정보보호 투자 기준 선정에 관한 소고

공희경[a] 전효정[a] 김태성[b]

[a]충북대학교 경영정보학과 박사과정
361-271 충북 청주시 흥덕구 개신동 12
Tel: 043-276-3343, Fax: 043-273-2355, E-mail: konghk@paran.com, muroii@lycos.co.kr

[b]충북대학교 경영정보학과 부교수
361-271 충북 청주시 흥덕구 개신동 12
Tel: 043-261-3343, Fax: 043-273-2355, E-mail: kimts@chungbuk.ac.kr

Abstract

정보보호의 중요성에 대한 인식은 매우 높아졌으나 정보보호에 대한 투자는 인식수준만큼 확대되지 않고 있다. 이는 정보보호 투자는 기업의 정보이용환경에 많은 변화를 가져오지만 투자효과에 대한 세부적 분석과 투자대상이 명확하지 않고, 그 효과를 측정하기 어려운 것이 주요원인이다. 본 연구에서는 기업과 조직에 적합한 정보보호 투자를 위한 선행 과제로 비용 및 효과요인을 분석하고자 한다. 이를 통해 기업에 적합한 정보보호 투자 대안을 선정하기 위한 연구모형을 제시한다.

기업의 정보보호 투자 의사결정시 계량화하기 어려운 기준들을 이용해서 합리적인 투자 대안을 선정하는데 활용될 수 있을 것이다.

Keywords:

정보보호 투자; 비용요인, 효과분석 요인

서론

정보사회의 도래와 인터넷의 확산으로 정보보호의 중요성이 증가함에 따라 기업과 조직에 있어서 정보보호는 경쟁적 우위를 확보하기 위한 도구임과 동시에 비즈니스를 안정적으로 수행하기 위한 필수 경영 요구사항으로 등장하고 있다[1]. 그러나 기업과 조직의 정보보호 투자가 지속적으로 증가함에도 불구하고 정보보호 성과 측정을 위한 체계적 방법이 제시되지 않고 있어 정보보호 투자 효과를 객관적으로 예측하거나 투자 의사결정을 하는데 어려움이 있다. 또한 정보보호의 투자효과를 대부분 정성적으로 서술하는 형태여서 효과의 수준이나 요인들이 미치는 영향을 분석하는 것은 불가능하다.

본 연구에서는 기업과 조직의 정보보호 투자가 기업의 비즈니스 측면과 정보보호성에 미치는 영향을 분석하기 위해 정보보호 투자의 비용 및 효과요인을 분석하고자 한다. 또한 정보보호 투자효과를 정량적 효과와 정성적 효과로 분석한 연구모형을 통해 정보보호 투자에 대한 의사결정지표를 제시하고자 한다.

정보보호 투자의 경제성 분석 접근방법

정보보호에 대한 투자는 크게 정보시스템 관리 및 유지에 대한 투자로 볼 수 있다. 정보시스템 투자와 관련된 기존연구를 살펴보면 정보시스템에 대한 투자가 조직의 생산성 증대 및 여러 가지 긍정적 효과와 연관성이 있는 것으로 나타나고 있다[2, 3, 4, 5, 6, 7, 8]. 그러나 정보시스템의 투자 효과 중 어느 부분이 정보보호 투자로 인해 발생한 효과인지를 구분하기는 매우 어렵다. 또한 이러한 효과를 객관적으로 분석할 수 있는 분석체계에 관한 연구도 매우 부족하다. 정보보호에 대한 투자의 정량적 효과에 대한 연구는 최근부터 시작되었다. 본 연구에서는 정보보호 투자 분석과 관련된 기존 연구를 고찰하고자 한다.

정보보호 투자의 사회적, 경제적 연구

정보보호에 대한 사회적, 경제적 연구의 필요성에 대해 Soo Hoo(2000)는 보험 산업과 기업에서 정보보호 문제에 대한 연구의 필요성을 분석하고 효율적인 투자 규모와 효과 등에 대한 논의의 필요성을 제기하였다[9].

Gordon et al.(2002)는 정보의 취약성과 잠재적 손실을 매개변수로 이용해 기업의 정보보호에 대한 최적의 투자수준을 고려하는 경제적 모델을 제시하여 기밀성, 무결성, 가용성 등의 정보보호 목표를 효율적으로 달성할 수 있도록 적합한 투자모델을 제시하였다[10].

Cavusoglu et al.(2004a, 2004b)는 정보보호 투자 시 관리자가 고려해야 할 여러 요인들을 분류하였다[11, 12]. Bodin et al.(2005)의 연구에 따르면 AHP기법을

이용하여 CFO(Chief Financial Officer)를 대상으로 정보보호 투자 평가안을 도출하고 정보보호관리자가 평가 측정할 수 있는 정보보호 수준을 제시하였다[13]. 또한 Tanaka et al.(2005)는 정보보호 투자와 정보보호 취약성의 관계를 일본의 e-local 정부의 실증 데이터를 바탕으로 비용효과 대비 접근방법과 내쉬균형이론을 적용하여 분석하였다[14].

