기업 정보보호 투자에 대한 경제성 평가의 접근방법에 관한 연구

남 상훈*·임 종인**

요 약

본 연구는 기업이 정보보호 투자시 필요로 하는 경제성 평가의 접근방법을 제시한다. 기업은 윤리경영을 기초로 사업과 서비스를 통한 수익창출을 목표로 한다. 그리고 기업은 안정적인 사업, 서비스의 정보환경을 확보, 유지하기 위해 지속적인 정보보호 활동을 통하여 Risk를 줄이는 작업을 해오고 있다. 기업의 정보보호 활동과 패턴은 초기의 정보보호 기본기능을 도입, 구축하는 단계에서 탈피하여 점진적으로 종합적인 관리체계로 발전되고 있으며 이와 병행하여 산출되는 정보와 정규화되는 Data를 기초로 정량적인 관리가 이루어 지는 시점에 와 있다.

기업의 정보보호 투자에 대한 경제적인 효과를 체계적으로 평가하고 관리하는 활동은 아직도 초기 단계에 머무르고 있다. 그러므로 기업이 정보보호 투자시 발생되는 피해비용의 감소와 사업 및 서비스 등에서 예측되는 경제가치 창출에 대한 기대효과의 정량적인 관리를 통해 투자의 기준을 제시하여 기업에서 효과적인 정보보호 투자가 이루어지도록 함에 있다.

I. 서론

기업의 존재이유는 윤리적인 경영하에서 수익창출을 통하여 인류사회에 기여함에 있다. 기업은 사업환경의 변화와 다양한 Risk의 증가에 대한 전략을 수립하여 대응, 발전해 오고 있다. 기본적으로 시스템의 복합성이 증대되고 있을 때 Risk도 함께 증가하게 된다[1]. 특히 정보보호에서의 Risk관리는 움직이는 표적을 관리하는 것과 같이 동적이면서, 정량적인 관리가 요구된다. 기업의 정보보호 활동과 패턴은 이제 정보보호 기본기능을 도입, 구축하는 초기에서 탈피하여, 점차적으로 관리 체계안으로 수렴되고 있으며 산출되는 정보보호 관련정보와 Data의 정규화를기초로 정량적으로 관리되는 시점에 이르고 있다.

기업의 정보보호 영역을 포함하여 정보보호의 특징으로 100%의 정보보호는 달성될 수 없으며, 사용자의 편리성을 제한하며, 가시적인 이익을 얻을 수 없다라고 일반적으로 이야기되어 왔다. 그러나 정보보호의 투자는 이제 정량적인 관리를 통해 가시적인 이익을 얻어가야 한다는 것이 필요하다. 기업은 Risk를 줄이기 위한 지속적인 노력으로 투자를 할 때, 기업의 경영층은 다른 분야와 마찬가지로 정보보호의 경제적 가치를 동일하게 묻게 된다. 그러나 정보보호의 영역이 적용초기이며 그 피해 발생의 예측이 어려운 점과 신규사업에 대한 부가가치의 창출에 얼마나 기여하고 참여되는 지를 예측하기 어렵기 때문이다. 정보보호는 Risk에 대해 이를 방지하기 위해 투자하는 비용과 정보보호 활동을 통해 얻게되는 기대효과 등이 아직은 정성적인 수준에 있으며, 단지 기술적인 보안활동과 기준에 있어서 정량적인 기준과 관리적 보안영역에 있어 인증 등의 객관적인 기준에 의해 관리되고 있다. 정보보호의 개선을 위해서 그 수준이 계측되고 정량적으로 관리되는 것이 필요하다. 그리고 정보보호의 투자는 정보보호의 특성을 고려되어 무형자산의 피해의 감소에 대한 자산보호의 측면을 고려 추진하여야 하며, 정보보호가 핵심요소로 작용하는 사업 및 서비스측면에서 그 경제가치의 창출을 고려하여 접근, 추진되어야 한다.

* 남 상훈, 고려대 정보보호대학원 박사과정, 011-750-9385, swnam@sktelecom.com

** 임 종인, 고려대 정보보호대학원 원장, 02-3210-2357, jilim@korea.ac.kr

II. 기업의 정보보호와 투자

1. 정보환경 변화와 정보보호 Risk

1) 정보환경의 변화

정보환경의 변화는 기업에게 기회와 위기의 상황을 동시에 만들어 내고 있다. 이제 우리는 정보화가 성숙된 단계인 유비쿼터스 사회로 진입하고 있으며, 기업도 이러한 변화속에서 기회를 염두에 두고 언제 어디에서도 적용할 수 있는 새로운 사업과 서비스를 준비하고 있거나 전개하고 있다. 기업경영 및 고객정보의 의존도와 활용성이 높아진 상황에서 언제 어디서 그 정보를 사용하게 되는 편리성과 함께 취약성과 함께 정보보호의 위협에 노출될 가능성이 증가하게 된다.

인터넷의 사용은 2004년말 236만명이 증가하여 3,158만명에 이르고 있다. 더구나 그중 1,192만명이 초고속 인터넷을 사용하고 있는 상황이다 [2].

<표1> 한국 인터넷 이용자수 변화추이 (이용자수 단위: 천명)

구분	1997년	1998년	1999년	2000년	2001년	2002년	2003년	2004년
이용자	1,634	3,103	10,860	19,040	24,380	26,270	29,220	31,580
증가율(%)	123.5	189.9	250.0	75.3	28.0	7.8	1.2	5.0

* 출처: 통계로 본 국내 인터넷 현황, 한국인터넷진흥원

유비쿼터스 사회는 고객의 요구을 기초로 정보기술외에 생명공학 등의 다양한 기술이 융,복합화되는 상황에서 심각한 해킹, 웜/바이러스 유포, 네트워크 불법침입, 불건전 정보유통 및 개인정보유출 등과 같은 정보화의 역기능이 우려된다. 기업은 이러한 변화의 시대에 성공적인 사업과 서비스를 전개하기 위하여 경쟁우위 요소로 경제성의 정량적 가치평가를 통해 정보보호에 투자하고 관리해 가는 것이 필요하다.

2) 변화에 따른 정보보호 Risk

기업은 변화를 수용하고 그 변화에 서 예측되는 Risk를 적극적으로 기회로 전환시켜 나갈 때 발전해 간다. 기업은 Risk를 파악하며 지속적인 수익모델을 찾아 전략과 대책을 수립해 가는 이유이다.

