금융산업 Highlights

Information Asset

금융기관 고객정보자산의 위험관리 방향

최근 금융정보 유출 사고 사례를 통해

송기정 상무
금융산업 본부

02-6676-1988
ksong@deloitte.com

비대면화 금융 환경은 반드시 '안전한 인프라'가 전제 되어야 한다

지난 10년간 금융산업은 빠르게 전자화 / 비대면화 (Faceless) 되어오고 있다. 현재 비대면 거래 비중은 전체 금융거래의 87%에 이르며, 모바일 뱅킹 사용자가 4천 만 명을 넘어섰고, 온라인 상거래규모 또한 55조 원에 이르고 있다. 또한 스마트폰의 대중화, 소셜 네트워크 서비스 등 인터넷 기반의 신규 비즈니스 모델 출현으로 금융산업의 전자화 / 비대면화는 더욱 가속될 전망이다.

그러나 금융거래의 '전자화 / 비대면화' 는 그 자체가 지닌 위험성 때문에 필수적으로 역기능을 수반하며, 따라서 반드시 '안전한 인프라'가 전제 되어야 한다.

그러나 지난 10년간 사이버 침해사고를 포함한 정보보호 사고는 10배 이상 증가하여 왔으며 이로 인한 기업의 유무형적 손실은 10조 원 이상으로 추정된다. 특히, 최근 카드사의 개인신용정보 유출 사태는 금융기관으로 하여금 지금까지와는 다른 패러다임으로 고객정보자산을 보호할 것을 요구하고 있다.

2013년 금융기관 정보보호 예산과 IT보안인력 현황

금융권역	정보보호 예산	IT보안인력	전체 인력
은행 (18개사)	141억	24명	6823명
증권 (49개사)	23억	4명	840명
보험 (41개사)	43억	7명	1560명
카드 (8개사)	111억	18명	2115명
평균 (116개사 평균)	54.4억	9.1명	2111명

SOURCE : 금융감독원

정보보호 예산 대비 집행비율

금융권역	2010년	2011년	2012년
은행 (18개사)	81.5%	92.9%	75.2%
증권 (49개사)	76.4%	78.1%	53.8%
보험 (41개사)	82.7%	78.55%	46.25%
카드 (8개사)	69.9%	90.8%	61.8%
평균 (116개사 평균)	79.6%	85.9%	61.9%

SOURCE : 금융감독원

정보보호 예산은 증가한 반면 실제 예산 집행률은 낮아졌다

금융기관의 정보 보안 투자 추세 및 시사점

최근 금융권 정보보안 예산이 너무 적었다는 비판적인 시각이 지배적이지만, 사실 '과거 금융권이 안전한 인프라'확보에 소극적이기만 했던 것은 아니다. 2011년 4월 농협사태 이후 6월 정부는 IT 보안강화 종합대책을 발표하여, IT 보안인력과 예산비율(IT예산의 7% 이상)을 감독규정으로 명시하였다. 이로 인해 은행권의 경우, 정보보안 예산 비중이 2010년 3.4% 수준(금융권 전체로는 3.2%)에서 2013년 9.3%로 비약적으로 증가하였으며, 이는 Global 은행들의 33%가 1~3%를 투자하는 수치와 비교하더라도 양적으로는 긍정적인 방향이라고 평가해야 할 것이다.

- **다만 예산 책정 시, 감독규정 (5/5/7 Rule*) 준수를 목적으로 직접적으로 정보보호와 관련되지 않은 예산을 포함시키거나, 인력 산정 시에도 단순 PC 및 네트워크 유지/보수 인력을 포함시키는 등의 문제가 발견되고 있다.**
- **실제 정보보호 예산 집행률 역시 '11년 85.9% 에서 '12년 61.94%로 전년대비 24% 포인트 낮아지는 등 오히려 투자집행에 소극적인 경향을 보이고 있다.**

정보보호 투자 포트폴리오 관리가 필요하다

이는 많은 금융기관들이 감독기관의 강력한 정책 집행에 따르기 위해 정량적인 가이드라인을 맞추고 있으나, 이렇게 증가된 투자가 실질적으로 금융기관의 정보보호 수준 향상에 반영되지 못하는 비효율이 상존하고 있음을 의미 한다.

