 따라 기업에서는 정보보호 최고책임자를 지정해야 한다. 이 때 정보보호 최고책임자는 정보보호 또는 정보기술 관련 학위와 경력이 있는 자를 지정하여야 하며, 정보보호 최고책임자의 겸직이 제한되는 기업은 4년 이상의 정보보호 분야 경력자이거나, 2년 이상의 정보보호 분야 경력자로 정보기술 분야 경력과 합쳐 5년 이상인 자로 지정하도록 자격요건을 정하고 있다.

정보보호 최고책임자가 정보보호 분야 또는 유관 경력이 있더라도 고도화되고 지능화된 정보보호 위협으로부터 조직을 안전하게 보호하기 위해서는 다음과 같은 역량의 확보가 요구된다.

- 조직의 주요 비즈니스에 대한 이해
- 조직의 비즈니스와 연관된 정보보안 관련 법률에 대한 이해
- 정보보호와 관련된 정부/관련 기관의 규제 동향

- 정보보호와 관련된 이해관계자의 식별 및 이해충돌의 조정
- 정보보호와 관련된 관리적/기술적 보안 지식

정보보호 최고책임자는 조직의 비즈니스에 대해 이해를 하고 있어야 하며 조직의 정보보안과 관련된 내용을 경영진에게 충분히 설명하고 지원을 받을 수 있도록 내부 의사소통을 강화해야 한다. 정보보호와 관련된 법/제도적 요건이 지속적으로 강화되고 있으므로 이에 대한 식별과 조직에 미치는 영향을 분석하고 정보보호 규정에 반영하거나 필요한 내용에 대해 경영진과 의사소통해야 한다.

조직의 정보보호 관리체계를 구현하고 이행하기 위해서는 정보보호 부서와 IT 부서, 현업부서 간의 긴밀한 협조가 필요한데, 정보보호 부서의 주요 역할 중 IT 부서와 현업부서에 대한 통제와 점검/감사, 모니터링 등의 업무로 인해 이해충돌이 빈번하게 발생할 수 있다. 정보보호 최고책임자는 이와 관련하여 조직의 비즈니스와 정보보호 사이에 절충점을 찾을 수 있도록 이해충돌을 원만하게 조정할 수 있어야 하며 정보보호 관리체계의 효과적/지속적 이행과 침해사고의 예방을 위해 관리적/기술적 보안에 대한 이해가 필요합니다.

그렇다면 정보보호 최고책임자의 책임과 역할은 어떻게 될까? 아래 [그림 2-1]은 이에 대한 예시이다.

그림 2-1 정보보호 최고책임자의 책임과 역할

(1) 기업에 적용되는 법률

조직의 비즈니스에 따라 적용될 수 있는 법률의 종류는 다음과 같다.

표 2-1 정보보호 관련 법률

구분	법률
정보보호 및 개인정보보호 관련	• 정보통신망 이용촉진 및 정보보호 등에 관한 법률 • 개인정보 보호법 • 정보통신기반보호법 • 위치정보의 보호 및 이용 등에 관한 법률 • 부정경쟁방지 및 영업비밀보호에 관한 법률 • 산업기술의 유출방지 및 보호에 관한 법률
금융관련	• 신용정보의 이용 및 보호에 관한 법률 • 전자금융거래법
임직원 채용 관련	• 근로기준법 • 채용절차의 공정화에 관한 법률
기타	• 전자문서 및 전자거래 기본법 • 전자서명법 • 통신비밀보호법

본 교재에서는 기업의 정보보호 및 개인정보보호를 위해 필수적으로 준수해야 하는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'(이하 '정보통신망법')과 '개인정보 보호법' 위주로 살펴보고자 한다.

표 2-2 정보통신망법과 개인정보 보호법 비교

항목	정보통신망법	개인정보 보호법
구분	특별법	일반법
적용범위	정보통신망 이용촉진 및 정보보호 등에 관한 다른 특별한 규정이 있는 경우를 제외하고 적용	개인정보보호에 관해 다른 법률에 특별한 규정이 있는 경우를 제외하고 적용
적용대상	정보통신 서비스 제공자(영리 목적으로 서비스를 제공하는 사업자)	개인정보 처리자(업무를 목적으로 개인정보를 처리하는 기관/법인/단체/개인)
보호대상	이용자 (정보통신 서비스를 이용하는 자)	정보 주체 (처리되는 정보에 의해 알아볼 수 있는 사람)
수집 시 동의	동의	동의
위탁 시 동의	동의	고지
국외이전 동의	동의	동의
개인정보 제공	동의	동의
영리 목적의 광고성 정보의 전송 제한	동의 시 전송 가능	-
영상정보처리기기 설치 운영	-	안내판 설치 등 필요한 조치 적용
개인정보 영향평가	-	공공기관만 적용

아래는 각 비즈니스 유형별로 적용되는 법률에 대한 예시이다.

유형 1 **홈페이지를 통해 상품 홍보와 채용 사이트를 유지하며, 오프라인으로 직원을 채용하는 경우**

→ 정보통신망 이용촉진 및 정보보호 등에 관한 법률(홈페이지), 개인정보 보호법(직원 채용)

유형 2 **POS 등 오프라인을 통해 개인정보를 수집하고, 수집된 정보 중 문자메세지와 메일을 통해 마케팅을 수행하는 경우**

→ 정보통신망 이용촉진 및 정보보호 등에 관한 법률(문자메시지/메일을 통한 마케팅), 개인정보 보호법(POS를 통한 개인정보 수집)

유형 3 **서면신청서 및 계약서를 통해 수집된 개인정보와 구매 포인트를 홈페이지에서 조회하여 상품 구매에 활용하는 경우**

→ 정보통신망 이용촉진 및 정보보호 등에 관한 법률(홈페이지 계약정보 조회 및 상품 구매), 개인정보 보호법(신청서 및 계약서를 통한 개인정보 수집)

유형 4 **SNS를 통해 이벤트를 실시하는 경우**

→ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

(2) 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정보통신망법은 정보통신 서비스 제공자에게 적용되는 법률로 '정보통신서비스를 이용하는 자의 개인정보를 안전하게 보호'하고 '정보통신망을 안전하게 이용'할 수 있도록 할 목적으로 제정되었다.

> **제1조(목적)** 이 법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.

따라서 정보통신 서비스 제공자는 정보통신서비스를 이용하는 자의 개인정보를 안전하게 보호할 수 있도록 관리적/기술적 보호조치를 적용하여야 하며 이용자의 개인정보가 유출되면 신고해야 할 뿐만 아니라 운영 중인 홈페이지 등이 변조되거나 악성코드 유포 등을 한다면 관련 기관에 신고하여야 한다.

정보통신망법에서 자주 언급되는 용어에 대한 정의는 다음과 같다.

> **제2조(정의)** ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.
> 1. "정보통신망"이란 「전기통신사업법」 제2조 제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.
> 2. "정보통신서비스"란 「전기통신사업법」 제2조 제6호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.
> 3. "정보통신서비스 제공자"란 「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.
> 4. "이용자"란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
> 5. "전자문서"란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 표준화된 것을 말한다.
> 6. "개인정보"란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
> 7. "침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.

정보통신망법에 정의된 정보통신서비스 제공자의 정의 중 '영리를 목적으로 전기통신사업자의 전기통신 역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자'가 포함되어 있다. 따라서 제품에 대한 홍보 목적으로 홈페이지를 운영한다면 영리 목적으로 정보를 제공하는 것으로 정보통신망법이 적용된다.

정보통신망법의 구성은 다음과 같으며, 우리가 주목해야 할 장은 '제4장 개인정보의 보호'와 '제6장 정보통신망의 안정성 확보' 등이 있다.

표 2-3 정보통신망법의 주요 내용

장	주요 내용
제1장 **총칙**	• 법률의 목적, 용어정의 및 다른 법률과의 관계 정의 • 다른 법률과의 관계
제2장 **정보통신망의 이용 촉진**	• 정보통신망의 표준화 및 인증, 인증기관의 지정 등 • 정보통신망이용촉진 등에 관한 사업, 인터넷 이용의 확산
제3장 **삭제**	• 2015년 6월 22일 삭제
제4장 **개인정보의 보호**	• 개인정보의 수집 이용 및 제공 • 개인정보의 관리 및 파기 등 • 이용자의 권리
제5장 **정보통신망에서의 이용자 보호 등**	• 청소년유해매체물의 표시, 청소년유해매체물의 광고금지 • 정보통신망에서의 권리보호, 정보의 삭제요청 등 • 게시판 이용자의 본인확인, 이용자 정보의 제공청구 • 불법정보의 유통금지 등
제6장 **정보통신망의 안전성 확보 등**	• 정보통신망의 안전성 확보 등 • 정보보호 사전점검, 정보보호 최고책임자의 지정 등 • 집적된 정보통신시설의 보호 • 정보보호 관리체계의 인증, 개인정보보호 관리체계의 인증 • 이용자의 정보보호, 정보보호 관리등급 부여 • 정보통신망 침해행위 등의 금지, 침해사고의 대응 등, 침해사고의 신고 등, 침해사고의 원인 분석 등 • 영리 목적의 광고성 정보 전송 제한, 영리 목적의 광고성 정보 게시의 제한 • 중요 정보의 국외 유출 제한 등
제7장 **통신과금서비스**	• 통신과금서비스 제공자의 등록 등 • 통신과금서비스의 안전성 확보 등, 통신과금서비스 이용자의 권리 등 • 분쟁조정 및 해결 등, 손해배상 등
제8장 **국제협력**	• 국제협력 • 국외 이전 개인정보의 보호

기업에서 이용자의 개인정보를 이용하려고 수집하는 경우 다음 사항을 이용자에게 고지하고 동의를 받아야 하며 변경 사항이 있는 경우에도 동일하게 고지하고 동의를 받아야 한다.

❶ 개인정보의 수집·이용 목적
❷ 수집하는 개인정보의 항목
❸ 개인정보의 보유·이용 기간

정보통신서비스의 제공에 관한 계약을 이행하기 위해 필요한 개인정보로 경제적·기술적인 사유로 통상적인 동의를 받는 것이 곤란하거나 정보통신서비스의 제공에 따른 요금 정산을 위해 필요한 경우, 다른 법률에 특별한 규정이 있는 경우, 동의 없이 개인정보를 수집 이용할 수 있다. 14세 미만의 아동에 대한 개인정보를 수집할 경우 법정대리인의 동의를 받아야 하며 14세 미만의 아동이 개인정보의 처리와 관련된 사항을 고지할 때 이해하기 쉽도록 쉬운 양식과 명확하고 알기 쉬운 언어를 사용하여야 한다.

이용자의 개인정보를 수집하는 경우 정보통신서비스 제공을 위해 필요한 범위에서 최소한의 개인정보만 수집하여야 하며 최소한의 개인정보 수집 여부에 대한 입증 책임은 해당 기업에 있다. 이용자가 필요한 최소한의 개인정보 외의 개인정보를 제공하지 않는다는 이유로 서비스를 거부하지 않아야 한다.

제3자에게 이용자의 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그밖에 이와 유사한 행위(이하 "처리"라 한다)를 할 수 있도록 업무를 위탁(이하 "개인정보 처리위탁"이라 한다)하는 경우 ❶ 개인정보 처리위탁을 받는 자, ❷ 개인정보 처리위탁을 하는 업무의 내용을 이용자에게 고지하고 동의를 받아야 하며 변경되는 경우에도 동일하게 재고지하고 동의를 받아야 한다. 또한 수탁자가 이용자의 개인정보를 처리할 수 있는 목적을 미리 정의하여야 하며 관련 내용을 계약서에 포함하여 문서화된 형태로 관리해야 하며, 수탁사가 정보통신망법과 계약서 내용을 위반하지 않도록 관리 감독하고 교육하여야 한다. 대부분의 기업에서는 수탁사에 대한 개인정보보호 준수 여부를 년 1회 점검하고 있으며 수탁사의 유형, 규모, 처리하는 개인정보 등을 고려하여 현장점검, 설문지 작성 등을 통해 평가하고 있다. 한편, 수탁자가 개인정보를 제3자에게 재 위탁하고자 하는 경우 위탁자의 동의를 필수적으로 받아야 한다.

이용자의 개인정보를 처리하는 경우 다음 사항을 포함한 개인정보 처리방침을 홈페이지 등에

공개하여야 한다. 또한, 개인정보 처리방침을 변경하는 경우 이유와 변경내용을 지체 없이 공지하고 이용자가 언제든 변경된 사항을 알아볼 수 있도록 조치하여야 한다.

- 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법
- 개인정보를 제3자에게 제공하는 경우 제공받는 자의 서명(법인의 경우 법인명), 제공받는 자의 이용목적과 제공하는 개인정보의 항목
- 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법(개인정보를 보존하는 경우 보존근거와 보존하는 개인정보 항목 포함)
- 개인정보 처리위탁을 하는 업무의 내용 및 수탁자(해당 시)
- 이용자 및 법정대리인의 권리와 그 행사방법
- 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
- 개인정보 보호책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

개인정보처리방침은 해당 조직에서 수집/이용하는 이용자의 개인정보를 어떤 방법과 절차에 따라 안전하게 보호하고 파기하고, 관리 담당자는 누구인지 알려주기 위한 목적으로 작성되는 것으로써, 기업 내부의 개인정보보호 지침의 주요 내용을 참고하여 법에 명시된 항목에 대해 구체적인 방안으로 설명해야 한다. 수집/이용하는 개인정보의 항목과 수탁사, 제3자 제공업체 등은 서비스에 따라 달라질 수 있으므로 주기적으로 확인하여 변경이 발생할 경우 이를 처리방침에 포함해야 한다.

개인정보를 처리할 때 이용자의 개인정보가 분실·도난·유출·위조·변조·훼손되는 것을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적/관리적 보호조치를 수립하고 이행해야 한다.

- 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립 및 시행
- 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제 장치의 설치 및 운영
- 접속기로의 위/변조를 방지하기 위한 조치
- 개인정보를 안전하게 저장 및 전송할 수 있는 암호화 기술 등을 이용한 보안조치
- 백신 소프트웨어의 설치 및 운영 등 컴퓨터 바이러스에 의한 침해 방지 조치
- 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

정보통신망법의 적용을 받는 기업은 법률에 따라 개인정보 내부관리계획을 수립해야 한다. 개인정보 내부관리계획은 다음 사항을 포함하여야 하며 취급자에 대한 교육 등을 포함하고 있으므로 년1회 검토 후 개정하는 것을 권고한다.

- 개인정보 보호책임자의 지정 등 개인정보보호 조직의 구성 및 운영에 관한 사항
- 이용자의 개인정보를 처리하는 자(개인정보 취급자)의 교육에 관한 사항
- 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제 장치의 설치 및 운영
- 접속기로의 위/변조를 방지하기 위한 조치
- 개인정보를 안전하게 저장 및 전송할 수 있는 암호화 기술 등을 이용한 보안조치
- 백신 소프트웨어의 설치 및 운영 등 컴퓨터 바이러스에 의한 침해 방지 조치

개인정보에 대한 불법적인 접근을 차단하기 위해 ❶ 개인정보처리시스템에 대한 접근권한의 부여/변경/말소 등에 관한 기준의 수립·시행 ❷ 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영 ❸ 개인정보처리시스템에 접속하는 개인정보 취급자 컴퓨터 등에 대한 외부 인터넷망 차단 ❹ 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영 ❺ 기타 개인정보에 대한 접근통제를 위하여 필요한 조치를 적용해야 한다. 단, ❸에 해당하는 개인정보 취급자 컴퓨터의 외부 인터넷망 차단은 전년도 말 기준 직전 3개월간 이용자 수가 일 평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 기업만 적용대상이 된다.

개인정보처리시스템 접속기록의 위/변조를 방지하기 위하여 ❶ 개인정보처리시스템 접속일시, 처리내역의 저장과 로그 검토 ❷ 개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관해야 한다. 또한, 개인정보처리시스템 접속로그 및 처리로그 검토 시 과다 접근시도, 업무시간 외 접근시도와 과다 조회/다운로드/출력, 과다 마스킹 해제시도, 과다 암호화 해제, 업무시간 외 조회 등 이상행위 여부에 대해서도 확인해야 한다. 개인정보가 안전하게 저장/전송될 수 있도록 ❶ 비밀번호의 일방향 암호화 저장 ❷ 주민등록번호, 계좌정보 및 바이오정보 등에 대한 암호화 저장 ❸ 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송수신하는 경우 보안서버 구축 등의 조치 등 보안조치를 적용해야 한다. 암호화 시 안전한 암호화 알고리즘을 사용하는 지와 키의 길이 등에 대해 주기적으로 확인해야 하며 보안서버의 경우 인증서 유효기간과 암호화 알고리즘의 적정성에 대해 확인해야 한다.

수집/이용목적을 달성한 이용자의 개인정보, 개인정보의 보유 및 이용기간이 끝난 경우이거나 해당 사업을 폐업하는 경우 지체 없이 해당 개인정보를 복구/재생할 수 없도록 파기해야 한다. 다만, 다른 법률에 따라 개인정보를 보존해야 하는 경우 해당 법률이 정한 기간 동안 보관할 수 있다.

표 2-4 다른 법률에 따른 개인정보의 보존 기간

항목	보관기간
계약 또는 청약철회 등에 관한 기록	5년
대금결제 및 재화 등의 공급에 관한 기록	5년
소비자의 불만 또는 분쟁처리에 관한 기록	3년
표시/광고에 관한 기록	6개월

정보통신서비스를 1년 동안 이용하지 않은 이용자의 개인정보를 보호하기 위하여 ❶ 이용자의 개인정보를 해당 기간 경과 후 즉시 파기 ❷ 다른 이용자의 개인정보와 별도로 분리 저장해야 한다. 별도 분리 저장한 경우에도 내부적으로 기준을 정해서 특정 기간동안 저장 후 파기할 수 있도록 절차를 수립해야 한다. 분리 보관된 개인정보를 이용하거나 제공하지 않도록 안전하게 관리하여야 하며 기간 만료 30일 전까지 개인정보가 파기되는 사실, 기간 만료일, 파기되는 개인정보의 항목 등을 전자우편 등을 통해 이용자에게 통보해야 한다.

이용자는 개인정보 수집·이용·제공 등의 동의를 언제든 철회할 수 있으므로 이를 보장할 수 있는 절차를 수립하여야 하며 지체 없이 개인정보를 복구/재생할 수 없도록 파기해야 한다. 또한, 이용자는 본인에 대한 처리 사항을 열람이나 제공을 요구할 수 있으며 오류가 있는 경우 정정을 요청할 수 있다.

❶ 보유하고 있는 이용자의 개인정보
❷ 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황
❸ 개인정보 수집/이용/제공 등의 동의를 한 현황

이용자의 개인정보 이용내역을 년 1회 이용자에게 통지하여야 하며 ❶ 개인정보의 수집 이용목적 및 수집한 개인정보의 항목 ❷ 개인정보를 제공받은 자와 제공목적 및 제공한 개인정보의 항목 ❸ 개인정보 처리위탁을 받은 자 및 그 처리위탁을 하는 업무의 내용을 포함하여 전자우편, 서면, 모사전송, 전화 등을 통해 통지해야 한다.

(3) 개인정보 보호법

개인정보 보호법은 모든 개인정보 처리자에게 적용되는 법률로 개인정보의 처리 및 보호에 관한 사항을 정하여 개인의 자유와 권리를 보호할 목적으로 제정되었다.

> **제1조(목적)** 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.

정보통신망법은 정보통신서비스 제공자에게 적용되는 특별법이며 개인정보 보호법은 법인/공공/개인 등 업무 목적으로 개인정보를 처리하는 개인정보 처리자에게 적용되는 일반법이다. 즉, 정보통신서비스 제공자는 정보통신망법에 규정된 사항을 먼저 준수하고, 정보통신망법에 규정되지 않은 예를 들어 '영상정보처리기기 처리' 등과 같은 사항은 개인정보 보호법에 따라 준수해야 한다.

개인정보 보호법에서 자주 언급되는 용어에 대한 정의는 다음과 같다.

> **제2조(정의)** ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.
> 1. "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
> 2. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
> 3. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
> 4. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
> 5. "개인정보 처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
> 6. "공공기관"이란 다음 각 목의 기관을 말한다.
> 가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
> 나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관
> 7. "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.

개인정보 보호법의 용어 상 정보통신망법과 다른 항목은 ❶ 정보주체(정보통신망법에서는 '이용자') ❷ 개인정보 처리자(정보통신망법에서는 '정보통신서비스제공자') 등이 있으므로 적용되는 법률에 따라 적합한 용어를 사용해야 한다. 또한 개인정보 처리자와 개인정보 취급자를 구분해서 사용해야 한다. 개인정보 처리자는 업무를 목적으로 개인정보파일을 운영하는 법인, 즉 회사를 말하며 개인정보 취급자는 개인정보 처리자에 속해 있으며 개인정보를 처리하는 임직원을 의미한다.

개인정보 보호법의 구성은 다음과 같다.

표 2-5 개인정보 보호법의 주요 내용

장	주요 내용
제1장 **총칙**	• 법률의 목적, 용어정의 및 다른 법률과의 관계 정의 • 다른 법률과의 관계
제2장 **개인정보 보호 정책의 수립**	• 개인정보 보호위원회, 개인정보 보호위원회의 기능, • 자료제출 요구, 개인정보 보호지침, 국제협력
제3장 **개인정보의 처리**	• 개인정보의 수집·이용, 개인정보의 수집 제한 • 개인정보의 제공, 개인정보의 목적 외 이용·제공 제한 • 개인정보의 파기 • 민감정보의 처리제한, 고유식별정보의 처리제한, 주민등록번호 처리의 제한 • 영상정보처리기기의 설치·운영 제한 • 업무위탁에 따른 개인정보의 처리 제한 • 개인정보 취급자에 대한 감독
제4장 **개인정보의 안전한 관리**	• 안전조치의무, 개인정보 처리방침의 수립 및 공개 • 개인정보 보호책임자의 지정 • 개인정보 보호 인증, 개인정보 영향평가 • 개인정보 유출 통지 등, 과징금의 부과 등
제5장 **정보주체의 권리 보장**	• 개인정보의 열람, 개인정보의 정정·삭제 • 개인정보의 처리정지 등 • 권리행사의 방법 및 절차, 손해배상책임
제6장 **개인정보 분쟁조정위원회**	• 설치 및 구성, 위원의 신분보장, 조정의 신청 등 • 처리기간, 자료의 요청 등, 조종 전 합의 권고, 분쟁의 조정
제7장 **개인정보 단체소송**	• 단체소송의 대상 등, 전속관할 • 소송대리인의 선임, 소송허가신청, 소송허가요건 등 • 분쟁조정 및 해결 등, 손해배상 등

개인정보 처리자가 정보주체의 개인정보를 이용하려고 수집하는 하는 경우 다음 사항을 정보주체에게 고지하고 동의를 받아야 하며 변경 사항이 있는 경우에도 동일하게 고지하고 동의를 받아야 한다.

❶ 개인정보의 수집·이용 목적
❷ 수집하려는 개인정보의 항목
❸ 개인정보의 보유 및 이용 기간
❹ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 불이익에 대한 내용

개인정보 처리자는 개인정보를 수집하는 경우 목적에 필요한 최소한의 개인정보를 수집하여야 하며 최소한의 개인정보 수집이라는 입증책임은 개인정보 처리자에게 있다. 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 않는 다는 이유로 정보주체에게 서비스 제공을 거부하지 않아야 한다.

개인정보 처리자는 정보주체에게 동의를 받은 경우 정보주체의 개인정보를 제3자에게 제공할 수 있다. 동의를 받을 경우 다음 사항을 고지하고 동의를 받아야 하며 어느 하나의 사항이라도 변경이 있다면 이에 대해 알리고 동의를 받아야 한다. 또한 국외의 제3자에게 제공하는 경우에도 아래 사항을 정보주체에게 고지하고 동의를 받아야 한다.

❶ 개인정보를 제공받는 자
❷ 개인정보를 제공받는 자의 개인정보 이용 목적
❸ 제공하는 개인정보 항목
❹ 개인정보를 제공받는 자의 개인정보 보유 및 이용기간
❺ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

개인정보 처리자는 개인정보를 수집·이용 목적 범위를 벗어나 이용하거나 제3자에게 제공하지 않아야 한다. 개인정보 처리자는 보유기간의 경과, 개인정보의 처리 목적을 달성하여 해당 개인정보가 불필요한 경우 지체 없이 해당 개인정보를 복구 또는 재생 불가능한 방법으로 파기해야 한다. 단, 다른 법률에 의해 별도로 보존 기간이 있는 경우 해당 법률의 보존기간에 따라 보관할 수 있으며 해당 개인정보는 다른 개인정보와 분리하여 저장/관리해야 한다.

개인정보처리에 대하여 정보주체(법정대리인 포함)의 동의를 받을 경우 동의사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다. 동의를 서면(전자문서 포함)으로 받을 경우 개인정보의 수집 이용 목적, 수집 이용하려는 개인정보의 항목 등을 명확히 표시하여 알아보기 쉽게 해야 한다. 정보주체에게 홍보하거나 판매를 권유할 목적으로 개인정보 처리 동의를 받을 경우 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다. 만 14세 미만 아동의 개인정보를 처리하기 위해 동의를 받아야 하는 경우 법정대리인의 동의를 받아야 하며 법정대리인의 동의를 받기 위해 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.

개인정보 처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그밖에 정보주체의 사생활을 상당히 침해할 수 있는 개인정보(민감정보)는 정보주체에게 별도 동의를 받거나 법령에서 허용하는 경우를 제외하고 수집/이용하지 않아야 한다. 고유식별정보(운전면허번호, 여권번호, 외국인번호)는 정보주체에게 별도 동의를 받거나 법령에서 허용하는 경우를 제외하고 수집/이용하지 않아야 하며 고유식별정보를 수집/이용하는 경우 해당 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 암호화, 마스킹 적용, 마스킹 해제 시 책임자 승인, 접근권한 부여 등 안전성 조치를 적용해야 한다. 주민등록번호의 경우 법률에서 허용하는 경우를 제외하고 주민등록번호를 처리할 수 없다.

불특정 다수가 이용하는 화장실, 탈의실 등 개인의 사생활을 침해할 우려가 있는 장소의 내부를 볼 수 있는 장소에 영상정보처리기기(CCTV)를 설치 운영하지 않아야 한다. 영상정보처리기기를 설치 운영하는 자(영상정보처리기기 운영자)는 정보주체가 쉽게 인식할 수 있도록 설치목적 및 장소, 촬영범위 및 시간, 관리책임자 설명 및 연락처 등을 포함한 안내판을 설치해야 한다. 영상정보처리기기의 설치 목적과 다른 목적으로 조작하거나 다른 곳을 촬영하거나 녹음 기능을 사용하지 않아야 한다.

개인정보 처리자가 제3자에게 개인정보 처리업무를 위탁하는 경우 아래의 사항을 계약서 등 문서에 포함해야 한다.

❶ 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
❷ 개인정보의 기술적 관리적 보호조치에 관한 사항
❸ 위탁업무의 목적 및 범위

❹ 재 위탁 제한에 관한 사항
❺ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
❻ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
❼ 수탁자가 준수하여야 할 의무를 위반한 경우 손해배상 등 책임에 관한 사항

개인정보 처리자는 위탁하는 업무의 내용과 수탁자를 정보주체가 쉽게 확인할 수 있도록 홈페이지 등에 공개해야 한다. 만약 홈페이지에 게시할 수 없다면 사업장 등 보기 쉬운 장소에 게시하거나 신문 등에 공고하거나 연 2회 이상 발행하여 배포하는 소식지/홍보물/청구서 등을 이용하거나 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법 등을 사용할 수 있다. 위탁자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 수탁자를 교육하고 처리 현황을 주기적으로 점검하여 수탁자가 개인정보를 안전하게 처리하는지를 관리 감독해야 한다.

개인정보 처리자는 개인정보 취급자를 적절히 관리 감독하여야 하며 적정한 취급을 보장하기 위해 필요한 교육을 주기적으로 실시해야 한다.

정보주체의 개인정보를 처리하는 경우 다음 사항을 포함한 개인정보 처리방침을 홈페이지 등에 공개해야 한다. 개인정보 처리방침을 변경하는 경우 이유와 변경내용을 지체 없이 공지하고 이용자가 언제든 변경된 사항을 알아볼 수 있도록 조치해야 한다.

- 개인정보의 처리 목적
- 처리하는 개인정보의 항목
- 개인정보의 처리 및 보유 기간
- 개인정보의 제3자 제공에 관한 사항(해당되는 경우)
- 개인정보처리의 위탁에 관한 사항(해당되는 경우)
- 정보주체와 법정대리인의 권리 의무 및 그 행사방법에 관한 사항
- 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
- 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치 운영 및 그 거부에 관한 사항(해당되는 경우)
- 개인정보의 파기에 관한 사항
- 개인정보의 안전성 확보 조치에 관한 사항

개인정보 처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정해야 한다. 개인정보 보호책임자는 다음의 업무를 수행하여야 하며 업무 수행 시 정당한 이유 없이 불이익을 주거나 받지 않아야 한다.

❶ 개인정보 보호 계획의 수립 및 시행
❷ 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
❸ 개인정보 처리와 관련한 불만의 처리 및 피해구제
❹ 개인정보 유출 및 오/남용 방지를 위한 내부통제시스템의 구축
❺ 개인정보 보호 교육 계획의 수립 및 시행
❻ 개인정보파일의 보호 및 관리 감독
❼ 개인정보 처리방침의 수립/변경 및 시행
❽ 개인정보 보호 관련 자료의 관리
❾ 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

개인정보 보호책임자는 개인정보 보호와 관련하여 법률 위반 사실을 알게 된 경우 즉시 개선조치를 적용하여야 하며 필요시 경영진에게 개선조치를 보고하여야 한다.

개인정보 처리자는 개인정보가 유출되었음을 알게 되었을 경우 지체 없이 해당 정보주체에게 다음 사실을 알려야 한다.

❶ 유출된 개인정보의 항목
❷ 유출된 시점과 그 경위
❸ 유출로 인해 발생할 수 있는 피해를 최소화하기 위해 정보주체가 할 수 있는 방법 등에 관한 정보
❹ 개인정보 처리자의 대응조치 및 피해 구제절차
❺ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

개인정보 처리자는 개인정보가 유출된 경우 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 수립하기 위해 개인정보 유출사고 대응절차를 수립해야 한다. 개인정보 유출 사고 발생 시 고객센터의 상담원이 적절하게 대응할 수 있도록 대응 스크립트를 준비하며, 대외 의사소통 채널을 하나의 부서로 단일하게 만들어야 하며, 유출사고의 원인 분석을 위해 정보보호 부서/개인정보 보호부서, IT부서 및 외부 전문기관 등과 협조하여 분석을 실시해야 한다. 분석 결과 발견된 사항에

대해 필요한 경우 보안솔루션을 추가 구축하거나 개인정보보호 지침을 개정해야 한다. 1천명 이상의 정보주체에 대한 개인정보가 유출된 경우 한국인터넷진흥원에 지체 없이 신고해야 한다.

정보보호 및 개인정보보호 관련 법률은 지속적으로 제·개정 되고 있다. 따라서 법률은 1회성으로 확인할 것이 아니라 지속적으로 변경 사항을 확인하여 변경이 기업의 비즈니스에 미치는 영향을 파악하여 필요한 경우 사내 정보보호 규정에 반영되도록 관리하고, 임직원이 준수할 수 있도록 관리해야 한다.

