TCO 기반 정보보호 투자수익율(ROSI)에 대한 연구

A study on TCO-based Return on Security Investment(ROSI)

김정덕*, 박정은**

목 차

Key Words: ROSI, TCO, 정보보호 예산

Abstract

최근 정보보호의 중요성에 대한 인식이 확산되고 있음에도 불구하고 정보보호에 관한 적절한 투자가 이루어지지 않아, 효과적인 정보보호 시스템 구현이 지연되고 있다. 이는 전 세계적인 경제불황이라는 원인도 있겠지만, 정보보호 투자에 대한 정당화 논리가 부족하여 최고 경영자의 의사결정에 적절히 반영되지 않은 이유가 더 크다고 할 수 있다.

정보보호는 조직의 업무 수행에 수반되는 부대비용 개념으로 인식되어 왔으며, 이 결과, ROI와 같은 정보보호 투자에 대한 정당화 논리를 제공하지 못해 적절한 투자가 적절히 수행되지 못하였다. 따라서 최근에는 정보보호 투자에 대한 수익과 지출간의 관계를 통한 ROSI(Return on Security Investment) 분석을 통한 정당화 논리 전개에 대한 필요성이 대두되고 있다.

본 논문에서는 ROSI 산출에 대한 접근방법을 비교 분석하고 TCO(Total Cost of Ownership)를 이용한 ROSI 방법을 제시하고자 한다. TCO는 하드웨어 가격뿐만 아니라 기술지원 및 유지, 지원 인력 등을 모두 고려한 총 소유비용이다. 즉, 정보보호에 대한 정확한 총 비용을 구하는데 매우 적합하다고 할 수 있다. 본 연구의 결과는 기업들로 하여금 좀 더 효과적인 정보보호 투자 정당화 수단으로서 활용될 수 있을 것이다.

* 중앙대학교 정보시스템학과 교수, jdkim@cau.ac.kr, 017-322-6380
** 중앙대학교 정보시스템학과 대학원 석사과정, eun25@naver.com, 017-739-8040

Ⅰ. 서론

최근 정보보호의 중요성에 대한 인식이 확산되고 있음에도 불구하고 정보보호에 관한 적절한 투자가 이루어지지 않아, 효과적인 정보보호 시스템 구현이 지연되고 있다(CIO Research Reports, 2003). 적절한 투자가 이루어지지 못한 이유로는 CEO나 CFO들에게 정보보호 투자에 대한 객관적인 정당성이 충분히 제공되지 않았기 때문이다.

최고경영자층들은 미래에 발생할 수 있는 정보화의 역기능으로 인한 손실 부분을 미연에 방지할 수 있을지도 모른다는 점을 정보보호의 효익(benefit)으로서 생각하고 있다. 이는 지금까지 ROSI(Return on Security Investment)에 관한 연구의 부족과 또한 실제적인 정확한 수치의 ROSI가 존재하지 않았다는 것을 의미한다. 그동안 CIO들은 정보보호에 대한 투자를 위하여 공포, 불확실성, 의심 등의 막연한 두려움을 전제로 정당화하려 애썼다(Berinato, 2002).

그러나 이러한 공포전술(threat tactics)를 사용한 정보보호 투자에 대한 정당화 방법은 제한적이라고 할 수 밖에 없다. 공포전술은 곧 정보보호에 대한 부정적 인식을 결과함으로써 정보보호에 대한 투자는 조직을 운영하기위한 일종의 부대비용이라는 인식을 초래할 수 있다. 또한, 정보보호 투자에 대한 수익률을 CEO에게 확실하게 제시할 자료가 없기 때문에 CEO입장에서는 정보보호 투자안은 다른 투자대안에 비해 낮은 우선순위를 가질 수밖에 없었다.

따라서 정보보호 투자를 적정한 수준까지 실현하기 위해서는, 보다 객관적이고 정량적 방법에 근거한 ROSI 연구에 대한 요구가 최근 점증하고 있다.

