정보보호 투자 대비 효과 측정을 위한 사이버 피해액 계산 방법 개선

최찬영* · 박대우*

*호서대학교 벤처대학원

The Improvement on Cyber Damage Calculation for Return on Security Investment

Chan-young Choi* · Dae-woo Park*

*Hoseo Graduate School of Venture

E-mail : cchany@fsec.or.kr, prof_pdw@naver.com

요 약

2000년대 초반부터 많은 정보보호 관련자들은 정보보호 투자 대비 효과를 측정하고자 노력하였다. 그러한 노력으로 ROSI(Return On Security Investment)를 산출하는 여러 가지 방법 및 ROSI의 Return인 사이버 피해액을 계산하는 Gordon & Loeb 방법 등이 고안되었다. 하지만, 효과를 직접적으로 산출하기 힘든 정보보호의 구조적 특성, 관련 정보의 부족 및 사이버 피해액 산정 시 정성적인 요소가 포함되어 정확한 산출이 어렵다는 문제점이 존재한다. 본 연구는 현재까지의 연구 결과를 살펴보고 기존 방법들 중 가장 효율적이라고 생각되는 Gordon & Loeb 방법과 신진 방법 2가지에 대해 분석하고 개선된 방법을 설계하고자 한다.

ABSTRACT

Since the early 2000s, many information security professionals have sought to measure the effectiveness of information security investments. Such efforts have devised a number of ways to calculate the return in ROSI (Return On Security Investment) including the Gordon & Loeb method for calculating cyber damage. However, due to the characteristics of information security structure, the lack of relate information sharing, and many qualitative factors are included, the damage calculation is inaccurate.. This study reviews related studies, analyzes the Gordon & Loeb method and the Shin-Jin method, which are considered to be the most efficient of the existing methods, and designs improved methods.

키워드

정보보호의 특징, 사이버 피해액 계산, 정보보호 투자 대비 효과(ROSI), Gordon & Loeb 방법

Ⅰ. 서 론

2013년 3•20 대란, 2016년 I사 개인정보 유출 사건 등 큰 사이버 해킹사고가 발생할 때마다 이러한 사건의 재발 방지를 위해 정보보호 투자의 중요성이 언급되고 있다. 하지만, 관련 분야 전문가들도 적당한 정보보호 투자가 어느 정도이며 그에 대한 효과는 어떻게 측정하는지에 대해 명쾌히 설명하는 것이 쉽지 않다.

이와 같이 정보보호 투자 및 효과에 대해 쉽게 설명하지 못하는 주요한 이유는 정보보호의 구조적 특성, 관련 정보 공유의 부족 및 정성적인 요소의 포함이라 하겠다. 정보보호는 자동차 안전벨트나 소화를 위한 스프링클러와 같이 실제 사고가 발생하지 않으면 효과를 측정하기가 어려우며 실제 사고가 발생하였더라도 정확한 피해 예방 효과를 산출하기가 쉽지 않다[1].

또한, 자신의 사고 정보는 누구나 공유하는 것이 부담스러우며, 사고 발생 전 어떠한 규모의 해킹이 발생할지 예측하는 것이 쉽지 않으며 해킹 발생 후 기관의 이미지 추락 등을 포함한 전체 피해 규모가 어느 정도인지 정확하게 파악하기는 쉽지 않다.

이 외에도 정보보호 투자는 IT투자와 구분이 쉽지 않은 점 등 정보보호 투자와 효과에 대해서는 명확하지 않은 점이 많다.

이러한 불명확한 점을 그나마 가장 효과적으로 설명하고 있는 것이 ROSI이나 투자(I)와 효과(R)를 계산하는 방법에 대해서는 여러 연구가 다른 방법을 제시하고 있다.

본 논문에서는 정보보호 투자 대비 효과에 관련된 연구들을 살펴보고 기존에 연구된 방법들을 분석하여 ROSI의 효과(R)인 사이버사고 피해액 계산의 개선 방안을 제시하고자 한다.

II. 관련 연구

Scott Berinato는 ROSI가 랜덤적인 요소가 포함된 “The Game of Risk”이며, 정보보호의 투자는 사이버 사고를 안 나게 하는 것이 아닌 사이버 사고가 일어날 것에 대해 준비 하는 것이라고 하였다. ROSI 계산에서는 보안패치 설치 시 어려움 등 중간단계의 요인들도 존재하여 투자에서 효과를 직접적으로 산출하기가 어려우므로 브랜드 이미지 향상 등의 soft return도 고려해야 하며, ROSI가 실증적이고 감정적인 계산이므로 기업의 보안에 대한 입장이나 기업내부 예산 집행 우선순위에 따라 ROSI 계산이 달라질 수 있다고 주장하였다[1, 2].