따라서 증가된 정보보호 투자·인력 등이 수준 향상에 효과적으로 반영되기 위해서는 정보보호 투자에 대한 '투자 포트폴리오 관리'가 필요하다.

* 5/5/7 Rule : 전자금융감독 규정(제8조 2항)에 따라 금융회사 등은 총 임직원 수의 100분의 5이상을 정보기술부문 인력으로, 정보기술부문 인력의 100분의 5이상을 정보보호인력으로 각각 확보하여야 하며, 정보기술부문 예산의 100분의 7이상을 정보보호 예산으로 확보하도록 권고하고 있음

지속가능한 정보보호 운영 효과성 확보가 핵심이다

최근 금융기관 주요 정보보호 사건 / 사례를 통한 시사점

최근 금융기관 관련한 정보보호 사건을 분석해 보면, 기업의 정보보호전략 측면에서 이미 핵심적인 정책, 지침 그리고 정보보호 솔루션 등을 갖추고 있음에도 이 부분이 제대로 작동되지 않는 운영 효과상의 문제점이 드러나고 있으며, 특히 외주 또는 제 3자에게 (3rd party) 주요 업무를 위탁하고 운영하는 과정에서 상대적으로 관리의 수준이 저하되고 있음을 지적할 수 있다.

- 최근 A사 사건의 경우, 기본적인 '외부자 보안 관리 정책'이 존재하였음에도 불구하고 핵심 IT시스템의 개발에 참여한 인력이 고객중요정보에 쉽게 접근 할 수 있는 환경을 제공하였고,
- B사 사건은 3rd Party 업체 두 곳을 해킹하는 것만으로도 B사의 개인정보를 충분히 얻어 냈고, 이를 통하여 추가적인 공격이 가능하기도 하였다.

기술적인 측면에서도 이전의 해킹이 뚜렷한 목적 없이 개인의 해킹실력을 과시하기 위하여 기업 네트워크를 무차별적, 비계획적으로 공격하였다면, 최근의 해킹 양상은 정보보호 수준이 상대적으로 취약한 외주 또는 3rd party를 경유하는 등 고도화, 타겟화 하는 경향을 보이고 있다.

- C사 사건의 경우, 보안이 취약한 아웃소싱 직원의 노트북에 악성코드를 감염시키고 6개월 이상 치밀하게 해당 금융기관의 정보를 수집하여 공격 (APT, Advanced Persistent Threat)하였고,
- D사 사건의 경우, 사전에 회사에 금전을 요구하는 협박을 하고 이것이 의도대로 되지 않자, 국외에 근거지를 두고 D사 협력업체의 취약점을 이용하여 해킹 하였다.

이처럼 최근 전략적·기술적 측면의 사건, 사고 대부분이 금융기관의 기존 정보보호 체계의 운영 효과성 취약부분과 3rd Party를 공략하는 모습이다.

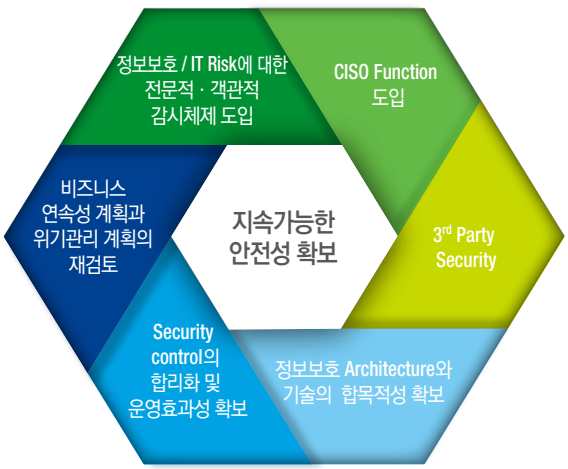
이런 사고 이후 적지 않은 금융기관들이 견고한 정보보안 체계 강화를 위해 추가적으로 정보보호 솔루션을 도입하거나, 더욱 복잡한 내부통제제도를 설계·적용하는 전략적 방향을 선택하고 있다. 이런 접근방식은 '보호를 위한 보호'구조가 되어 오히려 기업의 효율성만을 떨어뜨릴 위험이 있다.