다양한 기술이 융,복합화 되어가는 변화중인 현재, Risk는 시스템의 복잡도에 근거하여 정의해 볼 수 있다. 기본적으로 시스템의 복합성이 증대되고 있을 때 오류의 가능성을 피하기 어렵다. 시스템디자인의 오류란 개방적 체계로 조직을 이해하는 이론가들에 의해 발전한 개념으로서 예상치 못한 상황으로 인하여 사전에 설계된 시스템이 의도하지 않은 방식으로 작동함으로써 오히려 위기를 증폭시키는 결과를 낳는 시스템설계 과정상의 오류를 말한다. 이러한 시스템디자인의 오류는 체계자체가 복합적 인과관계(Complex-interaction)와 긴밀한 결합(tight-coupling)으로 이루어진 경우에 발생하는 오류다. 왜냐하면 기계와 인간의 상호작용들이 매우 복잡적으로 나타나고 또 그러한 상황자체가 매우 긴박하게 돌아가는 경우 불확실한 경우의 수가 기하급수적으로 많아지므로 사전에 이 모든 상황에 적절한 대처를 할 수 있는 시스템을 설계하는 것은 쉽지 않은 일이다. 정보환경의 변화속에서 정보보호의 Risk의 증가도 복잡도의 증가에 의해 발생되며, 예측되는 현상이라고 보아야 한다 [3].

유비쿼터스 환경에서 더욱 무선을 기반으로 한 네트워크 환경으로 전환되어 가게 되는데, 무선환경은 유선환경보다 더 정보보호의에 취약한 상황이다. 무선의 AccessPoint에 접근이 더욱 용이하여 침해사고의 발생가능성이 높아진다. 정보의 기밀성과 무결성을 보장하기 어려워 지며, 도청도 더욱 쉬워질 것 이나 도청탐지는 어려운 취약점이 노출될 것이다. 이와 같이 정보보호의 Risk는 증가하므로 그

위협의 대상과 공격방법을 명확히 파악하고 대책을 수립하여 예방과 대응훈련을 강화해 나가므로써 취약점을 감소시켜야 한다.

<표2> 침해 대상별 정보보호 위협분류

구분	개인적 침해위협	기업의 침해위협	국가적 침해위협
대상	- 민간 사설망 - 개인용컴퓨터	- 기업망 - 금융, 항공, 교통,정보통신망등	- 국방,외교 및 공안망
주체	- 해커, 컴퓨터범죄자	- 개인적 침해위협 주체 포함 - 산업스파이,테러리스트 - 조직화된 범죄집단	- 국가정보기관 - 사이버전 전사
목적	- 금전, 명성획득 - 영웅심 발휘	- 범죄조직의 이익달성 - 사회, 경제적 혼란야기	- 국가기능 마비 - 국가 방위능력 마비
공격방법	- 컴퓨터 바이러스 - 다양한 유형의 해킹 - 서비스 거부공격 등	- 개인적 공격방법 포함 - 유,무선 도청 - 정보통신망 스니핑 등	- 개인, 기업적 공격방법포함 - 첨단 도청 및 암호해독 - 전자전 공격방법 등

3) 정보보호 Risk의 접근

기업은 정보보호의 위협을 식별하고, 위험의 규모를 결정하고, 대응책이 필요한 분야를 식별하는 일련의 과정으로 정보시스템 자원에 영향을 줄 수 있는 불확실한 사건들을 식별, 통제 또는 최소화하는 과정을 진행하게 된다. 통상 기업은 이러한 정보보호 Risk에 대해 위험회피(Risk Avoidance)와 위험이전(Risk Transfer), 그리고 위험감소(Risk Reduction, Mitigation)을 염두에 두고 보안활동을 전개하며, 때로 위험을 수용하기도 한다.

기업이 위험을 감소시킬 수 있는 대책을 채택하거나 구현하는 방법으로 취약성 감소, 발생가능성 감소, 영향 감소를 들 수 있다. 그리고 정보보호 대책의 선택기준은 결국 보안대책의 비용이 손실 발생확률과 발생시 손실을 반영한 결과보다 작을 때이며, 비용대비 효과가 클 경우이다[4].

기업은 정보보호의 Risk의 유형과 특성에 따라 정성적, 정량적으로 대책을 접근해 간다. 그러나 정보보호 특성상 정량적 접근방법의 결과는 현실과의 차이를 발생시킨다.

<표3> 정보보호 Risk의 정성적, 정량적 접근법

구분	정량적 접근법	정성적 접근법
개념	기대 위험가치 분석 = 위험발생확률 x 손실크기	- 손실크기를 화폐가치로 표현하기 어려움 - 위험크기는 기술변수로 표현
유형	- 수학공식 접근법 - 확률분포 추정법 - 확률지배 - 몬테카를로 시뮬레이션 - 과거자료 분석법	- 델파이법 - 시나리오법 - 순위결정법 - 퍼지행렬법 - 질문서법
주사용 지역	- 미국	- 유럽
척도	- ALE(연간기대손실)	- 점수(5,10점 척도), 언어표현
장점	- 비용/가치분석, 예산계획 - 자료분석이 용이함	- 금액화하기 어려운 정보의 평가 가능 - 분석시간이 짧고 이해가 용이함
단점	- 분석의 시간, 노력, 비용이 크다	- 평가결과가 주관적임

2. 보안 침해사고 피해, 대책과 투자

1) 보안 침해사고 피해

기업은 정보시스템의 활용도 증가 및 인터넷 등 네트워크를 통한 상호연결의 증가와 해커들 간의 자유로운 정보교환 그리고 정보시스템 관리자의 기술적 역량부족 및 정보보호에 대한 인식부족으로 해킹사고는 지속적으로 증가하고 있다[2].

<표4> 한국 연도별 해킹 및 웜/바이러스 침해사고 발생추이 (단위: 건)

구분	2000년	2001년	2002년	2003년	2004년	2005년9월
해킹	1,943	5,333	15,192	26,179	24,297	29,692
웜/바이러스	50,124	65,033	38,677	85,023	107,994	13,166

* 출처: 한국정보보호진흥원 KrCERT/CC 통계보고서

정보보호진흥원에 접수되는 공식적인 침해사고외에 기업의 대외이미지 및 신뢰도를 고려할 때 그 발생은 더욱 크다. 그리고 공식적으로 통계를 통한 체계적인 피해액의 산출 및 관리가 미흡한 상황이다. 단지 정보보호전문업체가 이벤트적으로 보안사고 발생시 기사에 포함하여 추정 발생 피해와 피해액을 발표하거나 정보보호전문기관 등의 담당자가 예측자료를 작성하여 세미나등에서 발표하는 수준이다.