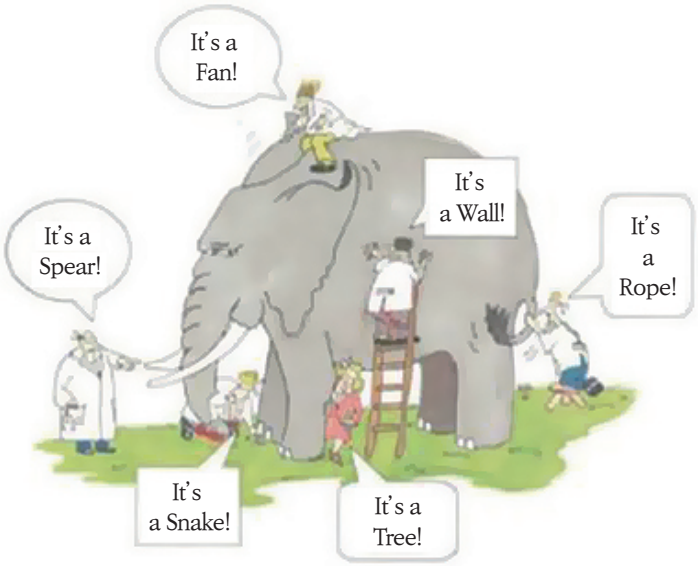
※ 정보보호 및 개인정보보호 관련 법률의 제·개정 사항은 국가법령정보센터(Http://www.law.go.kr)에서 확인 가능하다.

2. CISO가 꼭 알아야 할 보안

랜섬웨어, 갠드크랩, 악성코드, 개인정보 유출, 산업기밀/영업비밀 유출 시도, 홈페이지 변조 시도, 악성코드 감염 등 기업은 다양한 보안 위협에 직면해 있다. 새로운 최신 기술이 나타나면서 기업이 보안 위협에 대응하는 방법도 고도화되지만 해커와 같은 외부 위협요인도 공격기법이 고도화된다.

정보보호 최고책임자는 소속 조직의 정보보호 수준을 정확히 알아야 할 필요가 있다. 정보보호 조직 구성원의 역량, 보안 아키텍처 및 아키텍처에 따른 이행여부, 임직원 보안 인식 수준 등 다양한 측면에서 평가된 보안 수준이 해당 조직의 보안 수준을 나타낼 수 있다. 정보보호 컨설팅에 따른 취약점 수준이나 정보보호 관리체계에 따른 결함의 개수 등은 조직의 보안수준을 결정하는 요소 중 일부일 뿐 결정적 요소는 아니다. 아래의 그림과 같이 조직의 일부 영역에 대한 보안평가가 조직 전체의 보안 수준을 나타낸다고 오해할 수 있다.

그림 2-2 정보보호 수준에 대한 단편적 평가



출처: HelloT 첨단뉴스, 2018.06.07.

정보보호 솔루션의 도입 및 설치 시 도입 효과를 명확히 경영진에게 설명해야 한다. 마치 특정 정보보호 솔루션을 도입하면 모든 보안 사고를 예방할 수 있을 것이라고 설명한다면 당장은 경영진을 설득할 수 있겠지만 장기적인 관점에서 볼 때 정보보호 조직은 비용은 많이 쓰는 데 효과가 없는 부서로 오해할 수 있다. 정보보호 최고책임자는 정보보호 부서의 최고 직급자가 아닌 경영진의 일원으로서 경영진과 의사소통을 해야 한다.

조직의 정보보호 수준을 결정하는 요소는 여러 가지가 있지만 궁극적으로는 사람, 즉 임직원이다. 따라서 임직원의 정보보호 인식을 강화할 수 있도록 다양한 교육과 활동을 통해 임직원의 인식 수준을 변화시켜야 한다. 이때 주의할 사항은 이러한 활동이 일회성 활동이 되지 않아야 한다는 것이다. 다양한 정보보호 인식제고 프로그램을 만들어 지속적으로 임직원의 정보보호 인식을 제고할 수 있는 절차를 수립해야 한다.

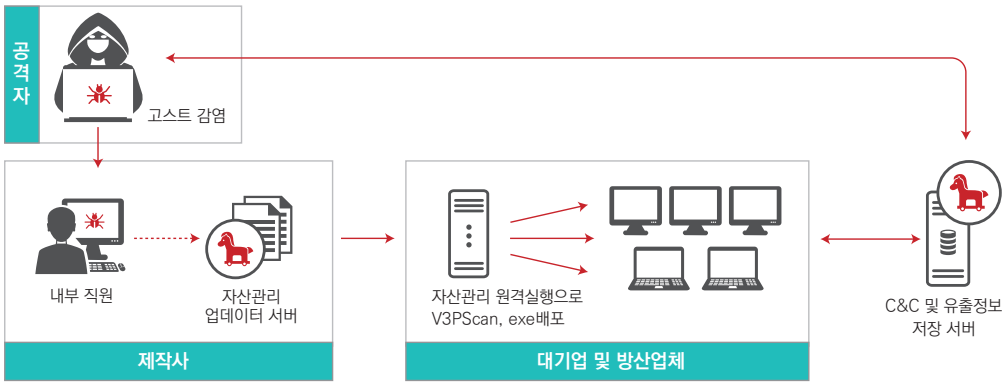
정보보호 최고책임자는 타사의 침해사고 사례에 대한 원인분석을 통해 유사사고가 해당 조직에 발생하지 않도록 정보보호 솔루션의 구축 또는 정보보호 규정의 개정 등을 실시해야 한다. 정보보호 솔루션 구축 시 내부 정보보호 아키텍처를 활용하거나 중장기 계획에 따른 도입 필요성 및 타당성을 충분히 검토한 후 도입해야 한다.

(1) 보안사고 사례

공급망 보안 공격

공급망 보안 공격은 주로 개발사 시스템이나 업데이트 서버 등을 해킹하여 악성코드를 숨기는 방식을 사용한다. 심층방어(Defense-In-Depth) 체계를 갖추고 있는 기업이나 기관을 직접 공격하는 방식보다 공격 대상과 연결되어 있지만 상대적으로 보안이 취약한 대상을 이용하는 것이 공격자 입장에서는 쉽기 때문이다. 백신 등을 포함한 업데이트 파일을 제조사로부터 전달받을 경우 악성코드 감염, 소스 프로그램의 변조 여부를 파악하기는 쉽지 않고 제조사가 전달한 파일을 신뢰하고 사용할 수밖에 없는 환경이다. 패치 적용 시 패치파일을 즉시 적용하지 않고 일정 기간 안정화 여부 등을 면밀히 검토 후 패치해야 한다. 또한 외부에서 원격접속을 통해 패치를 진행하는 경우 전용선 또는 전송구간 암호화를 적용하고, 내부망 서버 또는 설비에 직접 접속하는 것이 아닌 원격접속서버(Remote access server)를 통해 접속할 수 있도록 통제해야 한다.

그림 2-3 공급망 공격 사례



출처: 안랩

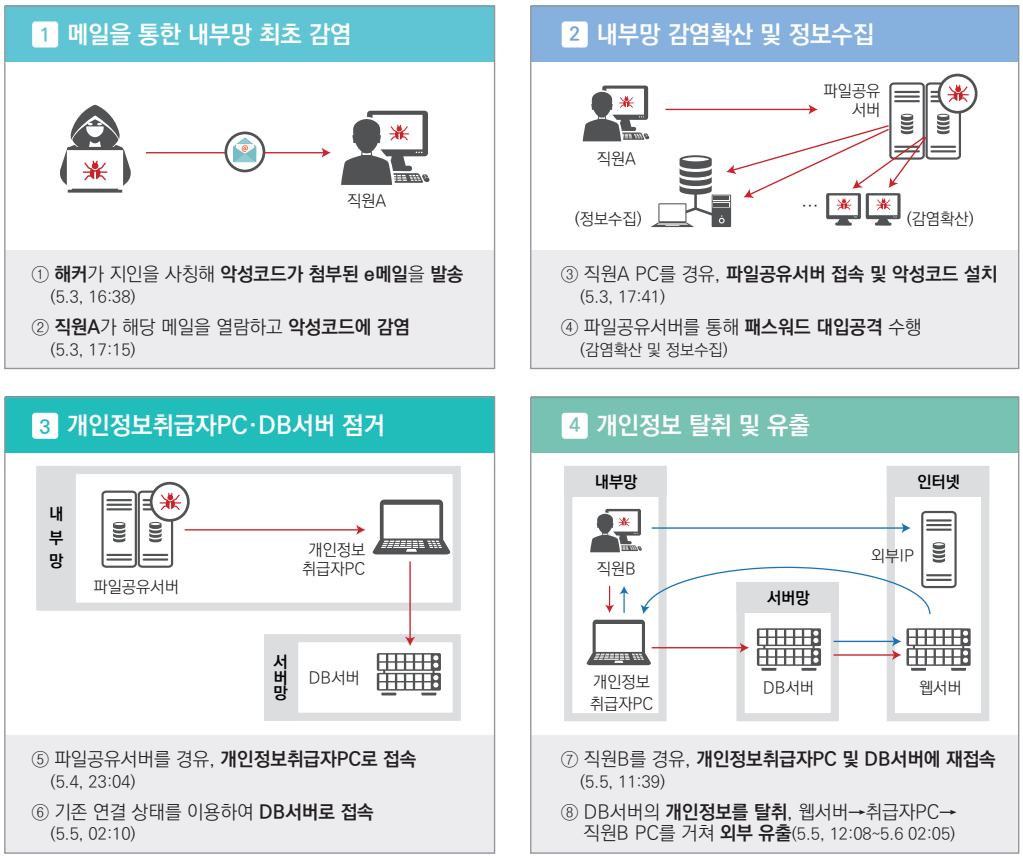
크립토재킹(Cryptojacking)

크립토재킹은 해커가 암호화폐를 채굴하기 위해 피해자에게 가하는 사이버공격의 한 형태이다. 체크포인트社의 위협 인텔리전스분석팀 책임자는 "문제는 웹사이트, 서버, PC와 모바일 상의 모든 곳에서 크립토재킹이 일어나고 있다는 사실"이라며 "전 세계 55%의 조직이 영향을 받고 있다"고 말했다. 크립토재킹으로부터 자신을 보호하는 가장 간단한 방법은 크립토재킹 차단기를 설치하는 것이다. 즉, 크립토재킹 코드와 관련된 도메인 목록을 차단하는 브라우저 확장을 추가하는 것이다. 브라우저 채굴을 차단하기 위해 특별히 만들어진 세 가지 확장 기능은 안티마이너(AntiMiner), 노코인(NoCoin), 그리고 마이너블록(MinerBlock)이다.

I사 개인정보 유출 사고

I사 개인정보 유출사고는 해커가 내부직원 PC를 악성코드에 감염시킨 후 정보 수집을 통해 DB 계정/패스워드를 수집하였으며 개인정보처리시스템 DB에 접속하여 확보한 개인정보를 외부로 유출한 것으로 조사되었다. 또한 DB 접속 시 세션 타임아웃 미적용, 망분리 운영 미흡 등의 취약점이 발견되었다. ISMS-P 인증을 유지하는 기업은 대부분 관리자페이지 및 서버/DB 접속 시 세션 타임아웃을 설정하고 있으며 개인정보 취급자에 대해 망분리하여 인터넷이 접속되지 않는 환경으로 구성하고 있다. 개인정보 취급자는 개인정보처리시스템에 접속하여 개인정보를 조회/변경/삭제 등 처리할 수 있는 직원 뿐 만 아니라, 서버/DB/네트워크 장비에 접속하여 운영하는 운영자도 망분리 대상에 포함하는 것이 안전하게 서비스를 운영할 수 있는 방안이다.

그림 2-4 2016년 I사 개인정보 유출 사고 분석결과



출처: 방송통신위원회 보도자료, 2016.08.31

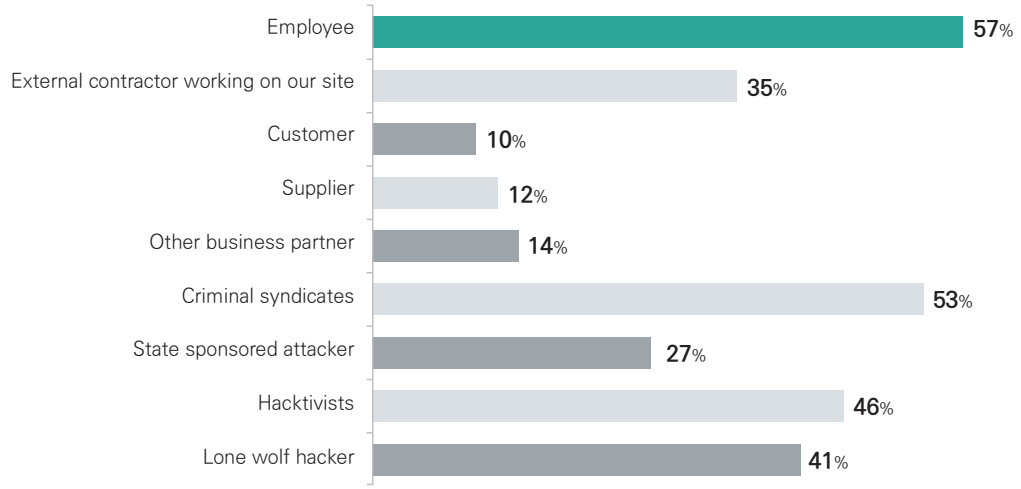
랜섬웨어

2018년 5월 전 세계적으로 워너크라이 랜섬웨어에 감염되는 사태가 발생하였으며 워너크라이에 감염되면 파일이 암호화된 후 $300를 비트코인으로 요구하는 메시지 창이 나타났다. 한국에서는 워너크라이로 인한 피해가 많지는 않았지만 영국, 우크라이나 등 일부 국가에서는 정부기관의 서버가 감염되는 등 피해가 심각하였다.

'워너크라이'의 유래는 Crypt와 Cry의 중의적 표현, '울고 싶니?'(Do You Wanna Cry?)와

'암호화 되고 싶니?'(Do You Wanna Crypt?)란 의미를 가지며, 랜섬웨어의 파일명은 'Wana Decrypt0r'로 '암호화 된 것을 풀고 싶니?'란 뜻이다. 이 사건은 NSA가 보유한 제로데이 취약점이 쉐도우브로커스라는 해킹그룹에게 유출되어 발생하였기에 이에 대한 비난도 많았다. 해당 취약점에 대한 보안패치를 2017년 3월 중순부터 제공했지만 업데이트를 하지 않거나 업무용 프로그램의 호환성 등을 이유로 백신, 방화벽 윈도우 업데이트하지 않은 업무용 PC, 또는 보안 패치가 끊긴 Windows XP가 설치된 PC들에서 많은 피해가 발생하였다. 한국에서는 인터넷호스팅 업체에서 랜섬웨어에 감염되는 백업된 자료까지 암호화되어 해커에게 비용을 지급하였음에도 서비스를 완전하게 복구하지 못한 사례도 있었다. 랜섬웨어로부터 조직을 보호하기 위해서는 운영체제에 대한 주기적인 업데이트를 실시해야 하며 PC 내 보관된 정보에 대해 주기적으로 백업하는 등의 방법으로 예방할 수 있다. 글로벌 컨설팅업체인 EY에서 조사한 사례에 따르면 "임직원이 정보유출 사고의 주체"라고 답변한 비율이 57%(중복 답변 포함)이다. 임직원은 본인의 실수 또는 외부의 유혹으로부터 쉽게 기업의 중요정보를 유출시킬 수 있다고 볼 수 있으며 이를 위해 정보유출 탐지 및 차단을 위한 솔루션을 구축할 뿐만 아니라 임직원의 인식제고를 통한 보안 역량을 강화해야 한다.

그림 2-5 정보보안 사고 주체



출처: EY GISS 2014

CISO
Chief
Information
Security
Officer

정보보호 최고책임자

길라잡이

기본편

III

정보보호 규정 수립

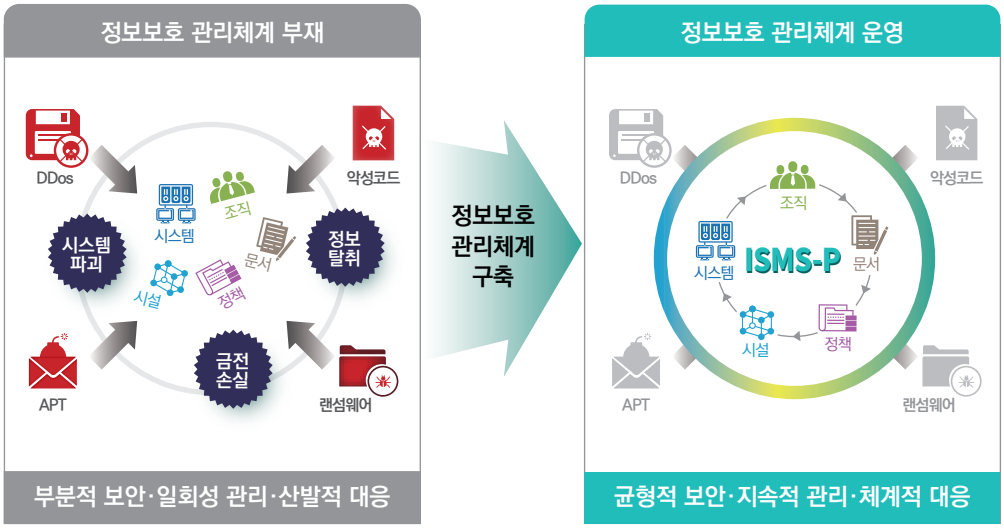
1. 정보보호 규정 개요
2. 정보보호 규정 작성방법
3. 정보보호 규정 사례 및 주안점

1. 정보보호 규정 개요

정보보호 관리체계는 정보통신망의 안전성 신뢰성 확보를 위한 관리적 기술적 물리적 보호조치를 포함한 종합적 관리체계이며 IT확산과 패러다임 변화, 사이버 침해 증가에 대비하는 조직 전반의 체계적인 위험관리 체계를 의미한다.

정보보호 관리체계를 수립하지 않은 기업은 정보보안 위협에 일시적 대응을 하며 당장 필요한 영역에서 부분적으로 보안을 수행하므로 동일 위협에 대응방안을 수립하여도 변형된 유사한 위협이 발생하면 대응하기 어려워진다. 따라서 체계적이고 지속적인 대응을 위한 정보보호 관리체계를 수립해야 한다.

그림 3-1 정보보호 관리체계의 정의



출처: KISA

정보보호 체계에 따른 지속적 관리와 체계적 대응을 하기 위해서는 수행주체와 방법, 주기 등이 명시된 정보보호 정책/지침을 수립하여야 임직원이 일관된 정보보호 활동을 수행할 수 있다. 문서화된 정보보호 정책/지침 등의 보안 규정이 없다면 임직원은 정보보호 활동을 임의적으로 수행하여 통제되거나 관리되지 않아 정보보호 수준은 지속적으로 하락하게 된다. 또한 수행주체가

명확하지 않다면 정보보호 활동이 정상적으로 수행되지 않거나 침해사고가 의심될 경우 원인분석에 오랜 시간이 걸리거나 분석되지 않을 수 있다.

문서화된 정보보호 정책/지침의 이행이 침해사고 또는 개인정보 유출 사고를 충분히 예방한다고 보기는 어렵다. 하지만 문서화의 효과는 침해사고 또는 개인정보 유출 사고의 피해범위를 감소시키고 사고 발생 시 신속한 사고 여부의 판단 및 빠른 대응을 보장할 수 있다. 문서화의 효과를 충분히 확보하기 위해서는 임직원에게 주기적이며 지속적인 정보보호 교육을 실시하고 훈련이 필요한 경우 주기적으로 훈련을 실시하여 개인이 수행하여야 할 정보보호 활동이 각자의 업무에 내재화될 수 있도록 지원해야 한다.

그림 3-2 정보보호 관리체계 수립의 효과

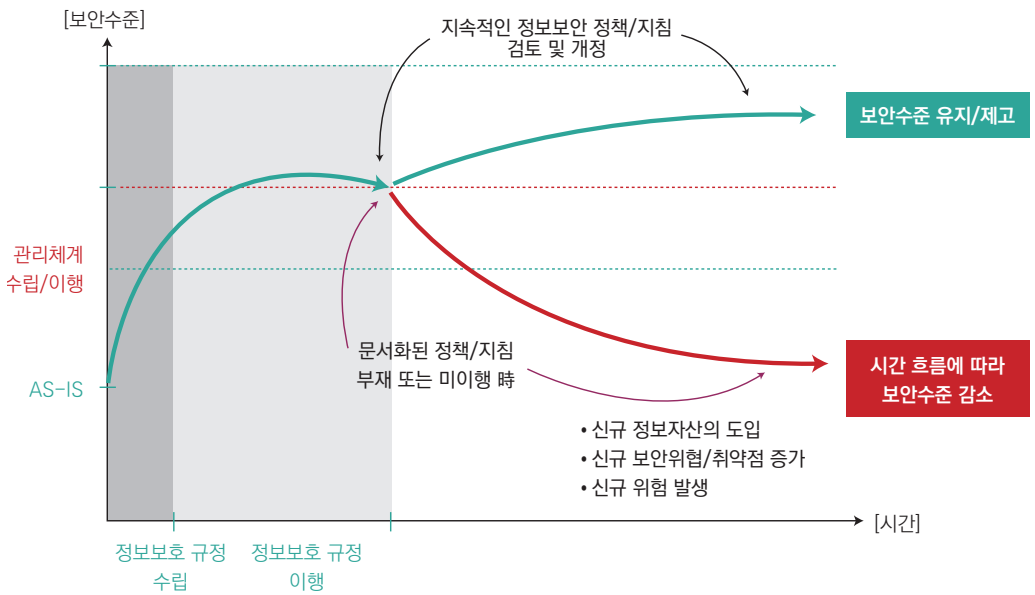
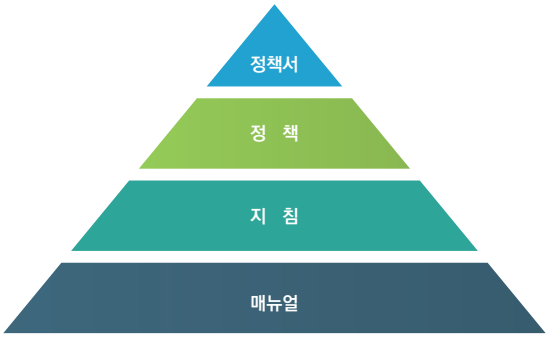


그림 3-3 정보보호 규정의 체계(예)



정보보호 규정에 대한 체계는 각 조직의 사규에 따른 체계에 따라 구성할 수 있다. 사규에 따라 정보보호 규정을 수립하더라도 정보보호 정책서, 정책, 지침, 매뉴얼/가이드 등의 체계로 구성하기를 권한다.

정책서는 정보보호에 대한 최상위 수준의 목표 및 방향, 원칙을 경영진이 제시하는 문서이다. 정책서는 정보보호 원칙을 제시하고 있으므로 하위 정책/지침을 작성할 경우 원칙을 위반하지 않도록 충분히 고려해야 한다. 기술의 발전에 따른 내부 정책/지침의 규정 수립이 따라가지 못할 경우 원칙에 입각하여 정보보호 절차를 수행하면 된다. 정책서는 비즈니스상의 중대한 변화(신규사업 추가 또는 사업 매각 등)가 있는 경우 검토하여 개정하면 된다.

정책은 정책서의 원칙에 따라 임직원이 준수하여야 할 구체적인 사항을 정의하며 조직의 경영철학을 반영해야 한다. 경영진은 정보보호에 대한 전반적인 목표와 방향을 포함하고 있는 정책을 제정 및 문서화하고 임직원에게 공표하고 정책을 준수할 수 있도록 통제해야 한다. 또한, 경영진은 정책에 영향을 받는 구성원에게 해당 정책을 충분히 설명하고 정책의 의도를 이해할 수 있도록 필요한 절차를 수행하며 내부 임직원뿐만 아니라 외부 협력업체 직원 등에도 적용해야 한다. 정책은 최소 년1회 주기로 검토하고 필요 시 개정한다.

지침은 정책 준수를 위한 구체적이고 세부적인 방법을 규정한 것으로 실무 기준을 제시한다. 통상적으로 개별 정보자산의 관리를 위한 지침, 개발 및 운영, 어플리케이션, 정보자산 관리, 위험평가 및 관리, 물리적 보안 등 세부적인 영역에 대해 규정을 한다.

2. 정보보호 규정 작성방법

정보보호 정책/지침 등 규정 수립 시 조직의 특성 및 IT/정보보안 문화를 고려하여 수립하여야 하며 다음 사항을 고려해야 한다.

(1) 상위조직의 규정 또는 법적 요건을 반영해야 한다.

해당 조직의 상위조직(지주사, 모회사 등)에서 제시한 정보보호 정책/지침과 해당 조직의 비즈니스와 관련된 법적 요건을 반영해야 한다. 개인정보 유출사고와 개인정보 오남용 사고가 빈번하게 발생함에 따라 개인정보 보호와 관련된 법률 및 행정규칙이 지속적으로 강화되고 있다. 제·개정되는 법률에 대해 식별한 후 내부 정보보호 규정에 반영해야 한다.

(2) 다른 규정에 동일한 내용을 규정하지 않아야 한다.

예를 들어, 계정 및 패스워드 관리를 서버/네트워크/정보보호 시스템/DB/개인정보처리시스템/응용시스템 보안 지침에 각각 반영하고 있다면 조항의 일부 사항이 개정될 경우 내용을 모두 찾아서 개정해야 한다. 패스워드 변경주기를 180일에서 90일로 변경 시 개정이 누락된 지침은 패스워드 변경주기가 기존과 동일하게 180일을 유지하게 된다. 특정 지침에 규정한 후 나머지 지침에서는 해당 조항을 준용하는 형태로 수립해야 한다.

(3) 수행주체와 방법, 주기를 명시해야 한다.

정보보호 조직, 현업부서 담당자, 개발자, 운영자, 임직원, 협력사 직원 등 정보보호 절차의 준수와 관련하여 다양한 이해관계자가 존재한다. 따라서 정책/지침의 각 조항은 누가(Owner) 수행할 지 수행주체를 명확하게 정의하여야 책임 추적성(Accountability)을 확보할 수 있고, 정보보호 활동에 대한 누락(Gray Zone)이 발생하지 않도록 관리할 수 있다. 정보보호 정책/지침의 각 조항에는 법적 요건, 조직의 정보보호 특성 등을 고려하여 주기를 정의해야 한다. 주기가 정의되지 않는다면 모든 정보보호 활동을 1회성으로 준수하기 때문에 적절한 보안수준을 확보하기 어렵다. 주기(반기/분기/월간/주간/일)에 대해 명확히 정의함으로써 정보보호 활동이 지속적으로 운영될 수 있다.

(4) 정보보호 규정에 대한 승인권자를 지정해야 한다.

정책서/정책을 제·개정하는 경우 이해관계자(협업부서 및 IT운영부서 등)와 해당 내용을 충분히 협의 검토해야 한다. 정책서/정책의 관리는 정보보호 부서에서 수행하지만 해당 조항에 따른 이행은 이해관계자가 수행하기 때문이다. 정책서/정책이 조직 내에서 영향력이 있으려면 경영진에 의해 검토되고 승인이 되어야 가능하다. 정보보호 규정에 따른 승인권자는 조직의 규모, 사규 등을 고려하여 결정하여야 하지만 정책서/정책은 경영진, 지침은 정보보호 최고책임자, 매뉴얼/기준/가이드는 실무부서 팀장이 승인하는 것을 권고한다.

(5) 명확한 표현을 사용해야 한다.

정보보호 정책/지침 각 조항의 내용은 명확하게 작성하여야 하며 '~~할 수 있다.'와 같이 선택의 의미가 아닌 '~~ 하여야 한다'와 같이 표현해야 한다. 또한 해당 조항의 내용이 많아서 해석이 달라지지 않도록 해야 한다. 단서 조항은 정보보호 통제에 예외를 허용하는 것으로 최소한으로 부여하여야 하며, 단서 조항이 포함된 통제가 충분히 성숙되면 해당 단서조항은 삭제해야 한다.

(6) 타사의 선진사례가 아닌 현재 수행하고 있는 보안활동을 문서화한다.

정보보호 수준은 높은 타사의 선진사례는 해당 조직의 문화, 업무 절차를 고려하지 않았기 때문에 해당 조항의 요구사항이 조직의 환경에 맞지 않고 과도한 활동을 요구할 수 있다. 따라서 법률 또는 상위기관에서 요구사항을 벗어나지 않는 범위 내에서 현재의 업무 절차를 문서화해야 한다.

강력한 정보보호 정책/지침은 임직원이 준수를 잘하면 정보보호 수준을 지속적으로 제고할 수 있다.

정보보호 수준이 높지 않은 조직은 강력한 정보보호 정책/지침을 수립하기 보다는 임직원이 충분히 준수할 수 있도록 수립한 후 지속적으로 강화하는 것이 정보보호 수준을 제고할 수 있다.

(7) 정보보호 감사 결과 및 타사 보안사고 사례를 검토하여 필요 시 개정해야 한다.

전사 정보보호 감사결과 많은 임직원이 위반하고 있다면 2가지 측면에서 검토해보아야 한다.

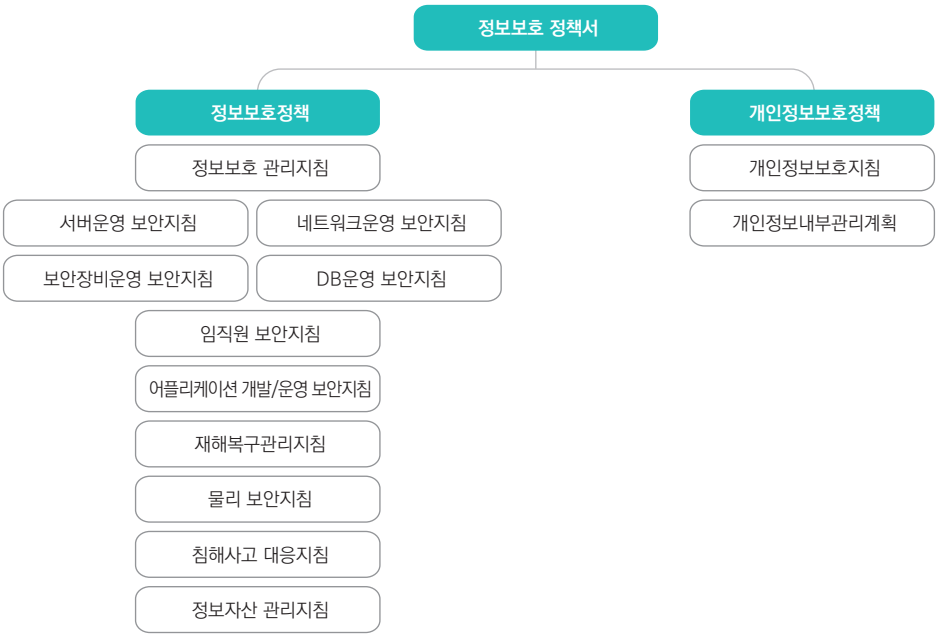
- 정보보호 규정이 과도한 지 또는 정보보호 규정이 누락되지 않았는지
- 정보보호 규정이 수립되어 있으나 인식 미흡으로 준수하지 않는지

정보보호 규정이 과도하거나 누락되어 있다면 해당 내용에 대한 정보보호 정책/지침을 수립하고 개정된 내용을 교육해야 한다. 정보보호 규정이 있음에도 준수하지 않는다면 임직원 정보보호 교육에 포함하여 인식을 제고해야 한다. 또한 타사에서 침해사고 또는 개인정보 유출사고가 발생하면 원인 분석 결과 등을 참고하여 정보보호 정책/지침에 해당 사고원인을 통제할 수 있는 조항이 있는 지 검토해야 한다.