정보보호 투자의 비용대비 효과분석에 관한 평가기준 연구

Scott(1998)은 정보보호에 대한 투자는 보호 받는 자산의 가치를 기준으로 평가하는 것을 제시하였다. 정보보호에 대한 투자는 일반적으로 장기적 측면의 보장적 성격이 강하므로 장기적 위험은 줄여주지만 단기적으로 정량적인 투자효과를 제공해주지 못하는 경우도 많다[15]. 이러한 특성으로 인해 정보보호의 투자효과를 체계적을 분석하고 정량화하기는 매우 어렵다. Scott(2002)은 정보보호의 통제가 부족한 경우에 발생할 수 있는 손실 요인으로 생생성 감소, 이익 감소, 기업이미지 낙후, 금전적 손실 등을 제시하였다[16].

Blakely(2001)는 정보보호에 대한 투자효과를 '투자효과=(이익증가분+비용절감분)/투자 비용'으로 정의하였다. 여기서 투자 요인에는 초기 도입 비용, 갱신비용, 관리 비용 등이 포함된다. 이익 증가분이란 정보보호에 대한 투자가 어떻게 기업의 이익 증대에 기여할 수 있는가를 의미한다. 정보보호에 대한 투자를 통해서 예전에는 위험 요인에 대한 우려로 추진하지 못했던 방법으로 업무를 수행할 수도 있을 것 이란 의미이다. 비용 절감분이란 정보보호의 측면에서 손실 예방이라고 할 수 있다. 즉, 위험이 현실화되었을 때 발생했을 손실이 정보보호 투자를 통해 어느 정도 예방되는가를 의미한다[17].

Witty(2001)는 정보보안의 투자 요인을 크게 하드웨어, 인적자원, 소프트웨어, 외부 서비스 및 물리적 보안의 다섯 영역으로 분류하였다. 이 영역을 다시 인증, 권한관리, 코드보호, 사이버 재난 대응, 컨텐츠 모니터링, 디지털 저작권 관리, 법적 책임준수, 암호화, 방화벽, 보험 가입, 인터넷 차단 통제, 침입 탐지, 인증 획득, 로깅, 감사, 악성코드 관리, 무결성 관리, 프라이버시 관리, 공개키 기반 구조, 레코드 기록 및 보관, 원격 접속, 위험 분석, 보안관리, 보안체계, 통합인증체계 등으로 세분화 하였다[18].

Cavusoglu et al.(2004)는 정보보호침해로 인해 금전적 손실, 회사적 책임, 신뢰도 하락 등이 발생한다고 가정하고 정보보호 담당자가 경제적 측면에서 관리할 수 있는 주요 요인을 정보보호침해 비용산정, 리스크 관리 기법, 비용 효과적 기술구성, 다양한 기술구성으로부터 오는 가치들로 정의하였다[11, 12].

선한길(2005)은 정보보호 투자에 대한 성과를 정보보호 사고의 감소, 자산의 손실건수 감소, 비즈니스 기회손실 감소, 타사 경쟁 시 손해 감소, 이미지 실추건수 감소, 사고발생시 신속한 처리 등으로 구분하고 측정항목화 하였다[24].

정보보호 투자의 비용 및 효과측정 요인

정보보호 투자의 비용요인은 유형 및 무형의 정보자산과 같은 설비와 인력 등을 의미한다. 비용 요인은 대부분 정량화가 가능하여 효과 요인에 비해 측정이 용이하다.

Harris(2001)는 정보보호 투자에 대한 비용 요인을 제품 구매 비용, 설계 및 계획수립 비용, 환경 구축 비용, 연동 비용, 유지보수 비용, 테스트 비용, 갱신비용, 운영 및 관리 비용, 업무에 주는 영향으로 나누었다.[19].

Roper(1999)는 정보보호에 대한 투자에 대한 비용 요인을 구매 비용, 유지보수 비용, 관리 및 운영 인력비용으로 분류하였다[20]. 반면, 정보보호 투자의 효과요인은 비용요인과는 다르게 정량화하고 측정하기가 어렵다. Gordon and Loeb(2002)은 순현재가치(Net Present Values)모형을 이용하여 투자의 최적수준을 분석하였다. 이와 함께 정보시스템 투자에 대한 효과분석으로 제시된 요인 중 정보보호투자 효과분석에 적용 가능한 요인들을 도출하였다[10].