공식적으로 기관과 민간의 침해사고 대응협의회 같은 기구에서 주기적인 발생 피해건의 현황과 예측 피해비용을 발표하여 기업들이 현황을 직시하고 적극 사업을 추진 대응하는데 정보를 제공하여 활용케 할 필요가 있다.

미국의 경우 리서치 전문기관인 컴퓨터이코노믹스사(Computer Economics Inc)에 따르면, 지난 2000년 바이러스 확산에 의한 총 경제손실은 17억1천만 달러였으며, 2001년에는 13억 2천만 달러에 달했다. 직접적인 손실외에도 정보보호 침해사고의 더 큰 문제점은 기업의 핵심 경영정보와 고객정보가 침해되고 유출되는 상황에서 입게되는 기업이미지의 실추를 들 수 있다.

지난 2000년 "마피아보이(Mafiaboy)"라는 인터넷아이디를 가진 15세 캐나다 소년은 아마존, 야후, e베이, CNN, E트레이드 등의 유명사이트를 잇따라 해킹하면서 큰 파장을 불러 일으켰다.

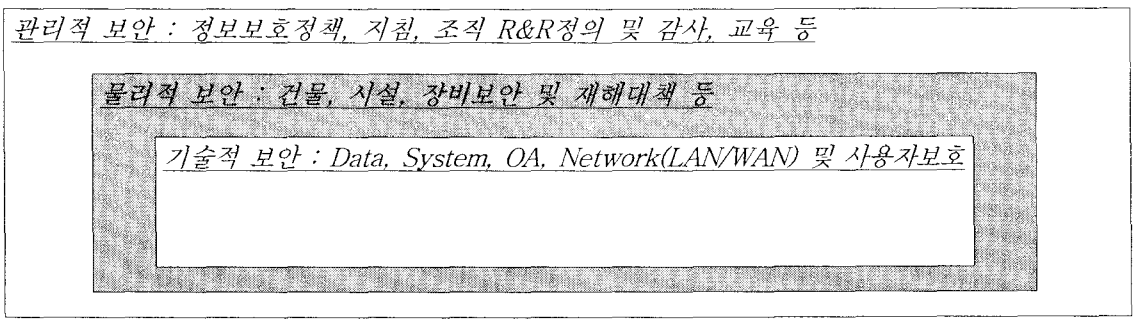
또 CD유니버스(CD Universe), 웨스턴유니온, 아마존의 자회사 비블리오파인드(Bibliofind)등 일부기업들이 고객의 신용카드 정보를 해커들에게 도난당하면서 상당한 기업이미지 실추를 경험했다.

또한 결국에는 관련 기업의 주가도 크게 하락시킨다. 마피아보이 해킹시 주가하락 규모가 수억 달러에 달하기도 했다[5].

2) 정보보호 대책

정보보호의 체계는 관리적 보호영역에 정책, 지침과 보안조직과 R&R을 정의하고 감사, 교육 등의 기능을 가지고 있으며, 물리적 보호는 건물, 시설 및 장비보안 및 재해대책을 포함하며 기술적 보호영역은 Data의 보호 System, OA, Network 및 사용자 정보보호 등으로 정의된다.

<그림1> 정보보호 체계



기술적 정보보호는 그 보호대상에 따른 Risk요소와 그 Risk를 염두에 둔 보호대책이 구분된다.

<표5> 대상별 기술적 정보보호 대책

구분	Data보호	System보호	OA보호	Network보호		사용자보호
				LAN	WAN	
보안대상	Disk,File상의 기업/고객정보	Mainframe Server	PC Phone, Fax	Switch,Router 무선인증서버	인터넷 전용Line	PC,핸드폰 단말기
Risk 요소	불법 위,변조 로그삭제 DB관리자공격	OS취약점공격 패스워드노출 비인가자접근	사내정보유출 신분위장 사용자	NW불법접근 NW인증취약 NW모니터링	도청 Data위변조 트래픽폭주	User정보유출 단말기복제 바이러스침투
보호대책	전자서명 접근제어List 백업 및 복구	사용자관리 Demon보호 로그관리,분석	사용자식별 화면통제 접근권한통제	암호화 라우팅,필터링 방화벽적용과 로그관리		암호화 개인정보분류 바이러스백신

기업의 정보보호 대책은 기반이 되는 체계위에서 기업내의 취약점을 찾아 대책을 수립, 적용하게 된다. 이제 기업의 정보보호는 국제적인 정보보호 정책 및 활동의 흐름과 정보통신부이 정보보호 활동과 관련공조를 고려하면 이젠 필수 추진항목이 되어가고 있다.

국제 경제협력개발기구(OECD)는 지난 1992년 네트워크화의 진전과 사회전체의 정보시스템에 대한 의존도가 높아짐에 따라 정보시스템의 신뢰성을 높이기 위한 정보보호가이드라인을 제정하였다. 이어 OECD는 점차 사이버테러에 대한 위험이 고조되고 범세계적으로 네트워크에 대한 상호연계정(Interconnectivity)과 상호의존성(Interdependency)이 증대되면서 정보보호환경이 변화하자 지난 2002년7월 정보보호 가이드라인을 전면 개정하였다.