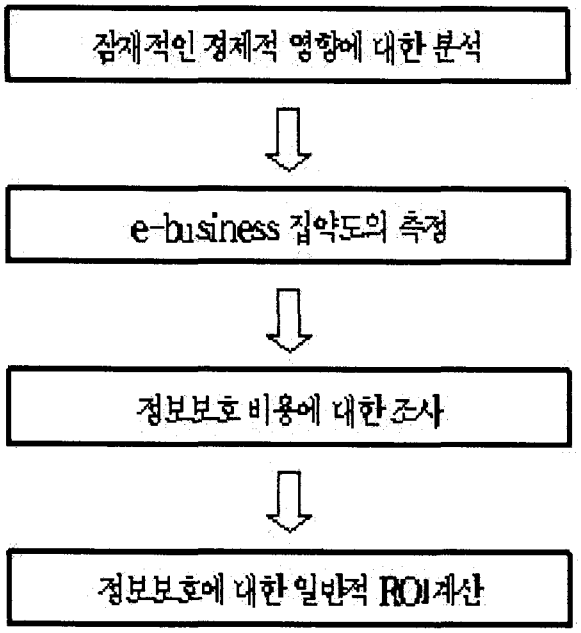
이러한 상황에 대응하기 위해 최근에 몇몇 연구들이 정량적인 ROSI 개발을 위해 수행되고 있다(Berinato, 2002). 따라서 본 논문에서는 지금까지 연구되었던 ROSI들의 접근방법들을 비교분석하여 실무에 사용되기 위해 필요한 이슈들을 도출하고자 하였다. 이에 기초하여 ROSI의 활용도 및 정확성을 제고하기 위해 TCO(Total Cost of Ownership)를 활용한 ROSI방법을 제시하였다. TCO는 가시적 비용뿐만 아니라 비가시적 비용까지 계산하므로 정보보호의 정확한 총 비용을 구하는데 매우 적합하다고 할 수 있다(김경근, 2001). 따라서 TCO를 이용한 보다 객관적이며 유연성있는 ROSI 접근방법의 결과는 기업들로 하여금 좀 더 효과적인 정보정보보호 투자 정당화 수단으로 활용될 수 있을 것이다.

Ⅱ. ROSI의 접근 방법

1. ROSI의 일반적 접근 방법

Computer Economics는 정보보호에 대한 일반적 ROSI분석을 〈그림1〉과 같이 도식화하였다 (Cisco Systems, 2003) .

〈그림1〉 일반적 ROSI 도출과정



해킹이나 침입의 결과로 인한 단일 조직체가 받는 경제적 영향은 다음과 같이 세가지 유형으로 구분할 수 있다.

1) 단기적인 경제적 손실 - 시스템의 손상, 사업 운영의 차질, 거래 및 현금 흐름의 중지
2) 중기적인 경제적 손실 - 공급망 내의 다른 조직체와의 계약 미이행, 소매 매출 손해, 조직체에 대한 부정적인 평판, 새로운 사업 개발의 지연
3) 장기적인 경제적 영향- 시장가치 하락, 투자자의 신뢰 저하, 주가 하락 등

e-비즈니스 기술에 많이 의존할수록 악의적 공격으로 받는 경제적 영향도 커지므로 이러한 부분을 다 고려한 총 경제적 영향을 분석해야 한다.

e-비즈니스 집약도의 측정단계에서는 정보시스템 직원 구성비율, 웹사이트를 통한 서비스 여부, 재택근무, 웹기반 B2B, B2C 거래여부, 웹사이트를 통한 EDI 등과 같은 웹기반을 토대로 한 수익의 창출이 높다면 집약도가 높은 상태이다. e-비즈니스의 집약도가 높을수록 정보보호에 대한 지출은 많을 것이다.

정보보호 비용에 대한 구성은 회사의 규모와 성격, 정부의 규제, e-비즈니스 집약도 등과 같은 여러 상황에 의해 영향을 받을 수 있다. 대체적으로 위험수준이 낮은 환경에서는 정보보호 지출이 적고, 금융기관처럼 위험수준이 높은 환경에서는 정보보호에 대한 지출이 많다.