3. 정보보호 규정 사례 및 주안점

정보보호 규정은 조직의 보호대상 또는 수행주체 측면에서 수립할 수 있다. 규정의 종류와 내용을 정의한 기준은 별도로 없으며 조직의 특성을 고려하여 수립하면 된다.

그림 3-4 정보보호 규정 사례



정보보호 관리지침은 정보보호 관리체계의 수립과 운영에 필요한 정보보호 조직, 정보보호 교육, 정보보호 감사 및 문서화, 내부 임직원의 채용 전/근무 중/퇴사 시 보안절차, 외부 계약 및 외부인 보안관리 등에 대한 규정을 포함한다.

서버운영 보안지침은 서버의 도입/설치 시 사전 보안성검토, 보안취약점 점검, 계정 및 패스워드 정책, 접근권한 검토, 로그 설정 및 분석, 접근통제, 백업 및 복구, 자산 폐기 등에 대한 규정을 포함한다.

네트워크운영 보안지침은 네트워크 장비의 도입/설치 시 사전 보안성검토, 보안취약점 점검, 계정 및 패스워드 정책, 접근권한 검토, 로그 설정 및 분석, 접근통제(ACL 정책), 불필요한 서비스/포트의 제거, 백업 및 복구, 자산 폐기 등에 대한 규정을 포함한다.

(보안장비운영 보안지침) 정보보호 시스템의 도입/설치 시 보안성검토, Rule set 설정 및 관리, 계정 및 패스워드 설정 절차, 접근권한 검토, 로그 설정 및 분석, 불필요한 서비스의 제거, 백업 및 복구, 자산 폐기, Firewall/IPS/DDoS/SSL VPN/IPSec VPN 및 단말보안솔루션에 대한 운영 규정 등에 대한 규정을 포함한다.

(DB운영 보안지침) DBMS의 도입/설치 시 보안성검토, 계정 및 패스워드 설정, 암호화, 접근권한 검토, 로그 설정 및 분석, 백업 및 복구, 자산 폐기 등에 대한 규정을 포함한다.

(임직원 보안지침) 계정 및 패스워드, PC 지급 및 사용, 인터넷 및 이메일 사용, 모바일기기 사용, 소프트웨어 사용 시 보안절차 등에 대한 규정을 포함한다.

(어플리케이션 개발/운영 보안지침) 개발/운영의 분리, 보안 요구사항 분석, 정보보안 요건 정의, 계정/패스워드/인증/로그/접근권한 설계, 안전한 프로그래밍, 외주개발 보안, 형상관리 및 운영 이관, 소스 점검 및 취약점 점검, 변경 및 긴급변경 절차 등에 대한 규정을 포함한다.

(재해복구 관리지침) 재해복구 조직 구성, 업무중요도 및 영향분석, 업무 중요도에 따른 분류, RTO/RPO 평가, 재해복구계획 수립, 재해복구계획 훈련, 사후관리 등에 대한 규정을 포함한다.

(물리보안지침) 보안구역 지정, 통제구역에서 작업, 케이블 및 전원선 보호, 출입통제, 자산 반출입 통제, 사무실 보안, 영상정보처리기기 운영 등에 대한 규정을 포함한다.

(침해사고 대응지침) 침해사고 대응조직 구성 및 책임/역할, 침해사고 심각도 정의, 침해사고 징후 분석, 침해사고 접수, 침해사고의 대외기관 신고, 침해사고 조사, 침해사고 대응, 침해사고 복구, 사후관리 등에 대한 규정을 포함한다.

(정보자산관리지침) 자산 관리절차, 자산 식별 및 분류, 자산 중요도 평가, 자산의 도입 및 변경, 유휴장비의 관리, 자산의 폐기, 자산 등급 별 보호대책 등에 대한 규정을 포함한다.

(개인정보보호 지침) 정보통신망법 및 개인정보 보호법 등과 행정규칙을 내부적으로 준수하는 절차와 방법에 대해 규정하고 있다. 개인정보보호 지침은 법률의 내용을 동일하게 반영하는 것이 아니라 법률의 내용을 내부 업무절차, 정보보호 시스템 등을 통해 어떻게 구현할 지 실무적인 내용을 반영하는 것이다. 개인정보 보호법의 내용을 반영할 경우 공공기관과 관련된 내용은 일반기업에서는 개인정보보호 지침에 반영하지 않아야 한다.

(1) 정보보호 정책서

정보보호 정책서는 최고 경영진이 임직원에게 정보보호에 대한 원칙과 방향성을 제시하는 문서로 최고 경영진의 의지와 지원 사항을 포함해야 한다.

정보보호 정책서

새로운 기술의 출현에 따른 정교하고 지능화된 각종 위협은 IT 서비스를 제공하는 OOOO의 정보자산에 심각한 영향을 미칠 수 있다. Global leader로서 안전하고 개인화된 서비스를 제공하려는 OOOO의 노력에 정보보호 활동은 이제 선택이 아닌 필수 불가결한 요소가 되었다. 따라서, OOOO의 모든 임직원은 내부 및 외부로부터의 해킹, 정보의 유출 등 보안 위협으로부터 중요 정보자산의 손실과 그에 따른 업무의 지연 및 저하와 더불어 각종 법적, 사회적, 윤리적인 여파를 철저히 고려하여 이에 따른 적절한 대비책을 마련하는데 최선을 다해야 한다.
이에, OOOO은 다음과 같은 정보보호 원칙을 수립하고 선포한다.

(1) OOOO의 정보자산을 불법적인 접근과 유출로부터 보호한다.
(2) OOOO의 정보자산에 대한 기밀성, 무결성, 가용성을 유지한다.
(3) OOOO은 정보보호 관련 법적 보안 요구 사항을 준수한다.
(4) OOOO의 모든 임직원은 정보보호의 중요성을 인식하고, 사고를 적절하게 예방하며, 탐지, 대응할 수 있어야 한다.
(5) OOOO은 정보보호와 관련한 위험의 분석, 점검 및 감사를 주기적으로 실시한다.

OOOO은 이러한 정보보호 방침의 준수를 위해 필요한 시간과 자원을 투자하며, 정보보호를 관리하는 조직을 구성하여 운영한다. 정보보호는 특정 관리 조직으로만 수행될 수 없으며, 무엇보다도 모든 직원들의 참여와 책임이 필요하다. 따라서 모든 직원들은 정보보호의 중요성을 인식하고, 지속적인 관심을 가짐으로써 선포된 방침을 이해하고 준수하는데 최선을 다해야 한다.

20XX. 00

OOOO ㈜ 대표이사 홍 길 동

(2) 정보자산 관리지침 중 자산등급별 보호대책

정보자산 관리지침은 정보자산 분류기준과 중요도 평가 기준을 수립하고 기준에 따라 평가된 자산에 대해 자산등급 별 보호대책을 수립해야 한다. 모든 정보자산에 대해 동일한 보안대책을

적용하여 높은 수준으로 관리할 수 있다면 자산등급 별 보호대책은 필요하지 않다. 정보보호에 투자할 수 있는 예산에 한계가 있거나 관리 인력이 많지 않다면 자산등급 별 보호대책에 따라 중요도가 높은 자산을 우선적으로 보호해야 한다. 자산등급 별 보호기준이 없다면 중요 자산 중 일부 자산에서 보호대책이 누락되어 보안통제가 약화될 수 있다.

아래 내용은 자산의 등급별 보호대책 중 서버 자산에 대한 보호대책에 대한 사례이다. 정보자산의 등급을 세분화할 경우 등급별 서로 다른 보호대책을 차별화하기 곤란하므로 3단계 등급으로 분류하는 것을 권고한다.

제00장 자산의 등급 별 보호대책

제XX조 (서버 등급 별 보호대책)

① 1등급 서버의 보호대책은 다음과 같다.

1. 내부 네트워크에 설치하고 별도의 zone을 구성 운영하며 방화벽을 통해 접근통제를 실시한다.
2. 카드키와 지문인식 등 강화된 출입통제가 적용된 서버실에서 운영하여야 한다.
3. 사용자 인증 방식은 지식기반, 소유기반, 생체인식 기반 중 2가지 요소를 이용하는 방식을 적용하여야 한다.
4. 보안사고 및 치명적 장애에 대비하기 위해 상시 모니터링을 하여야 한다.
5. 보안사고를 예방하기 위해 서버 담당자는 분기 1회 취약점 점검을 실시하여야 한다.
6. 서버 담당자 이외에 관리자 권한을 부여하지 않아야 한다.
7. 접근통제 기능 또는 접근통제 시스템을 이용하여 접근 가능한 사용자와 IP에 대해 통제를 적용하여야 한다.

② 2등급 서버의 보호대책은 다음과 같다.

1. 내부 네트워크에 설치하고 운영하여야 한다.
2. 카드키 등 출입통제가 적용된 서버실에서 운영하여야 한다.
3. 사용자 인증 방식은 ID/PW를 이용한 인증을 적용하여야 한다.
4. 보안사고를 예방하기 위해 서버 담당자는 반기 1회 취약점 점검을 실시하여야 한다.
5. 접근통제 기능을 이용하여 접근 가능한 사용자와 IP에 대해 통제를 적용하여야 한다.

③ 3등급 서버의 보호대책은 다음과 같다.

1. 내부 네트워크에 설치하고 운영하여야 한다.
2. 카드키 등 출입통제가 적용된 서버실에서 운영하여야 한다.
3. 사용자 인증 방식은 ID/PW를 이용한 인증을 적용하여야 한다.
4. 보안사고를 예방하기 위해 서버 담당자는 년 1회 취약점 점검을 실시하여야 한다.
5. 접근통제 기능을 이용하여 접근 가능한 사용자와 IP에 대해 통제를 적용하여야 한다.

(3) 임직원 보안지침

임직원 보안지침은 계정 및 패스워드, PC 지급 및 사용, 인터넷 및 이메일 사용, 모바일기기 사용, 소프트웨어 사용 시 보안절차 등에 대한 규정을 포함한다. PC/단말은 회사에서 공식적으로 지급한 경우에만 사용하고 개인 PC를 반입하지 않아야 한다. 이메일은 회사의 공식 메일 시스템만 사용하여야 하며 인터넷을 통해 제공되는 상용 이메일은 사용하지 않도록 통제해야 한다. 소프트웨어의 경우 PC 지급 시 단말에 설치되는 보안솔루션을 사전에 설치하여 지급하며 회사에서 라이선스를 가지고 있는 소프트웨어를 사용해야 한다.

아래는 임직원의 계정 및 패스워드에 대한 규정 사례이다. 패스워드의 경우 정보통신망법의 '개인정보의 기술적 관리적 보호조치 기준' 또는 개인정보 보호법의 '개인정보의 안전성 확보조치 기준'에 규정된 사항을 준수해야 한다.

제XX조 (사용자 계정의 생성, 변경, 삭제)

① 사용자 계정의 생성 절차는 다음과 같다

1. 계정 신청자는 "사용자 계정 신청서"를 작성하여 소속 부서장의 승인을 받은 후 시스템 담당자에게 요청한다.
2. 시스템 담당자는 요청서를 접수 후 계정을 생성하고 요청한 권한을 부여하며 정보보호 담당자는 부여된 권한의 적정성에 대해 주기적으로 검토하여야 한다.
3. 그룹웨어 계정은 입사 후 HR시스템 담당자가 생성하며 부서 및 역할에 따른 접근권한을 부여하고 정보보호 담당자는 주기적으로 권한 부여 절차에 대한 적정성을 검토하여야 한다.

② 사용자 계정의 변경 및 삭제 절차는 다음과 같다

1. 직무변경 또는 퇴사자 발생 시 소속 부서장은 당사자로부터 "사용자 계정 신청서"를 받아 시스템 담당자에게 제출한다.
2. 시스템 담당자는 직무변경을 요청한 계정의 접근권한을 변경하며 퇴사자 계정은 퇴사 즉시 삭제한다.
3. 해당 부서에서 퇴사자의 계정이 필요하다고 요청하는 경우 정보보호 최고 책임자의 승인을 받아 최대 1년간 유지할 수 있다.

제XX조 (패스워드 생성 및 관리)

① 계정 생성을 통보받은 임직원은 즉시 로그인하여 초기 패스워드를 변경하여야 한다.

② 임직원은 패스워드 설정이 8자 이상의 영문자, 숫자, 특수문자를 포함하여야 한다.

③ 임직원은 패스워드를 90일 마다 변경하여야 한다. 단, 시스템 운영에 직접적인 미칠 수 있는 계정의 패스워드는 정보보호 최고 책임자의 승인을 받은 경우 예외로 할 수 있다.

④ 시스템 담당자는 이전 패스워드(3회)가 재사용하지 않도록 설정하여야 한다.
⑤ 시스템 담당자는 패스워드가 화면 상에 표시될 때 마스킹 처리하여야 한다.
⑥ 임직원은 패스워드가 노출되었을 경우 즉시 패스워드를 변경하여야 한다.
⑦ 시스템 담당자는 임직원에게 초기화된 패스워드 전송 시 SMS 등을 통해 통보하여야 한다.
⑧ 시스템 담당자는 패스워드 설정 시 다음 각 호에 해당되지 않는 패스워드를 사용할 수 없도록 설정하여야 한다.
1. ID와 동일한 패스워드
2. 회사명, 부서명, 서비스명 등과 관련된 약어 또는 단어
3. 사전에 등록된 단어
4. 동일한 문자 또는 숫자가 3자 이상 연속되는 패스워드
5. 문자 또는 숫자로 구성된 패스워드
6. 주기성 문자 (abcd, 1234 등) 및 키보드 상의 연속 배열 (asdf, qwerty 등)
7. 8자 미만의 패스워드

제XX조 (사용자 권한 관리)
① 시스템 담당자는 사용자에게 권한 부여 시 업무 수행에 필요한 최소한의 권한으로 부여하여야 한다.
② 시스템 담당자는 정보시스템을 오용 또는 악용하는 사용자의 권한을 제한 또는 회수할 수 있다.
③ 시스템 담당자는 접근권한을 검토한 후 3개월 이상 장기 미사용 계정은 잠금 설정하고 이후 3개월 동안 재사용 요청이 없는 계정은 삭제한다.

(4) 재해복구 관리지침

재해복구 관리지침은 재해 발생 시 핵심 업무 및 IT 서비스, 정보시스템의 연속성을 확보하기 위해 필요한 절차를 정의한다. 재해복구 관리지침을 기반으로 핵심 업무 및 IT 서비스 식별, 비즈니스영향평가(Business Impact Analysis)를 통한 복구 우선순위 결정, 복구 우선순위에 따른 복구목표시간(RTO), 복구목표시점(RPO), 훈련 방안 등을 포함한 재해복구 계획서를 수립해야 한다. 재해복구 계획서는 매년 훈련 후 훈련결과에 따라 필요한 사항을 개정해야 한다.

제XX조 (업무 중요도 평가)

① 재해복구 담당자는 IT서비스 및 업무의 연속성을 훼손할 수 있는 재해를 식별하고 재해 발생에 따른 영향을 분석하여야 한다.

② 재해복구 담당자는 매년 업무중요도 평가에 대해 재검토하여야 하며 재검토 시 시스템 담당자와 현업 담당자에게 지원을 요청할 수 있다.

③ 재해복구 담당자는 현업 담당자와 협의를 통해 복구목표시점(RPO)과 복구목표시간(RTO)을 정의하고 재해복구 책임자의 승인을 받아야 한다.

제 XX조 (재해복구 계획 수립)

① 재해복구 담당자는 화재, 지진, 정전, 건물붕괴, 시스템 중단 등 재해로 인한 업무 중단을 최소화하기 위해 재해복구 계획서를 작성하고 재해복구 책임자에게 승인을 받아야 한다.

② 재해복구 담당자는 재해복구 계획 수립 시 다음 사항을 포함하여야 한다.

1. IT서비스(업무) 식별
2. IT서비스의 복구 우선순위 선정
3. IT서비스의 복구목표시점(RPO; Recovery Point Objective)
4. IT서비스의 복구목표시간(RTO: Recovery Time Objective)
5. 관련 IT자원 및 설비목록 작성

③ 재해복구 담당자는 재해복구서에 다음 사항을 포함하여야 한다.

1. 평상 시/재해 시 조직 및 운영절차
2. 상황파악 및 통보/전파 절차 작성
3. 모의훈련
4. 유지관리

④ 재해복구 담당자는 재해 발생 시에 대비한 반출 요령을 마련하여 비상반출 물품에 대한 우선순위를 부여하여야 한다.

⑤ 재해복구 담당자는 시스템 담당자와 협의하여 재해발생 시 복구를 위한 비상운영 절차 및 복구절차를 수립하고 이에 대해 임직원에게 교육을 실시하여야 한다.

CISO
Chief
Information
Security
Officer

정보보호 최고책임자

길라잡이

기본편

Ⅳ

직원들에 대한 인식 제고

1. 프롤로그
2. 정보보호 인식… 왜 중요한가?
3. 정보보호 인식 제고 방안;
   기본 개념과 단계의 이해
4. 정보보호 인식 제고 방안;
   단계적이고 구체적인 방안들
5. 정보보호 교육 방안;
   직원의 생각을 바꾸게 하는 기법들
6. 보안문화 정착 방안;
   지속적으로 관리 가능한 정량화 기법
7. 에필로그

1. 프롤로그

(1) '보안의 기술화'를 넘어서는 시대; '보안의 법률화' 시대

기업의 정보보안 영역을 논할 때는 일반적으로 관리적 보안과 기술적 보안 그리고 물리적 보안 등으로 구분하고 있다. 여기서 말하는 관리적 보안이란 기업 내에서 처리되는 업무 프로세스를 중심으로 적용되어야 하는 보안절차와 확인사항을 문서로 수립하여 적용하는 보안이라고 할 수 있다. 그리고 기술적 보안이란 기업의 업무 처리를 위해서 도입/활용하고 있는 많은 기술적 도구와 장비를 보호하기 위해서 적용하는 기술적 수단이라고 할 수 있다. 반면 물리적 보안이란 인가받은 사람만 기업과 기업의 시설물에 출입하도록 하고 기업과 기업의 시설물을 보호하기 위하여 적용하는 보안이라고 할 수 있겠다.

이러한 구분방식의 관점에서 보면, 기존에는 기업 정보보안의 중심축이 관리적 보안보다는 기술적 보안에 있었다고 할 수 있다. 왜냐하면, 고객정보를 포함하여 기업의 정보를 훔쳐가는 대부분의 방법이 기술적 수단을 활용했기 때문이다. 이는 결과적으로 기업의 정보보안 영역에 있어서 기술적 보안이 강화되는 계기가 되기도 했다.

한편, 2011년 개인정보 보호법이 제정된 이후부터는 기업의 고객정보 보호와 관련된 여러 법률과 절차들이 기업의 관리적 보안 영역으로 들어오게 되었다. 특히 '개인정보 보호법'과 '정보통신망 이용촉진 및 정보보호에 관한 법률(이하 '정보통신망법')' 그리고 이러한 법률에서 파생된 여러 가지 지침과 가이드라인은 현 시대의 기업 정보보안에 있어서 반드시 준수해야 하는 필수적 법률과 지침이 되고 있다. 왜냐하면, 현재 많은 기업에서 정보보안부서의 직원 채용공고 시 담당업무에 '보안 컴플라이언스' 등과 같은 용어를 사용하고 있기 때문이다. 이와 같은 일련의 과정을 지나오면서 기업의 보안이 '보안의 기술화' 시대를 넘어서서 이제는 '보안의 법률화' 시대로 진화되었다고 할 수 있다. 이로 인해 정보보안과 관련된 법률로부터 자유로울 수 있는 개인, 기업, 단체, 공공기관은 없다고 해도 과언이 아닌 시대가 도래 했다고 할 수 있다.

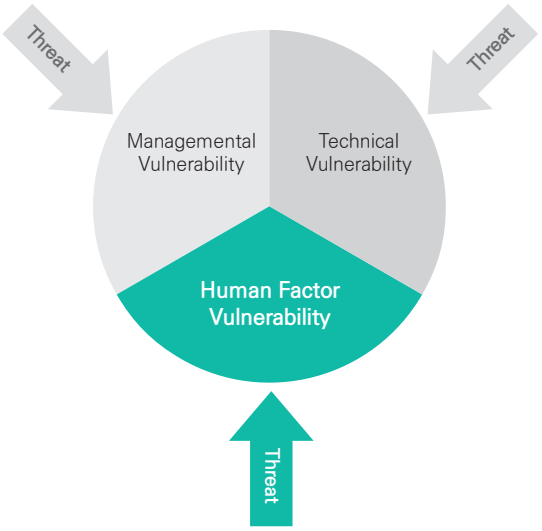
(2) 최근 집중되고 있는 보안위협의 접촉면; Human Factor

정보보안에 있어서 완벽한 보안은 있을 수가 없다. 왜냐하면, 공격자는 늘 새로운 공격기법을 개발하고 가장 취약한 부분으로 파고들기 때문이다. 다시 말해서, 오늘의 공격을 방어했다고 해서 내일의 공격까지도 방어할 수 있는 것이 아니라는 것이다. 이를 증명이라도 해 주듯이, 최근의 보안

위협은 관리적 보안과 기술적 보안을 단 한 번에 우회하는 영역에서 지속적으로 발생하고 있다. 그 대표적인 예가 바로 랜섬웨어(Ransomware)이다.

정보보안의 관점에서 볼 때 랜섬웨어의 가장 큰 특징은 기존의 '관리적 보안'과 '기술적 보안'을 가장 쉽고 가장 빠르게 우회할 수 있는 공격이라는 점이다. 이것이 가능한 이유는 이미 관리적 보안영역과 기술적 보안영역 내부에 있는 직원 즉, '사람'을 대상으로, 더 정확하게는 '사람의 생각'을 교두보로 활용하는 공격이기 때문이다. 이와 같은 랜섬웨어의 특징에 비추어 볼 때, 기존의 보안영역에서 기술적 보안영역이나 관리적 보안영역으로 포섭할 수 없었던 '사람의 생각 영역'을 경유 하는 보안 위협이 증가하고 있다고 할 수 있다. 따라서 현시대에서 기업의 정보보안을 담당하고 있는 정보보안전문가의 입장에서 본다면, 기존의 정보보안 영역에 이른바 'Human Factor'라고 하는 '사람의 생각 영역'에 대한 보안의 강화를 간과할 수 없게 되었다고 할 수 있다.

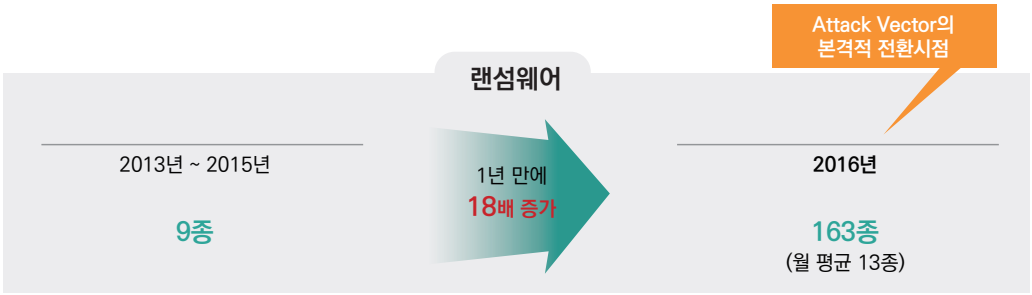
그림 4-1 최근 집중되고 있는 보안 위협의 접촉면



(3) Human Factor 취약점을 노리는 공격의 실제예시: 랜섬웨어

2017년 안철수연구소의 보안 이슈 자료와 보안세미나 발표자료에 의하면, 2013년부터 2015년 동안 나타났던 랜섬웨어가 9종이었는데 2016년에는 163종으로 증가하였다. 이는 무려 18배나 증가한 것인데, 여기서 알 수 있는 중요한 사실은 공격자의 공격벡터(Attack Vector)가 변화되었다는 사실이다. 기존에는 기술적 보안 통제를 침투하는 방식으로 공격이 이루어졌음에 반해 최근에는 기술적 보안 통제 영역 내에 있는 직원(즉, 사람)의 생각을 경유 하여 공격을 하는 방식으로 변화되었다는 것이다.

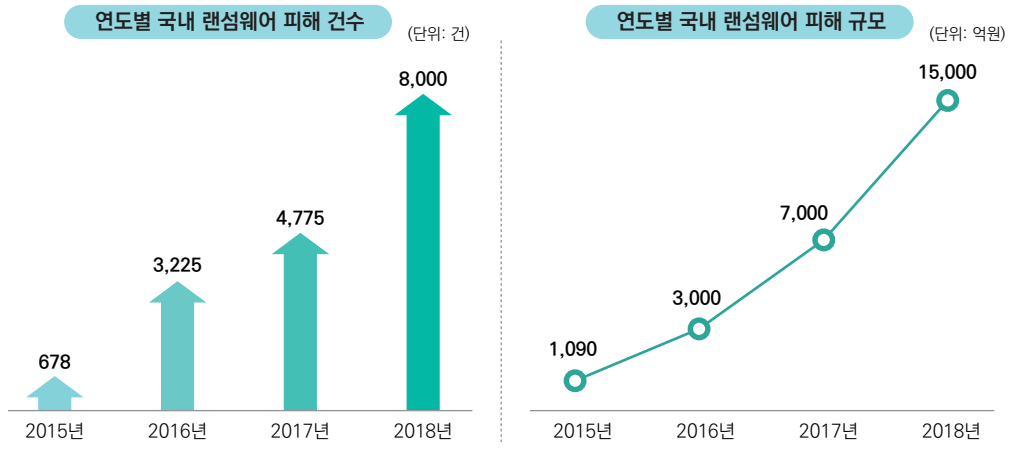
그림 4-2 공격벡터(Attack Vector)의 전환



이와 같이 사람의 생각을 경유하는 공격벡터의 변화는 공격자의 입장에서는 매우 비용 효과적인 상황인 반면에 기업 정보보안 입장에서는 매우 위협적인 상황이라고 할 수 있다. 왜냐하면, 공격자는 기술적 보안 통제를 극복하는데 필요한 시간과 노력을 들이지 않게 될 뿐만 아니라 기술적 보안 통제 영역 내에 있는 직원의 생각을 경유하여 기업이 보유하고 있는 정보나 가치를 확보할 수 있기 때문이다. 이러한 상황은 고스란히 기업 정보보안의 부담으로 작용하게 되므로 큰 위협이 될 수밖에 없다.

불행히도 이러한 위협은 2015년 이후부터 점점 더 증가하고 있다. 한국랜섬웨어침해대응센터의 자료에 의하면, 2015년 대비 2018년의 국내 랜섬웨어 피해 건수가 약 12배 증가하였으며 이와 비례하여 랜섬웨어 피해 규모도 약 13배가 증가하였음을 알 수 있다.

그림 4-3 국내 랜섬웨어 피해건수와 피해규모



출처: 한국랜섬웨어침해대응센터

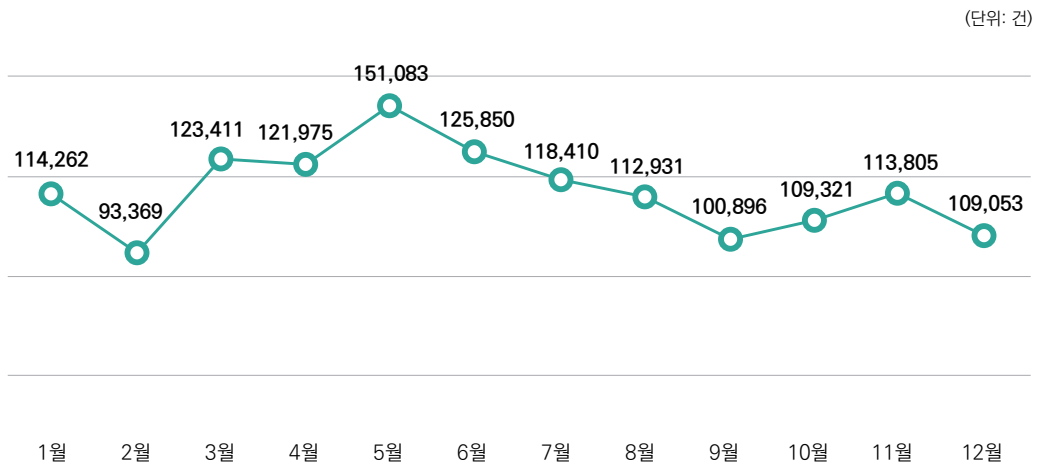
이러한 랜섬웨어는 대부분 '웹 사이트'를 경유하는 경로로 감염되지만, '회사 이메일'이나 'P2P 사이트'를 경유하는 경로로 감염이 되기도 한다. 정보보안의 관점에서 보면, '웹 사이트'나 'P2P 사이트'의 경우에는 기업 내 정보자산을 활용하여 해당 사이트에 대한 접속을 기술적으로 차단하는 것이 가능하다. 그렇지만, '회사 이메일'의 경우에는 기업 내부 또는 기업 내·외부 간 지속적인 이메일 전송이 필요하다는 점을 고려해 볼 때, 랜섬웨어 감염을 예방하기 위하여 회사 이메일 접속을 기술적으로 차단하는 것은 적합하지 않은 보안조치라고 할 수 있다.

그런데 공격자는 이와 같은 상황을 매우 잘 알고 있다고 생각된다. 왜냐하면, 최근 들어 회사 이메일을 경유하는 랜섬웨어 공격이 진화하고 있기 때문이다. 랜섬웨어 악성코드가 포함된 이메일 예를 들면, '남북간 긴장상황을 활용'한 이메일, '이미지 저작권 침해' 이메일, '교통범칙금 고지서'나 '택배 안내' 이메일, '고객 VoC' 이메일, '피고 소환장' 이메일 등이 그러하다. 특히 랜섬웨어 악성코드가 포함된 이메일을 기업의 인사부서 직원들을 수신자로 하여 '입사지원서'라는 제목으로 이메일 발송하는 공격방식을 보면, 공격자는 이미 공격목표 기업에 대한 정보를 알고 있다고 볼 수 있다. 게다가 최근에는 직장인들의 연말정산 시즌에 맞추어 '연말정산 관련' 이메일에 랜섬웨어 악성코드를 심어서 발송하고 있다.

(4) 악몽 같은 시나리오: 만약 랜섬웨어에 감염된다면?

보안뉴스를 통해서 기사로 낸 이스트 시큐리티(EST SECURITY)의 자료에 의하면, 이스트 시큐리티는 2018년 한 해 동안 약 140만 건의 랜섬웨어 공격을 차단하였는데 이는 매월 평균 약 10만 건 이상의 랜섬웨어 공격을 차단한 것으로 볼 수 있다.

