글로벌경영연구
第 23 卷 3 號
2011年 12月

기업 정보자산 보호를 위한 사이버보안 강화 전략

조 준 서*

Cyber-Security Enhancement Strategy for the Protection of Corporate Information Assets

Abstract

Information assets are more important since increasing and emphasizing of company's information assets in cyber economy. Rapidly development of IT including telecommunication and ubiquitous, especially, companies have troubled with protect and maintain of their information assets since the increasing of the possibility of unpredictable risks. There are happening the attacks and breach of security through the cyber space, then companies have caused economic losses and credit ratings have dropped.

In the paper, we investigate what are the security issues to protect company's information assets, then suggest the strategies of tighten up company's cyber security how the cyber risk will respond effectively.

Ⅰ. 서론

21세기 글로벌화가 본격적으로 시작되면서 인터넷의 발전은 누구도 예상하지 못할 만큼 엄청난 속도로 발전하고 있다. 네트워크와 정보기술의 발전과 함께 인터넷을 기반으로 한 사이버 공간은 국가 활동과 기업의 비즈니스, 국민 개개인들의 일상생활의 중요한 영역으로 자리 잡으며 정부, 국방, 정보통신, 에너지, 금융, 제조, 서비스 등 핵심적인 사회의 모든 부분을 포함하는 사이버 경제를 형성하고 있다.

이처럼 사이버 경제에 대한 의존성과 그 중요성이 높아지면서 개인정보침해, 산업기밀유출, 사이버 범죄, 사이버 테

* 한국외국어대학교 글로벌 경영대학

러, 사이버 전쟁 등 사이버 경제 분야의 잠재적 위험은 다양해지고 있으며 피해 범위도 점점 커지고 있다. 최근 사이버 공격이 경로의 다양화, 수준의 고도화 및 지능화, 조직화되어가면서 사이버 경제는 정부, 기업, 개인들에게 새로운 위험 영역이 되고 있다.

이에 대한 대응책으로 기업에서는 정보자산을 여러가지 통제 및 관리 수단을 통해 보호활동을 하고 있으나, 보안수준을 높게 요구할수록 업무 수행의 불편함으로 단기적인 효율성 및 생산성이 감소하게 되는 딜레마에 빠져있으며, 조직의 정보보호 투자가 지속적으로 증가함에도 불구하고 정보보호 성과는 불확실한 실정이다.

특히 사이버 경제에서 정보와 지적 재산이 경쟁력이고 또한 이 경쟁력이 수익과 직결되기 때문에 기업차원에서의 보안은 매우 중요하다. 기업의 경우 점점 증가하는 보안사고로부터 소송과 이미지 손실, 브랜드 가치의 하락 등의 피해 방지를 위해서 노력해야 한다. 이를 위해서 기본적으로 정보유출의 방지와 내부통제, 그리고 효율적인 데이터관리와 보안 등의 노력이 필요하다.

이러한 기업의 정보자산보호를 위해서 기업은 보호할 정보를 명확히 규정하고 수단의 구체화를 통해 이를 실현해야 하며, 기업의 중요한 정보자산이 무엇인지, 보호해야할 정보자산이 무엇인지, 그 가치가 무엇인지, 누가 보호할 것이지, 그리고 조직 내 정보는 어떻게 존재하고 있는지, 어떻게 보호할 것인지 등을 명확히 정의하고, 기업 내 보안 강화를 위해서는 사내교육을 통해 주기적으로 보안의식을 고취시키고, 보안에 대한 경각심 고취시키기 위한 노력을 해야 한다.

지금까지는 주로 기술적인 측면에서 기업의 사이버보안에 대한 논의가 이루어져 왔으나, 이번 연구에서는 정책적/관리적 그리고 의식적 관점에서 기업의 사이버 위험이 무엇인지(이기석, 2008), 그리고 미래에 발생 가능한 위험들이 무엇이 될 수 있는지를 연구하며, 사이버 경제의 확대로 발생할 수 있는 여러 보안적인 문제점들을 조사하고, 사이버 위험에 효과적으로 대응할 수 있는 기업의 사이버보안 강화 전략을 제시하고자 한다.

Ⅱ. 기업의 사이버 위험

기업의 경우 핵심 비즈니스 영역이 사이버 공간으로 이전되면서 산업기술을 포함한 기업의 영업 비밀들이 사이버 공격에 의해 누출되어 기업 경쟁력에 심각한 타격을 줄 수 있는 위험이 높아지고 있다. 또한 자신들이 수집한 고객의 정보를 사이버 공격으로부터 제대로 보호하지 못하고 유출시켜 기업경쟁력은 물론 개인 정보보호법제 위반 등으로 법적 책

임을 지게 되는 위험에 처할 수도 있다.

최근에 변화의 속도가 빨라지고 있는 지식 정보' 사회에서 물리적 기반보다 지적기반 사업이 증가하고 있다. 이러한 지적기반 사업에서는 인력이나 특허권과 같은 자산도 중요하지만 컴퓨터나 네트워크 상에 존재하는 기밀 사항도 증가될 수 밖에 없다. 즉 핵심 비즈니스들이 사이버 공간으로 이전 되면서 핵심 영업 비밀들이 사이버 공격에 누출되는 사례가 빈번해지고 이는 기업 경쟁력 저하, 기업 이미지 하락, 수익감소 등 심각한 타격을 주고 있다.

시만텍이 발표한 '2010 기업 보안현황 보고서'의 내용을 살펴보면 지난해 75%의 기업이 사이버 공격을 받은바 있다고 응답했다. 이 보고서는 한국의 50개 기업을 포함해 전세계 2,100개 기업의 CIO, CISO 및 IT 관리자들을 대상으로 실시한 설문조사 결과를 반영한 것이다.

사이버 공격으로 인한 기업의 손실도 막대한 것으로 나타났다. 고객 신용카드 등의 금융 정보와 고객 개인 신상 정보, 지적재산권 정보가 가장 많은 유출 사례로 조사됐고 보안 사고의 92%가 기업의 생산성, 매출 및 신뢰도 저하를 초래한 것으로 나타났다. 이러한 손실을 금액으로 환산해보니 연평균 2백만 달러에 달한 것으로 조사됐다. 아태 및 일본지역 기업들의 경우에는 사이버 공격으로 인한 손실 규모는 이보다 낮은 평균 76만 3천 달러로 분석됐다.

조사 기업 가운데 42%가 사이버 공격을 가장 심각한 위험 요소로 꼽았으며, 이는 전통적 범죄(17%), 자연재해(14%), 테러(10%) 등의 위험 요소들을 모두 합한 것보다도 높은 수치였다. 한국을 포함한 아태지역에서도 사이버 공격(38%)은 단연 최대 위험 요소로 꼽혔다.

Ⅲ. 사이버보안 현황

사이버보안은 위와 같은 사이버 공간에서의 위협으로부터 국가는 기반시설과 국가기밀을, 기업은 첨단기술과 기업비밀을, 개인들은 자신들의 개인정보를 보호하여 사이버 위험을 최소화하는 것을 말한다. 사이버보안의 목표는 사이버 공간에서 위험요소를 지속적으로 줄여나감으로써 사이버 공간을 안전한 국가행위, 안전한 기업행위, 안전한 일상생활이 이루어지는 신뢰의 공간으로 만들어 사이버 공간의 지속가능한 발전을 보장하는 것이라고 할 수 있다. 사이버 위험이 전 사회적으로 미치는 영향이 크고 특히 국가 안보와 국민 보호에서의 중요성이 높아지면서 국가는 국가 위기관리의 일환으로 사이버보안을 고려해야 한다. 이미 많은 국가들은 사이버 위험의 심각성과 보안의 중요성을 인식하고 국가 위기관리체제에 사이버 위기를 포함

시키고 사이버 경제 보안 강화를 추진하고 있다.