지속 가능한 안전성 확보를 위한 고려 사항

정보보호 관련 법규 강화와 금융기관들의 정보보호 투자확대 등의 노력에도 불구하고, 잇달아 발생하고 있는 사고를 근본적으로 예방하고 '지속 가능한 안전성 확보'를 위해서는 반드시 하여 아래와 같은 요소들을 고려하여야 한다

- 정보보안 전담 임원(CISO)과 조직 구성을 통한 기업 정보보호 위험관리의 전문성과 독립성 확보

  구성된 전담조직을 통해 기존의 '정보보호'와 '위험관리' 전략 리모델링
- 이런 전략하에서의 정보보호 통제구조와 아키텍쳐 합리화(Rationalization)
- 인증획득 등의 단발성 관리가 아닌 설계·구현된 통제가 유의미하게 지속적으로 작동될 수 있는 운영 효과성(Operational Effectiveness)의 확보방안 마련
- 그리고 3rd Party Security 관리, 비즈니스 연속성 및 위기확산 방지방안 (Crisis Management Plan), 제 3자에 의한 정기적인 모니터링 방안 등 간과하기 쉽지만 매우 중요한 정보보호 위험관리 영역도 전략에 포함하여 관리 필요

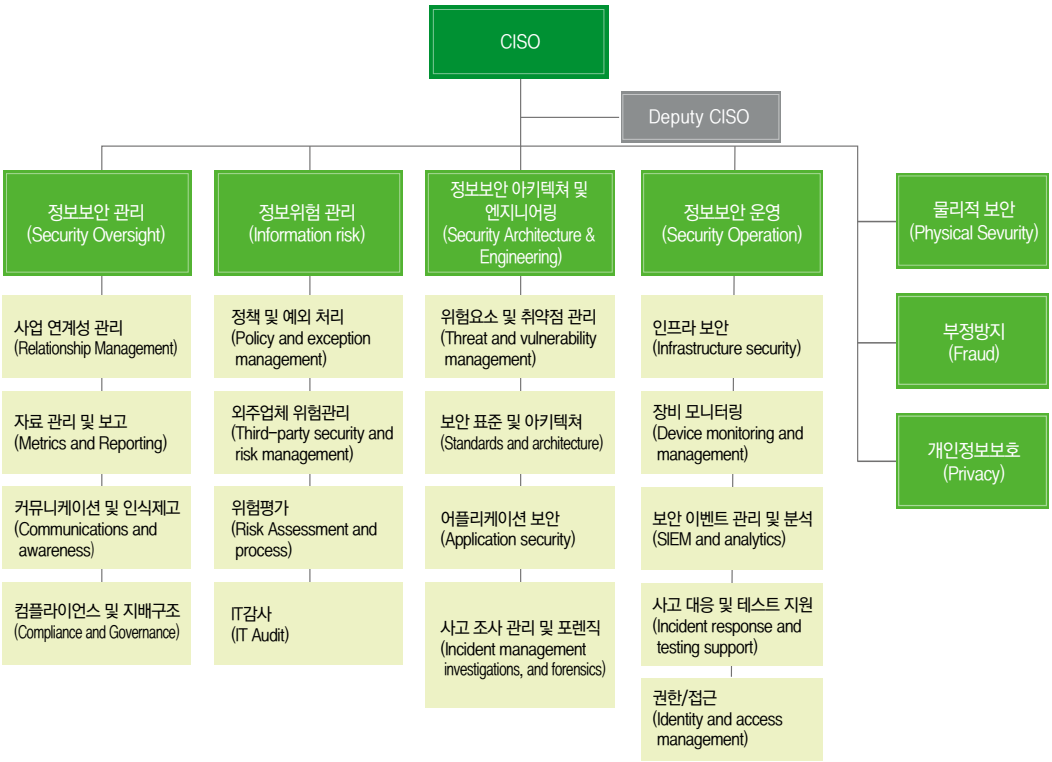


정보보호는 C-Level agenda로 격상 – 1세대 CISO의 역할이 중요!