그림 4-4 2018년 랜섬웨어 월별 차단통계



출처: 이스트 시큐리티

그런데 만약에 매월 10만여 건 이상 발생하고 있는 랜섬웨어 공격 중에서 단 한 건을 막아내지 못한다면 기업에서는 어떤 일이 벌어지게 될까? 특히 기술적인 접속차단이 부적합한 이메일을 경유하는 랜섬웨어가 수신되었고 정보보안에 대한 인식 수준이 낮은 직원 중에 누군가가 이러한 이메일에 있는 첨부파일이나 경유링크를 클릭하게 된다면 어떻게 될까?

일단은 랜섬웨어가 포함된 이메일의 첨부파일이나 경유링크를 클릭한 업무용 PC가 랜섬웨어에 감염될 것은 자명한 사실이다. 그러나 최근의 랜섬웨어는 단순히 업무용 PC 1대를 목표로 하고 있지 않기 때문에, 기업 내에서 운용하고 있는 서버나 데이터베이스 그리고 모든 업무용 PC뿐만 아니라 공유 파일도 감염시킬 수 있으며, 나아가서는 정보보안 부서의 승인하에 업무 목적으로 사용하고 있는 외장형 저장장치까지도 감염시킬 수 있다고 예상해야 한다.

랜섬웨어에 감염되면 감염 그 자체로 상황이 끝나는 것이 아니라 그 반대로 감염 그 자체로 새로운 국면이 시작된다. 즉, 랜섬웨어에 감염된 장비나 파일의 암호를 확보하기 위해서는 공격자에게 일정액의 비용을 지불 해야만 한다. 일반적으로는 업무용 PC 1대 당 약 300만 원 정도의 비용이 든다고 보고 있다. 하지만, 기업이 입게 될 전체 피해를 고려해 볼 때, 이렇게 지불 되는 비용은 빙산의 일각에 불과하다. 왜냐하면, 비용의 지불 이외에도 그보다 더 큰 피해가 빙산의 몸통을 구성하고 있기 때문이다. 이러한 내용을 기반으로 하여 발생할 수 있는 시나리오를 예상해 보면 다음과 같다.

악몽 같은 시나리오

◆ 상황

최근에 꽤 유망한 웹/앱 기반 서비스를 제공하고 있는 어느 스타트업 회사가 랜섬웨어에 감염되는 사고가 발생하였다. 이 스타트업 회사는 연 매출 약 1,000억 원의 성과를 내는 회사로서, 업무용 PC 263대를 운영하고 있고 이 회사의 서비스를 이용하고 있는 월 평균 이용자는 약 100만 명에 달하고 있다. 이 회사에서는 안전한 서비스 유지와 고객의 개인정보 보호를 위해서 필요한 기술적 보안조치를 적용하고 있었다. 랜섬웨어 감염사고의 원인을 조사를 해 본 결과, 다른 회사에서 이 스타트업 회사로 최근에 이직을 해 온 경력직 직원이 회사 이메일 내에 있는 첨부파일을 클릭/실행하였고 이 경력직 직원의 업무용 PC를 경유하여 전사 업무용 PC가 랜섬웨어에 감염되는 사고로 확인되었다.

그림 4-5 랜섬웨어에 대한 손실비용(예시)

컴퓨터의 몸값비용 : 789,000,000원 = 약 300만원 × 263대 컴퓨터

+

이 외 고려해야 하는 손실비용

- **PC 미사용으로 인한 손실** (기존의 일, 주, 월 매출액)
- **브랜드가치 훼손** (최소 연 매출액의 약 1%)
- **시장점유율 상실** (최소 연 매출액의 약 1%)
- **이용자 이탈** (최소 월 평균 이용자의 약 10%)
- **인프라 피해 복구 및 보완책 도입 비용** (PC 재 구매, 정보 재 수집, 업무 프로세스 재 구축 등)
- **고객 보상 비용 및 법무 비용**

◆ **빙산의 일각**

일반적으로 랜섬웨어에 대한 몸값(Ransom)은 업무용 PC 1대당 300만 원 정도로 보고 있으므로, 이 회사가 공격자에게 지불 해야 하는 비용은 300만 원 X 업무용 PC 263대 = 7억 8천 9백만 원이 된다. 이 회사가 연 매출이 약 1,000억 원에 이르는 회사인 점에 비추어 볼 때, 랜섬웨어에 대한 몸값이 7억 8천 9백만 원이라는 것은 크지 않은 비용이라고 생각할 수도 있다. 그렇지만 여기서 중요한 것인 이 몸값은 그저 시작에 불과하며 전체 피해를 구성하는 한 부분 즉, 빙산의 일각일 뿐이라는 사실이다.

◆ **빙산의 몸통**

- 업무용 PC 미사용으로 인한 손실

  업무 처리와 고객 서비스에 필요한 업무용 PC 263대와 여기에 저장되어 있는 정보를 전혀 사용하지 못하게 되는 손실비용이 발생하게 된다. 그리고 이러한 손실비용은 시간의 흐름(예: 일, 주, 월, 분기, 반기 등)에 비례하여 증가하게 된다.

- 서비스 브랜드가치 훼손

  이 회사가 창조하고 쌓아 온 서비스의 브랜드가치가 훼손된다. 브랜드가치의 훼손 비용을 연 매출액의 1%만 계산해도 10억 원에 이르는 손실이 된다.

- 시장 점유율 상실

  회사의 존재가치는 이윤 창출이며 이러한 이윤 창출을 위해서는 시장 점유율이 매우 중요할 수 밖에 없다. 그런데 웹/앱 기반의 서비스를 제공하고 있는 회사가 랜섬웨어에 감염된다면 당연히 기존의 시장 점유율을 일정부분 상실할 수 밖에 없다. 시장 점유율 상실 비율을 연 매출액의 1%만 계산해도 10억 원에 이르는 손실이 된다.

Human Factor 취약점을 경유하여 사람의 생각을 흔드는 공격… 당신의 방어수단은 무엇입니까?

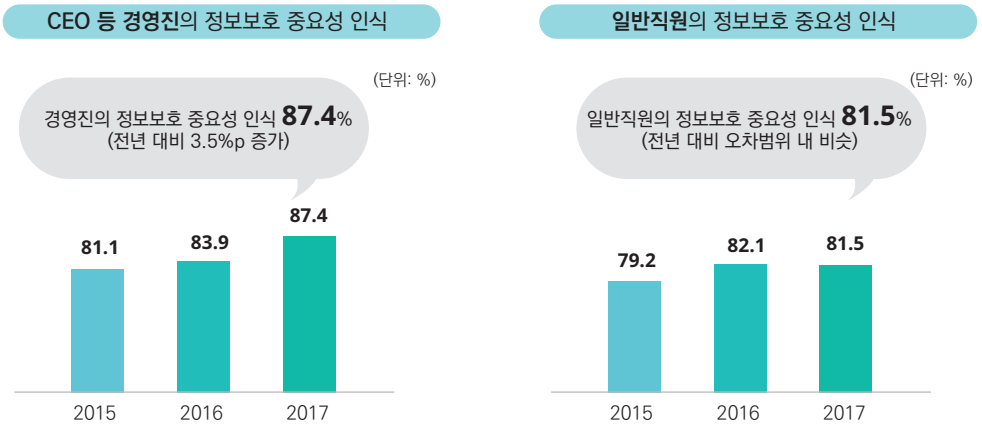
랜섬웨어처럼 Human Factor의 취약점을 경유하여 사람의 생각을 흔드는 공격에 대비하는 방어수단을 구축할 때 가장 우선적으로 검토해야 하는 것은 무엇일까? 그것은 당연히 공격의 경유지인 기업을 구성하고 있는 구성원의 생각 즉, '사람의 생각'이다. 특히 정보보안 관련 법률로부터 자유로울 수 있는 직장인이 없을 정도인 현재 상황에서, 기업의 구성원들이 정보보안의 중요성을 어느 정도로 인식하고 있는가를 검토하는 것은 Human Factor 취약점을 보완하는 데에 매우 중요한 판단기준으로 활용할 수 있다.

2. 정보보호 인식… 왜 중요한가?

(1) 구성원들의 정보보호 인식 현황

과학기술정보통신부에서 기획하고 한국인터넷진흥원에서 수행한 「2017 정보보호 실태조사」에 의하면, 2015년부터 2017년의 기간 동안 'CEO 등 경영진의 정보보호 중요성 인식'은 평균적으로 87.4%로 나타났으며 '일반 직원의 정보보호 중요성 인식'은 81.5%로 나타났다.

그림 4-6 기업 구성원의 정보보호 중요성 인식 수준



출처: 2017 정보보호 실태조사

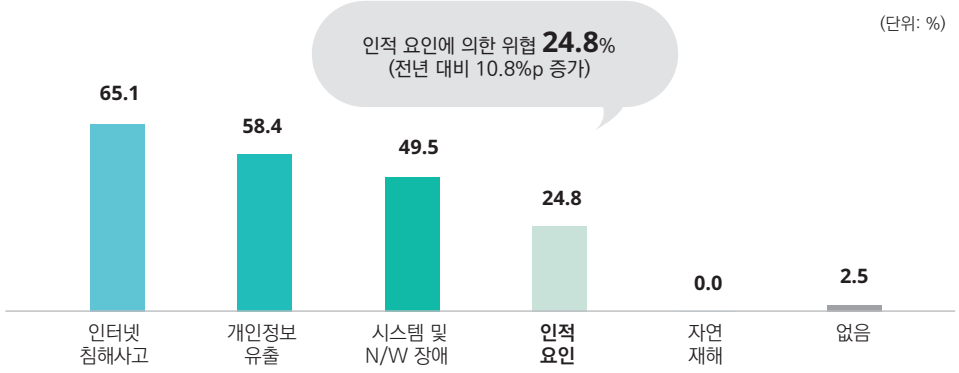
(2) 사람이 정보보호의 위협요인이 되는 현실

1) 나타난 숫자

기업의 구성원 즉, 사람이 정보보호의 위협요인이 될 수 있는 비율은 얼마나 될까? 관리적·기술적으로 수립하여 적용하고 있는 정보보안 체계를 위협하는 요인은 생각보다 상당히 많겠지만, 각 요인을 가장 큰 카테고리로 분류하고 이에 대한 각각의 비율을 명시적으로 확인할 필요가 있다. 한국인터넷진흥원은 앞서 살펴본 「2017 정보보호 실태조사」가 발표된 이듬해에 「2018 정보보호 실태조사」를 발표하였는데 이 조사 결과에 의하면, 정보보호의 위협요인을 ⅰ)인터넷 침해사고 ⅱ)개인정보 유출 ⅲ)시스템 및 N/W 장애 ⅳ)인적 요인 ⅴ)자연재해 등의 카테고리로 분류하였다.

각 카테고리별 위협요인의 비율을 보면, ⅰ)인터넷 침해사고: 65.1% ⅱ)개인정보 유출: 58.4% ⅲ)시스템 및 N/W 장애: 49.5% ⅳ)인적 요인: 24.8% 등으로 나타났다. 이러한 위협요인 중에서 인적 요인이 정보보호에 위협요인이 된다는 비율을 살펴보면, 2017년에 14%였으나 2018년에는 24.8%를 차지하고 있음을 알 수 있다. 이는 전년(14%)과 비교해 볼 때 무려 10.8%가 증가한 비율인데, 이는 기업 구성원들 사이에서 '사람으로 인해 정보보호 체계가 위협받을 수 있다는 경험적 또는 예측적 인식'이 커지고 있다고 해석할 수 있다.

그림 4-7 정보보호 위협요인 분석



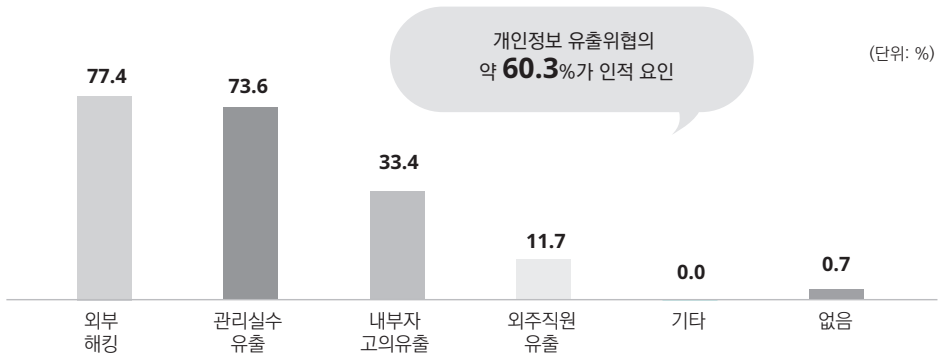
출처: 2018 정보보호 실태조사

2) 숨겨진 숫자

〈그림 4-7〉에서 볼 수 있는 것처럼, 정보보호의 위협요인 중 인적 요인의 수치가 24.8%로 나타난 것은 결코 작은 비율이 아니다. 그런데 사실 〈그림 4-7〉에는 숫자로 나타나지 않은 또 다른 인적 요인이 숨겨져 있다. 그것은 바로 '개인정보 유출(58.4%)' 카테고리에 숨겨져 있다. '개인정보 유출요인'을 살펴보면, ⅰ)외부 해킹 ⅱ)관리실수 유출 ⅲ)내부자 고의 유출 ⅳ)외주 직원 유출 등이 그 세부 요인으로 작용하고 있는데, 여기서 '외부 해킹'을 제외한 '관리실수 유출'과 '내부자 고의 유출' 그리고 '외주 직원 유출'도 인적 요인에 의한 것임을 알 수가 있다.

'개인정보 유출요인'에 숨겨져 있는 정보보호 위협요인 중 인적 요인의 비율 또한 상당히 큰 비중을 차지하고 있다. '관리실수 유출'이 73.6%, '내부자 고의 유출'이 33.4%, '외주 직원 유출'이 11.7%의 비율을 차지하고 있다.

그림 4-8 개인정보 유출요인에 숨겨져 있는 인적 요인



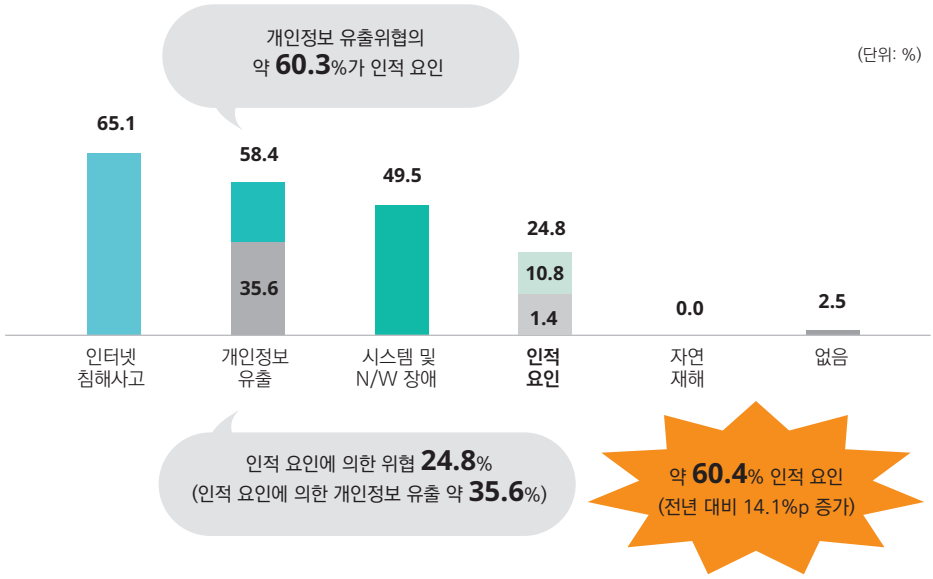
출처: 2018 정보보호 실태조사

이처럼 전체 '개인정보 유출요인' 내부에 숨겨져 있는 정보보호 위협요인 중 인적 요인의 비율은 무려 60.3%에 달하게 된다. 다시 말하자면, 정보보호 위협요인 중 58.4%을 차지하고 있는 '개인정보 유출'의 60.3%에 해당하는 35.6%도 정보보호 위협요인 중 인적 요인이라고 해석을 할 수 있다.

3) 행간의 의미를 더한 숫자

결과적으로 볼 때, 정보보호 위협요인 중 기존의 인적 요인(24.8%)에 포함되지 않은 또 다른 인적 요인(35.6%)이 '개인정보 유출요인' 내에 숨어 있었다고 볼 수 있다. 따라서 정보보호 위협요인 중 인적 요인의 비율을 판단하는 경우에는 기존의 인적 요인(24.8%)과 '개인정보 유출요인'에 숨어 있는 인적 요인(35.6%)을 더하여 판단하여야 한다.

그림 4-9 행간의 숫자를 더한 정보보호 위협요인 중 인적 요인의 비율



출처: 2018 정보보호 실태조사

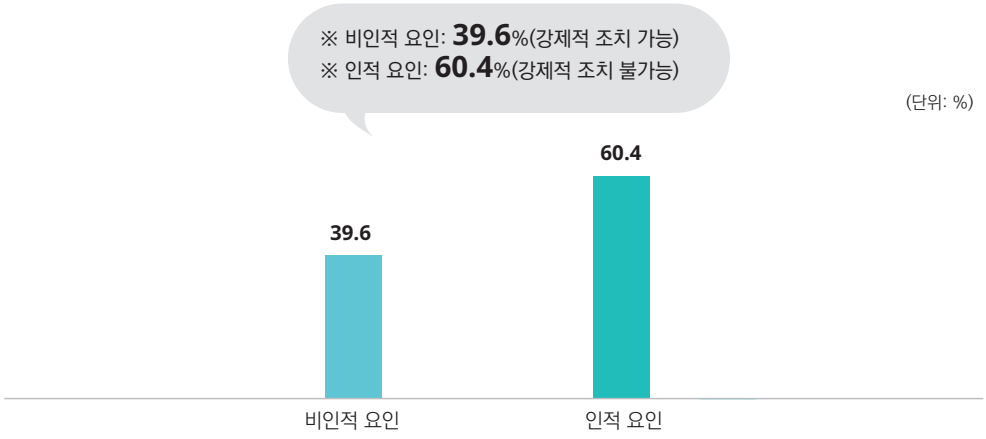
이에 비추어 볼 때, 정보보호 위협요인 중 '사람으로 인해 정보보호 체계가 위협받을 수 있다는 경험적 또는 예측적 인식'의 비율인 인적 요인의 비율은 무려 60.4%로써, 이는 전년 대비 14.1%나 증가한 비율이라고 할 수 있다.

(3) 정보보호 인식이 중요한 이유

1) 정보보호 위협요인의 절반 이상; '사람'

한국인터넷진흥원이 조사한 「2018 정보보호 실태조사」결과에 행간의 의미를 더하여 정보보호 위협요인을 '인적 요인'과 '비인적 요인'으로 구분한다면, 인적 요인이 60.4%이므로 비인적 요인은 39.6%에 해당하게 된다. 이와 같은 비율에 근거하여 보면, 정보보호 위협요인의 절반 이상이 사람이라고 할 수 있다.

그림 4-10 비인적 요인과 인적 요인의 비율



출처: 2018 정보보호 실태조사

〈그림 4-10〉에서 간과해서는 안 되는 두 가지 특징이 있는데 ⅰ)비인적 요인보다 인적 요인의 비율이 훨씬 더 높다는 점 ⅱ)비인적 요인은 기술적 보안 통제를 통해 강제적인 조치가 가능한 반면, 인적 요인의 경우에는 강제조치가 불가능하다는 점이다. 이러한 특징을 고려하여 입·퇴사시 작성하는 보안서약서(이른바 'NDA')를 활용할 수는 있겠지만, 그렇다고 하더라도 사람의 생각 영역을 경유하는 공격의 양상을 고려해 볼 때 보안서약서로는 사람의 생각영역을 효과적으로 통제하는 방안이 될 수는 없을 것이다.

2) 가장 약한 연결 고리; '사람의 생각 영역'

정보보호 인식 제고를 고려함에 있어서 '사람의 생각은 언제든지 바뀔 수가 있다'는 대전제는 상당한 부담으로 작용하게 된다. 왜냐하면, 현시점에서 정보보호 인식 제고의 수준이 높은 부서나 직원이라고 하더라도 향후 부서/업무의 변경이나 업무적 이슈에 따라서는 정보보호 인식 수준이 언제든지 달라질 수 있기 때문이다. 결국, 기업의 정보보안 체계에 있어서 직원 즉, '사람 특히 사람의 생각 영역'은 가장 약한 연결고리가 될 수밖에 없다.

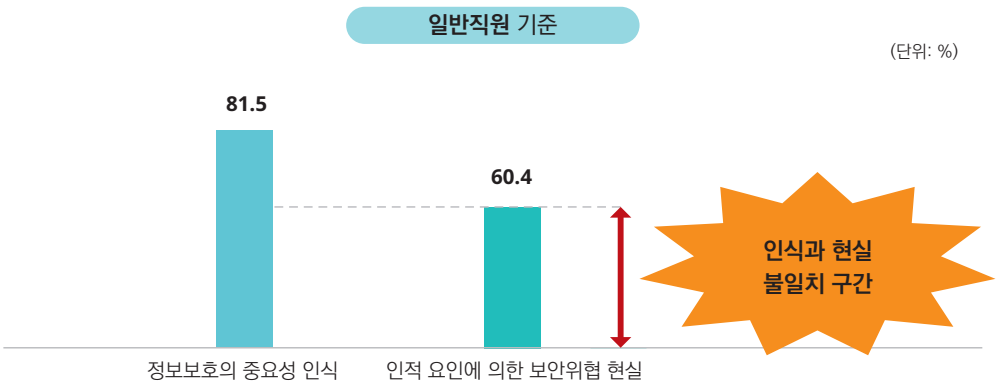
(4) 아이러니한 현상의 순환 고리

보안의 법률화 시대에서 기업활동을 하는 과정에서는 법률이 정하고 있는 정보보호 체계를 수립하고 적용하여야 한다. 그래서 법률에 기반을 두고 있는 관리적 보안체계와 기술적 보호조치는 필수적이고도 최소한의 정보보안 체계라고 할 수 있다. 따라서 법률기반의 정보보안 체계에서는 '법률의 준수'가 곧 '정보보안 체계의 유지'로 이어져야 하며 이는 당연한 논리적 구조하고 할 수 있다. 그런데 이와 같은 당연한 논리적 구조를 한순간에 무너뜨리는 현상이 나타나고 있다. 특히 기업의 구성원 즉, '사람의 생각 영역'에서 이러한 현상이 두드러지게 나타나고 있는데 이에 대해 살펴보면 다음과 같다.

1) 인식과 현실의 불일치

앞서 본 〈그림 4-6〉에서 알 수 있듯이 81.5%의 일반 직원들이 정보보호가 중요하다고 생각하고 있다. 그리고 이러한 정보보호에 대한 중요성 인식 비율은 매년 증가하고 있는 추세이기도 하다. 그런데 〈그림 4-10〉에서 보았듯이 정보보호의 위협요인 중 무려 60.4%가 인적 요인 즉 사람에 의해서 정보보안 체계가 흔들릴 수 있다고 나타났다. 이러한 모순적인 상황은 '인식과 현실의 불일치'라고 말할 수 있다. 즉, 정보보호가 중요하다고 생각하고 있음에도 불구하고 업무 현실에서는 잘 지켜지지 않는다고 해석할 수 있는 것이다.

그림 4-11 인식과 현실의 차이



2) 기술보안 우회

관리적 통제와 기술적 보호조치가 적용된 정보보안 체계가 운용되고 있는 기업에서 직원들이 업무를 수행하는 방식은 크게 보면 두 가지 방식이 있을 수 있다. 즉, ①정보보안 체계를 준수함으로 인해 안전하지만, 직원이 업무를 수행하는 데 다소간 불편한 방식과 ②정보보안 체계를 준수하지 않음으로 인해 위험하지만, 직원이 업무를 수행하는데 편리한 방식이 그러하다. 사람의 생각 영역에서는 이 두 가지 방식을 두고 어떤 방식을 선택할 것인지에 대해 고민하게 되는데, 불행하게도 '위험하지만 편리한 방식'을 선택하려는 경향이 큰 것으로 보인다. 다시 말해 사람의 생각 영역에서는 '안전하지만 불편한 방식' 보다는 '위험하지만 편리한 방식'을 선택할 가능성이 더욱 높다고 할 수 있다. 대부분의 기업에서는 외부 침입 또는 내부 유출 등에 대비하기 위하여 기술적 보호조치를 운용하고 있는데, 기업의 구성원 중에서 이러한 기술적 보호조치를 우회하려는 시도 내지는 실제로 우회하는 경우가 바로 '위험하지만 편리한 방식'을 선택한 결과로 나타나는 행동이라고 할 수 있다.

3) 관리보안에 대한 저항

정보보안 체계를 운용하고 있는 기업에서는 기본적으로 '정보보안 정책'이라는 관리적 보안 통제를 전사 직원을 대상으로 적용하고 있다. 그래서 전사 직원들은 업무를 수행하는 과정에서 정보보안 정책에 따른 여러 가지 절차를 준수하고 필요한 경우에는 정보보안 부서의 승인과 검토를 거쳐야 하는 경우도 있다. 이러한 일련의 과정을 거치면서 기업 내에 관리적 보안 통제가 기능을 하게 되는 것이다.

그런데 이러한 관리적 보안 통제에 대해서 잘못된 관점을 가지고 불평을 하는 구성원이 언제나 있기 마련이다. 특히 이러한 구성원들은 자신이 준수해야 하는 관리적 보안 통제 절차에 대해서 부정적인 관점을 가지고 있다. 예를 들어 특정한 시스템 개발이나 업무 기획에 대해 정보보안 부서가 보안성 검토를 해 본 결과 개발 환경이나 업무 프로세스를 변경해야 한다고 하면, '정보보안 때문에 일이 안된다' 혹은 '일을 하라는 거냐? 말라는 거냐?', '개발이나 업무의 진행이 안 되면 정보보안부서가 책임질 거냐?'라며 자신의 주변에 정보보안에 대한 불평과 불만을 늘어놓기 시작한다. 즉, 자신의 업무 관점에서만 생각하고 판단하다 보니 정보보안 특히 관리적 보안 통제를 자신의 업무를 수행하는 데 방해가 되는 걸림돌로 인식을 하게 되고 결과적으로 관리적 보안 통제에 저항을 하는 것이다.

이처럼 관리적 보안 통제에 대해서 부정적인 인식을 가지고 저항을 하는 구성원들이 모르거나 인정하지 않는 두 가지 사실이 있다. 첫 번째는 보안이 법률화되었다는 사실이다. 즉, 기업마다 해도 되고 안 해도 되는 것이 아니라 필요 최소한의 범위 내에서는 반드시 준수해야 하는 것이 관리적·기술적 보안 통제인 것이다. 두 번째는 정보보안 부서도 고유의 업무를 수행하고 있다는 사실이다. 즉, 개발 기획이나 업무 기획 단계에서 정보보안 관점의 보안성 검토를 하고 정보보안과 관련된 제반 업무를 수행하는 것이 다른 부서의 업무를 방해하기 위함이 아니라 정보보안 부서 고유의 업무를 수행하기 위함이라는 사실이다.

주지하다시피 2018년 1월부터 서울특별시 시내버스를 탑승하는 경우에는 다른 승객의 안전을 위하여 뜨거운 음료를 들고 탑승하지 못하도록 하고 있으며, 이러한 경우에는 버스 운전자가 탑승을 거부할 수 있고, 버스 내에서 음식물을 먹는 승객에게 하차를 요구할 수도 있다. 이와 같은 안전 통제의 근거는 바로 서울특별시 조례이다. 이러한 서울특별시 조례를 근거로 하여 뜨거운 음료를 들고 버스에 탑승하고자 하는 승객에 대해 탑승을 거부하거나 버스 내에서 음식물을 먹는 승객에 대해 하차를 요구하는 경우에 버스 운전자에게 저항하는 승객은 거의 없다. 비슷한 예로, 도로교통법에서는 보행자와 운전자의 안전을 위해서 도로의 무단횡단을 금지하고 있다. 그리고 이러한 규정을 위반하여 무단횡단을 하는 보행자에게는 교통경찰관이 범칙금을 부과할 수도 있다. 이와 같은 상황에서 무단횡단을 한 보행자가 교통경찰관에게 저항하는 경우도 거의 없다.

그런데 아이러니하게도 법률화된 정보보안 체계에 의해 보안업무를 수행하는 정보보안 부서나 정보보안 담당자에게는 너무나 당연한 듯이 저항을 하는 경우가 자주 나타나고 있다. 모두에서 말한 바와 같이 현재는 '보안의 법률화 시대'이다. 즉, 기업에서 운용하고 있는 관리적 보안 통제와 기술적 보안 조치는 법률에 의해서 적용되고 있는 것이다. 그리고 이에 기반하여 정보보안 부서의 고유한 업무(예: 정책과 절차 수립, 보안성 검토, 보안 점검, 보안교육, 보안 정책 위반자 관리, 기술적 보안 조치 운용 등의 업무)가 기업 내에서 실행되는 것이다. 따라서 기업의 관리적 보안 통제와 기술적 보안 조치에 불만이 있는 구성원은 정보보안 부서를 대상으로 저항할 것이 아니라 법률 개정을 담당하고 있는 국회를 대상으로 저항해야 할 것이다. 왜냐하면, 보안이 법률화된 현재 상황에서 기업 내 보안수준을 완화하기 위해서는 법률을 개정해야만 가능한 경우가 상당히 많기 때문이다.

3. 정보보호 인식 제고 방안; 기본 개념과 단계의 이해

(1) 정보보호 인식 제고의 기본 개념; 생각의 스위치 자극

기업의 구성원들을 대상으로 '정보보호 인식의 수준을 높인다'는 말을 바꾸어 말하면, 정보보호에 대한 구성원들의 생각을 긍정적인 방향으로 바꾼다는 말이 된다. 이 말은 결국 사람의 생각을 바꾼다는 것인데, 사람의 생각을 제3자가 바꾼다는 것은 거의 불가능하다고 보아야 한다. 왜냐하면, 사람의 생각 영역은 지극히 주관적이고 개인적이며 경험적인 영역이기 때문이다. 그럼에도 불구하고 기업의 정보보안 체계를 유지하고 개선하기 위해서는 기업 구성원 즉, 사람의 생각을 긍정적인 방향으로 바꾸어야만 한다. 특히 최근에 나타나고 있는 보안 위협의 접촉면이 Human Factor로 집중되고 있고 실제로 이러한 접촉면을 통해서 공격과 피해가 나타나고 있는 점을 고려해 본다면, 정보보호에 대한 사람의 생각을 긍정적인 방향으로 바꾸어야만 하는 이유는 충분하다고 본다.