정보보호에 대한 일반적인 ROI계산 측면에서 고려해야 할 몇 가지 변수가 있다. 정보보호 비용을 측정하는 과정에서는 위협 수준을 재평가 한 후에 필요할 수도 있는 기존 비용도 고려된다. 첫째, 정보보호에 지출된 금액이다. 둘째, 기존의 위협 수준을 파악하거나 최소한 그에 대해 알려진 내용을 확실히 파악해야 한다. 셋째, 조직체들을 공격으로부터 보호하는 특별조치를 취하도록 요구하는 법률 및 규정들을 들 수 있다.

이렇게 구해진 악의적 공격으로 인한 경제적 영

향에서 총 예상 정보보호 비용을 뺀 나머지 금액이 정보보호지출에 대한 ROI가 된다.

ROSI = 공격으로 인한 경제적 영향
- 총 예상 정보보호 비용

2. 아이다호 대학의 ROSI

2000년과 2001년에 아이다호 대학교 연구팀은 가시적 자산에서부터(감가상각을 고려해 금액으로 측정되는 자산) 비가시적 자산(소프트웨어 A는 소프트웨어 B보다 3배의 가치가 있다는 식의 비교가치로 측정되는 자산)까지 모든 자산에 가치를 부여하고 미국방부가 개발해 널리 사용되고 있는 해킹의 종류 분류법에 따라 비용도 다르게 측정했다. 이렇게 해서 만든 공식은 다음과 같다[2].

(R - E) + T = ALE
R - ALE = ROSI

R = 침입으로부터 복구하기까지 소요되는 연간 비용
E = 침입을 탐지함으로써 얻게 되는 손실 절감액
T = 침입 탐지 도구 비용
ALE = 연간예상손실액(Annual Loss Expectancy)

이 방식은 침입탐지시스템 도입에 따른 ROSI를 도출하는 방식을 제시한 것으로 개념적으로도 불분명하고 또한 실무적으로도 적용하기는 매우 어렵다고 할 수 있다. 관련 공식에 의하면 ROSI는 (E - T)로 정의할 수 있는데, E와 T에 대한 구체적인 계산방식도 제시되지 않고 있으며 실제적으로 관련 데이터를 수집하기도 용이하지 않다. 즉, 손실 절감액(E)을 정확히 정의내리기는 쉬운 일이 아니다. 이를 위해서는 많은 데이터가 필요할 것이다. 복구 비용(R) 역시 환경과 공격에 대한 노출 정도에 따라 다양하기 때문에 확실히 산출하기가 매우 어렵다.

3. CMU의 ROSI

카네기 멜론 대학교(CMU)는 CERT의 데이터를 이용하여 모델을 만들었다. CERT는 1988년 당시 아주 제한적 공중망(나중에 인터넷으로 확대)의 10%를 감염시킨 웜 바이러스의 공격 이후 미 정부가 수립한 기관이다. CERT는 정보보호 결함들을 기록하고 위협들을 추적하는 업무를 수행한다. 그들이 정의한 변수들은 공격의 유형과 공격 빈도수, 어떤 하나의 공격이 특정회사에서 발생할 확률과 그 공격이 가져온 피해액, 그리고 어떤 방어책이 사용되었는지 그것의 도움이 얼마만큼 이였는지 등이다.

연구자들은 이 데이터를 사용해 공격 엔진을 만들어 가상기업과 접목시켰다. 이후 어떤 일이 일어났으며 그 네트워크가 어떻게 공격을 이겨냈는지를 기록하였다. 또한 연구자들은 공격변수 예를 들어 방어력을 높이거나 공격의 빈도를 높여 그 네트워크가 어떻게 대응하는지를 조사하였다. 이 모의실험을 통해서 나온 결과들은 X축의 비용과 Y축의 생존력(여기서 생존력 0은 회사가 공격에 완전히 당했다는 뜻이며 1은 공격을 받았지만 전혀 영향을 받지 않았다는 뜻이다.)으로 표시한 곡선을 만들었다(Berinato,2002). 이 곡선은 처음에는 거

2) http://www.itsam.com/trend/it_content

의 수직으로 상승하지만 이후 점점 증가율이 낮아지는 모양을 보이고 있다. 즉 ROSI는 많이 투자할수록 증가하지만 그 상승률은 감소한다는 뜻이다. 연구자들은 이 곡선과 무차별곡선[3]을 겹쳐 비용과 생존력의 결합을 통하여 최적의 정보보호투자 지점을 제공하여 준다고 말한다(Berinato, 2002).