1. 국내 보안 현황

사이버보안의 현실은 매우 위험하며, 그 미치는 범위도 매우 크다. 그러나 실제로 사이버보안의 부실로 인해 야기되는 피해액은 아직 정확하게 추정되지는 않지만 그 피해액은 예상보다 클 것으로 판단되며, 중요한 것은 앞으로의 상황이다. 1994년 인터넷이 상용화된 이후 정치경제 및 사회에 엄청난 속도로 영향을 미치고 있다. 모든 사회 전반 활동이 인터넷으로 연계되지 않거나 영향을 미치지 않는 것은 거의 없다고 해도 과언이 아니다. 이러한 여건에서 공공기관에 노출된 사이버 위협의 유형 및 발생건수는 시간이 갈수록 늘어나고 있다. 기업의 피해 역시 급속히 증가하고 있으며, 개인에게 미친 영향도 매우 크다. 미국의 경우 미국정보기관과 대기업의 90%가 컴퓨터보안과 관련한 사고 경험을 했으며, 그중 70%는 해결책이 알려진 외부 침입에 취약점으로 인해 발생되었으며, 60%는 해커 등에 의한 서비스 중단되었으며, 80%는 충분하지 못한 보안정책으로 인해 발생된 것으로 나타났다(유은재, 윤미영, 2009).

국내에서도 2003년 1월 25일 인터넷 대란의 경험을 계기로 국가 위기관리 차원에서 사이버 안전 확보의 중요성을 인식하고 기존의 안보개념에 사이버보안을 포함시켰으며, 국가사이버안전 관리규정을 마련하고 이를 2010년 4월 16일부터 시행하였으며, 국가 사이버 안전센터를 설립하는 등의 노력을 하고 있다. 한국은 정보화지수가 세계 5위 안에 드는 자타 공인 IT강국인데 반해 세계경제포험(WEF)의 보안서버(49위)와 스위스 IMD의 사이버보안(22위) 등 정보보호 수준은 많이 떨어지는 상황이다. 지난해 국가공공기관이 7,588건의 해킹을 당했으며, 2007년 추산 국내 80개 공공기관 중 80%, 44만 개 민간기업의 95.3%가 보안관련 전담조직이 없는 등 높아지는 사이버 위험 발생 가능성과 사이버보안의 중요성에 비해 실제 국내 사이버보안 현실은 이에 미치지 못하고 있다(이현영, 2011).

2. 기업의 보안 현황 및 문제점

사이버 위험은 기업에게 급속히 다가오면서 정보자산보호의 중요성을 인식시키고 있다. 2010년 국내 기업의 25.8%는 정보보호 정책을 수립하고 있으며, 내부 사용자 대상의 정보보호 지침을 제정·운영하고 있는 기업은 25.5%로 나타났다. IT관련 책임자 즉, 정보관리책임자(CIO)는 18.7%, 정보보호책임자(CISO)는 14.5%, 개인 정보관리책임자(CPO)는

44.8%인 것으로 나타났다. 정보관리 책임자와 정보보호 책임자의 경우, 업종별로는 금융 및 보험업이 타 업종에 비해 높았으며, 규모별로는 종사자 수가 많은 사업체일수록 IT관련 업무의 총괄 책임자의 임명율이 높게 나타났다. 정보보호 전담조직을 공식적으로 운영하고 있는 기업은 14.5%이며, 개인정보보호 전담조직을 운영하고 있는 기업은 32.7%로 전년 대비 각각 6.2%p와 3.0% 증가하였다. 정보보호 전담조직의 경우, 업종별로는 금융 및 보험업에서, 규모별로는 종사자 수가 많은 사업체일수록 운영율이 상대적으로 높았다.

사이버보안강화를 위해서는 교육이 매우 중요하다. 2010년 기준 정보보호 교육을 실시하고 있는 기업은 18.4%에 불과했다. 정보보호 교육을 실시하고 있는 기업 중 82.4%가 '일반직원' 대상의 교육을 실시하고 있으며, 웹 사이트를 통해 개인정보를 수집하는 기업의 60.5%는 '개인정보 관리자' 대상의 교육을 실시하고 있다. CEO 등 경영진에 대한 정보보호 교육 실시는 52.5%로 일반직원에 비해 낮은 비율을 차지하였으며, 외부인력(협력업체/아웃소싱/업체직원) 대상 정보보호 기초교육'을 실시하고 있는 사업체 비율은 크게 낮았다. 정보보호 교육 필요성 인식이 낮고, 그 결과 실시하는 비중도 낮다고 할 수 있다.

정보보안을 강화하기 위해서는 투자가 필수적인데 국내 기업의 정보보호 투자비율은 2010년 기준 36.5%에 불과했으며, 63.5%는 정보보호에 대한 투자가 없다고 응답하여 아직까지 대부분의 사업체가 정보보호 투자에 미진한 것으로 나타났다. 정보보호 투자가 이루어지는 기업의 19.9%는 정보보호 관련 투자가 전년 대비 증가했다고 응답하였으며, 규모가 큰 기업일수록 정보보호 투자가 증가한 것으로 나타났다. 정보보호 지출이 없는 사업체의 정보보호 지출이 없는 이유를 물어본 결과, 정보보안 사고로 인한 피해가 거의 없어 필요성을 느끼지 못 한다는 응답이 과반수를 넘어 가장 많았으며, 이어서 정보 보호에 관심이 없다 등의 의견이 나타났다. 즉 대부분의 기업에서 정보보안의 중요성 자체를 인식하지 못하고 있다.

일반적으로 기업체 중 정보보호 업무를 외부에 '아웃소싱한다'고 응답한 사업체는 9.4%로 나타났다. 정보보호 업무를 아웃소싱하는 사업체 중 현재 이용중인 정보보안 서비스로 유지보수, 인증서비스, 보안관제, 보안컨설팅, 교육 훈련 서비스 등을 위하여 아웃소싱을 한다고 한다.

인터넷 침해사고 피해를 경험한 기업은 '웜・바이러스, 트로이잔', '애드웨어・스파이웨어' 감염 피해를 경험한 기업이 상대적으로 많다. 특히 종사자 수 250명 이상의 기업은 종사자 수 50명 미

만의 소규모 기업 대비 약 4～5배의 '해킹', 'DoS', 'DDoS' 공격 피해를 경험하였다. 정보보안 침해사고 피해 발생 건수 및 피해액 모두 증가하는 추세이다.

한편, 기업에서 가장 우려하는 정보보안 위협은 '해커, 컴퓨터 범죄자', '퇴사한 전 직원', '현 직원' 등이라고 한다. 기업의 보안의 주 위험은 사실 기업의 내부적인 직원에게 있다는 것이 통계에 의해 밝혀졌다. 이는 기술적인 보안문제도 중요하지만 직원들 자체의 보안의식 개선이나 교육을 통한 보완이 반드시 필요하다. 기업이 직면하는 위험은 무엇보다도 기업의 정보자산보호가 가장 시급한 문제이며대표적인 기업 보안의 문제점은 <표 1>과 같다.

<표 1> 기업 보안의 문제점

문제점	현황
미약한 보안 예산 비중	◦ 선진국 기업들은 IT보안 예산과 인력을 전체 IT예산과 인력의 7～8% 유지 ◦ 국내기업들은 3～5% 수준
보안 인력 부족	◦ 2010년 신규 지식정보보안 인력의 수요에 비해 50% 정도의 공급이 부족하고, 장기적으로 30~40% 이상의 높은 인력 부족 현상을 겪을 것으로 예상 ◦ 최고 정보보호 책임자(CISO)는 2010년 6529개 기업중 14.6%
인적관리 문제	◦ 내부자의 사이버 테러 가능 ◦ 많은 기업이 동일한 ID와 패스워드 몇 가지를 여러 사람 또는 팀 전체가 공유해 사용
보안 시스템 미비	◦ 기업이나 공공기관이 사용하는 대규모 전산 시스템은 반드시 백업 시스템을 운영 ◦ 국내기업은 주 센터 외에 백업센터 한 곳만 운영하고 있어 위험에 노출
보안인식 부족	◦ 기업 내 구성원의 인식부족 ◦ 정보보안에 대한 사용자나 관리자들의 인식 수준 부족 ◦ "나만 아니면 된다"는 방만적 의식
기업의 내부비밀의 유출에 따른 비용의 증가	◦ 상대기업의 회사영업상 비밀을 유출하려는 시도 ◦ 고객에 대한 정보는 고객을 확보한다는 측면에서 보면 가장 직접적이고 영향력 있는 정보 ◦ 기업의 정보관리 비용과 보안비용 등 비용증가
보안망 하청 구조에 따른 문제점	◦ 기업들이 보안과 관련 하여 외주용역을 맡기는 것은 사이버보안에 드는 비용을 줄이기 위함 ◦ 사이버보안에 대한 인식부족의 연장으로 내부정보 유출이라는 문제점 발생 ◦ 보안망 하청 구조로 인한 보안의 전문성 수준 저하

2011년 9월 개인 정보보호법 시행을 앞두고 정보보안에 대한 중요성이 강조되고 있다. 개인 정보보호법이 시행되면 비즈니스를 영위하기 위해 정보보안이 불가피해지기 때문이다. 지금까지 이윤추구에만 전념했던 기업들도 개인정보보호에 눈을 돌릴 수밖에 없게 된다.

