사이버보안 투자 비용효과분석 방안 선정에 관한 연구

김수진*, 김정덕**
*중앙대학교 융합보안학과
**중앙대학교 산업보안학과
e-mail : top44313@gmail.com

A Study on the Selection of the Cost-Benefit Analysis for Cybersecurity Investment

Sujin Kim*, Jungduk Kim**
*Dept. of Security Convergence, Chung-Ang University
**Dept. of Industrial Security, Chung-Ang University

요 약

사이버 위협이 고도화, 지능화되면서 사이버보안 사고로 비롯한 유무형 손실이 점차 증가추세에 있으며, 이러한 피해를 최소화 하기 위해 사이버보안에 대한 필요성이 증대되고 있다. 기업에서는 각종 규제와 법률에 근거하여, 또는 신뢰할 수 있는 서비스를 고객에게 제공하기 위해서 보안 솔루션, 보안 서비스, 보안 컨설팅 등 다양한 방면에서 보안에 대한 투자를 늘리고 있다. 기업의 보안에 대한 투자는 비용과 효과를 분석하여야 효율적이고 효과적인 투자일 것이나, 아직은 이에 적합한 방안이 제시되지 않고 있다. 따라서 본 연구는 사이버보안 환경에 적합한 비용/효과 분석 방안으로 CMU SQUARE 팀의 비용효과분석 프레임워크를 선택하였고, SQUARE 의 프레임워크를 기반으로 사이버보안 투자에 적합한 비용/효과 측정 방안을 제시하였다. 특히 기존의 금전적 효과에만 치중되어 연구가 부족했던 정성적 효과를 고려하여, 사이버보안 투자에서 발생되는 효과를 종합적으로 측정할 수 있도록 한다. 본 연구의 결과는 사이버보안과 관련된 투자의 비용/효과를 산출함으로써 기업의 보안 투자 방안 추진의 기준이 될 것이다.

1. 서론

최근 사이버 공격으로 인하여 기업의 막대한 손실이 염려되고 있으며, 이에 따라 최고경영층은 사이버보안 투자의 필요성을 인식하고 사이버보안 투자에 많은 비용을 지출하고 있다. IDC 는 2016 년도 한해의 사이버보안 투자금액을 총 737 억달러로 추정하였다. . 하지만 사이버보안에 투자했을 경우 그 효과 여부에 대해서 기업은 여전히 의구심을 가지고 있다.

글로벌 보안컨설팅업체 EY 에서는 글로벌 정보보안 설문조사에서 사이버위험을 위한 고려사항으로 경영진의 지원 및 거버넌스, 정책 및 절차, 사람, 기술, 인식제고, 자산목록, 벤더사 감독, 지속적인 모니터링, 보고체계, 지속적인 개선 등 총 10 가지를 선정하였다. 이러한 사이버보안 고려사항이 적절히 반영된 보안투자를 분석하기 위해서는 사이버보안 투자에 대한 비용과 효과를 측정하고 평가할 수 있는 절차와 방법이 수립되어야 한다.

따라서 본 연구에서는 최근 이슈로 부각되고 있으며, 피해액이 급증하고 있는 사이버보안 투자에 기업이 투자 했을 경우, 비용효과분석 방법을 도출하기 위하여 기존 문헌연구를 기반으로 사이버보안에 투자했을 경우 적절한 비용효과분석 방안을 선정하여 제시하고자 한다.

2. 정보보호 투자의 비용효과분석

2.1 정보보호 투자의 비용, 효과 요인

정보보호 투자의 비용은 보안사고와 직접적으로 연관이 있는지 여부, 보안 투자 비용의 가시화 여부에 따라 총 4 가지를 구분하여 직접/간접 비용,, 명시적/잠재적 비용으로 구분한 Gorden, Loeb(2006)의 접근방법이 있으며, KISA(2015)는 보안 솔루션의 비용을 제품의 도입 및 구축할 때의 비용, 일반 유지관리 비용, 해당 제품의 보안성 서비스에 따른 비용 등 총 3 가지로 구분하여 산출하였다. <표 1>과 <표 2>는 기존 정보보호 투자 효과 측정 관련된 기존의 연구를 재정리하였다. 기존 연구동향을 분류하면 크게 두 가지 방법으로, 사이버보안 투자 효과를 분석하기 위한 지표를 선정하여 도출하거나, 전체 위험 발생가능성을 정량화하여 연간 예상손실액(ALE: Annual Loss Expectancy)을 집계하여 효과를 산출하는 방법으로 분류할 수 있다. 사이버보안 투자의 효과 척도가 매우 다양하고, 사이버보안 투자에 대한 범위가 명확하지 않아서 투자 의사결정에 어려움이 있으며, 정확한 사이버보안 투자의 비용효과분석이 주요 이슈임을 알 수 있다. 본 연구는 <표 1>과 <표 2>의 기존 연구를 분석하여 사이버보안 투자의 비용효과분석에 필요한

효과를 종합적으로 도출하고 정성적 및 정량적 분석 방법에 적용할 수 있도록 제안한다.