이 방법은 비용과 효용성(Utility)의 접점에서 최적 투자점을 찾아내는 경제적 분석에 기초하고 있어 개념적으로는 타당성이 있으나, 정보보호 효용성의 정량화 문제와 정보보호 비용에 대한 구체적인 산출방식이 제시되지 않은 점 등 문제점을 가지고 있다.

4. 기존 ROSI 방식의 한계

위에서 분석한 세가지 접근방법을 통해 살펴본 ROSI 연구는 아직까지 초보적인 수준이라고 할 수 있으며, 실무에서 사용되기 위해서는 아직도 해결해야 할 이슈가 많다고 할 수 있다.

우선 ROSI를 산출하려면 투자로 인한 효익에 대한 부분과 투자소요 비용에 대한 부분 등 크게 두 부분에 대한 계산 방식이 요구된다.

투자로 인한 효익 또는 성과를 산출하는 것은 쉽지 않은 작업으로 기존의 연구는 대부분 예상손실의 감소 등 재정적인 차원에서 산출하고 있다. 그러나 최근에는 정보보호 성과를 BSC(Balanced Score Card) 접근방법에 기초하여 조직 내외부의 관련 이해관계자(정보보호직원, 고객, 공급자, 정부기관 등)의 생산성 향상 및 만족도, 법적 준거성 제고 등 비 재정적인 효익을 포함하려는 노력들이 시도되고 있다(홍기향, 2003). 이와 같이 재정적 및 비재정적인 효익을 정량적으로 표현할 수 있는 기법에 대한 보다 심층있는 연구가 요구된다.

정보보호 투자 비용을 정확히 산출하는 것도 쉽지 않은 작업으로 기존의 연구는 주로 정보보호 대책의 도입 비용 만을 고려하는 경향이 대부분이었다. 그러나 정보보호 대책의 지속적인 효과를 보기 위해서는 대책의 적절한 유지보수 비용이나 지원 비용을 고려해야 한다.

본 연구는 ROSI 연구의 단계적인 발전을 위해 우선 정보보호 투자비용 산출 부분에 초점을 맞추어 이를 보다 정확하게 산출하며 투자비용 산출 의사결정에 유연성을 부여한다는 의미에서 TCO 방식을 적용시키고자 노력하였다.

Ⅲ. TCO의 개념

TCO(Total Cost of Ownership) 개념은 1987년 가트너 그룹의 빌 커윈에 의해 시작되었다. 그는 PC를 5년간 소유하는데 발생하는 총 비용을 산정하는 TCO 모델을 개발하였으며, 그의 발견사항은 소프트웨어와 하드웨어를 구입하는 비용은 TCO의 20% 정도 차지하며, 상당한 IT지원비용이 시스템의 원활한 운영을 위한 유지 및 관리, 기술지원, 교육 등에 필요하다는 것이었다. 또한 사용자들이 예산에는 반영되지 않는 동료로부터의 기술 지원을 받고 있다는 것을 지적하였다(Witty.

3) 무차별곡선(indifference curve) : 가로축을 X상품의 수량으로 하고 세로축을 Y상품의 수량으로 할 때 X의 a량과 Y의 b량을 결합한 데서 얻을 수 있는 만족도와 동등한(무차별의) 만족을 주는 X와 Y의 여러 가지 결합을 연결한 곡선.

Roberta , et al, 2001). 한마디로 PC를 활용하는데 눈에 보이는 비용만을 고려하는 접근법이 바람직하지 않다는 것을 지적한 것이라고 할 수 있다.

TCO는 한마디로 PC 한 대당 투입되는 전체 비용, 즉 하드웨어, 소프트웨어, 교육, 관리 비용 등을 모두 통합한 비용을 의미한다. 이는 단순한 제품 가격뿐 아니라 관리비 등 눈에 보이지 않는 비용을 최대한 절감해 경영 효율을 높이자는 취지가 담겨져 있다.