하지만, 아직 국내 기업들의 정보보안에 대한 인식은 많이 부족하다. 하루하루 살아가기 바쁜 대부분의 기업들은 여전히 '비즈니스가 먼저'라는 생각을 하고 있고, 개인 정보보호가 남의 일처럼 손을 놓고 있어 문제이다.

많은 기업들에서는 지금도 보안이 투자 후순위로 밀리고 있으며, 비즈니스에 방해되는 동시에 불편하고 짜증나는 일로 인식되고 있다. 그러나 앞으로 개인정보보호법이 시행되면 많은 부분들이 달라지게 될 것이다. 정보보안에 소홀히 하는 기업들은 비즈니스 자체를 하는 게 힘들어질 수도 있다. 오히려 비즈니스를 잘하기 위해 보안이 필요해지는 것이다.

최근 정보보안에 대한 변화는 기업이 정보보안을 잘못해 정보가 노출되면 경쟁사에 뒤쳐지거나 고객들로부터 신뢰를 잃거나 할 수 있으며 이는 회사의 경쟁력 뿐만 아니라 명성에 영향을 미치는 중요한 요소로 인지하고 있다. 최근 발생했던 인터넷 쇼핑몰 A사, 정유사인 G사, 금융사인 H사 등의 보안 사고는 그동안 힘들게 쌓아올린 회사의 명성이 순식간에 무너지기 쉽고 씻을 수 없는 불명예를 안게 된다는 것을 확인시켜 줬다.

현재 기업들이 가장 크게 우려하는 부분이 앞으로 보안사고 발생 시 패널티나 손해배상 비용도 만만치 않을뿐더러, 회사의 이미지가 나쁘게 형성될 경우 영업, 마케팅적인 손해가 크다는 것이다. 앞으로의 보안이 중요한 이유이다.

Ⅳ. 기업의 사이버보안 강화 전략

오늘날 기업이 관리하는 정보 자산들은 급격히 확대되고 중요해짐에 따라 정보자산의 중요성은 날로 중요해지고 있다. 특히 기업의 비즈니스는 정보화의 가속화, 인터넷의 보편적 보급, 유비쿼터스 환경실현 등 IT 기술의 눈부신 발달로 환경이 변화되었고, 새로운 비즈니스 기회제공으로 매출 및 이윤도 극대화되고 있다.

그러나 성공적인 정보화의 이면에는 다양한 정보화 역기능이 필연적으로 발생하게 되는데, 실제로 증가하는 수많은 정보를 제대로 보호하고, 관리하기가 어려워지고 있다.

최근 정보보호 패러다임은 네트워크 보안에서 콘텐츠 보안으로 변화하고 있는 등 각종 정보 유출 위협에 항상 노출되어 있다. 기업에서는 전자적 형태의

데이터가 제대로 관리되지 못하고 있으며, 비인가자에 의해 무단으로 유출되거나, 컴퓨터 바이러스 등 악성 코드에 의해 외부에 노출되는 등 내부 정보유출에 따른 경제적 손실 증가 및 대외 신인도 추락이 발생하고 있다. 또한 국내 유수 기업의 핵심 기술, 고객정보 유출, DDoS 공격 등 크고 작은 보안 사고들이 끊임없이 발생하고 있다.

이에 대한 대응책으로 기업에서는 정보자산을 여러 가지 통제 및 관리 수단을 통해 보호활동을 하고 있으나, 보안수준을 높게 요구할수록 업무 수행의 불편함으로 단기적인 효율성 및 생산성이 감소하게 되는 딜레마에 빠져있으며, 조직의 정보보호 투자가 지속적으로 증가함에도 불구하고 정보보호 성과는 불확실한 실정이다.

특히 사이버 경제에서 정보와 지적재산이 경쟁력이고 또한 이 경쟁력이 수익과 직결되기 때문에 기업차원에서의 보안은 매우 중요하다. 기업의 경우 점점 증가하는 보안사고로부터 소송과 이미지 손실, 브랜드 가치의 하락 등의 피해 방지를 위해서 노력해야 한다. 이를 위해서 기본적으로 정보유출의 방지와 내부 통제, 그리고 효율적인 데이터관리와 보안 등의 노력이 필요하다.

본 연구에서 현재 기업이 직면하고 있는 사이버 위험 중에서 이슈가 되고 있는 다양한 보안 강화전략을 관리적/정책적 관점 그리고 의식적 관점에서 제시하였다.

1. 관리적/정책적 관점

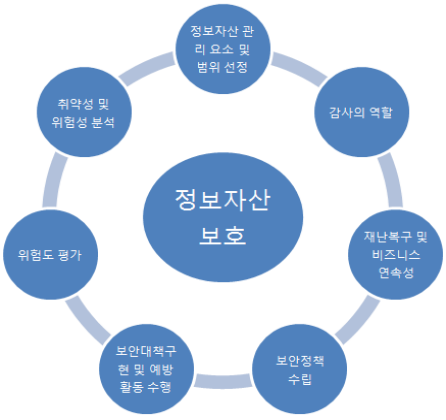
물리적, 기술적, 운영적 통제활동만으로 성취할 수 있는 정보자산보호는 제한적이며 기술적인 방법은 적절한 정책 및 관리와 지침으로 지원되어야 한다. 이러한 정보보호 관리체계는 종합적이며 체계적으로 구축하여야 취약점을 가능한 한 줄일 수 있다. 이러한 정보자산보호 관리체계를 구축하기 위해서는 여러 가지 다양한 관점에서 관리적/정책적 방안이 반영되어 통제 방안들과 상호보완적으로 운영체계가 구축되어야 한다.

1.1 정보자산보호 및 통제를 위한 프레임워크 구성

기업체에서 효율적으로 정보자산보호 활동을 관리하기 위해서는 정보자산보호 프레임워크를 우선 수립하여야 한다. 하지만 이에 앞서 정보기술의 빠른 변화로 지속적으로 발생되는 신규 위협에 대응하기 위해서 정보자산보호의 구성은 [그림 1]과 같이 분류할 수가 있으며 각각의 단계가 상호 유기적으로 작용해야만 한다.

정보자산보호를 위한 정책 및 조직수립은 최고 경영자의 정보보안에 대한 의지와 최고 정보보호 책임자의 역할을 명

시하여 기업환경에 적합한 보안정책을 수립하여야 하며 이러한 정책을 효율적으로 실현하기 위한 정보보호 조직체계를 구성, 해당 조직별 역할과 책임을 분명히 해야 한다.



[그림 1] 정보자산보호 프레임워크 구성

기업의 정보자산보호를 위한 기본적인 프레임워크는 [그림 1]과 같이 구성될 수 있다.

첫째, 정보자산보호에서 구체적으로 관리해야 할 요소와 그 범위를 설정하는 것이며 이에 관한 취약성 및 위험성을 식별하여야 한다. 이때 자산 위험도 평가에 대한 업무가 선행되어야 한다.

둘째, 취약성 및 위험성을 분석하고 이에 관한 위협평가와 각각의 보호대책을 선정하는 것이다.