그렇다면 정보보호에 대한 기업 구성원들의 생각을 바꾸어야 한다는 사실을 대전제로 두고, 정보보호 인식 제고라는 목표를 달성하기 위해서는 어떻게 하면 구성원들의 생각을 바꿀 수가 있을까? 이 물음에 대해 필자의 경험에 의하면 '사람이 생각하는 스위치를 자극'하면 가능하다는 답을 줄 수가 있다. 즉, 구성원의 주관적이고 개인적인 생각을 직접 바꾸는 것이 아니라 구성원이 경험했거나 경험할 수 있는 특정한 이슈를 통해 정보보호에 대해 고민해보도록 만들고 이러한 고민에 따라 구성원 스스로를 위함과 동시에 기업이 추구하는 선택을 하도록 하는 것이다. 이와 같은 개념에 기반하여 정보보호 인식 제고를 시작한다면, 구성원들의 관점이 기존의 '당연한 편리함'에서 '편리한 안전함' 또는 '안전함'으로 바뀔 수 있을 것이라 생각한다.

(2) 정보보호 인식 제고의 단계

사람의 생각을 스위치를 자극하는 방법으로 정보보호 인식의 수준을 높이는 단계는 기본적으로 ⅰ)접점 식별 ⅱ)단계적 조치 ⅲ)유지/개선의 단계로 나눌 수 있다. 즉, 기업이 추구하는 정보보안 체계의 수준과 기업 구성원이 생각하는 업무적인 편리함의 접점을 먼저 찾은 후에, 이러한 접점을 기준선(Baseline)으로 하여 정보보호 인식을 단계적으로 높여 나가며 이를 유지/개선하는 단계라고 할 수 있다.

그림 4-12 정보보호 인식제고 기본단계

1) 인식과 현실의 접점 식별; 잘못된 식별과 잘된 식별

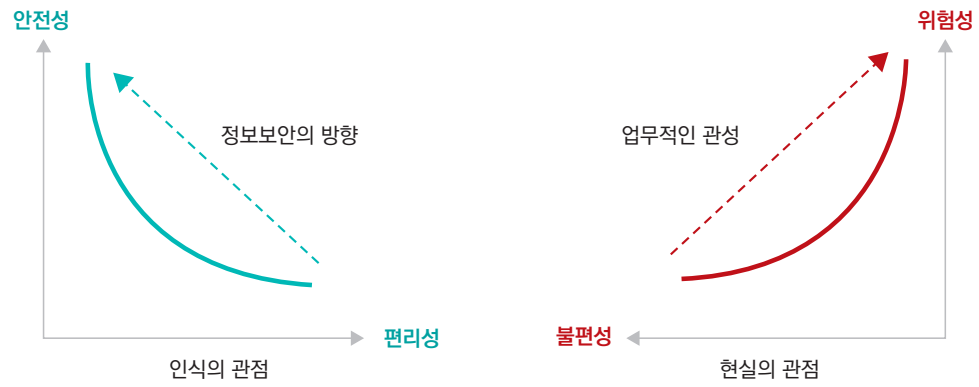
① 잘못된 식별

일반적으로 기업 구성원들의 정보보호 인식수준을 판단하는 경우에 구성원들이 생각하는 정보보호의 중요성 인식을 기반으로 판단하곤 한다. 이러한 방식처럼 판단한다면, 「2017 정보보호 실태조사」에서 일반직원들의 정보보호 중요성 인식 수준이 81.5%이므로 기업의 정보보호 인식 수준을 81.5%라고 보아야 한다. 그리고 정보보호의 관점에서는 '안전성'과 '편리성'이라는 속성을 반비례 관계로 두고 기업 내에서 정보보안 체계를 활용한 통제를 적용하고 있다. 그렇기 때문에 이 두 속성을 연결하는 선상 위에서 구성원들의 보안인식 수준을 판단하고 있다는 것이다(그림 4-13 참조).

그러나 이러한 관점은 정보보안 체계가 추구하는 방향에 대해 구성원이 어떻게 생각하고 있는가에 대한 결과값일 뿐이다. 따라서 이 결과값에는 구성원들이 업무를 현실적으로 수행하는 일반적인 방식 즉, 업무적인 관성이 포함되어 있지 않다.

반면에 기업의 구성원들이 업무를 현실적으로 수행하는 방식을 살펴보면, '안전하더라도 불편한 방식'보다는 '위험하더라도 편리한 방식'을 선호한다는 것을 알 수 있다. 그리고 이러한 업무 방식에 대한 경험이 누적되어 결국은 업무 처리 과정에서의 '편리함'을 추구하는 관성이 만들어졌다고 할 수 있다. 정보보호의 관점에서 말하는 '위험'에 대한 구체적인 지식과 경험이 없는 구성원의 집단에서는 업무 처리 과정에서의 '편리함'을 추구하는 관성이 어쩌면 너무나도 당연한 현상일지도 모르겠다. 그러하다 보니 정보보안 업무를 직접 수행하지 않는 구성원들의 관점에서는 '위험성'이라는 속성은 고려대상이 아니고 오직 '편리성'이라는 속성이 업무 처리 방식에 관한 생각과 행동을 결정하는 데 중요한 결정변수로 작용하고 있는 것이다(그림 4-13 참조).

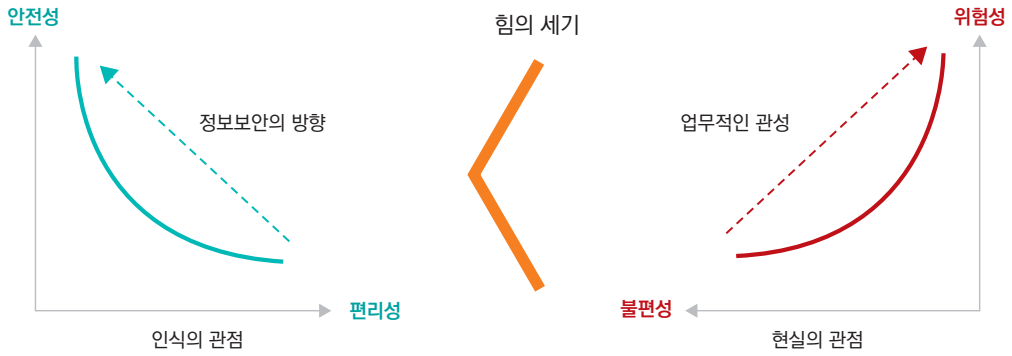
그림 4-13 (좌)정보보안 체계에 대한 중요성 인식의 방향 , (우)업무적인 관성에 의한 현실의 방향



그러나 정보보호 인식수준을 높여야 하는 정보보안 부서나 정보보호 최고책임자(CISO)의 입장에서는 기업 구성원들이 당연시하고 있는 '편리함을 추구하는 업무처리의 관성'을 그대로 놓아두어서는 안 된다. 왜냐하면, 구성원들이 업무를 수행하는 환경에서는 '정보보안의 방향이 추구하는 인식의 관점'보다 '편리하게 업무를 처리하고자 하는 현실적인 관점' 의 힘이 더 세기 때문이다. 그리고 힘의 세기가 이와 같은 구조를 갖추게 되는 이유는 구성원들의 생각영역에서 정보보호라는 '통제의 힘'보다 편리한 업무처리라는 '관성의 힘'이 더 우세하기 때문이다(그림 4-14 참조).

이러한 '관성의 힘'을 적시에 '통제'하지 못하게 되는 경우에는 업무 처리 과정에서 더이상 '정보보호의 중요성 인식'은 큰 고려대상이 되지 못하게 되고 '편리한 업무적 관성'만을 추구하는 엔트로피(Entropy) 상태가 될 수도 있다.

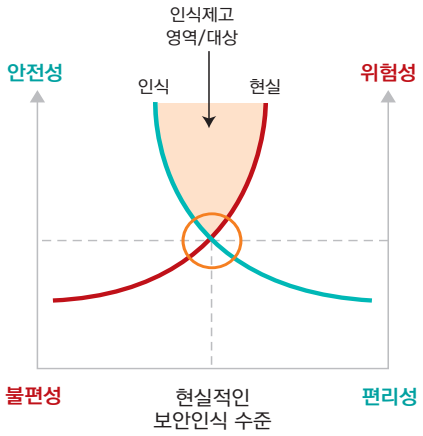
그림 4-14 인식의 방향과 현실의 방향 간 생각하는 힘의 세기



② 잘된 식별

정보보호 인식 제고를 위한 인식과 현실의 접점을 식별함에 있어서 가장 중요한 것은 판단의 객체를 대상으로 판단의 잣대를 적용해야 한다. 즉, 기업 구성원(객체)을 대상으로 하여 정보보안 통제(잣대)를 적용해야 한다는 것이다. 그래야만 통제를 통해 정보보안이 추구하는 방향에 대해 업무 현실에서 구성원들이 어느 정도로 수용하고 있는지를 알 수 있기 때문이다. 따라서 정보보호에 대한 인식과 업무 현실의 접점을 식별하기 위해서는 '편리함'을 추구하는 업무 처리의 관성을 현명하게 활용할 필요가 있다. 특히 제대로 된 접점을 식별하기 위해서는 우선 정보보안 체계에서 실행되는 각종 통제에 대해서 구성원이 저항을 하는 현실적인 이유를 분석한 후, 이러한 '현실적인 이유'와 '정보보안 체계가 추구하는 통제' 간의 교차지점(Crossing Point)과 차이(Gap)를 파악하는 것이 매우 중요하다. 왜냐하면, 이들 간의 교차지점(Crossing Point)이 현실적인 보안 인식 수준이 되고 이들 간의 차이(Gap)가 바로 인식 제고의 영역/대상이 되기 때문이다(그림 4-15 참조).

그림 4-15 인식과 현실의 접점 식별



2) 정보보호 인식 제고 기법의 단계적 적용; 지속적 상승 단계와 순간적 하향 상황

① 지속적 상승 단계

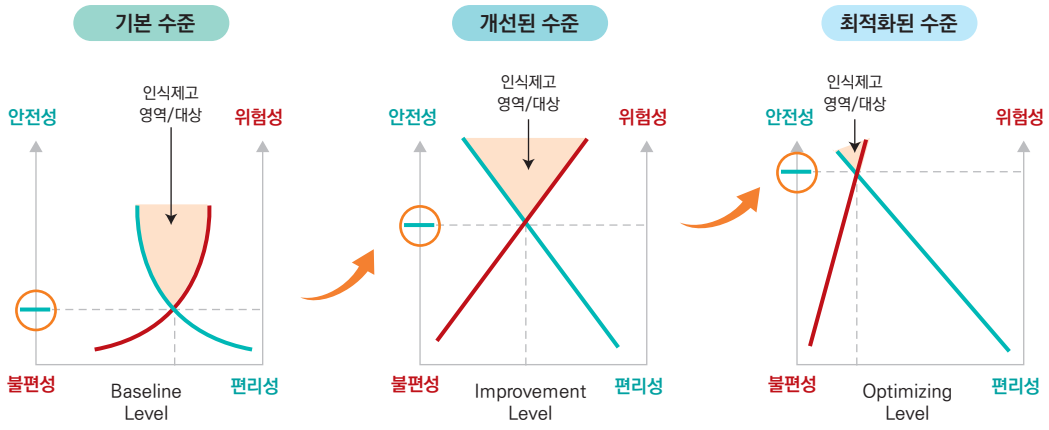
앞선 과정을 통해서 현실적인 보안 인식 수준인 인식과 현실의 접점이 식별되고 나면, 이 접점의 수준을 '기본 수준'을 삼고 정보보호 인식 수준 향상을 위한 다양한 기법을 지속적으로 적용해 나갈 수 있다. 먼저 '기본 수준' 단계에서는 정보보안 통제에 대해서 구성원들의 저항이 거의 없는 상태라고 할 수 있다. 왜냐하면, 이 단계는 정보보안 통제가 거의 힘을 발휘하지 못할 뿐만 아니라 구성원들의 업무환경에서 '편리함을 추구하는 업무적인 관성'이 더 우세한 단계이기 때문이다(그림 4-16의 '기본 수준' 참고).

'개선된 수준' 단계로 접어들면, 정보보안 통제에 대해서 구성원들의 저항이 시작/가중되는 현상이 나타난다. 왜냐하면, 이 단계로 접어들었다는 의미는 기존에 거의 힘을 발휘하지 못하고 있던 정보보안 통제가 힘을 발휘하면서 정보보안 체계의 수준이 향상되고 있다는 것을 의미하기 때문이다. 다시 말하자면, 강화되는 정보보안 체계가 구성원들에게 불편함을 초래하기 때문에 이에 대한 저항이 시작되는 것이고 시간이 흐름에 따라 이 저항은 점점 더 가중되는 단계로 나아가게 된다. 따라서 이 '개선된 수준' 단계에서부터는 본격적으로 정보보호 인식 제고를 위한 다양한 통제 활동을 수행하여야 한다(그림 4-16의 '개선된 수준' 참고).

'최적화된 수준'의 단계가 되면 기업 내 정보보안 체계에서 적용하는 통제가 상당한 힘을 발휘하게 된다. 그래서 이 단계에서는 업무 처리 과정에서 정보보안체계를 준수하는 것이 당연시되는 환경으로 변화된다. 따라서 구성원들에 대한 정보보호 인식 제고 활동이 일정부분 축소될 수 있다(그림 4-16의 '최적화된 수준' 참고).

정리하자면, 인식과 현실의 접점인 '기본 수준' 단계를 제대로 식별해 내고, 이를 토대로 하여 '개선된 수준' 단계로 정보보호 인식 제고의 수준을 향상 시킨 후 최종적으로 '최적화된 수준'의 단계로 나아가야 한다. 이러한 일련의 단계를 거치면서 결과적으로 기업 내 정보보안 체계의 수준이 강화될 뿐만 아니라 구성원의 생각 영역에 있는 정보보호 인식의 수준도 지속적으로 향상될 수 있다.

그림 4-16 정보보호 인식수준의 상승 단계



② **순간적 하향 상황**

기업을 구성하는 몇 가지 중요한 요소 중 가장 중요한 요소가 직원 즉, 사람이라고 해도 과언이 아니다. 왜냐하면, 사람을 기반으로 조직을 구성하고 업무를 진행하기 때문이다. 이러한 매커니즘은 고스란히 정보보안 체계에도 영향을 미치게 된다. 즉, 사람을 대상으로 정보보안 통제를 적용하게 되고 사람을 통해서 정보보안 정책이 준수되며, 사람에 의해서 정보보안 체계가 위협받게 된다는 것이다. 특히 정보보호 인식이 사람의 생각 영역에 있다 보니, 정보보호 인식

수준을 높이는 과정에서는 사람이 매우 중요한 연결고리가 될 수밖에 없다.

예를 들어서 정보보호 인식을 향상시키기 위해 긴 시간에 걸쳐서 지속적으로 노력해 온 어느 기업이나 부서 내에 새로운 직원이 들어오는 경우에는 이 새로운 직원에 의해서 기존의 구성원들이 가지고 있던 정보보호 인식 수준이 흔들리거나 하향곡선을 그리는 경우가 매우 많이 발생하고 있다. 이러한 현상이 발생하는 가장 중요한 원인은 사람의 '생각 영역에 대한 보안 통제의 한계'라고 할 수 있다. 다시 말해 다양한 보안 통제 기법을 통해 긴 시간 동안 정보보안 인식의 수준을 향상 시켰다고 하더라도, 이는 '통제'라는 강제적(?) 수단의 결과인 것이지 구성원 간의 자발적인 참여의 결과는 아니라는 것이다. 그렇기 때문에 긴 시간을 통해 지속적인 상승 단계를 거친 정보보호 인식 수준이 한순간에 하향하게 되는 것이다. 따라서 정보보호 인식 수준이 '최적화된 수준' 단계에 이르렀다고 하더라도, 이 수준을 유지/개선하고자 하는 특별한 노력이 없이는 이 단계에 계속 머물러 있을 수는 없게 된다는 점을 기억할 필요가 있다.

3) 정보보호 인식 제고 수준의 유지/개선; 문화화와 정량화

정보보호 인식제고의 수준이 '최적화된 수준'의 단계를 유지/개선하기 위해서는 기업 내에서 정보보안 체계가 문화화되어야 하고 이러한 문화가 지켜질 수 있도록 하는 정량화된 지표를 활용할 필요가 있다. 특히 기업 내의 정보보호 인식 수준을 지속적으로 유지/개선하기 위해서는 구성원의 환경(승진, 업무 변경, 부서이동 등)이나 구성원 자체의 변경(신규입사, 경력 입사 등)에 따라 흔들리지 않는 환경을 구축해야만 한다. 이를 위해서 구성원의 자발적 참여를 유도하는 문화를 구축함과 함께 구성원들의 자발적 참여 여부를 가시적으로 정량화할 수 있는 수단을 적용할 필요가 있다. 이에 대해서는 후술하는 '6. 보안문화 정착 방안; 지속적으로 관리 가능한 정량화 기법'에서 상술하기로 한다.

4. 정보보호 인식 제고 방안; 단계적이고 구체적인 방안들

앞서 살펴본 것처럼 정보보호의 인식 수준을 높여야만 대응이 가능한 위협이 증가하고 있는 현시점에서 직원들에 대한 정보보호 인식 제고는 기업에서 반드시 수행해야 하는 매우 중요한 정보보호 활동이라고 할 수 있다. 그러나 사람의 생각 영역에 해당하는 '정보보호에 대한 인식'의 수준을 높인다는 것은 쉬운 일이 아니다. 그렇다면 어떤 방법으로 정보보호의 인식 수준을 높일 수 있을까? 이 질문에 대한 대답을 이제부터 상세하게 설명해 보고자 한다. 물론 본지에서 필자가 제시하고 있는 방안들이 완벽하고 완전한 방안이라고는 할 수 없겠으나, 정보보안 분야 특히 정보보호 인식 제고 분야에서 오랜 기간 몸담아 왔던 필자의 경험과 노하우를 토대로 제시하는 방안이라고 보면 좋을 것 같다.

(1) 접점 식별; 조직문화 이해

1) 조직성향 파악

정보보호 인식 제고에 있어서 가장 첫 단계는 바로 '인식과 현실의 접점'을 식별하는 것이다. 이를 위해서는 먼저 조직의 성향을 파악하는 것이 중요하다. 여기서 말하는 조직은 '기업 전체'가 되어야 하겠지만, 이해의 편의를 위해 '부서 단위'의 조직으로 해 두자. 왜냐하면, 부서마다 업무를 처리하는 방식과 문화가 다르기 때문이다. 한편, 인식과 현실의 접점을 식별하기 위해 조직성향을 파악하는 단계에서는 우선 성향파악에 집중하고, 각 성향에 대한 보안 조치는 향후 과제로 남겨두고 단계적으로 적용해야 한다.

그리고 조직의 성향을 파악하는 방법으로 ⅰ) 속도 중심적인지 ⅱ) 속도에 비해 방향을 얼마나 고려하고 있는지 ⅲ) 잘못된 방향에 대한 교정 프로세스가 있는지에 대한 지표를 활용할 수 있다. 이와 같은 지표를 기반으로 조직의 성향을 파악하는 두 가지 이유가 있다. 첫 번째 이유는 기업 내 여러 조직의 성향을 한 가지 유형으로 평가할 수는 없기 때문에 정보보안 관점에서 반드시 고려해야 하는 세 가지 지표를 대입하여 조직의 성향을 세분화하기 위함이다. 두 번째 이유는 조직 내에 '보안성 검토 프로세스의 존재 여부'와 '보안성 검토 프로세스의 실제 준수 여부'를 알 수 있기 때문이다.

① 속도 Vs. 속도와 방향

인식과 현실의 접점을 식별해야 하는 대상 조직의 구성원이 생각하는 정보보호에 대한 인식과

이 조직의 구성원이 실제로 업무를 수행하는 현실을 가장 잘 알 수 있는 방법은 이 조직이 '속도 중심적'인지를 먼저 살펴보는 것이다. 왜냐하면, 정보보안 부서의 입장에서는 기업 내에 편제된 모든 부서가 성과 지표인 '속도' 외에도 안전 지표인 '방향(예: 기업 내 제 규정, 특히 정보보안 정책 등)'도 함께 고려하기를 바라지만, 대부분이 조직 현실은 성과 지표인 '속도'만을 고려하고 있기 때문이다.

➔ 향후 보안 조치 이러한 조직의 성향을 식별했다면 CISO 입장에서는 향후 이 조직이 업무 수행과정에서 '방향'도 함께 고려할 수 있는 관리적 절차와 기술적 수단을 적용해야 할 것이다.

② 속도와 방향; 일시적 Vs. 지속적

어떤 조직의 경우에는 업무적인 속도 외에 방향을 함께 고려하는 조직도 있을 수 있다. 이러한 조직은 '속도와 방향'을 함께 고려하는 조직성향을 가지고 있으므로 '속도'만을 고려하는 조직에 비하여 인식과 현실의 접점 수준이 높다고 할 수 있다.

➔ 향후 보안 조치 이러한 성향을 가진 조직이 파악된다면 CISO는 이 조직의 성향이 유지/개선될 수 있는 환경을 구성해 주어야 한다. 왜냐하면, 현재의 조직성향은 일시적 현상일 수 있으며, 조직의 구성원이 변경되면 언제든지 달라질 수 있기 때문이다. 따라서 조직의 구성원이 변경되더라도 이 조직의 성향이 지속적으로 유지될 수 있는 환경을 구성해 주는 것이 현명한 방안이라고 생각된다. 이러한 방안으로는 예를 들면, '속도와 방향'을 함께 고려하는 이 조직의 성향을 기업 내 전사 조직을 대상으로 하여 '안전한 업무 실행의 표본'으로 공개하는 것이다. 이렇게 하면 이 조직의 성향이 지속될 가능성이 높아질 뿐만 아니라 다른 조직에서도 표본화된 선례를 무시하기는 어려울 것이다.

③ 잘못된 방향에 대한 교정 프로세스 유무

정보보안과 관련된 관리적 절차와 기술적 수단의 중요성을 인지하고 이를 업무에 반영하고 있는 조직이 있다고 가정을 해 보자. 그런데 업무에 따라서는 정보보안 부서의 검토를 거쳐야 함에도 불구하고 이 조직 자체적인 해석에 의해서만 정보보안 절차를 반영한다면 어떤 경우에는 정보보안 체계에 반하는 잘못된 방향으로 업무가 진행될 수도 있다. 이러한 경우에 잘못된 방향을 교정하는 프로세스가 있는지를 확인하는 것도 조직의 성향을 파악하는데 중요한 지표가 될 수 있다. 그리고 이러한 성향을 가진 조직은 '속도와 방향'을 함께 고려하는 조직보다 인식과 현실의

접점 수준이 높다고 할 수 있다.

향후 보안 조치 이러한 성향을 가지고 있는 조직을 식별했다면, CISO는 이 조직이 필요한 경우에 교정 프로세스(예: 보안성 검토 적용 등)를 활용할 수 있도록 조치하여야 한다.

2) 컴플라이언스 수준 파악

조직의 컴플라이언스 수준을 파악하는 방법으로 ⅰ) 관련 법령/고시 숙지 여부 ⅱ) 관련 법령/고시의 업무 적용 여부 ⅲ) 법령/고시의 변화관리 여부라는 지표를 활용할 수 있다. 이러한 지표를 가지고 조직의 컴플라이언스 수준을 파악하는 이유는 조직 내에 '보안 컴플라이언스 기능'이 작동되고 있는지 그리고 조직 내 '보안성 검토 전담자'가 있는지를 파악하기 위함이다. 정보보호 관련 법령/고시의 변화관리가 되고있는 조직의 경우에는 대부분 보안성 검토 전담자를 두고 있다.

① 관련 법령/고시 숙지 여부

보안이 법률화된 현재, 정보보호 특히 고객의 개인정보보호 업무는 비단 정보보안 부서 만이 업무가 아닌 기업 전 조직과 구성원에 부여된 업무라고 해도 과언이 아니다. 게다가 직원은 개인정보의 주체이므로 조직의 구성원임과 동시에 다른 기업의 고객이 되기도 한다. 그렇기 때문에 개인정보보호에 관한 기본적인 법령과 필수적인 고시 내용은 숙지하고 있어야 한다. 예를 들면 기업의 정보보안 체계에서 「개인정보 보호법」과 「정보통신망법」이 갖는 위상이나 이 법령에 따른 「안전성 확보조치 기준(고시)」에서 준수해야 하는 주요 내용이 그러하다. 그렇지만 현실적으로 보면 고객의 개인정보보호 업무는 정보보안 부서 고유의 업무이며 본인들과는 무관하다고 인식하고 있는 조직이나 구성원이 상당히 많이 있다.

향후 보안 조치 이러한 조직을 식별했다면, CISO는 각 법령과 고시를 기반으로 하여 정보보안 부서 이외에 다른 조직에서 준수해야 하는 기본적이고 필수적인 내용을 선별하여 전사에 공지하고 주기적으로 모니터링 해야 한다. 특히 개인정보 유출이 직원의 부정행위로 인한 경우에는 해당 직원이 형법(예: 컴퓨터 등 장애, 업무방해 등)에 의해서 처벌받을 수도 있다는 점을 인지시킬 필요가 있다.

② 관련 법령/고시의 업무 적용여부

기업의 정보보호와 관련된 법령과 고시 등을 인지하는 것과 이를 실제 업무에 적용하는 것은 마치 정보보호의 중요성을 인식하는 것과 이를 현실적으로 준수하는 것과 같은 상황이라고 할 수 있다. 즉, 대부분의 조직에서는 「개인정보 보호법」이나 「정보통신망법」의 역할과 기능을 인지하고 있으며, 이러한 법령에서 파생된 「안전성 확보조치 기준(고시)」 중에서 주요한 내용도 인지하고 있다. 그렇지만 이러한 법령/고시를 인지하고 있는 것과는 별개로 이를 해당 부서의 업무 프로세스에 적용하고 있는 조직은 많지 않을 것이다. 왜냐하면, 애써 불편한 방법으로 업무를 처리하고 싶지 않기 때문이다. 다만, 기업의 정보보호와 관련된 법령/고시 등을 전혀 인지하지 못하는 조직보다는 이를 인지하는 조직이 인식과 현실의 접점 수준이 더 높다고 할 수 있다.

➔ 향후 보안 조치 이러한 조직을 식별했다면, CISO는 기업의 정보보호와 관련된 법령/고시에서 규정하고 있는 관리적 절차와 기술적 보호조치 등을 선별하여 이를 각 조직의 업무에 반영할 수 있는 관리적 방안과 기술적 수단을 적용하여야 한다. 그리고 이러한 관리적 방안과 기술적 수단이 필요한 이유 및 준수 방법 등에 대한 주기적인 교육이 반드시 병행되어야 한다.

③ 법령/고시의 변화관리 여부

기업의 정보보호와 밀접하게 관련된 법령(예: 개인정보 보호법, 정보통신망법, 신용정보보호법 등)도 타법 개정이나 정부 정책 등의 변경을 이유로 개정이 되기도 한다. 특히 최근에는 '개인정보의 보호와 개인정보의 활용'의 균형을 찾기 위해 위 법령의 개정 작업이 진행 중이다. 이러한 법령이 개정되고 나면 당연히 이러한 법령에 근거를 두고 있는 「안전성 확보조치 기준(고시)」의 내용에도 변경이 뒤따르기 마련이다. 따라서 만약 이러한 법령/고시가 변경된다면, 관련 업무를 수행하는 조직에서 그 내용을 인지할 필요가 있다. 만약에 정보보안 부서가 아님에도 불구하고 이러한 법령/고시의 변경내용을 파악하고 있는 조직이 있다면 이 조직에 내재된 인식과 현실의 접점 수준은 높은 편이라고 할 수 있다. 그렇지만, 정보보안 업무를 고유한 업무로 수행하고 있지 않은 대부분의 조직에서는 이처럼 법령/고시의 변경까지는 파악하지 못할 가능성이 상당히 높다.

➔ 향후 보안 조치 이러한 조직을 식별했다면, CISO는 정보보안 부서를 통해서 가장 최신의 법령/고시 내용을 선별하여 전사 조직에 공지함과 동시에, 현재 적용 중인 업무 프로세스와 개정된 법령/고시 간의 간극(Gap)을 찾아 업무 프로세스를 변경시켜야 한다.

3) 보안사고 동향에 대한 이해수준 파악

보안사고 동향에 대한 조직의 이해수준을 파악하는 방법으로는 ⅰ) 동종업계 보안사고 인지 여부 ⅱ) 보안사고 사례 전파 채널 존재 여부 ⅲ) 보안대책 수립/적용 여부라는 지표를 활용할 수 있다. 이러한 지표를 활용하여 보안사고 동향에 대한 조직의 이해수준을 살펴보는 이유는 조직 내에 '위험평가 프로세스 존재 유무'와 '위험평가 실시 유무'를 파악하기 위함이다.

① 동종업계 보안사고 인지 여부

타산지석(他山之石)이란 말이 있다. 특히 정보보안 업계에서는 이 말이 가지는 의미를 매우 높게 평가하고 있다. 왜냐하면, 우리나라에서는 개인정보 보호법이 발효된 이후 현재까지 매우 많은 보안사고가 발생했을 뿐만 아니라, 매우 다양한 업종에서 보안사고가 있었기 때문이다. 이러한 점에 비추어 볼 때, 동종업계에서 최근에 발생한 보안사고를 인지하고 있는지 여부는 인식과 현실의 접점을 식별하는데 매우 중요한 지표가 될 수 있다. 불행 중 다행인 점은 최근에 개인정보보호가 큰 이슈가 되고 있다 보니 동종업계에서 발생한 보안사고에 대해서 정보보안 부서가 아니더라도 인지하고 있는 부서가 있다는 점이다. 하지만 만약 동종업계에서 최근에 화두가 되고 있는 보안사고에 대해서 전혀 인지하지 못하는 부서의 경우에는 인식과 현실의 접점 수준이 낮다고 평가할 수 있다.

➔ 향후 보안 조치 이러한 조직을 식별했다면, CISO는 동종업계에서 최근에 발생한 보안사고의 사실관계와 현재의 수사 또는 재판 상황을 전사 조직을 대상으로 공지할 필요가 있다. 이에 더하여 동종업계가 아니더라도 전사 조직이 인지할 필요가 있다고 판단되는 다른 보안사고에 대해서는 카테고리 별(예: 외부침입, 내부유출, 노출, 분실, 관리 부주의 등)로 선별하여 사실관계와 수사/재판 상황 그리고 판례 등을 정리해 둘 필요가 있다. 이렇게 정리해 둔 자료는 외부에서 유사 보안사고가 발생하는 경우 즉시 전사 공지용 자료로 활용할 수 있다.

② 보안사고 사례 전파 채널 존재 여부

보안사고가 이슈화되면, 유사 사고 발생을 예방하기 위해서 이슈화된 보안사고 내용을 전사 조직에 전파하여야 한다. 왜냐하면, 이러한 과정을 통해서 전사 조직의 경각심을 고취 시키고 조직 자체적인 진단을 수행할 수 있기 때문이다. 그런데 보안사고 사례를 전파할 채널이나 방법이 없는 조직이라면 인식과 현실의 접점 수준이 낮다고 평가할 수 있다.

➔ 향후 보안 조치 이러한 조직을 식별했다면, CISO는 정보보안 부서가 전사 조직을 대상으로 보안사고 사례를 전파할 수 있는 채널(예: 사내 공지 창, 정보보안 알림창, 전사 이메일, 전사 메신저 등)을 발굴하여 활용하는 방안은 적용해야 한다. 그리고 만약 여건이 허락된다면 정보보안 부서가 전파한 보안사고 사례를 각 조직 내에서 한 번 더 전파할 수 있는 부서보안담당자를 활용하는 방안도 검토해야 한다.