<표5> OECD 정보보호 가이드라인 보안원칙 (OECD 2002.7)

구분	내용
인식(Awareness)	참여자들은 정보시스템과 네트워크 정보보호의 필요 및 보안을 향상시키기 위해 무엇을 할 수 있는지 인지하고 있어야 함
책임(Responsibility)	모든 참여자들은 정보시스템과 네트워크 정보보호에 책임
대응(Response)	참여자들은 보안사고를 방지, 탐지, 대응하는 데 시기 적절하게 협력
윤리(Ethics)	참여자들은 타인들의 적법한 이익을 존중해야만 한다
민주성(Democracy)	정보시스템과 네트워크의 정보보호는 민주사회에서의 근본적인 가치들과 조화되어야 함
위험평가(Assessment)	참여자들은 위험평가를 실시하여야 함
보안설계와 이행 (Design & Implementaton)	참여자들은 정보보호를 정보시스템과 네트워크의 핵심 요소로 포함시켜야 함
보안관리 (Security Management)	참여자들은 보안관리에 있어 포괄적인 접근방식을 도입해야 함
재평가(Reassessment)	참여자들은 정보시스템과 네크워크 보안의 재검토 및 재평가를 해야하며 정보보호정책, 관행, 도구, 절차등에 적절한 수정을 하여야 함

3) 정보보호에 대한 투자

정보보호에 대한 투자는 점진적으로 늘고 있지만, 아직도 기업이 사업의 매출과 수익을 염두에 든 상황에서 단순한 정보보호의 피해발생시 손실비용에 대한 감소효과를 생각하고 있다. 그리고 정보보호의 이해가 높아진 지금에도, 투자가 활발하게 이루어지지 못하고 있다. 여기엔 정보보호의 정량적 효과와 투자대비 경제적 효과를 명확히 제시하기 어려운 점등을 들 수가 있다.

(1) 국외 정보보호 투자 (미국을 중심)

미국 기업들의 정보보호의 투자는 IT예산의 8%정보를 투자하고 있으나, 국내 기업인 경우 2% 안팍이며, 대기업의 일부가 정보보호와 관련된 모든 비용을 포함하여 5%를 상회하고 있다.
미국 예산관리국(OMB)에서 발표하는 국방부(DOD), 에너지부(DOE), 법무부(DOJ), 보건복지부(HHS), 항공우주국(NASA) 등의 20여 정부기관들에 할당된 정보기술분야와 정보기술 보안분야에서의 지출액의 합계는 2002년 9.11테로 이후 정보기술 보안분야의 비중이 2.81%에서 5.56% 수준으로 급증하여 정보기술 보안분야에 적극적으로 투자가 이루어 졌다.
그리고 2003년부터 정보기술 분야의 지출액이 두드러지게 증가한 것은 2002년말에 신설된 국토안보부(DHS)에 대한 정보기술 분야의 예산규모가 확대되었기 때문으로 보인다.

<표6> 미 연방정부 기관의 정보기술 및 정보기술 보안분야 지출액 (단위: 10억 달러)

구분	2001	2002	2003(예상)	2004(예상)	2005(예상)
정보기술	46.1	48.6	52.6	59.3	59.8
정보기술 보안	1.3	2.7	4.2	4.7	N/A
보안 비중	2.81%	5.56%	7.98%	7.93%	N/A

* 자료: 예산관리국 (2003)

(2) 국내 정보보호 투자

2004년말 한국정보보호진흥원이 실시한 중소기업 실태조사에 의하면 총 IT비용에 중기업인 경우 6.1%, 소기업인 경우 2.2%를 투자하는 것으로 나타났다. 선진국의 수준에 매우 저조한 상황이다.
국내 공공기관의 정보보호 예산은 전체 IT예산중 5%미만이나 미국의 경우 10.6%를 투자하고 있다. 자체 전담인력 보유율도 5~13%, 가장 기본적인 침입탐지시스템의 설치율도 26~56%에 불과 한 것으로 나타났다. 해킹피해의 경험도 소기업이 24.1%, 중기업이 27.5%에 이르렀다.
이처럼 OECD국가중 초고속인터넷의 보급률이 1위이며, 인터넷 이용인구가 3000만명을 넘어선 상황이며, 인터넷 이용률 역시 세계최고 수준인 70%에 육박하고 있다. 최근 2년간 전자상거래 규모는 연평균 70% 이상 증가해 국내총생산(GDP) 대비 전자상거래 규모가 30%를 넘어서고 있다.
현재 국내,외 정보보호의 적정 투자기준은 없다. 미국의 공공기관의 정보보호의 투자가 IT총예산의 10.8%가 민간부문이 5%에 육박하고 있는 경우를 고려하여 국내의 민간 및 공공기관의 정보보의 예산이 IT총 예산의 5%이상이 되어야 하는 것이 바람직하다고 이야기하고 있다.
이를 위해 OECD회원국으로서 선진 각국의 정부 및 기업의 정보보호부문에 대한 투자대비 정보보호부문의 적절한 투자의 비율을 정의하여 적극적으로 추진하는 것이 향후의 무역장벽으로 작용이 예측되는 Security Round에 대응하는 것이 필요하다.

III. 정보보호 투자의 경제성 평가

1. 경제성 평가 접근개념

기업의 정보보호의 투자결정 요인은 기업에서 기본적으로 기업이 위험요소라고 판단하는 보안사고를 적정한 투자로 막고, 대외적인 사업과 서비스에 정보보호 기능을 부가하게 될 경우에 이로 인한 기업의 수익에 긍정적인 효과를 고려하는 것이다.
후자는 수익으로 연결되지 않는 경우에 이에 대한 부정적인 영향을 미치게 되는 경우이다.
전통적으로 경제학적 접근방법은 새로운 사회적인 현상이 어느 정도 정규화되거나 그 현상에 대한 충분한 자료가 축적된 이후에 비로소 이론적으로나 실증적으로 그 사회현상을 규명하는 식의 궤적을 그려왔다. 개인정보보호, 스팸메일등의 정보보호와 관련한 여러 가지 사회현상이 시작된 지는 꽤 오래되었으나, 최근 들어 정규화 되거나 그에 대한 보다 구체적인 자료가 축적되었다고 보이며, 정보보호에 대한 경제학적 접근방법은 지금보다도 앞으로 더욱 활발해질 것으로 보인다[5].

<표7> 정보보호 투자에 대한 경제적 개념

구분	내용
경제적 유인성	정보보호로 인한 위험을 가장 관리하고 방지할 수 있는 경제주체에게 책임(Liability)이 부과되어야 한다고 주장
Network의 규모특성	하나의 네크워크에 속한 사람이 많아질수록, 그 네크워크의 가치가 증가하는 현상
비대칭적 정보	비대칭적인 정보는 정보가 한쪽에만 존재하고, 다른 쪽에는 존재하지 않는 상황 즉 정보가 비대칭적으로 분포되어 있는 상황
가격차별과 개인정보	정보기술이 발전함에 따라 개인정보에 대한 보호를 강화하는 방식과 그것을 침해하는 방식의 발전이 동시에 가능해졌음에도 불구하고 현재까지는 개인정보의 침해가 그것의 강화보다는 훨씬 폭넓게 관찰되며 사회적으로 문제되고 있슴

IT산업의 특성은 다음과 같은 Network의 외부성, 규모의 경제특성, 시스템적 효과의 특성을 가지고 있다.