셋째, 보호대책의 효과적 구현 및 사고예방 활동을 전개하는 것이며 정보보안 교육 및 홍보를 같이 실시해야 한다.

넷째, 위험도 평가가 필요하다. 보안과 정보시스템 통제에 자원을 투입하기 전에 기업은 어떤 자산이 보호가 필요하며 위험에 대해 어느 정도로 취약한지를 먼저 파악해야 한다. 기업은 정보자산의 가치, 취약지점, 문제발생의 대략적 주기, 손실 가능성 등을 파악해야 한다.

다섯째, 보안정책의 수립이 요구된다. 보안정책은 정보 위험도의 순위와 수용 가능한 보안 목표 식별, 그리고 이러한 목표를 달성하기 위한 방법의 식별을 위한 명세서로 구성된다.

여섯째, 재난복구 계획과 비즈니스 연속성에 대한 계획이 필요하다. 재난 사건이 발생하였을 경우 기업의 정보시스템에 대해서 기술적 이슈나 재난복구 서비스에 초점을 둔 계획이 있어야 한다. 또한 재난 발생 후 기업이 비즈니스 업무를 재가동하도록 핵심 비즈니스 프로세스를 파악하고 시스템 정지시에 핵심 업무 기능을 처리할 행동 계획을 세워야 한다.

마지막으로 감사의 역할을 강화해야 한다. 감사는 기술, 절차, 문서화, 훈련, 인력에 대해 점검한다. 감사업무는 모든 통제 취약점을 목록화하고 순위를 매기며 그 발생 가능성을 추정한다. 또한 각 위협에 대한 재정적, 조직적 영향도 평가한다.

정보자산보호 관리영역은 균형된 일정한 수준을 유지하는 것이 매우 중요하다. 전반 적인 보안 수준이 높다고 해도 어느 한 영역이 취약하게 된다면 취약한 한 영역으로 인해 실질적인 보안 수준은 낮게 되므로 전체적인 균형감을 가지고 종합적으로 정보자산보호 관리수준을 올려 나가는 것이 중요하다.

1.2 기업의 정보보호 정책수립

정보자산보호 정책은 기업이 보유하고 있는 비밀 및 정보를 다양한 위협으로 부터 보호하고, 불법적인 정보유출을 사전에 예방하여 회사의 가치 및 정보자산의 손실을 최소화하기 위한 기업의 정책을 규정한 것이다. 정보자산보호 정책은 최고 경영자에 의한 승인을 반드시 필요로 하며 경영자는 조직전반에 걸쳐 정보자산보호 정책이 효과적으로 작용될 수 있도록 명확하게 정책방향과 원칙을 제시하고 그 의지를 모든 조직원에게 명시해야 한다.

정보자산보호보안 규칙에서는 규정에서 정한 원칙을 시행하기 위해 필요한 관리 영역별로 절차 등을 기술하여야 하며, 프로세스 관점에서 효율적인 통제와 관리가 이루어 질 수 있도록 각종 보호대책 수립 및 관리시스템 등의 도입을 고려해야 한다. 정보자산보호 기준에서는 규칙에서 정한 절차를 시행하기 위해 필요한 세부절차 및 구체적 방법 등에 관하여 정의한 것으로 사업장별 조직의 특성에 맞도록 기준을 수립 하여 시행해야 한다.

이러한 정보자산보호 정책은 일관성을 확보하는 것이 무엇보다도 중요하며, 주기적인 검토와 평가를 통해 지속적인 업데이트를 해야 한다.

1.3 정보자산보호 조직 확립

기업 내 정보자산을 총괄적으로 조정 및 관리하는 최고보안 책임자인 CSO의 전문성과 독립성 확보가 요구된다. 보안에 대한 책임을 질 수 있는 정보보호 책임자 있어야 하는 것은 당연하며 보안사고는 항상 발생 가능성이 있기 때문에 사고발생시 피해를 최소화하기 위해 리스크관리 체계가 잡혀 있어야 한다.

더불어, 보안관리 체계의 운영에 따른 독립적이면서 균형적인 권한을 갖는 정보보호 조직의 운영이 요구된다. 내부보안 조직의 권한의 강화가 필요하고, 제 3의 기관에 의한 기업의 보안 수준의 평가 강화가 요구되며, 이 평가 결과는 공공기관 또는 자체 경영 평가에 반영할 필요가 있다.

정보자산보호 정책을 체계적이고 효율적으로 집행하기 위해서는 전문화된 조직 및 협의회 등 체계를 갖추어야 한다. 정보자산보호 조직은 책임자, 담당자, 주관부서, 기능부서로 구분하고 각각의 역할과 책임을 명확히 하여 탄력적이며

효율적인 관리가 이루어질 수 있도록 구성되어야 하며 조직은 <표 2>와 같다.

1.4 위험관리

정보자산보호 프레임워크 수립과정 중 가장 중요한 부분은 각 조직이 당면한 위험에 대한 올바른 평가와 그에 대안 방안 수립일 것이다. 이러한 위험평가를 통해서 정보자산보호 요구사항 분석이 가능한데, 위험평가는 한 조직이 가지고 있는 정보자산에 대한 위협의 종류, 위협의 영향, 위협의 발생 가능성을 평가하는 과정으로 정보 및 다른 자산들의 비밀성, 무결성, 가용성 상실에 따른 잠재적 결과, 정보보호 실패 가능성이 포함 되며, 이를 통해서, 정보자산보호 통제방안 도입에 따른 지출과 정보보호 실패가 기업에 미치는 피해가 균형을 이루도록 통제방안을 선택할 수 있다.

한편 위험관리(risk management)는 정보자산보호 위험을 인식하고 적절한 용내에서 필요한 통제 방식을 선택하여 위험을 적절히 통제하는 과정으로써 조직의 환경 변화, 새로운 위협, 취약 점 고려하여 항상 도입된 통제방식이 효율적으로 적절히 운영되는지 항상 확인 필요하다.

즉, 급변하는 보안 위협환경에 빠르게 대응함으로써 위험을 줄이고 비즈니스의 연속성을 보장하는 중요한 활동이다. 현재의 위기관리 체계가 급변하는 보안 위협에 대한 충분한 대응력을 유지할 수 있는지 지속적이고 반복적인 점검이 필

<표 2> 정보자산보호조직

조직	역할
정보자산보호 책임자 (CSO)	◦ 전사적 차원에서 정보시스템은 물론 인적, 물적 보안체계를 안전하게 관리하고, 운영과 통제를 책임지는 최고위직 임원. ◦ 기업에서의 CSO의 역할은 기업의 비전과 경영상황, 사업 분야에 대한 고찰을 통해 전사 차원의 정보보호 정책과 운영 절차 결정, 정보시스템을 비롯한 주요 업무에 대하여 취약성 분석과 위험 분석을 실시하여 적정한 위험수준을 유지.
정보자산보호 담당자	◦ 부서 내 정보자산보호 관리업무를 담당, 부서 내 업무에 정통하고 보안의식이 투철한 관리자 또는 선임사원이 그 역할을 수행.
정보자산보호 주관부서	◦ 전반적인 정보보안 정책수립, 집행, 감독, 진단 및 사후관리 등을 담당하는 조직.
정보자산보호 기능부서	◦ 정보자산보호 각 분야의 업무를 집행하는 부서로서 전사적 정보보안 정책에 맞춰 업무방향을 수립, 집행하는 동시에 책임과 권한을 가진다.
보안담당자 통제 및 관리	◦ 보안 분야에서 빼 놓을 수 없는 중요한 요소가 보안을 전담하는 사람을 통제 관리.

요하다.

1.5 변화와 사후관리

보안 제품의 도입과 구축이 보안 환경을 조성하는 일차적인 투자라면 잘 만들어진 환경을 원활하게 돌아갈 수 있도록 하는 체계를 정립하는 데 노력을 기울여야 한다. 이는 첨단 정보에 대한 접근체계를 구축하는 것뿐만 아니라 내외부적인 침해사고 발생 시 전사적인 대응 프로세스를 마련하는 것을 포함한다. 아울러 보안 전담 조직을 구성, 보안 관련 업무를 지속적으로 수행해 나갈 수 있도록 해야 할 것이다.