<표 1> 정보보안 투자의 효과 측정 – 지표기반

연구자	효과
Cavusoglu(2004)	금전적 이익 회사적 책임 감소 신뢰도 증가
Davis(2005)	운영비용 감소 순익 증대
Scott(2002)	생산성 증가 이익증가 기업이미지 개선 금전적 이익
김영일(2012)	고객정보에 대한 사회적 책임 강화 고객만족도 제고효과 업무효율성 증진효과 기업경영 개선
선한길(2005)	정보보호 사고의 감소 자산의 손실건수 감소 비즈니스 기회손실 감소 타사 경쟁시 손해감소 이미지 실추건수 감소 사고발생시 신속한 처리
안선옥(2009)	전략적 효과 경제적 효과 관리 효율성 리스크 관리 서비스 활용도 업무 효율성

<표 2> 정보보안 투자의 효과 측정 – ALE 기반

연구자	연간예상손실액(ALE)
CMU(2004), KISA(2012)	ALE = Average_Incident Loss * Estimation_Frequency
Tasiakis(2010), Yedji(2011)	ALE = Single Loss Expectancy * Annualized Rate of Occurrence
양재영(2009)	ALE = Single Loss Expectancy * Annualized Rate of Occurrence / Single Loss Expectancy * (Asset Value * Exposure Factor)

2.2 비용효과 분석 방법론

<표 3>은 다양한 종류의 비용효과분석 방법론을 특징과 함께 정리한 것이다. 각각의 비용효과분석 방법은 사용되는 척도의 종류에 따라 정량적 및 정성적 분석이 가능하다.

<표 3> 보안 투자의 비용효과분석에 관한 연구

방법론	내용
NPV	정보의 취약성과 잠재적 손실을 매개변수로 하여 보안에 투자될 당시의 투자가치를 평가하여 현재가치에 대한 효과를 도출
ROSI	보안활동에 대한 투자로 얻을 수 있는 산술적 이익을 분석하여 위험으로 인한 손실 될 가치와 가능성 수치화
WiBe	경제효율성과 관련된 변수를 수익성, 긴급성, 전략적 중요성, 대내외 이미지 개선효과 등 4 가지로 분류하여 측정
BSC	보안 투자성과를 재무, 고객, 내부 프로세스, 학습 및 성장 등의 4 개 관점에서 평가하여 측정지표 도출
비용효과분석	보안의 여러 대안에 대한 투자효과 검증에 사용하는 방법으로, 여러 대안들에 대한 효과를 위험과 연간예상손실액을 추정하여 분석

CMU 에서 진행된 정보보안 프로젝트의 비용효과분석 프레임워크는 데이터의 유무에 따라 다른 계산식을 제시하고 있다. 보안 투자의 비용효과분석을 수행해야할 기업이 연간 손실의 데이터가 없는 경우에는 국가 연간 평균 손실의 데이터를 근거로 산출할 수 있도록 하였다. 따라서 데이터가 부족한 중소기업에서도 CMU SQUARE 팀의 비용효과분석 방법에 따라 사이버보안 투자의 비용효과분석을 수행할 수 있다.

<표 4> CMU SQUARE 비용효과분석 프레임워크의 변수

변수	계산식
Residual risk	Baseline risk * Bypass rate
Baseline cost	Baseline risk * AL
Residual cost	Baseline risk * Bypass rate * AL
Tangible benefit	Baseline cost – Residual cost
Total benefits	Tangible benefit + Intangible benefit
Benefit/Cost Ratio	Total benefits / Total Implementation costs

- Baseline risk: 보안 솔루션의 부재시 조직에 사고 발생 위험정도
- Residual risk: 보안 솔루션이 적절히 설치되었음에도 발생하는 조직의 사고 위험정도
- Bypass rate: 보안 솔루션이 마련되어 있음에도 불구하고 위협이 침투할 확률
- AL(Annualized Loss): 연간 손실액
- Tangible benefit: 유형효과로, 위의 변수들의 계산식을 통해 정성적 방법으로 측정
- Intangible benefit: 무형효과

3. 사이버보안 투자의 비용효과분석 방안

3.1 사이버보안 투자 고려사항

기존의 정보보호 비용 측정 관련 연구를 바탕으로 사이버보안 투자의 비용을 <표 5>와 같이 정리하였으며, 다음 비용들의 총합으로 사이버보안 투자의 비용을 산출 할 수 있다.

<표 5> 사이버보안 투자의 비용

구분	특징
제품도입 및 구축비	사이버보안 솔루션의 도입, 구축시에만 공급가로 지불되는 비용
유지관리	구매한 제품을 최적의 상태에서 활용, 유지하기 위해 제공되는 비용
보안성 지속 서비스	제품을 활용하여 정보의 훼손, 변조, 유출 등을 방지하기 위한 기술 기반의 서비스 비용

사이버보안 투자 비용 = 제품도입 및 구축 비용 + 유지보수 비용 + 보안성 지속 서비스 비용

또한 기존정보보안 투자 효과 측정 관련 연구 <표 1>을 바탕으로, 사이버보안 투자의 무형효과를 평가하기 위한 기업의 고려사항을 프로세스, 조직, 전략, 환경 4 가지 관점에서 <표 5>와 같이 분류하였다.