Kim과 Leem(2002)은 정보시스템 투자에 대한 효과를 운영적 효과와 경쟁우위를 달성시키는 전략적 효과로 분류하였다. 운영효율을 증대시켜주는 운영적 효과는 금전적 형태, 수치적 형태 또는 정성적 형태로 표현된다. 운영적 효과에는 비용절감, 이익 증대, 의사결정 수준 향상, 업무 기능 향상 등을 제시하고 있다[21].

정보보호 투자 평가기준 연구모형

본 연구에서는 정보보호 투자의 비용요인과 효과측정요인을 재 분류하고 중복되는 항목 등을 제거하여, 이를 바탕으로 평가기준을 크게 정량적 평가기준과 정성적 평가기준으로 범주화 하였다. 이는 정보보호 투자의 경제성 분석에 관한 문헌연구와, 정보시스템 투자효과 분석에 관한 문헌연구를 바탕으로 도출하였다. 정보보호투자의 비용과 효과를 분석하기 위한 기준 모형은 다음과 같다.

표 1 - 평가요인 선정을 위한 문헌조사

연구자	선행연구의 평가요인	본 연구의 평가요인	유형
Scott	생산성 감소	재무적효과	정량적
	이익 감소	재무적효과	정량적
	기업이미지 낙후	기업 이미지	정성적
	금전적 손실	재무적효과	정량적
Blakely	초기도입비용	제품 가격	정량적
	갱신비용	운영비용	정량적
	관리비용	운영비용	정량적
Witty	하드웨어	제품가격	정량적
	소프트웨어	제품가격	정량적
	인적자원	운영비용	정량적
	외부서비스	운영비용	정량적
	물리적 보안	제품가격	정량적
Harris	제품구매비용	제품가격	정량적
	설계 및 계획수립비용	운영비용	정량적
	환경구축비용	운영비용	정량적
	연동비용	운영비용	정량적
	유지보수 비용	운영비용	정량적
	테스트 비용	운영비용	정량적
	갱신 비용	운영비용	정량적
	운영 및 관리비용	운영비용	정량적
	업무에 주는 영향	재무적효과	정량적
Roper	구매비용	제품가격	정량적
	유지보수비용	운영비용	정량적
	관리 및 운영 인력비용	운영비용	정량적
Cavusoglu et al.	금전적 손실	재무적효과	정량적
	회사적 책임	기업이미지	정성적
	신뢰도 하락	기업이미지	정성적
선한길	정보보호사고 감소	기술적 필요성	정성적
	자산손실건수 감소	재무적 효과	정량적
	비즈니스기회 손실 감소	재무적 효과	정량적
	타사 경쟁 시 손해 감소	재무적 효과	정량적
	이미지 실추건수 감소	기업 이미지	정성적
	사고발생시 신속한 처리	기술적 필요성	정성적
Kim and Leem	비용절감	재무적 효과	정량적
	이익증대	재무적 효과	정량적
	의사결정수준 향상	기술적 필요성	정성적
	업무기능향상	재무적 효과	정량적

정보보호 투자의 비용 및 효과 평가 기준은 정량적 평가기준과 정성정 평가기준으로 구분하였다. 정량적 평가기준으로는 제품가격, 운영비용, 재무적 효과로 구분하였으며, 정성적 평가기준으로는 기업이미지 향상과 기술적 필요성으로 구성하였다.

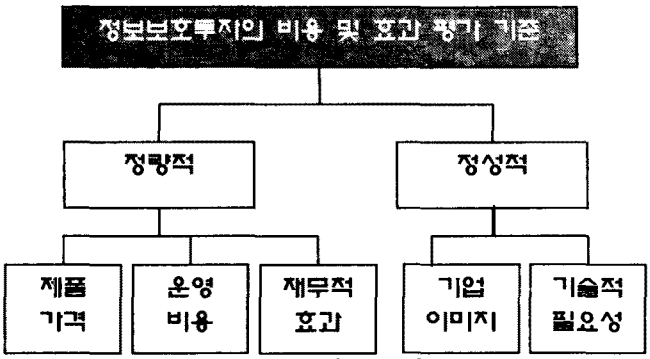

그림1 - 연구모형

결론 및 향후 연구방안

본 연구에서는 정보보호 투자의사결정 및 경제성 분석에서 고려되는 정보보호 투자의 비용요인과 효과분석 요인을 도출하고, 연구모형을 제시하였다. 기존연구를 통하여 평가기준들을 재 분류하고 이론적 기준을 도출하였다. 향후 연구에서는 본 연구에서 도출한 평가기준과 요인들을 보완하여 평가기준과 요인의 중요도 비용요인과 투자 효과요인을 분석한 연구모형을 제시하고 델파이 기법과 설문을 통해 실증적으로 분석하고자 한다.