정보자산관리를 위해서는 많은 관리항목들이 존재하는데 이러한 관리항목들은 프로세스화 되어 있어야 하고 그 프로세스는 효율적이어야 한다. 그래서 또 다른 취약성이나 정보유출의 가능성이 없도록 완벽한 통제와 관리가 이루어져야 한다.

변화관리란 프로세스화 되어 있는 관리항목들을 지속적으로 개선해 나감으로써 완벽한 수준의 통제/관리로 이어질 수 있도록 해나가는 것이다. 이를 위해 각종 관리항목들에 대한 프로세스 수립 및 적정성 여부를 지속적으로 확인해야 하며 또 다른 신규 위험 요소 식별/분석 및 개선노력이 뒤따라야 한다.

사후관리란 정보보안 진단으로 정보보안 활동 및 관리가 기업의 보안정책에 따라 효과적으로 실행이 되고 있는지를 점검하기 위해 정기/불시/야간/특별진단 등 다양한 형태로 실시되어야 하며 이를 통해 정보보안의 위협요소를 제거하고 개선대책을 수립하여 향후 정책에 반영함으로써 정보자산보호 수준을 향상시키는 것이다.

사회적으로 문제가 되는 보안사고들이 발생할 때 마다 기업은 사고의 유형을 세부적으로 파악하고 동일한 사고가 발생하지 않도록 철저히 원인을 파악하고 예방책을 마련해야한다.

1.6 정보보안 인프라 투자 확대

기업의 보안에 대한 적극적인 투자와 이에 대한 인식의 전환이 필요하다. 과거에는 보안사고가 터지면 회사의 이미지나 주가에 미칠 영향이 두려워 일단 덮고서 내부적으로 해결하려했고 정보보안에 대해서 안일한 인식과 함께 숨기려는 경향이 있었다. 다행히도 이러한 사고방식이 많이 달라지기는 했지만 아직도 미흡한 수준이다.

현대 사회의 IT 환경은 하루가 다르게 변하고 있다. 기업의 업무 환경도 빠르게 변화하여 인터넷을 이용해 재택근무를 하거나 이동 중 스마트폰으로 이메일을 확인하고 회의실로 이동해서 회의를 할 때는 무선 랜을 이용하여 사내 전산망에 접속한다. 이러한 새로운 환경에서는 새로운 정보보안 문제는 큰 이슈이다. 새로

운 정보보안 문제는 기존에 구축되어진 정보보안 인프라를 가지고 예방 및 방어할 수 없다. 결국 정보보안 인프라에 대한 투자가 적극적으로 이루어져야 해결할 수 있다. 하지만 우리는 정보보안에 대한 투자가 인색한 것이 사실이다.

최근에 와서 정보보안에 대한 인식이 조금씩 바뀌고 있고 투자가 발생하는 것은 사실이나 지속적이고 장기적인 투자가 아니라 일회성 투자라는 측면이 선진국과 비교된다. 현재까지 전체 예산 중 보안 분야에 5%를 집행하도록 돼 있지만 선진국의 경우와 같이 약 10% 보안 예산이 집행되도록 권고하고 있다. 선진국들은 정보보안을 인프라 측면에서 이미 수많은 투자를 해 왔으며 그만큼 IT 환경의 보안대책이 어느 정도 안정화를 가져온 상태에서 지속적으로 투자를 하고 있다.

예로써 금융회사인 경우 정부 당국은 IT예산의 5%를 보안에 투자하도록 권고하고 있지만 이를 지키는 곳은 드물다. 금융권 보안 예산 현황에 따르면 2010년 시중 16개 은행이 IT예산 가운데 보안에 쓴 비중은 3.4%에 불과했다. 지금까지 보안 사고가 나도 대충 넘어간 경우가 많아 기업들이 보안 투자는 적게 해놓고 나중에 문제가 생기면 그때그때 대처하려는 유혹을 받게 된다. 하지만 이번 N사사태가 보여주듯이 보안 사고는 기업에 치명적일 수 있다. 그러므로 기업들은 사이버보안에 대한 투자를 비용으로 인식하지 말고 투자수준을 강화해야 한다.

정보보안에 대한 투자를 인프라로 인식하게 될 때 기업은 정보보안 문제로부터 점차 개선될 수 있을 것이다. 정보보안에 대한 투자를 비용으로 인식하는 기업 경영진들이 있을 때, 기업은 여전히 정보보안 문제에 노출 될 수밖에 없다. 기업은 정보보안에 대한 투자의 시선을 긍정적으로 바라볼 필요성이 있다. 정보보안에 대한 투자로 인해 기업의 정보가 안전하게 관리된다면 국제적인 경쟁에서 대외 신인도 향상 및 고객의 신뢰성을 확보하는 기대 이상의 효과를 볼 수 있는 결과를 가져오게 될 것이다.

1.7 기업 간 협력 증대

사이버보안을 위한 협력이 다양하게 발전되고 있지만 국내에서는 제대로 된 공조체계를 갖추지 못하고 있어 문제이다.

최근에는 국가와 보안업체간의 협력도 강화되는 추세다. 2009년 미국 연방수사국(FBI)은 1100억 달러 이상의 이득을 취한 사이버 범죄 집단을 소탕했다. 이 작전에는 마이크로소프트, 트렌드마이크로 등 주요 글로벌 보안 업체들이 함께 참여한 것으로 알려져 산업계와의 공조체계 구축이 큰 역할을 했다는 평가를 받고 있다. 하지만 우리나라는 아직

이렇다 할 국가 간 협력체계 구축이나 산업계와의 상시적인 협력 체제 마련이 돼 있지 않은 상황이다(유은재, 윤미영, 2009).

다른 국가와의 공조체계 구축은 물론 민간 기업들과도 상시적인 협력 이 이루어질 수 있도록 보다 체계적인 시스템을 만들어야 한다. 최근 발생한 H사나 N사의 해킹 사건처럼 해외 IP추적 등 해외 사이버보안 조직과의 협력이 중요한 상황에서 이와 같은 체계의 마련이 더욱 절실하다.

우리나라는 DDoS, 주요 기관 해킹 등 보안 사고가 터진 당시에만 활용할 일시적인 협력 체계를 구축하고 있다. 사건이 발생한 다음 해결하기에 급급하지 않고 평소에 보안을 예방하기 위해 보안업체 혹은 전문기관 간의 상시적인 보안 협력 체계를 구축해야 한다. 이러한 협력 관계를 통해 기업 간 서로 부족한 보안체제를 보안, 보충하여 사이버보안을 강화 시킬 수 있다.

1.8 보안 인력 확보

안정된 보안전문 인력이 양성되기 위해서는 오랜 시일이 요구된다. 일반 IT개발자, 전산담당자는 2~3년이면 숙련된 엔지니어가 완성되지만 우수한 보안전문 인력은 최소 10년이 걸린다. 예를 들어서 N사에서 이번 사고 발생 후 셧다운 조치가 조금 더 늦어 원장 자체가 지워졌다면 얼마나 큰 더 큰 사고로 이어졌겠는가. 위기관리에 대응능력을 갖춘 전문인력을 반드시 양성해야한다. 또 직원들의 보안 의식 교육 역시 금융권에서 하나의 비즈니스로 연계해 금융보안 인력을 양성할 수 있는 체계를 갖춰야한다. 금융에 대한 지식과 보안에 대한 지식을 두루 갖춰서 위기 발생시 뛰어난 대처능력을 발휘할 수 있는 전문인력을 양성해야한다.

1.9 모바일 보안

기업의 업무 환경에서 모바일 기기 활용이 갈수록 증가하고 있는 만큼 모바일 기기의 효율적인 도입과 이에 대한 보호 및 관리 전략은 기업의 최우선 과제가 된 상황이다. 기업들은 IT의 소비자화, 모바일 환경의 확산, 소셜 미디어의 출현, 스마트 그리드, 가상화 및 클라우드 컴퓨팅 도입 증가 등으로 새로운 보안 및 관리상의 어려움을 해결해야 한다(이건희 외, 2010; 은성경, 2010).