〈표1〉 TCO의 주요 구성 요소

구성요소	세부내용
자본비	• 하드웨어 관리비용 • 소프트웨어 유지보수 비용
기술지원 비용	• 헬프데스크 운영 비용 • 신상품 소개 비용 • 서버 등의 운영 비용 및 유지 보수 비용
네트워크 관리비용	• 데스크 탑 관리 비용 • 시스템 백업 비용 • LAN 관리 등과 같은 사용자 관리 비용
인건비	• 정보시스템 부문이 아닌 최종 사용자 집단에 의해 발생하는 비용 • 파일 관리 및 자체적 문제점을 파악하는 활동 비용

각 구성요소는 〈표1〉에서 보는 바와 같이 각각의 비용 세목으로 분류되어 기업은 TCO의 세부 항목별로 자산을 측정해 회사 전체의 기술 비용을 파악할 수 있다.

따라서 TCO는 어느 곳에서 비용이 발생하는가를 이해하는데 매우 효과적이다(김경근, 2001).

물론 TCO의 항목에 들어가는 무형의 가치(예를 들어, 새 시스템이 도입되어 교육을 할 때 중단되는 업무시간, 사용법을 완전히 익히지 못한 동료를 도와줄 때 소비되는 시간, 시스템에 장애가 발생해 멈췄을 때 발생하는 비용, 벤더의 경험 등)들을 금액으로 환원한다는 것이 예측에 불과할 수도 있지만 예측도 완벽한 불확실성보다는 나을 것이다.

이에 대한 의견으로 나온 것이 TCO의 각 영역에 정확한 수치를 지정하는 대신 확률분포에 따라 TCO 수치를 기입하는 것이다(CIO Magazine, 1998). 확률분포는 하나의 가치가 2개의 수치량 사이에 있을 경우의 확률이다. 이후 기업은 이들 수치 구간과 신뢰율을 한쌍으로 함으로써 TCO수치를 위한 신뢰구간을 계산할 수 있다. 따라서 기업은 자사 데스크탑 TCO가 5천~1만5천달러 사이에 있다고 99%로 확신하거나, 6천~1만달러 사이에 있으면 신뢰율은 89%라고 말할 수 있다. 즉, 다시 말해서 TCO모델은 각 기업에 맞게 수정되어야 하며 정확한 수치가 아니라 범위로 제시되어야 더 의미가 있음을 알 수 있다.

처음 TCO는 PC에 들어가는 총비용을 파악하기 위해 만들어졌지만 최근엔 영역을 크게 넓혀나가고 있다. PC, 서버, 스토리지는 물론 소프트웨어 분야에서도 TCO가 활용되고 있다. 이제 TCO는 IT분야의 투자에서 고려해야 할 가장 중요한 항목으로 자리잡았다(김경근, 2001).

이윤추구를 목적으로 하는 기업에서 비용을 낮춘다는 것은 당연히 추구해야 할 항목이다. 또한 이것은 기업의 경쟁력 강화로 이어진다.

가트너 그룹의 TCO수석 설계사중 하나인 빌 커윈은 기업이 스스로의 TCO모델을 구축할 수 있는 방법과 관련해 몇 가지 조언을 했다(CIO Magazine, 1998).

첫째, 기업은 스스로 알고 있다고 생각하는 것보다 더 많이 알고 있다. 대부분의 기업은 누가 어떤 훈련에 참여하고 있는지, 지원 인력은 얼마나 많은 전화 질문에 응답하고 있는지, 하드웨어와 소프트웨어에 얼마나 투자하고 있는지 등을 추적하고 있다. 기업이 완전히 해체되지 않은 한, TCO는 보통 주변에 널리 있는 정보를 수집하는 일이다.

둘째, TCO를 분석하는 일이 엄청나고 기념비적인 업적이 되어서는 안된다. 1개월 동안 2명의 인력이 비용 절감 기회를 파악하기에 충분한 정보를 입수할 수 있어야만 한다.

셋째, 인터뷰를 통해 가설들을 점검한다. "관리자와 최종사용자들에게 문제가 있을 때 어떻게 대처하는가를 질문하라."고 커윈은 말한다. 일례로 '옆자리의 동료를 부르는가', '아니면 지원부서에 전화를 하는가' 등이다.