③ 보안대책 수립/적용 여부

옆 동네에서 가스레인지 사용 후 가스밸브를 잠그지 않아 화재가 발생했다고 가정을 해 보자. 이런 뉴스나 기사를 접하게 되면, 우리 집 가스밸브도 한번은 확인하는 것이 인지상정이다. 보안사고에 대한 조직의 태도도 마찬가지라고 생각된다. 즉, 동종업계에서 발생한 보안사고가 이슈가 되고 있다면, 한 번쯤은 우리 기업 내에서 유사 사고가 발생할 가능성이 없는지에 대해 확인하는 기능이 있어야 한다는 것이다. 만약에 이러한 확인 기능이 이미 존재하는 조직이라면 이는 인식과 현실의 접점 수준이 매우 높은 조직이라고 할 수 있다. 현실에서는 일반업무 조직보다는 정보보안 부서에서 이러한 확인업무를 담당하고 있을 것이다. 다만, 여기서 중요한 것은 유사 사고 발생 가능성을 확인한 이후의 조치나 대책이 일반업무 조직에 적용되고 있는가 여부이다. 즉, 동종업계 보안사고가 이슈화되고 있을 때 유사 사고의 발생 가능성을 줄이기 위해 정보보안 부서에서 수립한 조치나 대책이 기업의 전사 조직에 적용되고 있는지를 판단해야 한다는 것이다. 만약 동종업계의 보안사고가 이슈화되고 있음에도 불구하고 기업 내 조직에서 어떠한 조치나 대책이 적용되지 못한다면 경우에는 인식과 현실의 접점 수준이 낮다고 평가할 수 있다.

➔ 향후 보안 조치 이러한 조직을 식별했다면, CISO는 이슈화되고 있는 보안사고를 예방할 수 있는 조치나 대책을 수립하여 먼저 CEO에게 보고하여야 한다. 왜냐하면, 이 경우의 조치나 대책은 기존에 적용하지 않던 새로운 조치나 대책일 가능성이 높기 때문에 CEO의 승인 없이 적용하는 경우에는 일반업무 조직의 저항이 클 수가 있다. 따라서 이런 경우에는 새로운 조치나 대책의 필요성을 CEO에게 먼저 보고 후 적용의 승인을 얻는 것이 좋은 방법이다. 이렇게 하면 새롭게 적용되는 보안 조치나 대책에 대한 저항을 최소화할 수 있다. 그리고 필요하다면 새로운 보안 조치나 대책에 대한 설명과 함께 직원들의 궁금증을 해소시켜 줄 목적으로 공청회를 한 후에 전사에 적용하는 것도 좋은 방법이 된다.

(2) 단계적 조치; 속도 조절

앞서 여러 가지 지표를 활용하여 정보보안 체계에 대한 인식과 현실의 접점을 식별하였다면, 이제부터는 조직의 정보보호 인식의 수준을 높여 나가는 단계적 조치들을 적용하여야 한다. 정보보호 인식 제고를 위한 단계적 조치를 적용할 때 중요한 점은 조직 구성원의 저항을 최소화하는 방식으로 적용하여야만 정보보호 인식 제고라는 목표를 달성할 수가 있다는 점이다. 이와 같은 관점에서 볼 때, 정보보안 체계 내에서 정보보안 전담부서가 주관하는 '통제의 속도'와 이러한 보안 통제를 준수해야 하는 조직의 '통제의 수용속도'를 조절하는 것이 매우 중요하다. 이를 위해서 다음과 같은 방법을 적용해 볼 수 있다.

1) 팀플레이

기업에는 일반적으로 정보보안 업무를 수행하는 전담부서가 있기 때문에 다른 조직의 구성원들은 정보보안 업무는 전담부서만의 업무라고 생각하곤 한다. 물론 정보보안 전담부서가 수행해야 하는 고유한 업무(예: 정책 수립, 보안 컴플라이언스 검토, 보안성 검토, 보안 점검, 보안 교육 등)가 있기는 하지만, 기업의 정보를 보호하는 업무는 기업 구성원 모두가 함께 수행해야만 가능한 업무이다. 즉, 기업의 정보보안 업무는 정보보안 부서와 다른 조직이 함께 수행하는 팀플레이여야 한다. 왜냐하면, 기업의 정보보안 체계를 유지하는 것이 정보보안 부서만의 업무가 아니라 기업의 모든 구성원이 함께 지켜야 하는 '공동의 가치'이기 때문이다.

① 보안 통제 수용속도 식별

정보보안 전담부서와 다른 조직 간의 팀플레이를 위해서 가장 먼저 해야 하는 것은 다른 조직의 '보안 통제 수용속도'를 식별하는 것이다. 즉, 정보보안 전담부서의 관점에서 '통제의 속도'만을 토대로 보안 통제를 적용하는 것뿐만 아니라 실제로 보안 통제를 준수해야 하는 조직의 관점에서 '보안 통제의 수용속도'를 식별해야 한다는 것이다. 예를 들어 기획부서가 수립한 새로운 사업기획에 대해 정보보안 부서가 보안성 검토를 하는 상황이라면, 정보보안 부서의 입장에서의 '통제의 속도'뿐만 아니라 기획부서의 입장에서 '통제의 수용속도'를 함께 고려하여 보안 통제의 속도를 조절해야 한다는 것이다. 왜냐하면, 정보보안 체계가 유지된다는 말에 내포된 의미는 '보안 통제'와 '통제에 대한 수용'이 마치 주고받는 대화처럼 양방향이 유지된다는 것을 의미하기 때문이다.

② 속도의 기준은 상대방

앞서 살펴본 것처럼 '보안 통제'와 이러한 '통제에 대한 수용'이라는 양방향성이 유지되어야 정보보안 체계가 유지된다. 그렇다면 여기서 보안 통제의 속도와 통제수용의 속도가 다를 경우에는 어떻게 해야 할까? 예를 들어 정보보안 부서 입장에서는 새롭게 개정되는 법령/고시에서 규정하고 있는 특정한 보안 통제를 빠른시간 내에 전사 조직에 적용하고자 하는 데에 반해 재무부서 입장에서는 재무·회계업무 시스템의 특성으로 인해 새롭게 적용되는 통제를 빠른시간 내에 수용할 수 없는 상황을 생각해 보자. 이러한 경우에 보안 통제의 속도는 정보보안 부서가 아니라 재무부서의 속도(더 정확하게는 통제의 수용속도)에 맞추어서 통제를 적용하는 것이 바람직하다. 따라서 이러한 경우에는 정보보안 부서장과 재무 부서장이 새로운 보안 통제를 완전하게 적용하는 시점을 함께 정해 두되, 재무부서의 업무 처리에 무리한 영향을 주지 않은 범위 내에서 새로운 보안 통제를 서서히 적용하는 것이 정보보안에 대한 저항을 최소화하면서 보안 통제의 수용속도를 높일 수 있는 방안이라 할 수 있다.

③ 합리적 근거에 기반하는 속도 조절

정보보안 체계의 유지라는 팀 플레이를 위해서 ⅰ) 보안 통제의 수용속도를 식별하고 ⅱ)통제 적용의 속도를 상대방 부서에 맞추는 것이 이상적이지만, 일정한 경우에는 이러한 이상적인 상황에 맞출 수 없고 정보보안 부서가 통제속도를 높여야 하는 경우도 있다. 예를 들면 웹 서비스상에서 이용자의 개인정보 이용이나 제공 등에 대한 동의절차가 누락 되어 있거나 1년 이상 미 이용자 계정을 파기 또는 분리하지 않는 것처럼, 기존의 서비스나 업무 방식이 이미 보안 컴플라이언스를 위배하고 있는 경우가 그러하다. 이러한 경우에는 빠른시간 내에 기존 서비스에 새로운 보안 통제를 적용해야만 한다. 이처럼 보안 통제의 속도를 빠르게 진행해야 하는 합리적인 근거(예: 법령/고시 위반, 보안 인증 결함 이행조치, 정부기관 보안 점검 지적사항 이행조치 등)가 있는 경우에는 관련 부서와 협조하여 정보보안 부서의 보안 통제를 빠르게 적용하여야 한다.

2) 소통

정보보안 부서는 기업 내 다른 조직과 지속적으로 소통을 해야 한다. 여기서 말하는 소통이란 업무협조 회의나 보안성 검토, 보안 공지, 보안 교육, 보안 점검, 타운홀 미팅 등을 말하는 것이다. 이처럼 정보보안 부서가 다른 조직과 지속적인 소통을 해야 하는 이유는 '정보보호라는 분산화된 책임'을 다른 조직도 함께 이행하도록 하기 위해서이다.

① 보안 개념은 기획단계에서부터!

일반적으로 보면 기획부서나 개발부서에서는 사업기획의 참신성과 사업성 그리고 실현 가능성 등에 방점을 두고 업무가 진행된다. 그러하다 보니 새로운 아이디어나 내·외부적인 기회가 생기면 자연스럽게 빠른시간 안에 사업 기획·시스템 개발을 실현하고자 한다. 그렇지만 정보보안 관점에서 볼 때, 이러한 과정에서 나타나는 중요한 문제가 있다. 즉, 정보보안 부서는 기획부서나 개발부서의 사업 기획·시스템 개발의 완성 단계에 이르러서 정보보안 관련 이슈 체크를 요청받게 되는데, 정보보안 이슈를 해소하기 위해서는 기획의 초기 단계로 돌아가서 수정해야만 하는 상황이 발생한다는 문제이다. 이러한 문제는 비단 정보보안 부서만의 문제로 끝나지 않고, 기획부서나 개발부서에게도 상당한 부담으로 작용할 수 있다. 이러한 문제를 사전에 방지하고 조직의 시간을 효율적으로 활용하기 위해서는 신규 사업이나 신규 서비스를 기획하는 시점에 해당 기획을 담당하는 부서가 정보보안 부서에게 보안성 검토를 요청하도록 해야 한다. 이를 위해서는 평소에 전사 조직을 대상으로 보안성 검토의 목적과 취지 그리고 요청 시점 등을 알 수 있는 소통 채널을 구축할 필요가 있다. 여기서 말하는 소통 채널이란 보안 공지나 보안교육 그리고 부서장급 회의 등이 있을 수 있다. 특히 이러한 소통과정에서는 의사결정권을 가진 상급 직위자가 기획안을 승인하기 전에는 실무자에게 해당 기획안에 대한 보안성 검토를 거쳤는지 그리고 그 결과는 어떠했는지를 반드시 확인하도록 요청하여야 한다.

② 상대방의 언어로!

사업이나 서비스 또는 마케팅 등의 실무를 담당하는 부서에서 정보보안 부서와 업무협조 회의 등을 하는 경우 간혹 분위기가 험악해지는 경우가 있다. 이러한 상황이 발생하는 가장 근본적인 이유는 실무부서와 정보보안 부서 간의 의사소통이 이루어지지 않음으로 인해 각자의 입장과 관점에서만 의사 표현을 하기 때문이다. 그런데 시간이 좀 흐른 후에 다시 그 실무부서와 업무협조를 해 보면 지난번 회의 때와는 달리 순조롭게 협조 회의가 진행되기도 한다. 이런 상황은 각자의 입장이 아니라 상대방의 입장을 고려하여 상호 간에 의사 표현을 하는 경우 발생하는 상황이다. 이러한 상황을 비추어 볼 때, 정보보안 부서는 상대방 조직의 언어로 의사소통을 할 필요가 있다. 즉, 기밀성과 무결성의 관점에서 파생되는 어려운 보안용어만을 사용하면서 상대방 조직과 의사소통하는 것이 아니라 상대방 부서의 업무 처리방식과 주요 용어 등을 활용하여 의사소통을 해야 한다는 것이다. 특히 정보보안 부서는 기업 내 정보보안 체계를 유지하기 위하여 다른 조직과 긴밀한 접점을 유지해야 하는 경우가 많이 있다. 이러한 접점을 유지하는 과정에서 상대방 조직의

관점과 업무용어를 활용하여 의사소통을 한다면, 정보보안 부서가 통제하는 관리적 보안에 대한 상대방 조직의 저항을 줄여 낼 수 있을 것이다.

③ '안 되는 방법'보다는 '되는 방법'으로!

전문성에 기반하여 운용되는 조직에서는 아무래도 전문적인 영역과 표준(예: 법령, 지침,자격, 경력, 수준 등)이 있기 마련이다. 정보보안 부서도 마찬가지로 전문적인 영역과 표준에 기반하여 운용되는 조직이다. 그러하다 보니 이러한 전문성에 반하는 요청사항에 대해서는 기본적으로 '그건 안 됩니다'라는 부정적인 표현을 할 수밖에 없다. 그렇지만 그러한 요청을 한 직원이나 부서의 입장에서는 자신들의 요청이 전문성에 반한다는 사실을 인지하지 못하고 있었을 가능성이 매우 높으며, 자신들의 요청을 실행할 수 있는 방법을 알고 싶어서 정보보안 부서를 찾는 경우가 대부분이다. 이러한 상황에서 상대방 조직이 정보보안 부서에 요청한 사항이 기술적 보안 조치에 위배 되어 '안 되는 방법'이라는 정의만 내리는 것은 좋은 소통 방법이 아니다. 왜냐하면, 이러한 상황들이 기술적 보안 조치를 우회하도록 만드는 계기가 될 수도 있기 때문이다. 따라서 이러한 경우는 기술적 보안 조치를 위배하지 않으면서도 상대방 조직의 요청사항을 실행할 수 있는 '되는 방법'을 함께 고민해 주는 것이 좋은 소통 방법이 될 수 있다.

④ 통제부서로서의 감정관리

정보보안 부서는 이른바 '통제부서'이다. 그래서 통제부서는 기업 내 많은 조직의 업무 내지는 절차에 대해 통제를 하여야 하고 이를 위해서 신규기획에 대한 보안성 검토와 업무 협조 회의, 보안 교육, 보안 점검 등을 수행하는 것이다. 그런데, 이러한 통제과정에서는 상대방 조직이 반발 내지는 반감을 표출하는 경우가 있다. 이러한 경우에 정보보안 부서가 감정관리를 잘못하게 된다면, 정보보안 부서는 통제부서로서의 권위를 잃을 수도 있다. 따라서 보안 통제과정에서 정보보안 부서는 업무적 전문성을 기반으로 통제를 하되, 상대방의 자극에 대해서 감정적으로 대응을 해서는 안 된다.

⑤ 새로운 보안 통제 적용 전에는 반드시 소통

기존에 없었던 보안 통제를 새롭게 적용한다는 것은 정보보안 부서의 입장에서는 당연히 보안체계를 강화하기 위해 필요한 조치라고 생각할 수 있다. 그러나 이에 대해 다른 조직의 입장에서는 업무 과정에서 새로운 불편과 절차가 생긴다고 생각할 수 있다. 앞서 강조한 바와 같이 '정보보안은 분산화된 책임'이다. 따라서 새로운 보안 통제의 적용에 대해 CEO의 승인을

받았다고 하더라도, 새로운 보안 통제를 적용하기 이전에는 기업 내 전사 직원을 대상으로 새로운 보안 통제의 취지·근거·준수 방법 등을 알게 해 줄 필요가 있다. 예를 들면, 곧 적용될 새로운 보안 통제에 관심 있는 직원이라면 누구나 참여할 수 있는 타운홀 미팅 또는 부서장 이상의 참여하는 회의 등에서 해당 내용을 알게 해 주는 것이다. 이러한 소통과정에서는 질문과 대답이라는 상호간 소통을 하게 될 텐데, 이 과정에서는 소통 없이 새로운 보안 통제를 적용했을 때 나타날 수 있는 저항을 미리 줄일 수 있다. 게다가 만약 새로운 보안 통제의 적용에 대해 CEO가 이미 승인을 했다면, CEO의 승인 여부를 문서로 알게 되는 것이 아니라 정보보안 부서(또는 CISO)로부터 직접 알게 되는 것이므로 정보보안 부서(또는 CISO)가 통제부서로서의 권위도 유지하는 효과도 있다.

3) 기다림의 미학

기업을 구성하고 있는 많은 조직 중에서 정보보안 부서의 직원은 정보보안 체계의 중요성을 잘 알고 있다. 그런데 이러한 인식은 정보보안 부서가 아닌 일반부서의 직원들에게도 존재하고 있다. 이렇게 말할 수 있는 이유는 「2017 정보보호 실태조사」에서 일반 직원들의 정보보호 중요도 인식 수준이 무려 81.5%에 해당하고 있기 때문이다. 다만, 앞서 설명한 바와 같이 일반부서에서는 '인식과 현실의 불일치'와 '기술보안 우회'의 가능성 그리고 '관리 보안에 대한 저항'하는 현상이 늘 나타나고 있다. 이러한 상황을 극복하고 기업의 정보보안 체계를 유지하기 위해서는 다음과 같이 몇 가지 단계적인 조치를 적용해 볼 필요가 있다. 왜냐하면, 정보보안 부서 '하나'일 때보다 동참하는 다른 많은 조직이 '함께'할 때 기업의 정보보안 체계가 유지될 수 있기 때문이다.

① 통제보다는 가이드를 하라.

정보보안 부서의 기본적인 기능이 '보안 통제'이다 보니 이러한 통제에 대해 일반부서의 입장에서는 항상 '통제를 받는다'는 생각을 하고 있다. 물론 필요한 경우에는 통제 그 자체에 목적을 두고 보안 통제를 실행해야 하겠지만, 위험한 상황이 아니라면 '통제'보다는 '가이드'를 하는 것이 일반부서의 동참을 이끌어 내는 데 효과적일 수 있다.

② 설명, 설명, 그리고 설명하라.

일반적으로 새로운 보안 프로세스가 기업의 전사 조직 내부로 이식되는 데 소요되는 기간은 6개월 이상 걸리는 것으로 보인다. 이 기간 동안 정보보안 부서는 엄청난 활동을 하게 된다. 여기서 말하는 활동이란 예를 들면, 보안 공지와 교육, 타운홀 미팅과 협조 회의 등이다. 그런데 이러한

활동을 한마디로 정의하자면 바로 '설명'이다. 즉, 새로운 보안 프로세스를 조직 내에 이식시키기 위하여 여러 가지 방법으로 설명하고 있는 것이다. 그런데 여기서 주의할 점은 보안 프로세스가 조직 내에 이식된 이후에도 지속적으로 설명을 해야 한다는 점이다. 왜냐하면, 지금 시점에서 보안 프로세스가 잘 이식된 조직이라고 하더라도 시간이 흐름에 따라 조직 내에서는 내재적인 변화가 발생 되기 때문이다. 이러한 변화의 예로는 조직 내의 인적 구성 변화, 업무 담당자 변경, 신규 업무 착수, 정보보안에 대한 구성원의 긴장감 변화 등이 그러하다. 따라서 CISO는 이러한 상황을 인지하여 보안 프로세스에 대한 지속적인 설명이 가능한 절차와 방법을 수립하여 적용할 필요가 있다.

③ 기다리고 있다는 것을 알게 해 주어라.

앞서 살펴 본 것처럼 일반직원의 81.5%가 정보보호의 중요성을 인식하고 있다. 하지만, 이러한 인식에 비해 일반직원들이 업무를 수행하는 현실 간의 불일치가 존재한다는 것도 우리는 살펴보았다. 이와 같은 불일치를 최소화 할 수 있는 방안으로 '기다리고 있다는 것을 알게 해 주는 방법'을 활용해 볼 수 있다. 즉, 보안 통제를 즉시 적용하는 것이 아니라 가능한 범위 내에서 보안 통제를 요청할 때까지 기다려 주고, 이렇게 기다리고 있다는 것을 알게 해 주라는 것이다. 예를 들어 특정 업무부서가 새로운 사업기획을 준비하고 있다는 내용이 정보보안 부서로 전달이 되면, 정보보안 부서가 곧바로 보안성 검토를 하자고 해당 부서에 요청할 것이 아니라 해당 부서가 보안성 검토를 요청할 때까지 기다려 주자는 것이다. 그리고 이러한 과정에서 정보보안 부서가 신규사업기획을 하는 부서의 보안성 검토 요청을 기다리고 있다는 것을 알게 해 주자는 것이다. 이렇게 한다면 기획의 초기 단계에서부터 보안성 검토를 적용할 수 있을 뿐만 아니라 기획단계에서 보안성 검토를 거쳐야 한다는 절차적인 인식도 높일 수 있게 된다. 아울러 신규사업을 기획하는 부서의 타임라인에 맞추어 정보보안 부서가 기다려 주었다는 사실 그 자체는 보안성 검토뿐만 아니라 기업 내 정보보안 체계에 대한 저항감도 완화 시킬 수 있는 좋은 선례가 될 수 있을 것으로 생각된다.

④ 충분한 수용의 시간을 주어라.

앞서 말한 것처럼 가능한 범위 내에서 보안 통제를 즉시 적용하지 않고 기다려 주거나 새로운 보안 통제 적용 전에 다른 조직과 지속적인 소통을 하는 이유는, 다른 조직이 보안 통제를 수용할 수 있는 시간을 주기 위함이다. 특히 필자는 이러한 수용이 시간을 보낸 조직과 그렇지

못한 조직이 정보보안 체계 수용하는 수준이 현저하게 다르다는 것을 종종 목격하였다. 따라서 CISO는 법령/정책에서 규정하고 있는 보안 통제를 적용하기 전에는 이 보안 통제를 준수해야 하는 조직에게 일정한 기간까지 충분히 고민하고 생각할 기회를 만들어 줄 필요가 있다. 이렇게 하면 해당 조직 내에서는 일정 기간 동안 내부적으로 회의와 토론 등의 활동을 하게 되는데, 이러한 활동을 통해서 보안 통제를 심리적으로 수용하게 되는 것이다. 필자의 경험에 비추어 볼 때, 이미 보안 컴플라이언스를 위반하고 있지 않은 상황이라면 1주일 정도의 시간이 합리적이라고 생각된다.

⑤ 넛지(Nudge) 효과를 활용하라.

정보보안 부서에서 보안 통제를 적용하는 경우에는 정책 수립 및 공지, 준수 모니터링 및 점검, 위반 현황 관리 등의 직접적인 방법들을 적용하게 된다. 물론 이와 같은 방법들은 그것 자체로 목적과 효과가 있는 통제방법이다. 그러나 다른 조직과의 소통을 목적으로 하고 있다면, 직접적인 방법의 적용과 더불어 간접적인 방법도 함께 활용하는 것도 좋은 효과가 있다. 간접적인 방법의 가장 좋은 예가 바로 넛지(Nudge) 방식이다. 여기서 말하는 넛지(Nudge)란 일반적으로 '팔꿈치로 툭 찌르다'라는 의미를 가지고 있는데, 강압적인 방법이 아닌 부드러운 방법을 적용했을 때 더 좋은 결과가 나오는 것을 '넛지(Nudge) 효과'라고 한다.

예를 들어서 최근에 큰 위협이 되고 있는 랜섬웨어에 대비하기 위한 새로운 정책을 수립하여 이를 공지하고, 준수 여부를 모니터링하는 직접적인 통제방법을 적용해야 하는 경우를 가정해 보자. 이런 경우에는 이와 같은 직접적인 통제방법과 더불어 넛지(Nudge) 방식을 활용한 간접적인 통제도 함께 적용할 수 있다는 것이다. 예를 들면 우리 기업의 조직과 구성원을 보호하기 위하여 정보보안 부서의 랜섬웨어 대응 담당자가 어떤 업무를 수행하고 얼마나 많은 수고를 하는지를 주요 내용으로 '정보보안 부서 직원의 일상'을 사내 공지용 기사로 만들어 공지하는 방법을 활용할 수 있다. 이렇게 간접적인 방법으로 보안 통제를 병행한다면, 직접적인 보안 통제에 대한 저항이 줄어들 뿐만 아니라 실제로 정보보안 체계에 대한 다른 조직의 수용력도 증가하는 것을 필자는 종종 경험하였다.

(3) 단계적 조치; 현상이 아닌 원인에 집중

정보보안 정책을 위반하는 것처럼 기업 내에서 구성원이 정보보안 체계를 벗어나는 것은 사실 하나의 '현상'이라고 할 수 있다. 그리고 이러한 현상은 어떠한 원인에 의해 결과적으로 나타나는 것이다. 물론 정보보안 관점에서는 이러한 '현상' 그 자체에 대해 보안 통제를 강화하는 것이 당연한 순리다. 그렇지만, 이러한 현상이 반복적으로 발생한다면 CISO는 이에 대해 깊은 고민을 해 보아야 한다. 왜냐하면, '현상'이 반복된다는 것은 다른 말로는 '원인'을 해결하지 못했다는 것이기 때문이다. 이런 관점에서 이하에서는 '현상'이 아닌 '원인'에 집중하는 데 도움이 되는 몇 가지 예시를 공유하고자 한다.

1) 나뭇가지가 아닌 바람이 중요한 이유

나뭇가지를 흔드는 것은 눈에 보이지 않는 바람이다. 이를 정보보안 체계를 벗어나는 경우에 대입해 보면, 정보보안 위반행위는 하나의 '현상'일 뿐이고 이러한 현상이 발생하는 '원인'은 따로 있다는 말이 된다. 예를 들어서 아침마다 실시되는 생활 보안 점검에서 유독 어느 한 직원이 문서를 방치하고 있고, 또 다른 직원은 퇴근 시 컴퓨터 전원을 종료하지 않았다고 가정해 보자. 이러한 상황에서 문서 방치와 컴퓨터 전원 미종료는 하나의 현상일 뿐이므로, 그 현상 자체가 문제 해결을 위한 원인이 될 수는 없다.

이러한 경우에 CISO는 정보보안 체계를 벗어나는 '현상의 원인'을 식별하여 보안 통제를 적용하여야 한다. 그리고 이처럼 현상이 아닌 원인에 집중하는 과정이 중요한 이유는 이 과정을 통해서 기업의 조직과 구성원이 가지고 있는 내재 된 취약점을 식별할 수 있고 이러한 취약점을 보완할 수 있는 특화된 보안 통제를 적용할 수 있기 때문이다. 그렇기 때문에 '현상'이 아니라 '원인'을 해결할 수 있는 과정을 거치는 것은 정보보호에 대한 저항을 최소화하면서도 정보보호의 중요도 인식에 큰 영향을 미치는 매우 중요한 단계적 조치라고 할 수 있다.

2) 원인별로 다른 보안대책

앞의 예를 그대로 활용하여 보자. '현상'에만 집중하고자 한다면 어느 직원이 아침마다 문서를 방치하고 있고 이러한 현상이 반복적으로 발생했을 때 정보보안 부서에서는 정보보안 위반경고장을 반복적으로 발부하면 끝나는 일이다. 그런데 이 직원이 반복적으로 문서를 방치하는 원인이 이

직원의 책상 위치 때문이라면 어떻게 하겠는가? 즉, 이 직원의 책상 위치가 다른 직원들이 잘 다니지 않고 눈에 띄지 않는 가장 구석 위치에 있다 보니 문서 방치에 대한 긴장감이 완화된 것이 문서 방치의 원인이라면, CISO로서 당신은 어떤 보안대책을 적용하는 것이 좋겠는가?

이 경우에는 이 직원에게 정보보안 위반경고장을 발부하기보다는 이 직원의 부서장에게 협조를 구하여 이 직원의 책상 위치를 좀 더 공개된 위치로 변경시켜 달라고 하는 것이 보안대책에 대한 저항을 최소화하면서도 훨씬 더 효과적인 보완대책이 될 수 있다. 그리고 이렇게 조치하게 되면 다른 조직에도 영향을 끼치게 되어서 구석 위치에 있는 책상을 사용하는 다른 직원들의 행동도 교정하게 되는 부수적인 효과도 얻을 수 있다.

하지만 어떤 경우에는 '원인' 그 자체가 매우 심각한 상황으로 판별되는 경우도 있다. 예를 들어서 앞뒤 주말을 붙여서 무려 10일 동안 휴가를 가 있는 직원의 컴퓨터가 모니터 전원은 종료되어 있으나 본체 전원 종료되지 않은 현상이 발생했다고 가정을 해 보자. 이 현상에 대해 정보보안 부서에서 가용할 수 있는 기술적 시스템과 장비를 동원하여 더 파악해 보니, 이 직원이 휴가를 출발하기 전에 업무용 컴퓨터를 통해서 가상화폐사이트에 접속하여 '예약판매 및 예약구매' 기능을 사용하고 있었다면? 이 경우에는 휴가 중인 직원의 컴퓨터가 종료되지 않은 것은 '현상'이 되고, 가상화폐사이트에 접속하여 예약기능을 사용하고 있는 것이 '원인'이라고 할 수 있다. 그런데 만약 이 경우에 이러한 원인을 파악하지 않고 단순하게 정보보안 위반경고장만 발부하고 이 위반 건에 대한 조치를 마무리한다면 이 건의 원인을 알고 있는 다른 직원들의 인식은 어떻게 될 것 같은가? 아마도 '걸리지만 않으면 되는구나! 걸리더라도 경고장만 받으면 되는구나!'라고 생각할 가능성이 높다.

허가되지 않은 사이트로의 접속 자체가 기업의 정보보안 체계를 상당히 위협할 수 있는 상황임을 고려해 볼 때, 특히 CISO 입장에서는 '원인'이 아닌 '현상'에 대한 조치만 적용하는 것은 나중에 더 큰 위협의 발생 가능성을 키우게 되는 것임을 기억할 필요가 있다. 따라서 이와 같이 정보보안 체계를 벗어나는 현상의 원인이 심각한 상황인 경우는 이에 맞는 보안 조치를 적용하여야 한다. 여기서 말하는 장기 휴가자의 가상화폐사이트 접속 및 예약기능 사용 사례의 경우에는 ⅰ) 업무용 PC 강제종료 ⅱ) 접속차단 가능한 가상화폐사이트 식별 및 이에 대한 접속차단 ⅲ) 허가되지 않는 사이트 접속 금지에 대한 전사 공지 ⅳ) 이 직원의 컴퓨터에서 가상화폐사이트에 접속한 이력 및 접속 이력이 있는 모든 직원 식별 ⅴ) 식별된 직원 및 차상급자 대상 정보보안 위반에 대한 공식 메일 발송 ⅵ) 휴가자 복귀 시 소명서 징구 ⅶ) 필요시 인사위원회 회부 등의 보안 조치를 고려해 볼 수 있다.

(4) 단계적 조치; 정보보호 투자의 근거

1) 법령과 지침

기업의 정보보안 체계를 유지하고 강화해 나가기 위해서는 정보보호 예산을 확보하는 것도 상당히 중요하다. 이를 위해서 금융업종의 경우에는 「전자금융감독규정」에 의해서 전체인력의 5%를 IT 인력으로 두고 이 중에서 5%는 정보보호 인력으로 구성하며 IT 예산 중 7%를 정보보호 예산으로 사용하도록 하고 있다. 다만, 이 '5·5·7 규정'은 금융업종에 해당하는 강행규정이기 때문에, 금융업종을 제외한 나머지 업종에서 종사하는 CISO 입장에서는 경영진을 설득하는데 활용할 수 있는 '정보보호 투자의 근거'가 아쉬울 수 있다. 예를 들어서 새로운 보안 위협에 대응하기 위하여 신규 보안시스템을 구축하고자 하는 경우, 구축에 필요한 비용을 재무부서와 협의를 하게 된다. 이런 경우에 CISO는 보안 위협에 대응하는 관점에서 구축비용의 필요성을 주장하게 됨에 반해, CFO는 비용효과의 관점에서 판단하게 된다. 이렇게 되면 결국은 CFO의 의견에 따라 구축비용은 승인되지 않는 경우가 종종 있다. 이런 경우에 CISO는 어떻게 CFO를 설득할 수 있을까?