특히 최근에는 스마트폰을 통해 무선 인터넷을 이용한 정보 및 콘텐츠 소비가 활발해지면서 보안위협의 노출 가능성 크게 증가하고 있는데, 스마트폰 분실 시 사용자의 개인정보, 금융정보, 기업정보 등 유출에 대한 방지 대책 부재한 상황이다. 스마트폰 이용이 증가하면서 무선랜을 통한 인터넷 이용이 증가하고 있으나 국내에 보급된 무선AP중 74%는

보안 미설정으로 보안상태가 매우 허술한 상황이다. 만일 보안이 설정되지 않는 경우, 누구나 무선AP에 쉽게 접속할 수 있어 해킹이 용이할 뿐만 아니라, 무선AP를 통해 연결된 컴퓨터나 스마트폰도 악성코드나 바이러스에 쉽게 노출될 위험이 매우 크다. 따라서 이러한 위험에 대한 대책이 필요하다.

더불어 GPS, LBS 등의 이용 확산과 함께 개인정보 등의 유출에 대한 대책 역시 필요하다.

1.10 내부 정보 유출 방지 체계

이는 내부의 중요 정보에 대한 명확한 분류체계를 해놓음으로써 중요 정보의 유통 과정을 감시하는 체계이다. 즉, 특정 정보를 누가, 언제 보았는지부터 시작하여 정보 흐름이 안전하게 지켜지고 있는지를 모니터링하는 방법이다. 따라서 중요 정보라 분류 되는 모든 정보가 추적될 수 있고, 안정성이 있도록 설계해야 한다. 문제 해결에 대한 해결책은 조직과 기술, 사람이 연계되는 것이 가장 좋은 해결책이라고 할 수 있다. 여기서도 마찬가지로 사람과 조직 관점에서는 외부자와 조직 내 내부자에 보안의식 강화가 먼저 선행되어야 할 것이라고 볼 수 있다. 기술 관점에서는 내부 정보 유출 방지를 위해서 PC, 서버, 네트워크, 어플리케이션과 같은 물리적 부분까지 정보 흐름전반에 걸친 보안체계 구축이 필요하다. 다시 말하여, 기존의 보안 시스템을 통합함으로써 하나의 시스템으로 작동하게 해야 하며, 중요 정보는 따로 보호 대상으로 선택하고 집중적으로 관리함으로써 내부자에 의한 불필요한 유출 사고를 사전에 막을 수 있어야 한다. 또한 위에서 말한 정보 흐름의 추적을 통해서 설령 유출 사고가 일어나더라도 추적이 가능할 수 있는 것이 중요하다.

2. 의식적 관점

아무리 좋은 보안 시스템과 체계를 갖춘다 하더라도 임직원들의 보안의식이 부족하면 기업의 내부 정보자산 유출을 막기는 어려울 것이다. 대부분의 정보자산 유출이 전/현직 직원들에 의해서 발생하고 금전적 문제와 관련돼 있다는 점은 이 같은 필요성을 뒷받침해 준다. 정기적인 정보보호 교육을 통해 임직원들이 올바른 보안의식을 가질 수 있도록 지원하는 데에 관심을 기울여야한다.

2.1 최고 경영진의 보안 의식 강화

기업의 사이버보안 강화를 위한 방법에는 여러 가지가 있겠지만 가장 중요한 점은 경영진이 보안을 어떻게 이해하느냐에 따라 달라진다. 보안 담당자나 관리자들이 보안에 대한 지식을 경영진이나 직원들에게 끊임없이 알리고 이해를

구하며 보안지식을 향상시키는 것이 기업의 보안 강화 및 향후 보안투자에 대한 지름길이다. 경영자의 보안의식이 강화되면 정보보안 담당자들이 정보보안 시스템 구축과 운영을 일관되게 추진할 수 있으며, 보안시스템에 대한 이해도가 높아져 문제가 발생했을 때 빠르게 대처할 수 있다. 경영자의 보안 마인드는 보안강화의 첫 단계이다. 경영자의 보안의식은 사내 그룹웨어 시스템을 활용해 보안에 대한 사용자 교육을 지속적인 추진으로 연결돼 전 직원의 보안의식 제고에도 영향을 미친다. 경영자의 인식 전환이 보안의식 강화를 위한 가장 빠른 길이라고 할 수 있다.

2009년 보안업체인 Ounce Labs사의 후원을 받아 보안연구소인 Ponemon Institute에 의해 실시된 설문조사에 따르면 핵심 보안이슈에 대해 최고경영진들과 고위 경영진들 사이에 입장을 좁히지 못하고 있어 문제가 되고 있는 것으로 드러났다. 대다수의 CEO들은 본인 회사의 보안 이슈에 대한 취약성을 심각하게 인지하고 있지 않았으며 또한 이러한 해킹공격을 받았을 때 현 상태의 보안 수준만으로 공격을 방어해낼 수 있다는 자신감마저 보이고 있었다는 것이 이번 조사에서 새롭게 밝혀진 상황이다. 하지만 CEO들에게 매일같이 보고를 일삼는 고위 경영진들의 의견은 이와는 정반대인 것으로 나타났다. 이들은 자신들의 기업 시스템 및 보안수준이 시간이 지날수록 취약해지고 있다는 점을 인식하고 있으며, 심지어 데이터 유출사고를 방지하는데 자사의 보안시스템에 대하여 자신감마저 잃은 상태라고 한다.

82%의 고위 경영진들이 자신의 기업체에서 데이터유출 사고를 경험한 적이 있다고 답했으며, 94%에 해당하는 응답자가 최근 6개월 내에 해킹 공격을 당한 경험이 있다고 답하였다. 또한 53%의 응답자는 자사 시스템에 대한 해킹의 빈도수가 시간별 또는 요일별로 지속적으로 이루어지고 있음을 밝혔다. 고위 경영진 중 오직 58%만이 자신의 기업 보안시스템에 대한 활용성과 보안성에 대한 확실한 자신감을 갖고 있는 것으로 나타났으며, 전체 응답자 중 32%만이 자신의 회사는 해킹공격을 당한 적이 없는 것으로 생각한다고 답하였다.

CEO들 중에서는 93%의 응답자가 자신의 기업 보안시스템에 대한 보안유출 사고에 대해 방어태세가 확고히 갖추어져 있다고 믿고 있는 것으로 나타났으며, 48%의 응답자가 자신의 기업 시스템은 공격에 노출되지 않았다고 생각하고 있다고 밝혀졌다. 이 외에도 기업 데이터를 보호할 책임이 누구에게 있느냐는 물음에도 양측의 의견은 사뭇 다른 것으로 밝혀졌다. CEO들 중에서 53%는 최고정보경영자들이 데이터보호에 책임이 있다고 답했으며, 고위 경영진들 중

25%도 이에 동의하고 있는 것으로 조사되었다. 그리고 누구에게 데이터보호에 책임이 있는지 없는지를 떠나 이들의 직종은 자리를 보존하는데 아무런 문제가 없는 것으로 받아들여지고 있었다.

전체 고위 경영진들 중 85%에 달하는 대다수는 자신들의 관리 및 감독 하에서 보안 사고를 예방하기 위한 노력이 실패로 돌아갔을 때 자신들이 직업을 잃는 것을 부당하게 여기고 있는 것으로 나타났다.

이와 같이 최고경영진의 보안의식에 대한 이해부족으로 보안에 대한 투자가 적게 이루어지고 그 결과 보안위협이 심화되게 된다. 따라서 최고경영진의 보안의식 강화가 기업의 사이버보안 강화 방안의 제 1순위라고 할 수 있다.

결국 보안강화를 위해서는 최고경영자(CEO)가 나서야 한다. CEO가 보안에 힘을 실어줘야 한다. 유능한 보안담당관을 육성하고 투자를 늘려야 한다. 선진국 사례를 참조해 보안 마스터플랜을 새로 준비해야 한다. 보안을 비용이 아닌 투자로 바라보는 관점 변화가 필요하다.