이 이야기는 다시 말해 많은 대화와 설문 등을 통하여 주변에 널려 있는 정보를 빠르게 수집하여 각각의 기업에 맞는 TCO모델을 구축하여야 한다는 말이다. 어떤 정해진 틀에 맞추는 것 보다 기업이 원하는 생산성과 환경을 고려하여 자신만의 TCO모델을 설정할 때 좀 더 정확한 TCO를 구할 수 있을 것이다.

전문가들이 말하는 TCO의 의미는 실제로 얼마의 비용이 발생하는가 하는 구체적인 수치가 아니라 비용을 줄일 수 있는 방법이 있다는 것을 인식하는 것이라고 말한다. 기업이 비용을 줄일 수 있는 여지가 있음을 파악하고 이를 위해 노력하는 것이 더 중요하다는 것이다(김경근, 2001; Witty. et al, 2001). 다시 말해 TCO는 비용이 어디서 발생하는가를 이해하는데 필수적이며 이를 통해 낭비될 수 있는 비용을 찾고 그것을 줄일 수 있는 기회를 기업에게 줄 수 있는 기업의 비용 절감을 위한 분석 기법이다.

Ⅳ. TCO 기반 ROSI 방식

일반적 ROI(Return on Investment)는 수익성과 경영성과의 측정이다. 즉 투자의 가치를 판단하고 보다 나은 경영 분석을 위한 자료로 활용될 수 있는 근거 산출을 위해 수치로서 투자의 효과성을 밝히고, 기업 프로세스가 기업의 이윤에 어떠한 영향을 미치는 가에 대해서 볼 수 있는 방법인 것이다(Geer, 2001). ROI는 수익을 발생하기 위한 기본적인 투자 근원을 고려하여 측정한다.

이는 물론 ROSI에서도 마찬가지이다. 기업이 정보보호에 투자하여 그 투자로 인하여 어느 정도의 수익성을 얻을 수 있는가를 측정하는 것이다. 이는 정보보호예산과 직접적으로 관련되는 이야기이며 CEO들은 좀 더 정확한 계산과 수치를 필요로 한다. ROSI는 하나의 방법으로 통합된 것이 아니라 기업의 환경과 규모, 성격에 따라서 많은 방법들이 활용될 수 있다. 그러나 대부분 기업들은 어떤 행위로부터 점진적으로 얻어진 이익을 의미하는 "회수(Return)"의 의미로서 ROSI를 사용한다. 만약, 1000만원의 정보보호투자를 통하여 어떤 기간 이후 1500만원의 이익이 있었다면 투자는 50%의 ROSI를 갖는다.

기업의 입장에서 정보보호 투자비용을 정확히 산출할 수 있다는 것은 예산적 측면에서 매우 중요하며 어려운 작업이다. 정보보호를 위한 물리적인 제품에 대한 지출은 직접 비용으로서, TCO의 개념에서도 알아보았듯이 극히 일부분이라고 할 수 있다. 따라서 투자비용을 구하는 공식에 직접비용과 간접비용 모두를 생각하는 TCO를 접목하여 ROSI를 구하는 방법이 필요한 것이다. TCO는 비가시적인 비용을 가시화시킴으로써 비용 대 효과가 분명해지는 장점을 갖고 있다.

1. 정보보호 TCO 모델

가트너 그룹에서 제시한("The Price of Information Security", 2001)방식에 의하면, 정보보호의 TCO는 크게 계정목록(Chart of account), IT 시나리오(Technical scenario), 그리고 정보보호 시나리오(Information security scenario)로 구성되어 있다. 첫째, 계정목록은 하드웨어, 인력, 소프트웨어, 외부 서비스, 물리적 정보보호와 같이 다섯 가지 부문으로 나눠질 수 있다. 이것은 또 여러 가지 정보보호 활동들(인증. 인가, 암호화, 방화벽, 정보보호 프로그램, 메시지의 무결성, 공개키기반구조, 위험평가, 싱글 사인 온, 원격 통제 등)과 관련된 항목들을 식별하는 것이다.즉, 계정목록은 기업의 정보보호를 위한 활동, 정보보호를 위해 지출할 수 있는 항목들을 열거해 놓았다.