1. CISO (Chief Information Security Officer) Function 도입

지난해 11월 금융위원회는 전자금융거래법에 일정규모이상의 금융기관에 CISO를 CIO와 분리하여 집행임원급으로 임명 하도록 의무화 하였다. 이는 일부 대형 금융기관에서 선도적이었던 CISO 운영이 보편화 되는 시발점이며, 정보보호가 이사회(BOD)나 C-Level Agenda로 격상됨을 알리는 신호탄이라 볼 수 있다.

Deloitte Global Security Survey에 의하면 글로벌 금융기관들의 80% 이상은 독립적인 CISO를 두고 있으며 전형적인 조직 구조와 CISO의 주요 역할은 다음과 같다.



전형적인 조직 구조와 CISO의 주요 역할

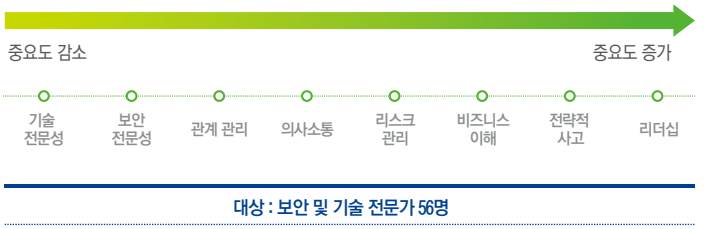
전통적으로 CISO의 역할이라고 여겨 왔던 '기술적 / 관리적인 정보보호 전략 수립 및 집행 기능'에 추가하여 '전사적으로 IT / 정보보호 위험을 진단 / 감사하는 기능' 과 '상시진단 (Continuous IT & security Audit) 체제의 도입과 운영기능'을 가지는 것이 매우 중요하다. CIO들은 경영전략과 연계된 IT 시스템을 갖추는데 역량을 쏟아 붓고 있고, 이에 따라 컴플라이언스에 대해 부분적인 책임만을 가지고 있는 경향이 있으므로 더욱 복잡해진 IT 컴플라이언스 환경에 대하여 이를 합리적으로 통합하고 집중적으로 관리하는 것이 CISO의 중요한 역할이 되어야 한다.

CISO라는 새로운 포지션이 아직은 생소하며, 어떻게 역할을 정립해 나가야 하는지에 대한 물음도 크다. 새로운 포지션 자체가 가지는 의미보다는 실질적인 위험관리가 시급한 기업들에게는 '누가 CISO 역할을 수행 하느냐' 가 훨씬 중요할 수 있다. 그렇다면 1세대 CISO에게 요구되는 경험과 역량은 무엇이고, 기업 내에서 역할은 무엇인지 짚어 볼 필요가 있다.

CISO – 기술적 전문성보다 리더십, 의사소통과 전략적 사고 역량이 더욱 중요하다

첫째 : 가장 중요한 역량은 리더십, 의사소통과 전략적 사고 이다

- CISO의 중요한 기본적인 책임은 최고경영진과 현업 리더들에게 정보보호가 어떻게 그들을 도울 수 있는지, 기술 / 전문가팀에게는 어느 정도의 정보보호 수준이 기업에 충분한 것인지, 최종 사용자들에게는 그들의 책임이 무엇인지를 효과적인 의사소통 하는 것이다.
- 따라서 기업 내 다양한 관련자와 계층들이 이해할 수 있는 공통언어 개발이 필요하다.
- 최근 CISO 대상으로 실시한 글로벌 리서치에 의하면, CISO가 가져야 할 가장 중요한 역량으로 리더십 (35%), 의사소통 및 관계관리 (25%), 비즈니스 이해 (20%)의 순이로 나타났으며, 정보보호기술에 대한 전문성은 10%에 불과하다.