CEO는 지켜야 할 중요한 정보자산이 무엇인지를 확인하고 전사 보안 조직을 구성해 보다 안전하고 효율적으로 이를 보호해야 한다. 아울러 보안과 관련된 법규에 대해 관심과 의지를 갖고 이를 준수하는 것이 무엇보다 중요하다. '보안은 회사를 지키는 것'이라는 것에 대해서는 누구도 이의를 제기하지는 않을 것이다. 그럼 CEO 입장에서 회사의 보안을 위해 무엇을, 누가, 어떻게 지킬 것인가에 대해서 확인하고 지시하는 것은 당연한 일일 것이다. 보안은 시설보안, 산업보안, 정보보안, 융합보안 등 여러 분야가 있으며 CEO는 회사와 관련된 모든 분야에 대해 관심을 가져야 한다.

2.2 고객정보관리에 대한 인식의 제고

기업이 확보하고 있는 고객의 개인정보는 기업의 기술정보와 같이 미래의 경제적 이익을 가져다주는 핵심자산이다. 경영학의 마케팅에서 기업은 고객을 평생에 걸쳐 거래기업에 대해 제공할 수 있는 잠재적 공헌도로 평가하고 있다. 고객정보는 고객으로부터 빌려온 자산이다. 기업은 개인정보를 제공한 고객에게 개인정보의 성실한 관리라는 책임을 지고 있다고 기업은 인식해야 한다. 기업의 고객 정보보호는 단순히 규제대응을 하지 못해서 발생하는 위험을 예방하는 차원의 활동 그 이상의 것이다.

개인 정보는 여러 사람, 즉 고객을 대상으로 하는 기업들이라면 어떠한 자산보다도 필요하고 훌륭한 자산이다. 반면 이러한 고객 정보가 외부에 유출되면 기업의 신뢰가 유출 되며, 기업이 집단 소송에 휘말리는 등 금전적인 피해 이외에도 2차, 3차에 이어진 피해가 기업에게 가해진다. 개인 정보 유출을 막기 위한 법은 국내에서나 해외에서나 점점 강화

되고 있는데, 지난 2010년 9월 30일에 국회를 통과한 '개인 정보보호법'이 그 한 예이다. 이 법은 2011년 9월에 시행되며, 개인에게는 소송을 통해 배상을 받아내거나 재판에서 승소하는데는 유리하겠지만, 기업에게는 더욱 불리한 상황이 될 것이므로 더욱 개인정보 유출 방지에 힘써야 할 것이다. 개인 정보 유출에 관한 문의는 2006년부터 계속 급증하고 있으며, 많은 내용들이 개인 정보나 사생활 침해, 주민번호 도용과 같은 직접적인 개인 정보 유출에 신경써야 함을 알 수 있다.

기업 내 고객정보 유출은 말 그대로 기업 내 축적된 고객정보가 외부로 유출된 경우로 포털 사이트나 인터넷 쇼핑몰, 통신업체, 은행 등에서 관리 소홀 또는 의도적으로 고객정보를 유출한 사례를 언론을 통해서 심심치 않게 볼 수 있다. 따라서 기업은 기업 내 보관되고 있는 고객정보에 대한 보다 철저한 보안관리 대책이 필요하며 고객정보가 기업의 핵심자산임을 인지하고 데이터베이스에 저장된 고객정보를 보호하기 위한 DB보안 솔루션 도입 및 내부자에 의한 고객정보로의 부적절한 접근을 방지하기 위한 시스템과 체계를 구축하는 등의 노력이 필요하다.

2.3 정보자산보호 교육 및 홍보 강화

정보자산보호 관리 및 실행의 주체는 임직원 개개인이다. 하지만 실제 현상은 그러하지 못하다. 임직원 개개인들은 본연의 업무를 가지고 있으며 정보자산보호의 중요성을 인식하지 못하기 때문에 정보보안 관리에 소홀해지기 쉽다. 그래서 정보자산보호 주관 부서에서는 임직원 및 협력회사 직원들에게도 정보보안 인식을 제고시키고 자발적인 보호관리 및 예방활동을 할 수 있도록 다양한 정보자산보호 교육을 실시하여야 한다. 교육과정은 신입사원 뿐만 아니라 직급별로 해당 직급의 수준에 맞게 정책, 인식 제고, 관련 법령 및 법적 책임, 사고 사례, 임직원의 보안관리 사항, 준수사항 등으로 구성 되어야 하며 필수과정으로 운영이 될 수 있도록 체계화해야 한다.

또한 교육과 홍보 내용은 이해 위주 또는 주입식 내용에서 탈피하여 필요성과 중요성을 인식하고 자발적인 참여와 실천을 유도할 수 있도록 생활 속에서 지켜야 할 준수사항, 사례중심으로 구성되어야 할 것이다.

특히 직원의 실수는 그 피해 범위가 훨씬 넓기 때문에 기업은 직원들에게 보안과 관련, 정기적인 교육을 실시해야 한다.

2.4 내부 인적관리 및 조직문화 개선

기업의 보안의 주 위험은 기업의 내부적인 직원에게 있다는 것이 통계에 의해 밝혀졌는데 이는 흔히 재택근무 시나

휴대용 기기를 사용하는 직원의 USB같은 기기가 기업보안을 유출시킬 수 있다는 점 때문이다. 이러한 문제점 때문에 직원들의 보안의식을 개선하기 위해 정보보호 교육은 아주 중요하다.

신규 및 경력 채용자 뿐만 아니라 재직자의 경우도 보안서약서, 보안교육 및 비밀유지 서약서 등을 준비해야 한다. 높은 이직률에 대비, 차별화된 보상시스템으로 안정을 유지하면서 주기적인 보안교육과 보안점검을 통해 내부자에 의한 기술유출을 방지하는 노력이 필요하다.

퇴직자는 많은 관심과 보안대책이 요구되며 보안담당자는 퇴직자의 정보반납 및 개인정보 삭제, 비밀유지 약정체결, 퇴직자 보안교육, 퇴직 후 진로 및 동향파악 등을 사전에 조치해 문제발생 시 유리한 결과를 가져 오도록 한다. 협력업체의 경우 신뢰를 바탕으로 편의성을 우선하는 관행이 있어 어려움은 있지만 기술협력, 기술자문, 투자협정, 컨설팅, 연구개발 시에는 반드시 비밀유지 계약을 체결한 후부터 진행해야 한다.

조사에 따르면 국내 기업의 20% 정도의 기업에서 중요기밀이 유출돼 피해를 본 적이 있고 피해기업의 기밀유출 횟수도 평균 3회에 달하는 등 피해가 심각한 것으로 나타났다. 오랜 시간 투자를 통해 이뤄낸 연구의 성과나 기술자료, 도면이나 소스코드와 같이 유출 시 기업의 투자비용 회수나 재투자가 어려운 정보유출의 경우 기업의 생존, 나아가 국가 전체의 산업 기반에도 영향을 미칠 수가 있다.

기업의 중요 정보에 대한 유출경로는 외부의 침입으로 인한 정보 유출보다는 기업 내부자에 의한 정보 유출이 훨씬 높은 비중을 차지하고 기밀정보의 접근 용이성으로 그 피해액도 내부자를 통한 유출이 훨씬 더 큰 경제적 손실을 주게 된다.

정보유출 등의 보안사고로 유발될 수 있는 기업 비즈니스 위험요인에 대한 경영층들의 관심이 커지면서 기업 정보보호의 중요성이 크게 부각되고 있다. 하지만 지금까지 외부 보안위협을 차단하기 위해 집중된 단위 보안솔루션 기반의 정보보호 대응방법으로는 이러한 변화에 대응하기에 한계가 있다.

실제로 보안인식 부족, 투자비용 및 인력제약 등으로 일부 대기업들을 제외하고는 체계적인 내부 정보보호를 할 수 있는 여건이 성숙되어 있지 않은 것이 현실이다. 지금껏 기업은 외부로부터의 보안침해 차단을 위해 방화벽이나 침입차단시스템 등을 도입하는 등 외부 보안 위협에 대응하는데 집중했을 뿐 실제 보안사고의 80% 이상을 차지하고 있는 내부 위협은 관용적 태도로 대응하고 있었다.