<표8> IT산업의 특성

구분	내용
Network의 외부성	네크워크 외부성이란 하나의 네크워크에 속한 사람이 많아질수록, 그 네크워크의 가치가 증가하는 현상
규모의 경제특성	공급측면에선 연구개발 및 제품출시를 반영한 높은 고정비용과 낮은 생산비를 반영한 무시할 만한 한계비용에 따라 규모의 경제를 갖게되며, 이는 생산이 증가할수록 평균비용이 감소하는 현상.
시스템적 효과	IT제품은 어느 한 가지가 독립적으로만 존재하여 기능하는 것이 아니라 소프트웨어와 하드웨어운영체계와 애플리케이션의 경우처럼 하나이상 다수의 상품이 결합할 경우에만 완결된 하나의 소비재로서 역할을 하는 시스템적 효과

그리고 위의 Network특성은 다음과 같은 IT시장의 현상으로 나타난다.

<표9> IT시장의 현상

구분	내용
고착현상 (Lock Effect)	사용자들이 하나의 제품에서 다른 제품으로 전환하기가 매우 힘든 상황이 쉽게 관찰
Winner takes all 현상	승자내지 선점자가 시장의 점유율이나 매출이나 이윤의 거의 대부분을 가져가는 방식
공급자와 협력관계	공급자는 시장에 빨리 진출하고 일단 진출한 후에는 자신의 제품과 보완적인 공급자와의 협력관계를 지속

그리고 이와 같은 현상은 정보보호에서 다음과 같은 현상으로 이어진다.

<표10> 정보보호의 시장현상

구분	내용
제품의 빠른 시장출시 (time to market)	시장 선점을 위해 제품의 출시를 가급적 앞당긴다는 사실은 반대로 제품이 정보보호의 관점에서 불완전할 개연성이 높아지는 것을 의미
애플리케이션 개발자와의 보완관계	시스템적인 효과가 있기 때문에 특히 운영체계 벤더에 있어 애플리케이션 개발자와의 보완관계가 필요
최종소비자의 중요성은 상대적으로 무시	그 제품에 고착되며 자연스럽게 소비하는 피동적인 이용자로 인식되어 중요성이 무시
비표준화적인 접근	애플리케이션 프로스램 인터페이스를 비표준화적인, 복잡하고 버그가 많게 만드는 것

일반적으로 정보보호가 이루어지기 위해서는 각종 위협으로부터 대처할 수 있는 기본적인 요소를 갖추어야 한다. 즉 비밀성(Confidentiality), 무결성(Integrity), 가용성(Availability), 인증(Authentication), 접근통제(Access Control)등이 보장되어야 한다. 그러나 이러한 요소를 만족시키기 위해서는 요소간 상충되는 측면이 발생하기도 하고 비용도 많이 소요된다. 그러므로 적절한 정보보호가 이루어지기 위해서는 기업에서 보유하고 있는 자산과 정보시스템이 가지고 있는 가치를 우선 파악하고 이에 대한 정보보호 위협의 위험성과 예상되나 손실을 평가하여 이에 대응하는 적절한 수준의 정보보호 투자가 이루어지는 것이 바람직 하다.

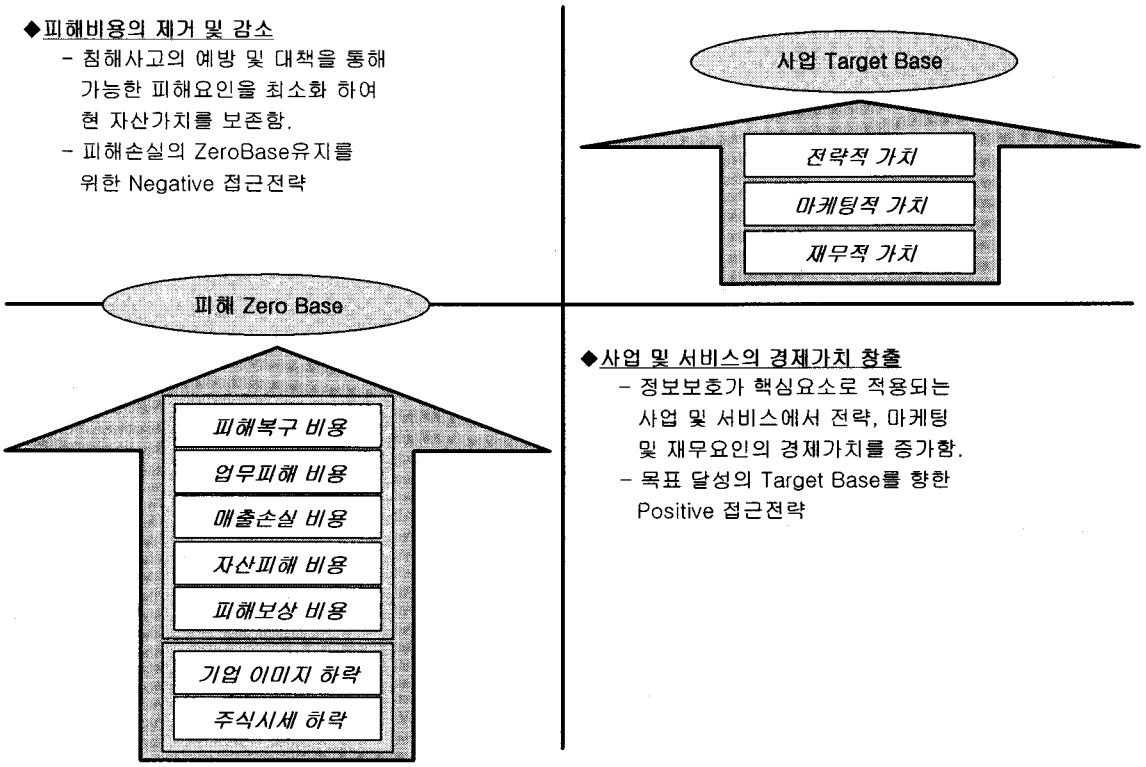
이를 위해 정보보호 투자에 대한 경제적 개념에 기초하여 시장의 현상을 파악하고 기업의 요구사항과 사업 및 서비스의 추진현황에 기초하여 분석하여도 투자에 대한 정략적 효과를 산정에는 기업내의 정책과 산정방향에 대한 작업방법과 기준에 대한 정의가 필요하다.