비금융권 기업의 정보보호 예산확보 및 투자에 대해서는 「정보통신망법」에 따른 '정보보호 조치에 관한 지침' 제3조에서 규정하는 별표 1을 활용해 볼 수 있다. 왜냐하면, 이 별표 1에서는 IT 부분 예산의 5% 이상을 정보보호에 투자하도록 하고 있기 때문이다. 이 규정이 강행규정이 아니라 권고규정인 점은 아쉽지만, 그래도 비금융권 기업을 대상으로 이와 같이 일정 비율의 정보보호 예산을 수립하도록 하는 규정이 있다는 것은 CISO 입장에서 큰 힘이 될 수 있다. 따라서 이를 근거로 하여 기업 내 전체 IT 부서에 배당되는 연간 예산의 5% 이상의 수준으로 정보보호 예산을 CFO에게 요청하는 방법을 활용할 수 있다. 이렇게 한다면, CISO 입장에서는 비록 권고규정이라 하더라도 법령상의 근거를 가지고 정보보호 예산을 확보하려는 노력을 다하게 되는 것이며, CFO 입장에서는 아무리 권고규정이라고 하더라도 법령상의 근거에 기반하고 있는 예산 요청사항에 대한 최종 의사결정의 부담을 안게 되기 때문이다.

물론 이와 같은 방식은 CISO와 CFO 간의 갈등을 유발할 수도 있다. 왜냐하면, 기업 내 정보보호 업무에 관한 최종의사결정권은 CISO에게 있는 것이고, 예산 요청에 관한 최종 의사결정권은 CFO에게 있기 때문이다. 다만 그렇다고 하더라도 이와 같은 방식을 적용해야 하는 이유는 기업의 전 구성원으로 하여금 정보보안을 '비용의 관점'이 아니라 '생존의 관점'으로 보도록 하기 위함이다.

2) 판례

주지하다시피 우리나라에서는 개인정보 유출사건이 매우 많이 발생하고 있으며, 이러한 현상은 개인정보 보호법과 정보통신망법이 강화된 이후에도 지속적으로 나타나고 있다. 다만 현시점에서 불행 중 다행인 점은 과거에 발생했던 개인정보 유출사건에 대한 법원의 판단이 나오고 있다는 점이다. 이러한 법원의 판단 즉, 개인정보 유출사건에 대한 판례는 CISO가 의사결정을 하는데 매우 중요한 활용해야 할 기준임과 동시에 정보보호 예산을 확보하고 투자를 얻어 내는데 활용할 수 있는 자료이기도 하다. 특히 정보보호 예산확보 과정에서 활용할 수 있는 판례를 소개하면 다음과 같다.

2012년 발생한 KT 개인정보 유출사건에 대해 2018년 1월 19일 서울중앙지방법원 민사항소4부는 '정보보호 규정 지켰다면, 회사 책임 없다'는 판결을 하였다. 이 판결에 내재 된 함의는 두 가지가 있다. 첫 번째, 정보보호 규정을 지켰다면 회사는 관리·감독상의 부주의가 없다는 의미이다. 두 번째, 정보보호 규정을 지키지 않았다면 회사는 관리·감독상의 부주의가 있다는 의미이다. 따라서 CISO는 이 두 번째 의미를 지혜롭게 활용할 필요가 있다. 예를 들어 정보보호 규정에 연간 정보보호 예산의 비율을 규정해 놓는다든지 아니면 CISO가 요청한 예산에 대해 CFO가 협조하도록 규정을 해 놓는 것이다.

2008년 발생한 오픈마켓 사이트 개인정보 유출사건에 대해 2018년 1월 25일 대법원은 '관리적·기술적 보호조치에 관한 고시를 준수하였다고 하더라도 사회 통념상 합리적으로 기대 가능한 보호조치를 취하지 않았다면 주의의무를 다하지 않았다고 인정할 수 있다'고 판결을 하였다. 특히 이 판결은 새롭게 식별된 위협에 대응하기 위한 정보보호 예산이 필요한 경우에 활용할 수 있는 판례이다. 즉, 정기적 또는 필요적으로 수행한 위험평가의 결과로 새로운 위협이 식별되었고 이 위협에 대응하기 위해서는 추가적인 시스템이나 인력이 필요한 경우에 CISO는 '사회통념상 합리적으로 기대 가능한 보호조치'를 위하여 정보보호 예산을 요청할 수 있다는 것이다.

2015년 발생한 뽐뿌 개인정보 유출사건에 대해 2018년 4월 14일 서울행정법원 행정14부에서는 '비용 절감 때문에 개인정보보호 조치를 다 하지 않았다면 이는 매우 중대한 위반에 해당한다'고 판결하였다. 즉 비용 절감을 위해 개인정보보호를 위한 관리적·기술적 보호조치를 다하지 않은 것은 방송통신위원회 과징금 산정 기준 중에 '매우 중대한 위반'에 해당한다는 것이다. 이러한 판결은 CISO가 기업 내 전체 예산 중에서 정보보호 특히 개인정보보호에 필요한 예산을 확보하는데 직접적으로 활용 가능한 판례라고 할 수 있다.

5. 정보보호 교육 방안; 직원의 생각을 바꾸게 하는 기법들

기업 구성원을 대상으로 하는 정보보호 교육은 정보보호 인식 제고를 위해서 반드시 적용해야 하는 단계적 조치이다. 물론 정보보호 교육은 현재까지 많은 기업에서 적용하고 있는 보안 조치 중 하나이다. 다만, 연간 정보보안 교육 일정에 따라 단순히 내용을 전달하는 교육을 해서는 안 된다. 즉, 정보보호 교육을 통해서 구성원들의 저항을 최소화하면서 정보보호 인식의 수준을 높일 수 있는 교육을 해야만 하는 것이다. 이를 위해서 정보보호 교육에 적용해 볼 수 있는 여러 기법을 공유하고자 한다.

(1) 단계적 조치; 강사의 관점부터 전환해야!

1) '의무'가 아닌 '의미' 있는 시간

기업의 내 정보보안 부서에서는 구성원들을 대상으로 매년 연간 정보보호 교육 일정을 수립하여 일정에 따라 정보보호 교육을 실행하고 있을 것이다. 그렇다 보니 대한민국에서 직장 생활을 하는 직장인이라면 현재까지 최소 1회 이상의 정보보호 교육을 들어본 적이 있을 것이다. 혹시 이들에게 지금까지 들었던 정보보호 교육이 효과가 있었는지에 대해 물어 본 적이 있는가? 아니면 정보보안 부서 입장에서 정보보호 교육의 효과가 있다고 보는가? 아마 두 질문에 대한 대답은 부정적인 대답으로 나올 확률이 더 높다. 이 말에 내포된 의미는 바로 지금까지의 정보보호 교육이 효과가 없었다는 의미이다. 그렇다면 정보보안 부서에서는 그렇게 많은 시간 동안 매년 반복적으로 정보보호 교육을 실행하고 구성원은 매년 반복적으로 정보보호 교육을 들어 왔음에도 불구하고 정보보호 교육이 목적하고 있는 효과가 없는 이유는 무엇일까? 그 이유에 대해서 필자는 '강사가 구성원의 생각을 바꾸게 하는 정보보호 교육'을 하지 못했기 때문이라고 판단하고 있다. 이러한 판단에 근거하여 보면, 결국 정보보호 교육의 성패는 강사의 통찰력에 좌우된다고 할 수 있다.

① 전달보다는 해석을!

현재와 같이 정보기반의 스마트 사회에서는 기업 구성원들이 고객의 정보를 보호해야 할 의무가 있는 '사용자'임과 동시에 다른 회사 서비스의 '이용자'이기도 하다. 이에 비추어 볼 때, 현재의 정보보호 교육은 기업 구성원이 '의무'적으로 참석해야 하는 교육이 아니라 기업 구성원들에게 '의미'있는 교육이어야 한다. 그렇기 때문에 정보보호 교육이 기업의 정보보안 정책의 내용을 전달하는데 급급할 것이 아니라 정책 내용을 해석해서 이해시키는 방식으로 진행되어야 한다. 이를

위해서는 교육용 PPT에는 정보보안 정책 내용을 기재해 두고, 실제로 교육 시에는 기재된 내용 그 자체를 설명하는데 시간을 활용할 것이 아니라 이러한 내용의 취지와 준수 방법 그리고 준수 시의 좋은 결과, 미준수 시의 나쁜 결과 등에 대해서 중점적으로 교육을 할 필요가 있다.

② 현상보다는 원인을!

앞서 살펴본 바와 같이 보안 통제는 현상이 아니라 원인에 집중하여 적용해야 한다. 이러한 매커니즘은 정보보호 교육에도 그대로 대입할 수 있다. 즉, 특정한 정보보안 정책을 교육하는 PPT 슬라이드에서는 이 정책을 위반한 사례를 교육 소재로 활용하고 당시 정책을 위반한 구체적인 원인을 함께 소개하는 것이 정보보안 정책 준수에 더 효과적인 방법이 될 수 있다. 예를 들어, '문서 방치 금지'라는 정보보안 정책을 기재한 슬라이드에서는 이러한 행위를 금지하는 취지와 준수 방법 등에 대해 설명함과 동시에 이를 위반한 사례의 구체적인 원인(예: 책상 위치, 가상화폐거래소 예약기능 등)을 공유하는 것이다. 물론 이러한 구체적인 원인별로 어떠한 보안 통제가 적용되었는지도 함께 공유하여 유사한 행위를 미연에 방지하는 데 활용해야 한다.

③ 지점/지사 방문 시 사례 활용

정보보안 부서의 업무 중에서는 본사 이외에 지점이나 지사에 방문하여 업무 처리를 해야 하는 경우가 있는데, 이때 간혹 정보보안 정책 위반 사례(예: 문서 방치, PC 미종료, 비밀번호 부착, 화면보호기 미설정 등)를 목격하게 된다. 이러한 사례는 정보보호 교육 시에 매우 중요한 교육 소재가 된다. 예를 들어 A라는 지점의 구성원을 대상으로 정보보호 교육을 실행하는 과정에서 비밀번호 관리에 관한 정책을 교육할 차례가 되었다고 가정을 해 보자. 이때 과거에 A 지점을 방문했을 때 정보보안 부서 직원이 목격하였던 '비밀번호 부착' 사례를 제시하고 재발 방지를 A 지점의 지점장에게 공개적으로 요청한다면 이 지점의 정보보안 정책 준수율은 상당히 높아질 것이다.

2) 직장 생활 그 자체가 보안교육

① 가능한 한 높은 직급자가 정보보호 교육

최근 들어서는 직급을 없애고 평준화된 체계로 된 기업도 존재하고 있기는 하지만, 일반적으로 볼 때 직장 생활에는 직급체계가 존재하고 있다. 이러한 직급체계는 비단 업무 과정에서만 가동되는 것이 아니라 정보보호 교육 과정에서도 상당히 좋은 기능으로 가동될 수가 있다. 예를 들어서 매월

신규입사자를 대상으로 CISO가 직접 정보보호 교육을 한다면 정보보호의 중요도 인식에 좋은 영향을 끼치는 선순환적 효과를 얻을 수 있다. 반대의 경우를 생각해 보면 이러한 선순환적 효과를 더욱 극명하게 이해할 수 있을 것이다. 즉, 팀장급 이상이 모여 있는 교육 장소에서 정보보안 부서의 사원급 직원이 정보보호 교육을 하는 상황을 상상해 보라. 정보보안 부서의 사원급 직원은 교육 자체를 부담스러워 할 것이고, 교육을 듣는 팀장급 직원들은 교육에 집중하지 않게 될 것이다. 이와 같은 상황을 고려하여 정보보호 교육을 실행할 때는 가능한 한 교육을 듣는 직원들보다 높은 직급자가 실행하는 것이 효과적이라고 할 수 있다.

② 컴플라이언스 목적보다는 직원의 안전을 강조하는 정보보호 교육

보안이 법률화된 현시점에서 보안 관련 법령/지침의 중요성은 아무리 강조해도 지나치지 않다. 특히 보안의 법률화로 인해 정보보안 부서 직원뿐만 아니라 기업의 모든 구성원도 보안 컴플라이언스 의무를 이행하여야 한다. 그럼에도 불구하고, 정보보호 교육 시에는 보안 컴플라이언스만 강조하는 것은 좋은 정보보호 교육이라고 할 수 없다. 이보다는 직원들이 안전하게 컴플라이언스 의무를 이행할 수 있는 방법을 강조하는 것이 훨씬 더 효과적인 정보보호 교육이 될 수 있다. 예를 들어서, 랜섬웨어 악성코드가 포함된 이메일의 첨부파일을 클릭한 경우 부담해야 하는 법적 책임에 대한 내용 보다는, 이러한 이메일의 선별방법과 신고 채널을 알려 주는 정보보호 교육을 해야 한다는 것이다. 이러한 관점에서 정보보호 교육을 들은 구성원은 정보보안 부서의 업무영역에 대한 이해가 높아질 뿐만 아니라 정보보안 부서가 실행하는 보안 통제의 필요성과 중요성에 대한 이해도 높아질 수 있다.

③ 일상을 파고드는 정보보호 교육

정보보호 교육을 한다고 하면 일반적으로는 연간 교육일정표에 따라 교육을 실행할 것이고 그 이후에는 특별한 이슈가 없는 한 공식적인 정보보호 교육은 거의 하지 않는 것이 직장 생활 간의 모습일 것이다. 그렇지만 직장 내 일상에서도 정보보호 교육을 할 수 있는 기회가 상당히 많이 있다. 예를 들어서 휴게실이나 엘리베이터에서 어떤 직원이 CISO에게 정보보안 체계와 관련된 문의를 해 왔다고 가정을 해 보자. 이러한 상황에서는 정보보안 정책의 범위 내에서 문의한 사항에 대한 대답을 해 주게 될 것이다. 물론 문의한 직원의 입장에서도 문의에 대한 대답을 들은 것이므로 대화는 여기서 마무리 될 것이다. 하지만 필자는 여기서 한 걸음만 더 나아가 보기를 권하고 싶다. 한 걸음의 예를 들면, 문의를 했던 직원에게 이메일을 보내는 것이다. 즉, 직원이 문의했던 내용과

이에 대한 CISO의 대답 그리고 대답의 근거(예: 법령이나 정책 등)와 함께 문의해 준 것에 대한 감사의 내용을 적어 이메일을 보내는 것이다. 이렇게 한다면, 이메일을 수신한 직원은 자신이 소속되어 있는 부서 내에서 정보보안 부서를 도와주는 직원이 될 가능성이 높아진다. 뿐만 아니라 이 직원은 정보보안 부서에게 자신과 비슷한 문의를 하려고 하는 다른 직원에게 자신이 수신한 메일의 내용을 근거로 해당 문의에 대한 상세한 설명을 대신해 주기도 한다. 필자의 경험에 비추어 볼 때, 직원들의 정보보호 인식 수준을 높이는데 이런 방법만큼 좋은 방법은 없다고 생각된다.

(2) 단계적 조치; 인식전환장치 발굴

정보보호 교육의 성공적인 요인은 정보보호 교육을 듣는 '구성원들의 생각에 변화를 유발시켰느냐'이다. 그렇기 때문에 구성원들이 기업의 정보보안 체계에 대해 가지고 있는 기존의 부정적인 생각에서 긍정적인 생각으로 바뀌게 하는 것이 정보보호 교육의 목적이 되어야 한다. 이를 위해서는 정보보호에 깊은 통찰력(Insight)을 가지고 있는 좋은 강사와 완성도 높은 강의 교안이 필요할 뿐만 아니라 정보보호 교육 시에 활용할 수 있는 '인식전환장치'를 발굴해 놓을 필요가 있다. 여기서 말하는 인식전환장치란 뉴스 기사나 역사적 사건을 토대로 구성원들의 생각의 스위치를 자극시킬 수 있는 이슈를 말하는 것이다. 이러한 이슈에 대한 예시를 들어 보면 다음과 같다.

1) 다른 관점, 다른 결과

어느 초등학교 앞에 굉장히 낡은 육교가 하나 있었는데, 너무 낡아서 계단이 허물어지기도 하고 육교의 다리 위에는 아래를 지나가는 자동차가 보일 정도로 구멍도 나 있었다. 이 육교에 대해서 일부 초등학교 학부모는 관할구청에 '계단을 오르내려야 하는 불편함'이 있는 육교를 허물고 편리하게 건너갈 수 있는 횡단보도를 설치해 달라는 민원을 제기하였다. 그런데 며칠 뒤에 다른 학부모들이 관할구청에 이 육교를 허물지 말고 유지해 달라는 민원을 제기하였다. 이 학부모들의 생각은 '비록 육교가 계단을 오르내려야 하는 불편함은 있지만, 초등학교 아이들에게는 횡단보도보다 안전한 수단'이라는 생각을 했던 것이다. 이에 대해 관할구청은 횡단보도 설치가 아니라 기존의 육교를 보다 깨끗하고 튼튼하게 보수했다는 기사를 본 적이 있다. 이 기사의 요지는 관점에 따라 결과는 완전히 달라진다는 것이다. 그리고 이 기사에서 얻을 수 있는 통찰력은 '안전함이 담보되지 않는 편리함만큼 위험한 것은 없다'는 것이다.

2) 감성자극

역사적으로 잘못된 것에 대한 감성을 자극하는 것도 정보보호 인식의 수준을 높이는 데 활용할 수 있는 좋은 장치이다. 대표적인 사례가 바로 '보행 방향'이다. 원래부터 우리나라는 1905년 고종황제 시절부터 우측통행을 실시하던 국가였는데, 일제 강점기에 좌측통행으로 바뀌게 되었다. 일제가 당시 우리나라의 보행 방향을 강제적으로 바꾼 이유는 자신들의 오랜 습성 때문이었다. 왜냐하면, 일본은 과거 사무라이들이 좌측 허리에 긴 칼을 차고 다녔는데, 이들이 우측통행을 하면 반대편으로 지나가는 사무라이의 칼과 칼이 부딪칠 가능성이 매우 높았다. 사무라이 세계에서 칼을 부딪친다는 의미는 도전의 의미이기 때문에 불필요한 살상을 미연에 방지하고자 일본은 사무라이 시대부터 좌측통행을 해 왔던 것이다.

이러한 역사적 내용을 인지한 후 우리 사회는 우측통행으로 보행 방향을 바꾸는 운동을 전개했다. 이처럼 오랜 기간 '좌측통행'을 해 오던 우리 사회가 '우측통행'을 시행하는 이유에 대해 설명하면, 좌측통행과 우측통행의 의미를 다시 한번 생각해 보게 된다는 것이다. 왜냐하면, 정보보호 교육을 들은 구성원들은 자신이 몰랐던 것에 대해 정보보호 교육을 통해서 새로운 사실을 알게 되는 것이기 때문이다. 새로운 사실을 몰랐다면 어쩔 수 없겠지만, 알았다면 새로운 사실에 대해 고민해보는 것이 인지상정이다. 이와 같은 인식전환장치를 활용한다면, 정보보호 교육을 듣기 이전에는 '당연히 편리해야 한다'는 생각만 했었지만, 정보보호 교육을 들은 이후에는 '그래도 안전해야 한다' 또는 최소한 '편리한 안전'에 대해 기업 구성원들에게 통찰력을 줄 수 있을 것이다.

(3) 단계적 조치; 메시지화

기업의 구성원들은 일 년에 한두 번 정도 즉, 한두 시간 정도 정보보호 교육을 듣게 된다. 기업 구성원의 입장에서는 이 시간을 통해서 자신들이 알아야 하고 준수해야 하는 정보보안 정책을 안내받게 되는 것이고, 정보보안 부서 입장에서는 이 시간을 최대한 활용하여 기업의 정보보안 체계를 강화하고 구성원들의 정보보호 인식 수준을 높이고 싶을 것이다. 그런데 문제는 정보보안 부서 입장에서는 교육시간이 너무 짧고, 반대로 기업 구성원의 입장에서는 전달받는 내용이 너무 많다는 것이다. 그러하다 보니 정보보호 교육의 효과가 기대에 미치지 못하는 문제가 있다. 이러한 문제를 해소하기 위해서 적용할 수 있는 방법으로는 '중요한 정보보안 정책에 힘을 실어 주는 짧은 메시지'를 활용해 볼 수 있다. 특히 반론의 여지가 없는 메시지를 작성하여 정보보호 교육시간에

활용해 볼 수 있다. 필자의 경우에는 다음과 같은 반론의 여지가 없는 간결한 메시지를 작성하여 정보보호 교육에 매번 활용하고 있다.

"고객의 정보는 고객의 것입니다!"
"정보보안은 분산화된 책임입니다!"
"브레이크가 고장 난 스포츠카는 속도를 자랑해서는 안 됩니다!"
"수익을 위한 투자가 필요하듯이 보안을 위한 비용도 필요합니다!"

필자가 이와 같은 메시지를 작성하여 정보보호 교육 시에 활용하는 가장 큰 이유는 간결한 메시지가 주는 파괴력이 있기 때문이다. 즉, 구성원의 입장에서 보면 짧은 시간 동안 많은 내용 전체를 기억할 수는 없지만, 교육 내용과 관련된 간결한 메시지는 기억할 수 있기 때문이다. 그리고 이렇게 구성원의 인식 속에 기억된 간결한 메시지는 향후 업무 과정에서 정보보안 체계에 대한 저항을 줄이는 효과로 이어질 수 있다.

(4) 단계적 조치; 실재하지만 인식하지 못했던 사실 제시

1) 정보보호 교육 효과가 좋지 않았던 이유

우리나라에서 직장 생활을 하는 거의 모든 구성원들은 정보보호 교육을 지속적으로 받아 오고 있다. 특히 개인정보 유출사건이 많아짐에 따라 정보보호 교육의 중요성은 더욱 커지고 있다. 뿐만 아니라 '정보보호 인증'의 요건과 통제항목에도 구성원을 대상으로 연간 일정한 시간 동안 정보보호 교육을 수행한 결과를 제시하도록 하고 있다. 그런데 이렇게 중요한 정보보호 교육임에도 불구하고 정보보호 교육의 효과는 생각보다 크지 않은 것이 사실이다. 심한 경우에는 정보보호 교육을 들은 구성원이 정보보안 체계에 대해 더욱 큰 저항을 하는 경우도 있다. 왜 이런 현상이 발생하는 것일까?

필자가 생각하는 가장 큰 이유는 '정보보호가 내 문제가 아니다'라고 생각하고 있던 구성원들이 정보보호 교육을 들은 이후 '정보보호가 내 문제구나!'라고 인식하도록 교육하지 못한 것이라고 본다. 한번 상상해 보자. 연간 정보보호 일정에 따라 바쁜 시간 중에 정보보호 교육을 수강하러 가는 구성원은 마치 남의 일처럼 느껴지는 정보보안 체계를 교육받는다고 생각하게 된다. 하지만 의미 있는 정보보호 교육이 되려면, 이러한 구성원들이 정보보호 교육을 이수한 이후에는 정보보안 체계를 유지하는 것이 구성원 스스로를 위하는 일이라는 것을 알게 해 주어야 한다. 이를 위해서

구성원이 누리고 있는 편리함의 이면에 존재하고 있는 실제의 위험함을 사실에 기반하여 제시한다면, '정보보호가 내 문제구나!'라고 인식시킬 수 있는 효과적인 교육방법이 될 수 있다고 생각한다.

2) 편리함 이면의 세계; 위험함

필자의 경험을 토대로 볼 때, 실제로 존재하고 있지만 구성원들이 인식하지 못하고 있는 위험한 사실을 정보보호 교육시간을 통해서 알려 주는 방법을 활용하면 매우 좋은 교육효과를 얻을 수 있다. 특히 내 문제가 아니라고 생각하는 순간 어느새 내 문제가 되어 버리는 정보보안에 대해 구성원들이 더 큰 경각심을 갖게 된다. 이러한 경각심을 고취시키는데 활용할 수 있는 몇 가지 소재를 소개하면 다음과 같다.

① 와이파이 그 이면의 위험함

필자가 지하철을 타고 있는데, 옆에 있던 어떤 모녀가 하는 대화를 우연히 들은 적이 있다. 그 대화 내용은 "엄마. 와이파이 안테나가 빵빵하니까 얼른 송금해!"라는 내용이었다. 즉, 와이파이 안테나가 잘 잡히는 지하철 구간에서 모바일 뱅킹을 하라는 것이었다. 물론 지하철 구간에서는 와이파이 사용이 무료이고 은행 업무를 모바일로 처리할 수 있다는 편리함의 관점에서 보면, 이 모녀의 대화가 무슨 문제가 있나 싶을 수도 있다.

그러나 이러한 편리함의 이면에는 위험함이 존재한다는 것을 정보보호 교육시간에 구성원들에게 알려 줄 필요가 있다. 여기서 말하는 '위험함'이란 바로 공짜 와이파이가 해킹에 매우 취약하다는 위험함이다. 만약 이 와이파이가 해킹되어 있다면, 마치 거미줄에 많은 곤충들이 걸려드는 것과 마찬가지로 이 와이파이로 정보를 보내는 모든 무선접속 신호가 노출될 수 있다. 따라서 정보보호 교육시간에는 구성원들에게 이러한 위험함을 알려 주면서 구성원 스스로의 안전을 위해서는 공짜 와이파이 존에서는 모바일 뱅킹을 자제하도록 인식시켜야 한다.

② 스마트폰 블루투스 그 이면의 위험함

빠르고 손쉬운 연결성의 측면에서 보면 스마트폰 블루투스는 최고의 편리성을 제공하는 기능이라고 할 수 있다. 이러한 블루투스 기능은 스마트폰 기기 간 정보의 연결은 당연하고, 헤드셋이나 키보드, 마우스, 스피커 심지어 게임패드와도 무선 연결이 가능하게 해 주는 편리함을 제공하고 있다.

그렇지만 이렇게 편리한 기능을 제공하는 스마트폰의 블루투스라고 하더라도 이 기능을 필요할 때만 사용해야 하는 것이지 이를 24시간 켜 두는 것은 매우 위험한 선택임을 정보보호 교육 시간에 구성원들에게 알게 해 주어야 한다. 필자의 경우에는 정보보호 교육 시간에 교육을 듣고 있는 구성원들에게 반드시 물어 보는 질문이 있다. 바로 "주무실 때 스마트폰 끄고 주무시는 분?'이라는 질문이다. 이 필자가 질문을 하면 대부분의 구성원들의 표정은 어이가 없다는 표정을 짓곤 한다. 이들이 어이가 없다는 표정을 짓는 이유는 '스마트폰으로 아침 기상을 위한 알람도 설정해 두어야 하고 인터넷도 검색해야 하고 음악도 들어야 한다는 등 여러 가지 용도로 사용하는데 왜 잠을 잘 때 스마트폰을 꺼야 하느냐'라는 생각에서 자신들도 모르게 나오는 표정일 것이다. 하지만, 블루투스가 켜져 있는 스마트폰을 통해서 도청을 하는 것은 정말 초급 수준의 해킹이라는 사실을 알려 주는 순간, 그리고 이러한 도청의 위험 때문에 일부 기업에서는 중요 전략회의 시 스마트폰을 소지하지 못하도록 한다는 사실을 알려 주는 순간, 구성원들의 얼굴에서 어이가 없다는 표정은 순식간에 사라지는 것을 필자는 잘 알고 있다. 이 때 필자는 "스마트폰을 끌 수 없다면 최소한 '블루투스'만이라도 끄세요!"라고 강조한다. 이러한 사실을 인식한 구성원은 최소한 스마트폰의 블루투스 보안은 자신의 안전과 사생활을 위해서 지켜야 하는 당연한 조치라고 인식하게 된다.

③ IP 카메라 그 이면의 위험함

한때 집 안에 IP 카메라를 설치하는 것이 유행처럼 번졌던 적이 있었다. 특히 집에서 반려동물을 기르고 있는 사람이라면 아마도 거의 대부분 IP 카메라를 집에 설치하여 반려동물을 관리하고 있을 것이다. 왜냐하면, 이러한 IP 카메라는 집 밖에서도 집 안의 모습을 실시간으로 볼 수 있다는 편리함이 있기 때문이다. 그래서일까? 필자가 정보보호 교육을 할 때 "집에 IP 카메라를 사용하고 있는 사람은 손들어 주세요"라고 요청하면 최소한 두 세 직원은 손을 들곤 했다.

그렇지만 이렇게 편리한 IP 카메라도 보안조치(예: 초기 아이디와 비밀번호 변경 등)를 하지 않는다면 해킹의 대상이 될 수 있다. 하지만 불행하게도 보안조치가 되어 있지 않은 많은 IP 카메라가 해킹을 당하여 집 안에 있는 피해자의 사생활이 침해되는 사건들이 발생하였다. 필자가 정보보호 교육시간에 강조하는 부분은 바로 '기본적인 보안조치'이다. 즉, IP 카메라를 구매했을 당시에 설정된 초기 아이디와 비밀번호를 구매자 자신만 알 수 있는 아이디와 비밀번호로 변경하기만 했었다면 이런 어이없는 피해를 입지는 않았을 것이라는 점을 강조하고 있다. 왜냐하면, 이러한 논리는 기업의 정보보안 체계의 유지/개선과도 맞닿아 있기 때문이다. 즉,

정보보안 부서에서 각 구성원 별로 업무용 컴퓨터에 대한 아이디와 패스워드 관리를 할 수 밖에 없는 이유를 굳이 설명하지 않더라도 이러한 IP 카메라 해킹 사건으로 업무용 컴퓨터에 사용하고 있는 아이디와 패스워드 보호의 중요성을 인식시킬 수 있기 때문이다.

④ Smart TV 그 이면의 위험함

Smart TV는 마치 스마트폰이나 컴퓨터와 마찬가지로 프로그램을 설치·실행할 수도 있고 인터넷과 SNS에 접속할 수도 있다. 또한 사용자 취향에 맞는 프로그램을 선별해 주기도 하고 기기 전면에 카메라가 내장되어 있어서 누군가와 영상통화를 하는 것도 가능하다.

그렇지만, 이렇게 편리한 기능이 탑재된 Smart TV는 기본적으로 와이파이나 인터넷을 이용하기 때문에 해킹의 대상이 될 위험이 상당히 높다. 특히 기기 전면에 내장된 카메라나 마이크를 통해 도청이나 사생활이 노출될 위험성은 더욱 높다고 할 수 있다. 필자는 이러한 사실을 정보보호 교육시간에 구성원들에게 인식시켜 주고 있는데, 그 후에는 '안전하게' Smart TV를 사용할 수 있는 방법에 대해 질문을 하는 구성원이 반드시 있다. 이 질문을 받으면 물론 안전하게 Smart TV를 활용할 수 있는 방법을 알려 주지만, 여기서 주목해야 하는 부분은 '편리하게' 사용하려고 구매한 Smart TV를 이제는 '안전하게' 사용하는 방법을 알고자 하는 욕구가 생겼다는 점이다. 이러한 현상들은 정보보호 교육을 듣고 있는 구성원들의 생각이 변화되고 있으며 최소한 정보보호 교육이 생각의 스위치를 자극하고 있다는 반증일 것이다.