그러나 최근 발생되는 대규모 정보유출의 원인이 내부의 위협으로부터 기인된다는 인식이 커지면서 이로 인한 피해방지를 위해 내부정보관련 보안솔루션

도입이 급격히 늘어나고 있다. 내부정보가 포함된 문서 자체의 보안 강화를 위해 e-DRM을 도입해서 기업 내 생성되는 모든 문서들을 암호화하고 있고, 인터넷을 기반으로 한 업무가 늘어나면서 직원들이 E-mail, 메신저, 인터넷 게시판 등을 통해 내부정보를 외부로 유출할까 두려워 필터링 솔루션을 보강하고 있다. 뿐만 아니라 저장매체를 통한 정보유출이 걱정스러워 DCS(Device Control System)까지 도입해 매체를 통제하고 있다.

기업비밀이 유출되는 경로가 아무리 다양하고 첨단화되어 있다고는 하나, 그 정보 유출 의 주체는 사람일 수밖에 없다. 또한 핵심 기밀유출의 80% 이상은 내부자의 소행 이라는 점에서 주요 정보의 비밀관리를 위해서 인원보안의 중요성은 두말 할 나위가 없다.

정보를 취급하는 중요도가 높은 핵심 인재의 경우는 인사부서와 긴밀히 협조하여 집중 관리를 하여야 하며 타 회사로의 전직을 방지하기 위한 각종 보상체계 등 제도적 인 뒷받침도 이루어져야 한다. 반면에 퇴직의 징후가 있거나 퇴직 시에는 기업의 핵심 정보의 유출 정황이 없는지 다양한 측면에서 관리함으로써 정보유출 예방을 강화해야 한다.

인적보안을 임직원, 협력업체, 퇴직자 관리로 크게 구분해서 살펴보면 <표 3>과 같다.

<표 3> 인적관리 분류

인적 분류	관리 내용
임직원 관리	◦ 전 임직원들에게는 기업의 비밀과 정보자산을 보호할 의무 ◦ 임직원의 비밀보호 의무를 확인/이행토록 하기 위해 비밀유지 서약서 ◦ 기업 비밀보호에 대한 중요성을 인식하고 기업 비밀을 보호하기 위한 적정한 보안관리 시스템을 도입하여 정보유출을 추적/통제/제어할 수 있는 기반을 확보 ◦ 안정적인 고용을 보장할 수 있는 유인정책과 임직원 스스로가 강한 주인의식과 책임감을 가질 수 있는 문화를 조성 ◦ 핵심인력 별도 관리
협력업체 관리	◦ 협력업체 장과 관계 직원들에게 비밀유지 서약서를 받아야 하며 보안교육도 실시 ◦ 협력업체와 계약을 체결 시에는 보안유지 조항을 반드시 계약서에 포함 ◦ 필요시 협력업체 방문 또는 보안지도 점검 등을 통해 기업의 정보자산이 유출되는 일이 없도록 조치
퇴직자 관리	◦ 재직기간 중 지득한 회사의 영업 비밀에 대한 보안을 유지해야 할 의무가 있으므로 퇴직자 비밀 유지서약서를 받아야 한다 ◦ 퇴직 전에 정보유출이 발생되지 않도록 PC, 정보저장매체 및 기타 자료에 대한 보안 조치를 강구

V. 결 론

정보통신분야의 눈부신 발전과 함께 초고속 정보통신망에 의하여 금융망/통신망/공공망 등 네트워크간의 연계를 통한 IT 인프라가 사회전체의 효율성을 높이는 단계로 성숙하며, 사이버 경제를 형성하고 있다. 하지만 이러한 눈부신 발전은 사이버공간의 취약성과 네트워크의 안정성이 일시에 무너질 경우 사회전체의 혼란이 발생할 위험을 내포하고 있는 것이다.

특히 기업의 경우, 이러한 발전과 함께 정보자산의 중요성을 다시 인식하게 되었고, 고의적인 보안사고와 더불어 기업내부 에서의 정보자원의 오용, 유출, 인적 실수와 같은 보안사고 등 내적 외적인 사이버 위험으로부터 기업의 정보자산을 어떻게 안전하게 보호해야 할지 노력하게 되었다. 이에 대한 대응책으로 기업에서는 정보자산을 다양한 통제 및 관리 수단을 통해 보호활동을 하고 있으나, 아직 미흡한 형편이다.

사이버 경제에서 정보자산이 기업의 경쟁력이고 또한 이 경쟁력이 수익과 직결되기 때문에 기업차원에서의 보안은 매우 중요하다. 기업의 경우 점점 증가하는 보안사고로부터 소송과 이미지 손실, 브랜드 가치의 하락 등의 피해 방지를 위해서 지속적인 노력을 해야 한다. 이를 위해서 기본적으로 정보유출의 방지와 내부통제, 그리고 효율적인 데이터 관리와 보안 등의 노력이 필요하다.

더불어 최근 추진되고 있는 국내외 정보보호 규제들은 기업의 능동적이고 책임성 있는 투명한 정보보호 활동을 요구하고 있다. 이는 앞으로의 기업 정보보호는 단순 보안인프라를 마련하는 것이 아니라 기업이 활용하고 있는 정보를 각종 규제에서 요구하는 합리적 보호수단을 마련하여 사회적, 윤리적 책임성을 가지고 활발하게 정보보호 활동을 수행하고 있음을 스스로 증명해야 되는 것을 말한다.

이번 연구에서는 기업이 다양한 사이버 위험으로부터 정보자산을 보호할 수 있는 보안 강화 전략에 대해서 관리적/정책적 관점 그리고 의식적 관점에서 논의 하였다. 사이버 경제가 지배하는 사회에서 기업의 정보보안의 중요성은 더욱 커질 수밖에 없다. 지속적인 관심과 투자, 그리고 연구 개발을 통해 기업정보자산을 안정적으로 보호할 수 있도록 해야 한다.

참고문헌

[1] 유은재, 윤미영, “주요국 사이버보안 추진전략과 시사점”, 한국정보화진흥원(2009).

[2] 은성경, “클라우드 컴퓨팅 보안 기

술 동향", 「정보보호학회지」, 제20권, 제2호(2010).
[3] 이건희 외, "스마트그리드 사이버보안 추진 현황", 정보보호학회, 제20권, 제5호(2010).
[4] 이기석, "네트워크 시대 사이버 보안의 문제점 및 정책대안", 「한국지역정보화학회지」, 제9권, 제1호(2008).
[5] 이현영, "경영대학원 사이버 범죄 실태와 대응 방안에 관한 연구", 인천대학교 석사학위 청구논문, 2011.
[6] 국정원, 방통위 "국가 정보보호 백서", 2010.
[7] 국회입법조사처, "국가 정보보호 정책현황과 개선방안", 2010.
[8] 금융보안연구원, "2011년 기업 정보보호 이슈 전망 보고서", 2011.
[9] 방통위, KISA "정보통신 서비스 제공자를 위한 개인 정보보호 가이드", 2011.
[10] 지식보안 정보산업 협회, "국내 정보보안산업 실태조사", 2010.
[11] 한국인터넷진흥원, "정보시스템 해킹/바이러스 현황 및 대응", 2009.
[12] 한국인터넷진흥원, "국가 정보보호 백서", 2010.
[13] 한국인터넷진흥원, "인터넷과 시큐리티 이슈", 2011.
[14] 한국인터넷진흥원, "인터넷 침해사고 동향 및 분석", 2011.
[15] 한국인터넷진흥원, "IT 기반의 국가사회 선진화를 위한 법제도 정비 연구", 2010.
[16] 한국정보화진흥원, "미래형사이버 범죄 대응전략연구", 2009.
[17] 한국정보화진흥원, "정보화 통계조사 및 동향분석에 관한 연구", 2009.
[18] Symantec, "Internet Security Threat Report 16호," 2011.
[19] www.security.ne.kr 한국기업보안연구원.
[20] www.fsa.or.kr 금융보안연구원.