2. 정보보호 경제성 평가 접근방법

기존의 기업이 바라보는 정보보호 투자는 피해비용의 감소를 통해 현재의 자산의 가치를 보존하는데 국한되어 있다. 그러나 기업의 정보보호에 대한 투자의 관점은 현재의 자산가치의 보존에 국한되어 있는 것이 아니라, 미래의 가치를 보존하기 위한 관점에 모아지고 있다.

정보보호 투자에 대한 경제성 평가는 자산의 보호차원의 피해비용의 사전제거 및 최소화와 신규사업/서비스의 지원시 타사대비 핵심경쟁우위를 확보하게 될 경우의 문제를 제거하므로서 얻게되는 이득을 정의하게 된다.

<그림2> 정보보호 경제성 평가의 접근방법



IV. 정보보호 투자의 경제성 평가

1. 경제성 평가기준

1) 경제성 평가의 접근

기업에서의 정보보호 투자의 경제성 평가기준은 정보보호에 투자를 하므로서 발생되는 피해비용의 예방을 통한 피해비용의 감소를 들수 있다. 그리고 정보보호도 신규사업과 서비스영역에 투자하므로서 경쟁우위 요소로 얼마나 활용되어 지나로 구분되어 질 수 있다.

기업의 피해비용 및 예방의 요소는 현재의 자산과 수준을 ZeroBase로 정의하고 이를 피해를 방지하는 Detection개념으로 접근하는 것이다. 기업의 신규사업, 서비스관련 정보보호의 투자가치는 일반적인 요소와 동일하게 가치를 산정하여야 한다. 이를 위해선 사전 해당 산업이 영향을 미치는 요소에 대해 Factor를 반영하는 Positive하게 접근하여야 한다.

(1) 피해비용의 제거 및 감소

기업에서의 피해비용은 직접손실비용과 간접손실비용으로 구분할 수 있다. 직접손실비용은 피해복구비용, 시스템장애로 인한 업무손실비용, 매출감소비용, 무형자산의 해킹과 유출이 있는 경우 현재 자산가치의 손실비용인 자산 피해비용 그리고 사고로 인한 피해고객 및 관련된 기업에게 지불하여야 할 비용으로 피해보상 비용을 들 수 있다. 간접손실비용은 조직의 외부 이지 하락과 내부 조직원의 사

기저하등에 미치는 이미지하락, 그리고 사고발생으로 미치는 주가하락을 들 수 있다.

(2) 사업 및 서비스 경제가치 창출
기존산업에 정보보호투자가 이루어 지는 경우: 신규사업,서비스의 창출요소는 크지 않다.
그러나 인터넷 사업의 경우, 고객정보와 개인정보의 유출이 시스템 사용의 편리성을 우위에 따라서 얼마나 더 그 크기를 확보하느냐는 전략적인 차원에서 BM과 설문을 통해 산정하는 것이 바람직 하다.

2. 피해비용의 제거 및 감소

1) 피해비용의 산정

(1) 기존의 산출기준

정보보호의 피해비용산정의 기존연구는 미국의 ICAMP-I,II결과와 일본 IPA연구를 들수 있다. ICAMP-I,II의 추진은 대학 캠퍼스 환경하에서 IT관련 사고 비용을 분석하고 모형화한 프로젝트 ICAMP(Incident Cost Analysis and Modeling Project)는 미국 CIC(Committee on Institutional Cooperation)에 의한 지원을 바탕으로 IT사고의 실질적 비용을 추정하기 위해 시작되었다 [6].
일본 IPA(Information Promotion Agency)는 2001년 보안대책 연구개발등 사업의 일환으로 일본 JNSA (네트워크 보안협회)에 정보보안 사고에 관한 조사프로젝트 추진하였다. 정보보안 사고와 관련된 피해액과 투자액 등의 실태를 파악하여, 이 조사 결과를 바탕으로 사고에 의한 피해액 및 대책비용의 산출모델 책정을 검토하고 현 시점에서 생각할 수 있는 하나의 안을 제시하고 있다 [7].

<표11> 정보보호 피해비용의 기존산출 연구비표 [6],[7]

구분	미국 ICAMP	일본 IPA연구
적용환경	대학 캠퍼스	이윤추구하는 일반기업
피해산출시점	피해복구 완료이후 산출	(좌동)
Data수집방법	사고발생 조직대상으로 직접 설문/ 인터뷰 조사후 피해액 산출	(좌동)
피해복구비용	내부근로자의 시간당 인건비 이용 (노동력 + 시설물)	내부근로자의 시간당 인건비 이용 (인건비 중심)
업무마비에 따른 피해액	사용자 측면에서 계산 시간당 인건비(수험료) 이용	IT감응도를 이용한 세부적 계산
손실이익	추가 인건비(근로자 + 사용자)의 28%	명확한 경우만 계산 대체수단등의 모호한 손실이익은 업무마비에 따FMS 피해액으로 간주
이미지하락	(피해복구비용 + 업무마비 피해액 + 손실이익)의 52%	N/A
주가하락	N/A	N/A

기존 연구의 고려사항은 미국 ICMP의 문제점은 손실이익, 간접피해액 산출시 사용되는 수치가 (28%, 52%)가 통계를 기초로 하고 있으나 국내환경에 적용가능한 것인지 검증이 되지 않아 실제 패해액과의 편차를 가지고 있을 것으로 판단되며, 일본의 경우 IT감음도등 피해액에 큰 영향에 미치는 파라미터의 수치를 주관적으로 판단할 수 있다. 실제 사례로 적용하려면 구체적인 데이터가 필요하다.

(2) 개선 산출기준

기업에서의 정보보호의 피해비용 산정의 기존연구인 피해비용이 복합적인 요인과 상황을 반영하여 도출되므로 직접손실비용과 간접손실비용으로 구분하고, 직접손실비용은

피해복구비용, 업무피해비용, 매출손실비용으로 구분하고 간접손실비용은 피해배상비용, 이미지하락 비용과 주식하락비용으로 구분하여 도출한다.