<표 6> 사이버보안 투자의 무형효과

구분	측정항목
프로세스	업무 기능성 향상 업무 안정성 향상
조직	근무 여건 개선 인력 능력 향상
전략	고객 만족도 향상 경쟁 우위 향상
환경	기업 이미지 제고 관련 법/규제 준수

사이버보안 투자의 유형효과는 <표 2>를 바탕으로, 평균 사고 손실액에 사고 빈도수를 곱하여 연간예상 손실액을 산출할 수 있다.

ALE = Average_Incident Loss * Estimation_Frequency

3.2 사이버보안 투자 비용효과분석 방법의 선정

본 연구에서는 <표 3>에서 도출한 비용효과분석 방법 및 특징을 종합적으로 고려한 결과, 사이버보안의 비용효과분석 방법으로 CMU SQUARE 팀의 비용효과분석 방법을 제안한다.

방법의 선택 이유로는 첫 번째로, 사이버보안에 대한 투자 비용효과 분석은 정량적 및 정성적 분석이 모두 필요하며, 두 번째로 사이버보안 투자에 대한 필요성은 제기되고 있으나 이에 필요한 관련 데이터가 부족한 기업에서도 비용효과분석을 수행할 수 있기 때문이다. CMU SQUARE 팀의 비용효과분석 방법은 연간예상손실액을 근거로 유형효과를 측정하기 때문에 기존의 지표를 기반으로 유형효과를 산출하던 비용효과분석 방법들과는 달리, 관련 데이터 수집이 의무사항이 아니라는 측면에서 사이버보안 비용효과분석 방법으로 가장 적절하다고 판단된다.

4. 결론

본 논문에서는 비용 절감의 관점 뿐만 아니라 무형적으로 나타날 수 있는 효과까지 고려할 수 있는 관점을 사이버보안 투자의 비용효과분석 방법 측면에서 고찰 하였다. 기존 연구에 대한 고찰 결과로 CMU SQUARE 의 비용효과분석 방법은 다음의 3 가지 측면에서 사이버보안 투자의 성과측정 방안으로 적합하다고 판단된다.

첫번째로 정량적 분석과 정성적 분석이 모두 가능하며, 두번째로 여러 대안에 대한 비용대비 효과를 가시적으로 확인할 수 있으며, 마지막으로 사이버보안의 비용효과분석을 위해 대규모 데이터 수집이 없어도 가능한 절차에 기초한 방법론으로 적용이 쉽고 용이하다.

향후 연구에서는 CMU SQUARE 팀의 보안 투자 비용효과분석 방법을 기반으로 구체적인 사이버보안 투자 비용효과분석 방법을 제시하고, 기업의 투자에 의사결정 권한이 있는 경영진의 설문을 통하여 적용 타당성 검증 작업이 필요하다.

참고문헌

[1] 공희경, 김태성, “BSC 관점에 의한 정보보호 투자효과”, 한국경영정보학회 춘계학술대회, 2008
[2] 김영일, 이재훈, “개인정보보호투자의 성과측정방안에 관한 연구”, 디지털정책연구학회, 2013
[3] 김정덕, 박정은, “TCO 기반 정보보호 투자수익률(ROSI)에 대한 연구”, 한국디지털정책학회 창립학술대회, 2003
[4] 선한길, “국내기업의 정보보호 정책 및 조직 요인이 정보보호성에 미치는 영향”, 한국경영정보학회 춘계학술대회, 2005
[5] 안선옥, 이희조, “AHP 기반 Security ROI 를 활용한 정보보호 투자성과 분석 연구”, 한국멀티미디어학회, 2009
[6] 양재영, “정보보안의 비용효과분석에 관한 연구”, 2009
[7] 한국인터넷진흥원, “정보보호 사전점검의 경제적 효과 분석 및 활성화 방안 연구 보고서”, 2012
[8] Blakley. B, "Returns on Security Investment: an Imprecise but Necessary Calculation", Secure Business Quarterly, 2001
[9] Davis, A. "Return on Security Investment Provin It`s Worth It", Network Security, 2005
[10] Gordon. L. A. and Loeb, M.P, "The Economics of information security investment", ACM Transaction on inforamtion and system security, 2002
[11] Peter Chen, Marno Dean, "SQUARE Project: Cost/Benefit Analysis Framework for Information Security Improvement Projects in Small Companies", Carnegie Mellon University, 2004
[12] Scott, D., “Best Practices and Trends in Business Continuity Planning”, U.S. Symposium/ITxpo, 2002
Witty R.J, et al., “The Price of Information Security”, Gartner Inc, 2001
[13] Harris, S., “CISSP All-in-One Exam Guide”, McGraw-Hill, 2001
[14] Roper, C.A., “Risk Management for Security Professionals”, Butterworth- Heinemann, 1999