⑤ SNS 그 이면의 위험함

최근에는 SNS를 통한 관계형성이 매우 성행하고 있으며, SNS를 이용하지 않는 사람이 거의 없다고 해도 과언이 아니다. 여기서 말하는 SNS란 계정만 가지고 있으면 누구나 볼 수 있는 공개형 SNS(예: 트위터나 페이스북 등)와 계정뿐만 아니라 가입한 사람만 볼 수 있는 폐쇄형 SNS(예: 카카오톡, 밴드 등)를 말하는 것이다. 이러한 SNS는 전 세계 어디에 있는 사람과도 공동의 관심사에 대한 관계 형성이 이루어질 수 있고, 형성된 관계를 통해 정보를 전송하는 속도도 매우 빠르다. 따라서 이러한 SNS의 기능은 소통을 추구하는 이용자에게는 엄청난 편리함을 제공하고 있다.

하지만 필자는 SNS가 아무리 편리하다고 하더라도 아직까지도 SNS를 사용하지 않는다. 왜냐하면, 정보보호와 디지털포렌식 그리고 법률을 전공한 필자가 판단해 보건대, SNS 공간은

사이버 범죄를 일으킬 수 있는 최적의 생태계를 갖추고 있기 때문이다. 그 근거로는 ⅰ) 전 세계 대다수가 이용하고 있다는 점(=공격 대상이 많다는 점) ⅱ) 주소 변경이 가능하다는 점(=공격자가 자신의 흔적을 숨길 수 있다는 점) ⅲ) 클릭을 쉽게 유도할 수 있다는 점(=피해자를 유인할 수 있다는 점) ⅳ) 무서운 속도(=지구 반대편까지 가는데 눈 깜짝할 속도) ⅴ) 사회공학에 취약하다는 점(=진위 여부를 확인할 방법이 없다는 점)을 들 수 있다. 그래서일까? 최근에는 SNS상에서 이성에서 환심을 산 뒤에 결혼이나 사업상의 이유를 들어 이성으로부터 금전적 이득을 취하는 로맨스 스캠(Romance Scam) 피해자들이 생기기도 했다. 필자가 정보보호 교육을 할 때는 이러한 내용을 구성원들에게 인식시킴과 동시에, 기업의 마케팅이나 홍보를 SNS상에서 하지 못하게 하고 특히 고객의 정보나 업무 정보를 SNS상에 올려서는 안 된다는 점을 반드시 강조하고 있다. 왜냐하면, SNS상에서 정보의 전파력이 워낙 크다 보니 이러한 SNS 채널을 통해서 마케팅이나 영업을 하고 싶어 하는 구성원이 반드시 있기 때문이다. 필자의 경험을 토대로 볼 때, 앞서 SNS의 위험성을 인식시킨 후 기업의 정보보안 정책상의 SNS 사용 금지규정을 설명하면 이에 대한 수용도가 상당히 높아질 것이다.

6. 보안문화 정착 방안; 지속적으로 관리 가능한 정량화 기법

정보보호 인식 제고의 단계를 간단하게 정리하자면, ⅰ) 인식과 현실의 접점을 제대로 식별하고 ⅱ) 인식의 수준을 높일 수 있는 조치를 단계적으로 적용해야 한다. 하지만 앞서 설명한 바와 같이 정보보호 인식은 사람의 생각 영역에 있는 것이므로 이를 강제화·자동화 할 수가 없다. 또한, 조직 내 여러 가지 변경 요인(예: 구성원의 변경, 업무 변경, 승진, 이직 등)에 의해서 정보보호 인식 수준은 언제든지 하향곡선을 그릴 수가 있다.

그러므로 정보보호 인식 제고의 마지막 단계는 ⅲ) 보안이 문화로 정착되는 단계여야 한다. 왜냐하면, '인식'은 개인의 영역이므로 언제든지 변화될 수 있지만, '문화'는 조직의 영역이므로 개인이 조직에 맞추게 되기 때문이다. 게다가 이러한 보안문화가 지속적으로 관리될 수 있고 정량화된 방식으로 유지/개선될 수 있도록 한다면, 정보보호 인식 제고가 언제든지 흔들릴 수 있는 개인의 생각 영역에 머물러 있지 않고 정량화가 가능한 조직의 관리영역으로 포섭시킬 수 있을 것이다.

(1) 유지/개선; 기회 활용

정보보호 인식 제고의 수준을 유지/개선하는 방법으로 '내·외부적인 기회'를 활용할 수 있다. 예를 들면 보안 인증을 취득해야 하는 상황이나 외부에서 발생한 보안사고 사례 전파 상황 그리고 정부가 주도하는 훈련이나 점검에 참여해야 하는 상황 등은 조직 구성원의 정보보호 인식의 수준을 유지하거나 개선하는 데 활용할 수 있는 좋은 기회가 될 수 있다. 이하에서는 이에 대해 상술하고자 한다.

1) 인증(ISMS-P / ISO27001 등)

정보통신망법에 의해 의무적으로 보안 인증을 취득하거나 유지해야 하는 기업의 경우에는 보안 인증을 위한 심사를 준비하는 시기와 인증심사가 완료된 후 사후조치를 하는 시기가 구성원들의 정보보호 인식 제고의 수준을 높일 수 있는 좋은 기회가 될 수 있다. 특히 의무적으로 보안 인증을 취득해야 하는 기업의 경우에는 '보안 인증의 취득 그 자체'가 경영진의 중요 관심사가 되기 때문에, 실무조직에서 정보보안 체계에 대해 저항을 할 수 있는 상황이 전혀 아니다. 따라서 이처럼 보안 인증 취득 준비 및 사후조치 시기는 '보안문화 구축의 교두보'를 확보할 수 있는 가장 좋은 기회이다.

또한 보안 인증을 취득하기 위해서는 수많은 통제항목의 요건을 충족해야만 한다는 것도 정보보호

인식의 수준을 높일 수 있는 좋은 기회가 된다. 왜냐하면, 평소에는 정보보안 체계에 대해 큰 관심이 없던 구성원들도 보안 인증 준비 및 사후조치 시기에는 통제항목의 요건을 충족시키는 데 참여 내지는 지원을 해야 하기 때문이다. 그리고 이러한 과정을 거치는 동안 인식과 현실의 접점이 자연스럽게 식별될 뿐만 아니라 이 접점의 수준도 상당 부분 높아지는 효과도 있다.

그리고 보안 인증심사에서는 '권고와 결함 사항'을 활용하는 것도 정보보안 체계를 강화하는 데 도움이 될 수 있다. 예를 들어 평소에 적용하고자 했던 보안 통제에 대한 구성원들의 저항이 커서 적용하지 못했던 경우, 이 보안 통제와 관련된 보안 인증 통제항목에 대해 '권고 또는 결함'을 받게 된다면 이에 대해서 사후조치 기간 내에 보안 통제를 적용하는 조치를 의무적으로 해야 할 것이다. 이러한 과정은 결국 특정한 보안 통제에 대한 저항을 극복할 수 있게 해 줄 뿐만 아니라 정보보호 인식의 수준을 개선할 수 있는 좋은 기회가 될 것이다.

2) 보안사고 사례 및 대응방안 전파

우리 주변에는 보안사고에 관한 많은 사례가 존재하고 있다. 예를 들면, 보안사고에 대한 언론 기사나 전문가 논평 그리고 수사결과와 판례 등이 그러하다. 이러한 사례들 중에 구성원들에게 공유할 필요가 있는 사례는 선별하여 전파하여야 정보보호 인식의 수준을 유지하는 데 도움이 된다. 다만 이러한 보안사고 사례를 전파하는 경우에는 기업의 정보보안 체계를 유지하는데 필요한 사례뿐만 아니라 구성원 스스로의 안전에 도움이 되는 사례도 선별하여 전파할 필요가 있다. 왜냐하면, 보안사고 사례에 대한 구성원의 관심을 유도함으로써 정보보호 인식의 수준을 높이는 계기가 될 수 있기 때문이다.

예를 들어서 랜섬웨어 보안사고 사례와 대응방안에 대해 전사 구성원에게 전파하는 경우에는 기업 내 업무용 컴퓨터와 시스템을 보호할 수 있는 대응방안뿐만 아니라 구성원이 자택에서 사용하는 개인용 컴퓨터와 스마트폰 등을 보호할 수 있는 방법도 함께 전파하는 것이다. 이처럼 보안사고 사례 전파 시에는 기업 관점에 대응수단뿐만 아니라 구성원 개인의 안전에 필요한 대응수단을 함께 기재하여 전파하는 방법을 지속적으로 활용한다면, 정보보호가 기업뿐만 아니라 구성원 개인의 안전과도 연결되어 있다는 사실을 구성원 스스로가 주지하게 될 것이다.

한편 보안사고 사례를 전사 구성원에게 전파하는 경우에는 전파하여야 할 내용을 가능한 한

간결하게 정리하여 전파하여야 한다. 왜냐하면, 내용이 너무 길거나 복잡하다면 구성원들이 전파받은 내용을 읽지 않는 경향이 있기 때문이다. 따라서 전파 내용 자체를 간결하게 기재하고 마지막에는 전체 내용을 아우를 수 있는 간결한 메시지(예: 안심하는 사람은 안전하지 않습니다!)로 마무리하는 것이 좋은 방법이 될 것이다.

3) 정부 주도 훈련/점검

매년 정부 기관에서는 사이버 공격에 대비하고 정보보안 체계의 강화를 위해 모의훈련과 보안 점검을 실시하고 있다. 민간 기업의 경우에도 이러한 모의훈련 내지는 점검에 참여할 수가 있는데, CISO는 이러한 훈련/점검에 참여하는 기회를 활용해 볼 필요가 있다. 특히 이러한 훈련은 실제 사이버 공격과 흡사한 방식으로 진행이 되기 때문에 사이버 공격의 위험성과 정보보안 체계의 필요성을 구성원에게 인식시킬 수 있는 아주 좋은 기회가 될 수 있다. 정보기관의 보안 점검도 마찬가지이다. CISO가 이러한 보안 점검을 신청하여 수검대상이 된다면, 일정기간 동안 보안 점검에 대비하는 정보보안 체계 정비와 강화 활동을 해야만 한다. 이러한 과정은 구성원들의 정보보호 인식의 수준이 자연스럽게 올릴 수 있는 기회가 될 것이다.

(2) 유지/개선; 공유, 공유, 공유

정보보호 인식이 수준은 사람마다, 업무마다, 시기마다 달라질 수 있다는 점을 이미 설명하였다. 이러한 점을 보완하기 위해서는 구성원들에게 정보보안 체계와 보안 통제의 목적과 방법 그리고 기대효과 등에 대해 지속적으로 공유하여야 한다. 필자가 생각할 때 정보보안 업무와 관련된 공유는 업무적 공유 방식(Out-bound)과 개인적 공유 방식(In-bound)이 있는데, 이에 대해 상술하면 다음과 같다.

1) 업무적 공유; Out-bound

업무적 공유는 전사 구성원을 대상으로 공유하는 방식을 말한다. 즉, 정보보안 부서가 화자(Speaker)가 되고 전사 구성원이 청자(Listener)가 되는 방식이다. 새로운 보안 정책 수립 및 시행을 공유하거나 보안 사고사례 공유하는 경우 등이 이에 해당한다고 할 수 있다. 이러한 경우에는 공유 채널을 단일화할 것이 아니라 다양한 채널(예: 그룹웨어, 이메일, 메신저, 보안교육 등)을

통해서 공유할 필요가 있다. 왜냐하면, 정보보안 공유사항에 대해 구성원들이 큰 관심이 없기 때문에 공유사항을 가능한 한 많이 노출하기 위함이다. 그리고 만약 전사 구성원들의 업무에 관련이 많거나 구성원들이 관심을 갖고 있는 공유사항에 대해서는 공청회 등의 방식으로 공유하는 것이 좋다. 왜냐하면, 이러한 과정을 거치면서 향후에 나타나게 될 저항을 미리 줄여 놓을 수가 있기 때문이다.

그리고 공청회 등에서 공유해야 할 사항이 다수인 경우는 저항이 큰 보안 통제부터 먼저 공유하는 것이 유리하다. 왜냐하면, 앞선 보안 통제에 비해 저항이 작은 보안 통제는 비교적 쉽게 수용을 하기 때문이다. 그리고 이 자리에서는 여러 명의 구성원이 새롭게 시행 예정인 보안 통제에 대해 저항을 하는 경우는 가장 큰 저항을 하는 구성원을 먼저 설득하는 것이 현명한 방법이다. 필자의 경험을 토대로 볼 때, 가장 큰 저항을 하는 구성원을 공개적으로 설득하면 나중에 가장 큰 조력자가 되기도 한다.

한편 정보보안 부서에서 업무적 공유를 하는 경우를 보면 일반적으로 새로운 보안 통제를 적용하기 전 단계에서 공유를 하고, 그 이후에는 이에 대한 업무적 공유를 잘 하지 않는다. 하지만, 업무적 공유는 정보보안 부서가 제공하는 하나의 서비스라고 생각하여, 새로운 보안 통제의 적용 '전 단계'뿐만 아니라 적용되는 '과정' 그리고 적용이 '완료된 시점'에서도 공유할 필요가 있다. 왜냐하면, 이러한 과정을 통해서 구성원에게 정보보안 체계에 동참하고 있다는 사실을 인식시킬 수 있기 때문이다.

2) 개인적 공유; In-bound

전사 구성원을 대상으로 하는 업무적 공유와 달리 개인적 공유는 특정 조직이나 특정 구성원과 관련된 개별적인 보안 이슈를 공유하는 것이다. 일반적으로 보면, 이러한 경우에는 특정 조직이나 구성원이 정보보안 부서로 보안 이슈를 문의해 오는 경우라고 할 수 있다. 그리고 이처럼 보안 이슈를 문의해 오는 조직이나 구성원은 이미 정보보안 부서의 고유한 업무를 인정하고 정보보호 체계의 필요성을 이해하고 있을 가능성이 높다. 따라서 이러한 조직이나 구성원이 문의하는 보안 이슈에 대해서는 보안 정책에 기록되어 있는 '통제기준'만을 설명할 것이 아니라 보안 정책을 위반하지 않으면서도 '안전하게 해결할 수 있는 방법'을 함께 찾아 줄 필요가 있다. 그리고 안전한 방법을 찾은 이후에도 해당 조직이나 구성원에게 연락하여 추가적인 이슈가 없는지 확인해 보아야 한다. 왜냐하면, 안전한 방법이라고 하더라도 기존에 없었던 해결방법이라면 그로 인해 새로운 보안 이슈가

생길 수도 있기 때문이다. 이러한 과정을 통해서 정보보안 부서가 통제만을 하는 부서가 아니라 실무부서와 함께 문제를 해결해 주는 부서라는 인식을 심어 줄 수 있다.

(3) 유지/개선; 객관적 지표의 수립 및 활용

미국의 경영학자 피터 드러커(Peter Ferdinand Drucker)는 "측정할 수 있으면 관리할 수 있고, 관리할 수 있으면 개선할 수 있다"고 말한다. 이러한 관점에 비추어 볼 때, 정보보호 인식의 수준을 지속적으로 유지/개선하는 많은 방법들이 있지만 정보보호 인식의 수준을 정량적으로 지표화할 수 있다면 다른 방법들에 비해서 더 효과적인 방법이 될 수 있을 것이다. 따라서 이하에서는 정보보호 인식의 수준을 지표화 할 수 있는 방안에 대해 설명하고자 한다.

1) 보안지표 수립기준

정보보호 인식은 사람의 생각 영역에 존재하고 있다. 이를 지표화한다는 것은 사실 쉽지는 않다. 하지만, 상세한 자료와 기술적 수단을 활용한다면 사람의 생각 영역에 있는 정보보호 인식의 수준을 정량적인 지표로 만들어 낼 수 있다. 왜냐하면, 사람은 생각하는 대로 행동하기 때문이다. 그래서 객관적으로 드러난 행동 내지는 행동의 결과를 기반으로 생각을 정량화할 수 있는 것이다.

① 현실적인 보안지표의 수집

이를 위해서는 먼저 현실적으로 수집 가능한 보안지표를 일정기간 동안 수집해야 한다. 여기서 말하는 보안지표란 생각 영역에 해당하는 '보안 인식 지표'와 생각한 대로 행동한 결과인 '보안 준수 지표'를 말한다. 보안 인식 지표의 예로는 보안교육 이수 여부, 보안 신고 건수, 개인적 공유 내용, 보안 가이드 요청 건수 등이다. 그리고 보안 준수 지표의 예로는 보안 정책 준수 건수, 보안 정책 위반 건수 등이다. 이러한 보안지표는 많으면 많을수록 객관적인 정량화가 가능하기 때문에 '보안 인식'과 '보안 준수'라는 카테고리로 나누어 많은 지표를 수집하는 것이 매우 중요하다. 필자의 경험에 비추어 볼 때, 지표의 다양성과 객관성을 유지하기 위하여 최소 1년 동안은 보안지표를 수집할 필요가 있다.

② 보안지표의 정량화 방식

보안지표를 수집하는 이유는 이를 수치화 즉, 정량화하기 위함이다. 현실적으로 수집 가능한 많은

보안지표를 정량화하는 방식은 '기본적으로 100점을 부여하는 방식'이다. 즉, 특정 시점(예; 연초 또는 입사 시 등)을 기준으로 100점을 부여하고, 특정 종점(예: 연말 또는 퇴사 시 등)까지 각 보안지표의 감점 요인과 가점 요인을 반영하여 수치화하는 방식이다. 이렇게 하면 생각 영역인 '보안 인식'과 행동 영역인 '보안 준수'를 점수로 산정할 수 있게 된다.

③ 보안지표 수집의 대상

보안지표를 수집하는 경우에는 구성원들만을 대상으로 하는 것이 아니라 전사의 모든 조직도 수집대상에 포함해야 한다. 즉, 구성원 개인의 인식과 행동뿐만 아니라 조직의 인식과 행동도 보안 관점에서 지표화해야 한다는 것이다. 따라서 구성원 개인의 '보안 인식' 및 '보안 준수'를 지표화함과 동시에, 이 구성원이 소속된 조직의 계층적 편제(예: 실, 본부, 팀, 파트 등)에 따라 각 조직 별 모든 구성원들에 대한 '보안 인식' 및 '보안 준수' 지표의 합계를 정량적으로 수치화해야 한다는 것이다.

2) 주기적인 누적관리

① 보안지표의 적용

보안지표 수집대상이 정해지고 각 수집대상에 대한 보안지표가 수집되고 나면, 특정 시점부터는 보안지표를 적용해야 한다. 즉, 특정 시점을 기준으로 하여 모든 대상(예: 구성원 개인 및 조직)에게 기본적으로 100점을 부여한 후 각 보안지표의 감점 요인과 가점 요인을 반영하는 것이다. 전사 구성원과 조직을 대상으로 보안지표를 효과적으로 적용하기 위해서는 기업 자체적으로 시스템을 구축하는 등 자동화 방식으로 적용하는 것이 가장 좋겠으나, 여력이 되지 않는 경우에는 보안지표 수집대상별로 엑셀 시트에 기본적으로 100점을 부여한 후 '보안 인식'과 '보안 준수' 지표에 감점 및 가점 요인 발생 시 이를 수치로 반영하는 방식으로 적용할 수 있다.

② 보안지표 현황 공유

특정 시점부터 보안지표를 적용하기 시작하면 최소한 부서장을 대상으로 각 부서의 보안지표의 현황을 주기적으로 공유하여야 한다. 예를 들면 분기 내지는 반기 단위로 부서의 구성원 각각의 보안지표 점수와 부서 전체의 보안지표 점수를 해당 부서장에게 공유하는 것이다. 이렇게 하면 부서장의 입장에서는 자신이 관리하는 부서의 보안 인식 수준에 대해 중간점검을 할 수 있게 되고 남은기간 동안 부서 내 보안 인식 수준을 높이고자 하는 관리적인 노력을 기울이게 될 것이다.

3) 보안지표의 전사 공개

① 부서별/개인별 순위화

예를 들어 연초부터 연말처럼 특정 시점에서부터 특정 종점까지 정량화된 최종 결과는 점수로 도출되기 때문에 이 점수를 기반으로 부서별 그리고 구성원 개인별 순위를 정할 수 있다. 즉, A 부서의 점수가 99점이며 이 점수는 전사 부서 점수순위에서 1위이며, 홍길동 직원의 점수가 95점이며 이 점수는 A 부서에서는 4위이고 기업 전체에서는 26위가 된다는 방식으로 점수를 산정하고 부서별/개인별로 순위화 할 수가 있다.

② 연간 보안지표 및 순위는 CEO 보고

일정기간 동안 집계된 보안지표와 순위는 반드시 CEO에게 보고하여야 한다. 왜냐하면, 보안지표의 수집대상에는 CEO도 포함되어 있기 때문에 CEO 스스로의 경각심을 높일 수 있을 뿐만 아니라 보안지표의 순위의 중요성을 기업 전 구성원에게 인식시킬 수 있기 때문이다.

③ 순위에 상응하는 보상과 보완 방안 적용

보안지표의 순위가 집계되면, 상위 순위에 상응하는 보상 및 하위 순위를 보완할 수 있는 방안을 적용해야 한다. 필자의 경험으로 볼 때, 개인 KPI 및 인사제도와 연계하는 방안이 가장 좋은 보상 및 보완방안이라고 생각된다. 예를 들어 보안지표 90점 이상의 경우에는 부서장이 해당 구성원에 개인 KPI에 가점을 부여하도록 하고, 보안지표 70점 미만인 경우에는 차년도 승진대상에서 제외하는 방식을 적용하는 것이다. 이는 정량화된 수치를 기반으로 인사관리를 할 수 있게 해 주기 때문에 KPI를 평가하는 부서장뿐만 아니라 인사부서에서도 상당히 선호하는 보상 및 보완방안이 될 것으로 생각된다.

④ 매년 보안지표 기준의 합리성 검토

한번 수립된 보안지표 기준을 조정하지 않고 매년 동일하게 적용할 수는 없다. 왜냐하면, 시간이 흐름에 따라 조직의 업무와 구성원 그리고 보안 정책 등에 변화가 생기기 때문이다. 따라서 보안지표의 기준에 대해서는 매년 합리성 여부를 검토하여야 한다. 그리고 이와 같은 합리성 검토의 결과 수정된 보안지표의 기준은 전사 구성원을 대상으로 공유하여야 보안지표에 대한 저항을 최소화할 수 있을 것이다. 그리고 이와 같은 과정을 거치면서 더욱 객관적인 보안지표의 기준이 수립될 것이며, 이러한 기준을 기반으로 적용되는 보안지표는 보안문화 형성의 필수 자원으로 활용될 수 있을 것이다.

7. 에필로그

(1) 정보보호 인식의 한계

지금까지 정보보호 인식 수준의 제고를 위해서 인식과 현실을 식별하고 이를 기반으로 다양한 단계적 조치를 적용하고 최종적으로는 보안을 문화로 만드는 단계까지 살펴보았다. "문화(Culture)는 전략(Strategy)을 잡아 먹는다"고 말한 피터 드러커(Peter Ferdinand Drucker)의 말처럼, 정보보호 인식을 높이기 위한 단계적 조치보다는 보안을 하나의 문화로 만드는 것이 보다 효과적인 정보보호 인식 제고 방안일 것이다.

그렇지만 '정보보호 인식'에도 어쩔 수 없는 한계가 있는데, 이하에서는 이에 대해 상술하고자 한다.

1) '다름의 현상' 발생; 사람, 환경, 시기

정보보호 인식의 수준은 여러 가지 요인에 의해 다르게 된다. 예를 들면 같은 부서라 하더라도 구성원마다 정보보호 인식의 수준이 다르고, 업무를 수행하는 환경에 따라 그리고 시기에 따라서도 정보보호 인식의 수준은 매번 다르게 된다. 이와 같은 '다름의 현상'은 정보보호 인식이 결국 사람의 생각 영역에 해당하기 때문에 나타나는 현상으로 보인다.

2) 자동화 불가능; 사람의 생각 영역

사람의 생각 영역에 있는 정보보호 인식의 두 번째 한계는 바로 '자동화가 불가능하다'는 것이다. 업무용 컴퓨터나 서버 등에 대해서는 보안시스템에서 정책을 적용하여 자동으로 보안환경을 설정할 수 있음에 반해 사람의 생각은 자동화 내지는 강제화가 불가능할 수밖에 없다. 그러하다 보니 정보보호 인식 제고가 정보보안 관점에서는 중요하면서도 실현하기는 어려운 난제로 분류되고 있는 것이다.

3) 환경 영향: 편리함으로의 쉬운 회귀

정보보호 인식만큼 환경의 영향을 크게 받는 영역도 없을 것이다. 특히 편리함으로 회귀하고자 하는 관성의 힘이 매우 크게 작용하는 것이 정보보호 인식의 세 번째 한계이다. 예를 들어서 정보보안 부서의 지속적이고 단계적인 노력의 결과로 어느 부서의 정보보호 인식의 수준이 상당히 높아졌다고 가정을 해 보자. 이제 이 부서는 업무 과정에서 보안 프로세스를 자연스럽게 수용하고 업무에

반영하게 될 것이다. 그러던 중에 이 부서에 새로운 경력직 직원이 입사 한 후, 자신이 다녔던 회사의 보안수준에 비해 이 부서의 보안수준이 불편할 정도로 높다고 불평을 한다면? 이 불평은 정보보호 인식의 수준을 한순간에 무너뜨리는 불평이 될 수가 있다는 것이다. 왜냐하면, 사람이라면 누구나 편리한 방식을 추구하기 때문이다.

4) '이용자 견인력'에 취약

정보보안 관점에 볼 때, 사용자는 기업의 직원이고 이용자는 고객이 된다. 따라서 직원이 사용자 입장에 서 있을 때는 기업의 정보보안 체계를 준수하고 정보보호 인식의 수준도 높아지게 된다. 하지만 이용자 즉 고객이 정보보안 체계에 대해 불편함과 불평을 호소하는 경우에는 직원의 정보보호 인식 방향이 다시 하향곡선을 그리게 된다. 예를 들어서 안전한 비밀번호 정책에 따라 비밀번호를 복잡하게 만들어서 사용하고 있는 직원이 고객으로부터 '고객용 비밀번호를 너무 복잡하게 만들게 되어 있어서 불편하다'는 말을 듣는다면, 이 직원은 자신의 업무용 컴퓨터 등에 적용하고 있는 비밀번호도 불필요할 정도로 복잡한 것이 아닌가 하고 생각하게 된다는 것이다. 결국, 이런 생각은 또다시 관리적 보안에 대한 저항으로 이어질 수가 있다.

(2) 정보보호 인식 한계의 보완방안

앞서 살펴본 바와 같이 정보보호 인식에 내재 된 불가피한 한계가 있다는 점은 인정할 수밖에 없다. 그럼에도 불구하고, 정보보안 체계를 유지하고 개선해야 하는 CISO 입장에서는 이러한 한계를 극복하거나 최소한 보완할 수 있는 방안을 활용하여 정보보호 인식의 수준을 반드시 관리하여야 한다. 이러한 보완방안으로는 기술적 수단을 활용하는 방안뿐만 아니라 관리적 절차를 활용하는 방안 등이 있는데, 이하에서는 이에 대해 상술하고자 한다.

1) 지속적인 모니터링과 행동 분석

일반적으로 사람은 생각하는 대로 행동하는데, 기업에서는 구성원의 행동을 확인할 수 있는 몇 가지 시스템이 있다. 예를 들면 네트워크접근제어(NAC) 시스템이나 정보유출방지(DLP) 시스템 또는 방화벽(F/W) 등이 있다. 물론 이러한 시스템은 기본적으로 기업의 정보보안 체계를 유지하기 위하여 운용되는 시스템이긴 하나, 이러한 시스템에는 구성원의 행동을 확인할 수 있는

간접지표(예: 접속 로그, PC 전원 미종료 시간, 악성코드 감염 현황 등)가 매일 누적되고 있다. 이와 같은 간접지표를 활용하여 '보안 인식' 지표와 '보안 준수' 지표의 점수를 가감하는 방식으로 구성원의 정보보호 인식을 지속적으로 모니터링해야 한다. 그리고 이러한 간접지표를 모니터링하다 보면, 보안지표 점수를 가감하는 상황을 벗어나서 내부적인 보안 위협의 상황이 관찰될 수도 있다. 이와 같은 경우 보안시스템에 누적된 여러 간접지표를 활용하여 해당 구성원의 업무 방식과 행동을 분석해야 하고, 필요한 경우에는 보안감사로 전환해야 하는 경우도 있다.

2) 주기적인 보안 인식 평가

사람의 생각은 언제든지 변화할 수 있다는 전제하에 구성원들의 정보보호 인식에 대해서는 주기적으로 평가를 해 보아야 한다. 예를 들면, 부서장급 이상에게 분기 내지는 반기마다 공유하는 부서별 보안지표 현황을 통해서 평가할 수도 있다. 또한, 앞서 본 것처럼 보안시스템 내에 누적되어있는 간접지표를 통해서도 평가할 수 있으며, 보안 점검의 결과나 정보보안 체계에 대한 불만 제기 등을 통해서도 평가할 수 있다. 따라서 CISO는 보안지표 평가, 간접지표 평가, 보안 점검, 보안 불만 내용 집계 등의 과정을 통해서 구성원들의 정보보호 인식을 주기적으로 평가하여야 한다.

3) 의사결정과정에서 보안 철학 확립

정보보호 인식의 수준을 일정한 수준으로 유지한다는 것은 쉬운 일은 아니지만, 의사결정과정에 '정보보안 상의 이슈'를 반드시 고려하도록 한다면 최소한 의사결정을 거치는 사안에 대해서는 일정한 수준의 정보보호 인식을 유지 수 있다. 예를 들어 부서장 이상의 직급자가 주어진 권한 내에서 의사결정 즉, 결재를 하는 경우에는 결재 대상 사안에 대해서 반드시 '정보보안 이슈'를 검토하도록 의사결정과정을 체계화하는 것이다. 이렇게 하면 부서장 결재 시에는 실무적인 관점에서 정보보안 이슈를 검토하게 되고, 차상급자를 거쳐 최종적으로 CEO가 결재를 하는 의사결정과정에서는 관리적인 관점에서 '정보보안 이슈'를 확인하게 되므로 체계화된 의사결정과정에서 정보보호 인식의 수준을 유지하는 데 도움이 될 수 있다.

4) 보안선언서(Security Statement) 활용

전사 구성원으로 하여금 정보보호에 대한 최소한의 인식을 유지하도록 하는데 활용할 수 있는 또 하나의 관리적 방안은 바로 '보안선언서'를 작성하여 CEO의 서명을 받아 액자에 넣은 후 각 사무실과 회의실에 부착해 두는 것이다. 예를 들어서 간단한 보안선언문과 함께 "고객의 정보는 고객의 것이다"라는 문구 하단에 CEO가 서명을 한 보안선언서를 부착해 두는 것이다. 이렇게 하면 정보보안 체계와 관련하여 실무부서와 업무적인 논쟁을 하는 경우에 중요한 판단기준으로 활용할 수가 있다.

정보보안의 최대 수준과 최대 한계의 '척도'는
정보보안에 관한 경영진의 철학입니다.