대상 : 보안 및 기술 전문가 56명

SOURCE : Q2 2013 North America/EMEA Role of The CISO Online Survey

단순 Compliance 측면에서의 대응이 아닌 기업의 경쟁력 확보 차원의 공격적인 전략이 필요하다

둘째 : CISO는 기술우월주의 (Techno-Machismo)의 산물이 되어선 안 된다

- 기술과 비즈니스가 고도로 융합되어 훨씬 복잡해진 기업환경에서 최고경영진들이 CISO에게 원하는 것은 특정 사건이나 법규에 대응하기 위해 반사적으로 급조된 정보보호 기술(솔루션)투자 계획이나 PIMS, ISMS 등의 인증 획득 계획이 아니다.
- 균형잡힌 시각의 비즈니스 케이스와 위험관리 관점의 전략적 사고, 지금까지와는 다른 혁신적인 정보보호 전략 그리고 결국 기업의 비즈니스 가치를 어떻게 보호할 것인지에 대한 궁극적인 대답을 기대하고 있다.
- 단순히 IT보안 프로젝트와 인력을 관리하는 전통적인 역할에서 탈피, 요구되는 법규나 표준이 기업에 쉽게 적용 될 수 있는 방안을 모색하고, 비즈니스 어플리케이션에 가치를 더하여야 한다.

셋째 : 현재 트렌드를 반영한 주요한 역할 수행이 필요하다

- 현재 정보보호 위험의 핵심 화두는 '개인정보보호'와 '중요정보 유출방지'이다. 정부가 적극적으로 개입하여 천문학적 과징금 부가(매출액의 3%) 등의 강력한 대응이 예고 되므로 CISO는 기업 내에서 이와 관련된 챔피언이 되어 위험관리를 하여야 한다.
- 다만, 이러한 이슈에 대해 법률에 준거하는 수비적 자세 보다는 이를 기업 경쟁력을 끌어 올리는 공격적인 도구로 활용하는 전략도 필요하다.

외주 및 3rd Party 에 대한 관리가 중요해 지고 있다
– '확대된 기업'개념 도입 필요

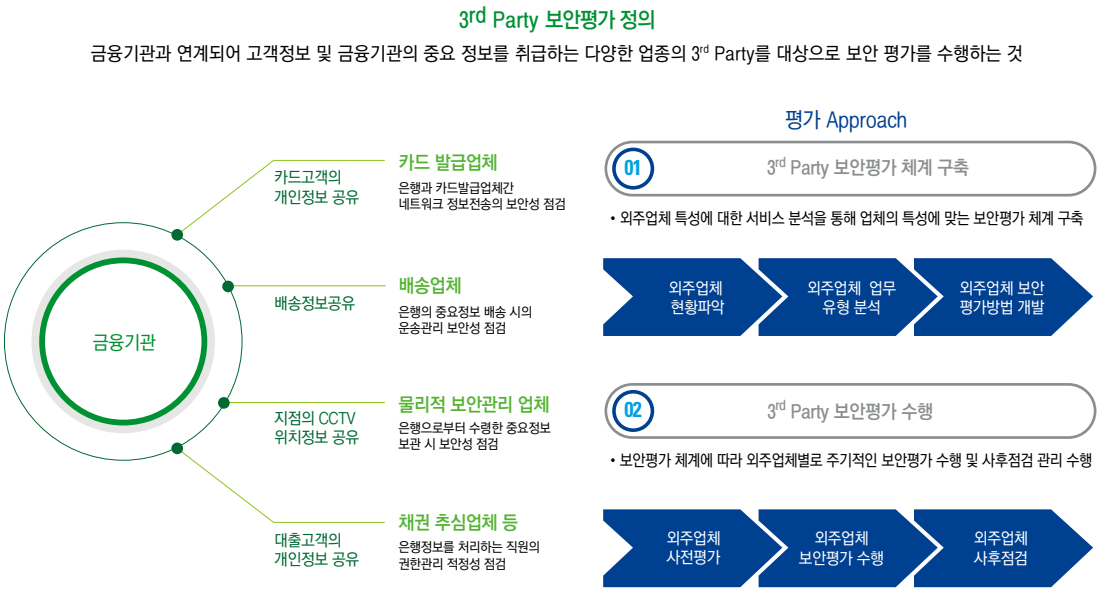
2. 3자 (3rd party) security 강화 – Seamless Security within extended enterprise

'90년대 후반부터 금융기관은 비용절감 및 핵심역량 강화를 위한 비핵심역량 부분의 아웃소싱을 확대해오 면서 확대된 기업 (Extended Enterprise)화 되고 있다. 이러한 확대된 기업의 특성 중 하나는 연관된 3rd Party 업체들이 금융기관의 일부 부서처럼 운영되고 있어, 필연적으로 금융기관의 고객정보를 공유한다는 점이다.