<표12> 피해비용 개선 산정항목

구분		내용
직접 손실비용	피해복구비용	사고 발생후 일어난 사고를 복구하여 사고직전의 상황으로 되돌리는 데 투입된 각종 인건비와 HW/SW에 대한 비용
	업무피해비용	사고발생으로 업무장애로 인해 미치게 되는 피해비용
	매출손실비용	사고에 의해 기업이 사업, 서비스를 하지 못해서 발생되는 매출의 피해비용으로 기업의 IT자산에 의존하는 업태에 따라 일반매출 손실과 특수매출손실로 구분
	자산피해비용	사고로 인한 피해대상 자산의 현재자산가치를 산정한 비용
	피해보상비용	사고로 인한 피해고객 및 기업에게 지불하여야 할 비용
간접 손실비용	이미지 하락	조직의 외부이미지 하락, 내부 조직원의 사기저하등 사고 발생시점으로부터 발생하는 그 사고의 눈에 보이지 않는 장기적 여파
	주식시세 하락	사고 발생에 의해 사내,외 투자가들의 투자결정의 회피를 통해 주시가격에 미치는 손실비용

여기에서 직접손실비용은 구체적인 수식에 의해 산정요인들을 반영 손실비용으로 정의하고 간접손실비용은 기업내,외의 지속적인 조사,분석을 통한 통계정보의 기준정의에 의해 산정한다.

<표13> 개선 산정항목별 산정기준

구분		내용
직접 손실비용	피해복구비용	내부 추가 인건비 + 외부 인건비 + HW/SW수리 및 구입비용
	업무피해비용	업무피해 시간 x 단위시간당 야근비용
	매출손실비용	일반매출 손실비용 = 직원의 시간당 인건비 x 영향받은 직원수 x 업무 정지시간 x 업무종류에 따른 피해(%) x 업무종류에 따른 IT의존도(%) x 직원의 매출기여도(%)
		특수매출 손실비용 = 해당 분야의 시간당 매출액 x 업무정지시간 x 특정 IT자산의 피해율(%)
	자산피해비용	사고발생직전 자산현재가치 = 자산(유,무형)에 기인한 이익 / 자본화율
	피해보상비용	약관이나 계약서에 명시된 기준이나 객관적인 피해보상기준에 의해 산정된 비용
간접 손실비용	이미지 하락	사고에 의한 기업 이미지하락으로 매출감소와 이미지 회복에 투입되는 홍보비등의 대한 설문조사와 통계적 정보의 분석등으로 도출
	주식시세 하락	사고발생에 의한 일정기간내의 주식시세 하락에 대한 범위를 산정하여 사고유형 및 등급별 주시시세 하락에 대한 통계적 분석, 도출

피해복구비용에서 내부추가인건비는 피해복구와 관련된 사내직원의 인거비로 정의하고, 외부인건비는 사고복구에 투입된 외부인력에 대해 지급된 금액만큼의 사고복구를 위해 투입되는 비용으로 한다. 그리고 사고로 인해 수리 및 추가구입하여야 HW/SW수리 및 구입비용을 고려한다.
업무피해비용은 사고로 피해시간에 하여야 할 업무를 별도로 야근에 의해 수행하는 것을 고려 산정하여 업무피해시간과 야근시간당 수당의 곱으로 하여 산정한다.

일반매출손실비용의 산정은 일반적인 조직들에서 발생하는 매출손실액을 말하는 것으로 특수 매출 손실액이 발생하지 않은 사업분야에서 발생하는 것을 뜻한다. 즉 피해자산이 매출에 영향은 미치지만 대체수단이나 잔업등으로 어느 정도의 매출이익을 유지하는 경우, 피해자산이 매출에 직접 영향을 미치지는 않으나 직원들의 업무에 지장을 초래하여 업무효율이 떨어지는 경우에서 발생하는 피해정도를 금액화하려는 것이다. 그리고 특수매출손실비용은전자 상거래소유 기업, 인터넷 서비스 제공기업등 사업분야중 특정분야가 명확하게 IT자산에 의존하는 일부 조직에게서 발생하는 매출관련 피해액으로 대체수단이 존재하지 않아 다른 노력으로 매출손실에 대한 복구가 불가능 하고, 타격 받은 IT자산의 피해정도가 명확히 매출손실로 연결되는 경우 발생하는 피해액이다.

피해보상 비용은 사고로 인해 입은 기업에 대해서만 피해보상 비용을 판단하는 거은 사고 발생 시 사고 복구 완료시에 정확한 금액수치로 나오기 때문에 실제로 고객이나 관련기업에 보상한 비용을 합산하여 적용하면 된다.
2002년 미국의 통계자료에 의하며 예방비용이 피해비용의 37%를 넘지 않으나, 사고발생시 사고발생 이틀내에 시장가치의 2.1%, 1.65억 달러의 손실이 발생한 경우가 발표된 바 있다[8].
그리고, 기업이미지 하락은 조직의 외부이미지 하락, 내부 조직원의 사기저하등 사고 발생시점으로부터 발생하는 그 사고의 눈에 보이지 않는 장기적 여파를 의미한다. 기업이미지의 저하, 직원사기 저하, 사고로 입은 정신적 피해 등은 향후 매출이나 조직의 업무수해에 영향을 미치기 마련이나 이를 금액화하는 것은 매우 어렵고 사업분야나 형태, 피해발생이유나 대처결과 등에 따라 그 정도가 크게 달라진다. 이미지 회복에 투입되는 홍보비 등의 대체수단과 설문조사, 통계적 수치적용 등의 방법을 생각해 볼 수 잇으나 그 수치에 대한 검증은 어렵다.

3. 사업 및 서비스 경제가치 창출

1) 사업 및 서비스의 전제사항

정보보호가 경쟁요소로 반영되는 사업 및 서비스인 경우에 정보보호는 부가가치를 창출하게 된다. 기존에 정보보호가 보험성격과 같다고 하는 것은 단순히 시설보안이나 보안시스템이나 IT환경의 정보시스템 등에 보안시스템에 투자하고, 발생되거나 예측되는 보안사고로 인한 피해비용의 제거 및 감소에 국한하였을 경우에 그러하다.
그러나 유비쿼터스 환경에서 다양한 융,복합화 되어가는 환경에서의 사업과 서비스에 정보보호가 전제가 된다고 하면, 시스템에 추가되는 보안기능으로 인한 Performace의 증가나 Response Time 의 추가를 고려하되, 안전한 기업경영정보, 고객정보 및 인터넷상의 거래정보의 관리등을 통해 고객의 만족도를 고려한 경제가치를 고려해야 한다.