둘째, IT 시나리오는 본사와 공장들의 지리적 위치, 기업의 총 자본금, 각 부서에서 일하고 있는 인력 수, 그리고 근무 형태 등으로 표현된 기업의 프로파일과 시스템 및 네트웍을 포함시키는 플랫폼, 즉 기업의 IT환경 프로파일을 말한다.

마지막으로 정보보호 시나리오는 IT 프로파일을 안전하게 기획, 운영하기 위해 필요한 정보보호 활동이나 프로그램 등을 의미한다.

정보보호 TCO 모델의 한 예로 한 중소 전자회사 TCO 세부 항목들은 다음과 같이 구분할 수 있다.

1) 하드웨어

- Network sniffer, 이메일 복구 서버, 정보보관용 서버, 통제관리 서버, 시스템 전용 로그 서버, 노트북, 프린터, 이동디스크 드라이버 장치, 팩스, 소모품 등이다. 각각은 그 개수까지 명확해야 하며 서버 같은 경우 어떤 OS를 탑재하고 있는가도 매우 중요하다.

2) 인력

- 이 단계에서는 수명주기(Life Cycle) 의 6 단계를 이용해 계산할 수 있다.

〈표2〉 Life cycle의 6단계와 담당인력

단계별	담당 인력
계획 단계	CEO, CIO
습득 단계	네트워크 엔지니어 전기 · 통신 담당 직원
실행 · 이행 단계	네트워크 엔지니어 전기 · 통신 담당 직원
경영 · 운용 단계	네트워크 엔지니어 전기 · 통신 담당 직원
개량 · 개선 단계	CEO, CIO 네트워크 엔지니어 전기 · 통신 담당 직원
유지보수 단계	네트워크 엔지니어

각각의 인력에 맞는 비용을 구할 때는 필요 인력들의 근무시간(예, 일주일에 5일 근무, 일주일에 3일 재택근무, 하루에 8시간 근무 등)과 그 효율성에 관하여 비용으로 측정해야 한다. 여기서 효율성이란 하루 8시간 근무 중 동료 직원들과의 잡담시간, 또는 책상 앞에 앉아서 딴 생각하는 시간 등을 뺀 실질적으로 근무에 투자하는 시간을 말하는 것이다. 또한 여기에는 각 직원들의 훈련비용도 포함된다.

각 필요 인력들을 더 세부적으로 구분하면 직무와 관련하여 데이터 입력, 시스템 운영자, 네트워크 관리자, PC 기술지원, 헬프 데스크, 시스템 엔지니어링, 시스템 프로그래머, 데이터베이스 관리, 에플리케이션 프로그래머, 문서 전문가, 전가상거

래 직원, 품질 보증, 정보 시스템 관리자, 사무 보조 등으로 나눌 수도 있다.

3) 소프트웨어

- 로그 분석 도구, 이메일 백업 소프트웨어, 이메일 운영 시스템, 이메일 호스트 소프트웨어, 통제 서비스 데스크 소프트웨어, 전반적 분석 소프트웨어, 복사 소프트웨어, 노트북 암호화 소프트웨어 등이 있다. 소프트웨어는 한번 구매해 놓으면 유지보수 할 일이 없으므로 몇 년이 지나도 그 가격은 변하지 않을 것이다.

4) 외부 서비스

- 한 마디로 통신 회선 비용으로 말할 수있는데 여기에는 빠른 속도의 연결 라인, 데이터라인, 팩스라인, 음성라인 등이 속할 수 있다.

물론 이 속성들은 각 기업의 환경과 정책에 맞게 바뀔 수 있다. 기업은 각 속성에 맞는 자료 수집들을 통하여 비용을 결정할 수 있다. 각 속성들의 비용을 모두 합하면 총 비용을 구할 수 있다.

이런 표를 근본으로 컴퓨터 시스템의 경우, 약간의 데스크탑, 파일 서버 및 어플리케이션 서버용 바이러스 예방 소프트웨어, 방화벽 제품을 비롯한 전형적인 정보보호 장치를 설치하는 경우 또는 기업의 정보보호 활동에 관해 투자를 한 경우, 각각에 대해 ROSI를 구할 수 있다. 여기서 나온 정량적인 ROSI를 통하여 악의적 공격으로 인한 경제적 손실 방지액 등과 같은 기업의 손익분기점을 구할 수 있을 것이다.