참고문헌

[1] Parker, D. B. (1997). "The Strategic Values of Information Security in Business", Computer & Security, Vol.16, pp.572-582.

[2] Alpar, P., Kim, M.A. (1990). "A Microeconomic Approach to the Measurement of Information Technology Value", Journal of Management Information Systems, Vol. 7 No. 2, pp. 55-69.

[3] Barua, A., Kriebel, C.H. (1991). "Information Technologies and Business Value : An Analytic and Empirical Investigation", GSIA Working Papers, 1991-17, Carnegie Mellon University, Pittsburgh, PA.

[4] Brynjolfsson, E., Hitt, L. (1996). "Paradox Lost? Firm-level Evidence on the Returns to Information Systems", Management Science, Vol. 42 No. 4, pp. 541-558.

[5] Kim, S., Leem, C.S.(2004). "Implementation of the Security System for In-stant Messengers", Lecture Notes in Computer Science, Vol. 3314, pp. 739-744.

[6] Kim, S., Leem, C.S. (2005). "Security of the Internet-based Instant Messenger: Risks and Safeguards", Internet Research: Electronic Networking Applications and Policy, Vol. 15 No. 1, pp. 88-98.

[7] Mahmood, M.A., Mann, G.J. (1993). "Measuring the Organizational Impact of Information Technology Investment: an Exploratory Study", Journal of Management Information Systems, Vol. 10 No. 1, pp. 97-122.

[8] Mitra, S., Chaya, A.K. (1996). "Analyzing Cost-effectiveness of Organizations: the Impact of Information Technology Spending", Journal of Management Informa-tion Systems, Vol. 13 No. 2, pp. 29-57.

[9] Soo Hoo, K.J. (2000). "How much is enough? A Risk-Management Approach to Computer Security", Center for International Security and Cooperation (CISAC), Stanford University, Stanford.

[10]Gordon, L.A., Loeb, M.P. (2002). "The Economics of Information Security Investment", *ACM Transactions on Information and System Security*, 5(4), pp.438-457.

[11]Cavusoglu, H.(Hasan), Cavusoglu, H.(Huseyin), Raghunathan S. (2004a). "Economics of IT Security Management: Four Improvements to Current Security Practices", *Communications of the Association for Information System*, 14, pp.65-75.

[12]Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004b). "A Model for Evaluating IT Security Investments", *Communications of the ACM*, 47(7), pp.87-92.

[13]Bodin, L.D., Gordon, L.A., Loeb, M.P. (2005). "Evaluating Information Security Investments Using the Analytic Hierarchy Process", *Communications of the ACM*, 48, pp.79-83.

[14]Tanaka H., Matuura K., Sudoh O. (2005). "Vulnerability and Information Security Investment: An Empirical Analysis of E-local Government in Japan", *Journal of Accounting and Public Policy*, 24, pp.37-59.

[15]Scott, D. (1998). "Security Investment Justification and Success Factors", Gartner Inc., Stamford, CT.

[16]Scott, D. (2002). "Best Practices and Trends in Business Continuity Planning", U.S. Symposium/ITxpo, Orlando, FL.

[17]Blakley, B. (2001). "Returns on Security Investment: an Imprecise but Necessary Calculation", Secure Business Quarterly, Vol. 1 Issue 2.

[18]Witty, R.J, Girard, J., Graff, J.W., Hallawell, A., Hildreth, B., MacDonald, N., Malik, W.J., Pescatore, J., Reynolds, M., Russell, K., Wheatman, V., Dubiel, J.P., Weintraub, A. (2001). "The Price of Information Security", Gartner Inc., Stam-ford, CT.

[19]Harris, S. (2001). "CISSP All-in-One Exam Guide", McGraw-Hill, New York, NY.

[20]Roper, C.A. (1999). "Risk Management for Security Professionals", Butterworth-Heinemann, Boston, MA.

[21]Leem, C.S., Kim, S. (2002). "Introduction to an Integrated Methodology for Development and Implementation of Enterprise Information Systems", Journal of Systems and Software, Vol. 60 No. 3, pp. 249-261.

[22]김상균 (2005). "인터넷 차단 시스템의 경제성 분석에 대한 연구", 한국컴퓨터정보학회논문지, Vol.10 No. 6, pp.269-278.

[23]권민영, 구본재, 이국희 (2006). "AHP 기법을 적용한 IT프로젝트 사전타당성 평가항목의 가중치 산출", Information Systems Reviews, Vol.8 No.1, pp.265-285.

[24]선한길 (2005). "국내기업의 정보보호 정책 및 조직 요인이 정보보호성에 미치는 영향", 한국경영정보학회 춘계학술대회, pp.1087~1095.

[25]공희경, 김태성 (2006). "정보보호 투자의 효과에 대한 동태적 분석", 한국경영정보학회 춘계학술대회, pp.400-405