2) 경제가치 창출

정보보호의 특성중 기밀성, 무결성, 가용성에 근거하여 정보보호가 경쟁사간 관련 사업과 서비스에 핵심 경쟁우위 요소로 활용되어 질 경우 다음과 같은 측면을 검토할 수 있다.

(1) 전략적 가치 측면

OECD가 2002.7월 제시한 "OECD 정보보호 가이드라인 보안원칙"이 향후 국가간 무역거래에 있어서 Security Round로 작용할 가능성이 많다. GATT(과세 및 무역에 관한 일반협정)가 WTO (세계무역기구) 변화해 가면서 무역에 관한 우루과이라운드가 뉴라운드로 그리고 도하라운드로 확대, 전개되는 것과 환경과 관련된 도쿄라운드와 같이 국가간의 장벽을 넘어 인터넷을 통한 해킹 및 웜/바이러스의 공동대응과 안전성의 수준을 위해 Security Round의 적용이 예측된다

그러므로, 정보보호의 활동과 이로인한 ISO17799 및 SSE-CMM의 인증등을 통한 기업에 적정한 보안수준의 객관적인 인증준비 추진은 기업의 경영전략의 기본요소이며, Governance의 확보, 유지 차원에서 필요하다.

(2) 마케팅적 가치 측면

기업의 사업과 서비스에 있어 고객정보와 거래정보의 안전한 관리 및 활용은 대 고객만족의 결정적 요인으로 작용한다. 서비스환경의 보안적 취약점으로 인한 고객의 서비스해지와 경쟁사로의 변경 등을 고려하는 고객에겐 정보보호의 안정성은 결정적인 요소로 작용한다.

특히 신규사업, 서비스의 개시와 Promotion을 통한 확대시에 안전한 서비스 추진전략과 안전성은 현재 인터넷상에서 이루어지는 사업과 서비스는 정보보호 투자중 "가격차별과 개인정보"의 요소는 사업과 서비스의 마케팅에서 결정적인 성공요인의 하나다.

(3) 재무적 가치 측면

기업이 가지고 있는 브랜드가치의 증가에 관련된 재무적 가치를 먼저 생각할 수 있다. 브랜드가치의 브랜드인지도, 브랜드선호도, 지각된 품질, 브랜드 안전성의 연상이미지의 요소등이 브랜드 가치향상에 관련되므로써 얻게되는 재무적 효과다. 경쟁브랜드의 정보보호 차별화에 의한 사업, 서비스 가치 평가의 우위도 향상요소로 작용한다.

신규사업 및 서비스의 경우 정보보호 투자초기엔 재무적인 가치 측면은 거의 미미한 상황이므로 무시할 수 있겠다. 그리고 지각된 품질의 고객이 서비스에 가지게 되는 품질요소중 성능, 디자인, 내구성, 안전성 등의 서비스와 관련된 지각이나 인식중에서 유비쿼터스의 정보보호 중요성을 생각할 때, 그 비중은 점차적으로 커질 것으로 예측된다.

V. 결론

정보화가 성숙되어 유비쿼터스 환경으로 변화해 가는 상황에서 기업이 변화를 수용하고, 적극적으로 예측되는 Risk를 제거하기위해 효과적으로 정보보호 활동을 전개하여야 함에 있어, 정보보호 투자에 있어 다음과 같은 사항에 기초한 경제성 평가의 접근방법을 고려하여 추진하는 것이 바람직 하다.

1. 기업의 정보보호는 이제 가시적인 이익을 염두에 두고 투자하여야 한다.

정보보호의 투자를 보험과 같은 선상에서 판단하며 단순히 피해비용의 제거 및 감소외에 정보

보호가 사업과 서비스에 핵심요소로 작용하는 영역을 찾아 경제가치 창출이 가능하다.

2. 기업의 정보보호 투자의 경제성 평가접근 방법은 피해비용 ZeroBase유지의 Negative접근전략과 사업 및 서비스의 Target Base지향을 위한 Positive접근전략을 고려할 수 있다.
3. 정보보호의 피해비용의 산정은 직접손실비용과 간접손실비용으로 구분하여 직접손실비용은 피해복구비용, 업무손실비용, 매출손실비용과 피해보상비용을 고려하며, 간접손실비용의 경우 이미지손실과 주식회사인 경우 주식시세의 손실을 염두에 두어 산정하는 것이 바람직하다.
   단, 간접손실비용의 경우 다양한 요소가 관련되므로 기업내에 정보보호이벤트를 염두에 두고 관련요소의 설문 및 지속적인 통계분석작업이 필요하다.
4. 정보보호 침해사고로 인한 피해산정의 직접손실 및 간접손실비용의 기준은 주기적으로 정보보호전략 및 실행부서에서 산정하고 그 결과를 평가해 가면서 관련 인자의 기준을 기업의 환경을 고려하여 최적화 나갈 필요가 있다.
5. 정보보호가 핵심 경쟁우위 요소로 활용되어 지는 사업 및 서비스에서 정보보호 경제가치는 전략적 측면과 마케팅적 측면 그리고 재무적 측면에서 고려할 수 있으며, 이의 산정을 위해 사업 및 정보보호담당자가 참여하는 설문 및 협의와 매출통계분석을 통해 경제가치를 산정해 갈 수 있다.

기업이 정보보호 투자시 발생되는 피해비용의 감소와 사업 및 서비스 등에서 예측되는 경제가치 창출에 대한 접근 개념을 정의하고, 이후 정보보호 투자에 대한 경제성 평가지표의 개발을 통해 기업의 정보보호 정량적인 관리를 좀 더 구체화하여 효과적인 정보보호 투자가 이루어지도록 함에 있다.

참 고 문 헌

[1] Jeremy Rifkin with Ted Howard, "Entropy", Penguin Books, 1989
[2] 정보통신부, "2005년 국가정보보호백서", 2005.6
[3] 이재열, "위험사회와 정보화의 명암", Information Security Review
[4] 이영환, "위험의 경제분석", 율곡프레스, 2004.10
[5] 신일순, "정보보호의 경제학적 의미에 대한 소고", Information Security Review, 2004
[6] CIC, "ICAMP(Incident Cost Analysis and Modeling Project)-I, ICAMP-II", 1998, 2000
[7] IPA, "Security Incident 관련 조사보고서 ver1.0", 2002.6
[8] L. Jean Camp & Stephen Lewis, "Economics of Information Security", KAP, 2004