2. TCO 기반 ROSI 방식의 장점

이렇게 TCO를 활용한 ROSI 분석은 단순히 기업의 투자수익률을 보여줄 뿐만 아니라 가시적 비용과 비가시적 비용을 일목요연하게 보여주므로 기업이 어느 부분에서 비용을 절감할 수 있는지 알 수 있게 해주는 장점을 제공한다.

일반적으로 TCO 관점에서의 비용 산정은 비가시적 비용까지 포함하므로 비용이 더욱 더 증가할 것이라 생각하지만 각각의 비용을 최소화해 줄 수 있다는 장점 때문에 오히려 ROSI를 높여 줄 수 있다.

V. 결론

본 논문에서는 ROSI 산출에 대한 여러 가지 접근 방법들을 알아보고 TCO를 활용한 ROSI 산출 방식을 제시해 보았다.

가시적 비용과 비가시적 비용을 합한 TCO는 좀 더 정확한 총비용을 구해낼 수 있으며, 이런 TCO를 활용한 ROSI 산출 방식은 정보보호 투자 수익률 뿐만 아니라 비용이 어디에서 발생하는지, 기업이 어느 부분에서 비용을 최소화 시킬 수 있는지를 알게 해주므로 최소 비용으로 ROSI를 극대화 시킬 수 있다.

TCO를 활용한 정량적인 ROSI는 기업의 예산편성과 투자와 같은 의사결정에 크게 영향을 미칠 것이다.

참고문헌

1. CIO Magazine, "TCO로 비용을 통제한다", Feb 20 1998

2. Cisco System, "네트워크 정보보호에 대한 투자수익", White paper, Jun 2003

3. Intel, "무선 LAN: 생산성 혜택을 투자수익(ROI)으로", 2003

4. 김경근, "IT경제에서의 TCO의 의미와 시사점", 「EMC 인포토피아 Magazine」, No. 14 Autuum 2001

5. 이종남, "TCO로 유지비용 40% 줄인다", 「CIO Korea」, Jun 20 1998

6. 홍기향, "정보보호 과정 및 통제가 성과에 미치는 영향", 국민대학교 대학원 박사학위 논문, 2003

7. Anderson, Larry, "Access Control & Security System", *Primedia Business Magazines*, Sep 1 1997

8. Berinato, Scott, "Calculated RISK", *CSO Magazine*, December 2002

9. Berinato, Scott, "Finally, a Real Return on Security Spending", *CIO Magazine*, Feb 15 2002

10. Berinato, Scott, "The security spending mystery", *CSO Magazine*, April 25 2002

11. Blakley, Bob, "An Imprecise but Necessary Calculation", *Security Business Quarterly*, Vol.1 issue 2, 2001

12. Briney, Andy, "2001 Industry survey", *Informnation Security*, October 2001

13. *CIO Research Reports*, "The state of Information Security, 2003", Sep 2003

14. Duffy, Daintry, "Safety at a Premiun", *CSO Magazine*, December 2002

15. Geer, Daniel. E., "Making Choices to Show ROI", *Security Business Quarterly*, Vol.1 issue 2, 2001

16. Karofsky, Eric, "Insight into Return on Security Investment", *Security Business Quarterly*, Vol.1 issue 2, 2001

17. Keen, Jack, "ROI's Secret Ingredient", *CIO Magazine*, 15 Jun 2003

18. Leach, John, "Security engineering and security ROI", *John Leach Information Security*, 2003

19. Slater, Derek, "Inside the sauage Factory", *CSO Magazine*, December 2002

20. Thieme, Richard, "What Insutance Can-and Can't-Do for Security Risks", *Security Business Quarterly*, Vol.1, issue 2, 2001

21. Witty. Robert, et al., "The Price of Information Security", **Garter**, 8 June 2001

22. http://www.itsam.com/trend/it_content22. [cited 2003.10.20]