하지만 정보보호의 특성상, 기업 내 가장 취약 보안 수준이 해당 기업 전체 보안 수준을 결정짓는다. 따라서 상대적으로 관리가 열악한 3rd Party 업체들의 정보보호 수준이 전체 기업의 정보보호 수준을 결정할 개연성이 아주 높다. 그렇기 때문에 3rd Party 업체들에 대한 보안수준 점검과 이에 대한 개선이 전체 가치사슬(Value chain)의 안전성 확보 관점에서 필수적이다.

최근 B사 사건의 경우 3rd Party 업체 두 곳을 해킹하는 것만으로도 B사의 개인정보를 충분히 얻어 낼 수 있었고, 추가적인 공격도 충분히 가능했다.

반면 3rd Party 업체들을 영향도에 따라 구분, 정기적으로 정보보호를 평가했던 글로벌 C은행의 경우 해당 업체들의 정보보호에 대한 노력을 유도하며 균질적으로 보안 수준을 유지했다.



3rd Party 보안성 평가 프로세스
(SPISA : Service Provider Information Security Assessment)

Security ≠ Technology

도입된 기술이 도입목적에 맞게 운영되고 있는지가 더욱 중요하다

3. 정보보호 Architecture와 기술의 합목적성 확보 (Security ≠ Technology)

정보보호의 완전성 확보를 위해 정보보호 아키텍쳐의 수립과 이에 따른 기술 도입과 운영은 필수적이다. 그러나 정보보호기술은 전사적인 보안전략을 구현하기 위한 하나의 수단이며, 보안 Architecture의 일부이다.

최근 Deloitte의 조사에 의하면, 오히려 보안기술은 중복 또는 과잉 투자의 조짐을 보이고 있고, 단일 솔루션 위주(Silo Approach)로 도입되고 있다. 더 큰 문제는 도입된 보안기술의 상당수가 도입 의도대로 설치·운영되지 못하고 있으며, 기업 내에 이런 다양한 기술에 대해 충분한 지식을 갖춘 전문가가 부재하다는 것이다.

이런 상황은 금융기관 대부분의 정보보호 조직이 IT부서에 속해 있었던 것과 연관 관계가 높다. 매년 정보보호 투자의 70% 이상이 보안기술 도입과 유지에만 집중되고 있으나, 도입된 기술의 25% 이상이 제 기능을 발휘하지 못하고 있다.

따라서 기업의 비즈니스 환경 변화에 따른 위험평가와 아키텍쳐의 정기적인 재검토 등이 선행되어야 하고, 이에 따라 솔루션의 도입은 오히려 지금보다 더욱 신중하게 결정되어야 한다. 이는 결국 비즈니스와 기술로부터 독립적인 CISO 기능이 필요한 이유이기도 하다.

아울러 도입된 정보보호 기술이 합목적적으로 운영되고 있는가를 지속적으로 측정 할 수 있는 KRI (Key Risk Indicator) 등 측정 가능한 평가 Framework를 도입하여 그 효과성을 지속적으로 모니터링 하여야 한다.

비현실적이고 방대한 정보보호 정책, 지침, 절차는 무의미하다

– 꼭 필요한 통제를 잘 지킬 수 있도록 하는 Rationalization 필요

4. Security control의 합리화(Rationalization)와 운영 효과성(Operational effectiveness) 확보

이미 대부분의 금융기관이 방대한 정보보안 정책, 지침과 절차 등을 보유하고 있다. 그러나 대부분 정보보안 부서만의 소유이며, 필요한 비즈니스 관련 부서들에 충분히 공유되거나 인지시키지 못하고 있는 것이 현실이다. 현실적인 위험을 반영하지 않은 사전식의 방대한 보안정책과 통제가 실 환경에서 준수되기는 쉽지 않다는 의미이다.

A사 사건의 경우만 하더라도 외부직원의 노트북 관리지침, 사내에서의 유무선 인터넷 사용 정책과 슈퍼유저(Super user)관리 권한 등의 지침과 절차 등이 존재하였지만, 유효하게 작동하지 않았다.

방대한 정책문서와 비현실적인 보안통제의 설계보다는 어떻게 운영의 효과성을 확보할 것인가가 더욱 중요하다. 오히려 문서화와 통제는 최대한 간결하게 합리화하고, 주제 중심이 아닌 역할 (role-based or employee-based) 중심으로 변화시켜 조직의 구성원 각자가 알아야 할 필요가 있는 보안정책과 통제만을 반드시 지킬 수 있는 환경을 만들어야 한다.

5. 비즈니스 연속성 계획과 위기관리 계획의 재검토

비즈니스 연속성 계획 (Business Continuity Management)은 발생 가능성은 낮지만, 그 영향이 매우 큰 비즈니스 리스크를 위한 계획이다. 비즈니스 연속성 계획은 매우 기술적이고 전문적인 분야이고 위험 발생 시 계획대로 작동할 것인지에 대해 검증하기 어려운 분야이지만 완전성을 정기적으로 점검하는 것이 중요하다.

특히, 정보보호가 기업의 비즈니스 연속성에 영향을 주는 주요 위험으로 인식되므로 이를 계획에 반영하는 것은 매우 중요하다.

사고 전 예방 대책에 대한 부분뿐만 아니라, 사고 후 관리 대책도 포함해야 한다. 즉 위기확산방지방안(Crisis Management Plan) 등 과 같은 사후 관리 대책을 치밀하게 준비해야 한다는 것이다.

최근 정보보호 사고 사례에서도 볼 수 있듯이 사고 이후 기업의 초동 대처가 사고를 통한 손실의 양을 결정짓는 결정적 요소가 되고 있다.

최고경영자의 대응 방법 부터 대 언론 대응 지침과 고객 및 내부 직원들에 대한 대응 지침 등의 위기확산 방지 방안은 반드시 치밀하게 사전에 수립하여야 만약의 사고 시에도 손실을 최소화하고 기업의 Reputation을 보호 할 수 있다.

정보보호와 IT관련 위험은 조직 내의 독립적인 팀 또는 외부의 전문팀으로부터 객관적으로 그 적절성을 평가 받아야 한다

6. 정보보호 / IT Risk에 대한 전문적·객관적 감시체제 도입

정보보호와 IT관련 위험관리는 객관성과 지속성 확보가 핵심이다. 정보보호의 속성상, 지속적으로 관련 통제가 준수되어야 하기 때문에 위험관리가 적합한 수준으로 설계 / 운영되고 있음을 확인 (Assurance) 받는 것은 매우 중요하다. 따라서, 조직내의 독립적인 Team 또는 외부의 전문 Team으로부터 객관적으로 그 적절성을 주기적으로 평가 받을 필요가 있다.

그러나 이런 전문팀은 정보보호 분야 뿐만 아니라 감사 (Audit) 기술 등에 대한 전문성도 요구되기 때문에 이런 팀을 기업이 자체적으로 보유하기 위해서는 쉽지 않은 것이 사실이며, 확인의 객관성을 확보하는 것도 쉽지 않다.

Deloitte ISMM(Information Security Management Model)에 따라 국내의 한 금융기관을 평가해 보면, 기술적 성숙도는 상대적으로 높은 반면 프로세스, 사람, 관리적인 측면에서는 아직 초기단계를 벗어나지 못하고 있는 것으로 파악된다. 따라서, 이미 언급한 운영의 효과성을 확보하고 대외적으로 정보보호의 완전성을 증명해 내기 위해서도 외부전문기관에게 정기적으로 객관적인 검토와 평가를 받는 체제가 반드시 필요하다.