김정덕외 1명은 ROSI 계산식의 한 요소인 투자 비용 산출을 위해 가트너의 TCO (Total Cost of Ownership) 모델을 이용하였으며, 또한 카네기멜론 대학의 공격의 유형, 공격 빈도 수, 공격 성공률, 공격의 피해액, 사용된 방어 방법의 요소를 고려하여 투자 비용 대비 효과(공격-방어율)의 상관관계 측정방법을 소개하였다. 카네기멜론 방법은 투자가 많아지면 공격 방어율이 상승하지만 방어율의 상승폭이 줄어들며, 이러한 곡선과 무차별곡선과의 교차점이 최적의 투자 지점이라고 제시한 방법이다[3].

권영옥외 1명은 정보보안 사고 발생 시 기업가치에 어떤 영향이 있는지를 주가로 측정하였으며, 국내의 정보보안 사고 사례를 연구한 결과 사고가 발생해도 기업가치(주식)는 거의 하락하지 않았기에 기업가치에 대해 보안투자 효과는 거의 없다고 하였다. 이러한 현상은 정보보안에 대한 우려 결핍증이 원인이라고 주장하였다[4].

공희경외 1명은 무형자산을 평가할 수 있는 균형성과표(BSC: Balanced Scorecard)를 이용하여 정보보호 투자의 정성적 효과와 정량적 효과의 인과관계 분석 모형을 개발하였으며, 이러한 분석으로 정보보호 기술적·인적 인프라를 구축하여 업무 연속성 보호를 하게 되면 고객이 만족하게 되고 결국 경영 성과로 나타나게 된다고 주장하였다[5].

Brecht외 1명은 정보보호 투자를 위한 비용에 대해 연구하여 정보보호 관리 체계 단계별 정보보안 비율을 제시하였다[6].

ENISA (유럽네트워크정보보호원)는 사이버 보안 사고의 비용(SLE)와 연 발생 확률은 추정하기가 쉽지 않고 산업, 기업 환경에 따라 해당 값의 차이가 클 수 있어 ROSI가 주관적으로 산출될 가능성이 높다고 하였으며, 사이버 보안 피해액 계산에서 가장 많이 인용되는 모델은 Gordon & Loeb 모델이라고 하였다[7].

Gordon외 1명은 보안 투자와 보안취약점 감소는 정비례하지 않으므로 보안 투자를 많이 할 필요가 없으며 투자 적정 비율은 예상 손실액의 37% 미만이라고 주장하였다[8].

신진은 국내에서는 ROSI 계산에 필요한 정보 획득이 어려우므로 정보보호의 경제적 효과 분석을 노턴사이버범죄보고서(2011)의 계산방법을 원용하여 사이버사고 피해액 추정하였다. 해외(24개국)의 피해액이 계산되어 공개되고 있으므로 우리나라와 해당 국가의 경제규모(GDP) 및 인터넷 사용자수를 비교하여 국내 피해액 추정하였으며, 계산 결과 GDP 기준 2010년 피해액은 22조원(영국은 48조원)이었으며, 인터넷 사용자수 기준 추정 피해액은 37조원(영국은 48조원)이었다. GDP 기준과 인터넷 사용자수 기준 계산 결과의 차이점은 우리나라의 인터넷 사용자수가 다른 국가에 비해 높기 때문이며 국내 사이버사고 피해액은 10~40조원일 것으로 추정하였다[9].

신영웅외 3명은 3·20 대란의 피해금액을 산출하고 사이버보안 투자의 경제적 효과를 분석하였다[10].

정성훈외 3명은 정보보호의 투자 집행 효과에 관한 연구에서 투자 대비 효과를 산출하기 힘든 사이버사고 피해액 등이 아닌 정보보호 관리체계(ISMS) 항목의 결함 수로 측정하였고, 예산의 규모보다는 수립된 예산을 충실히 이행하는 것이 정보보호 관리체계 항목 결함 수 감소에 큰 영향을 주며, 관리적 보안 영역에 대한 투자가 기술적, 물리적 영역에 대한 투자보다 더 효과적이라고 하였다[11].

김방룡외 1명은 정보보호 산업의 경제적 파급효과 및 기여도를 분석한 결과 정보보호 산업은 전반적으로 국민경제에 미치는 성장 기여도와 고용기여도가 미약한 것으로 파악되었다[12].

김원필은 IEEE 논문에 대한 정보를 빅데이터 분석하여 정보보호에서 활용이 많이 될 것으로 예상되는 기술은 빅데이터 분석 기술이며, 정보보안의 투자가 필요한 분야는 스마트폰, IoT, 클라우드 등임을 밝혀내었다[13].

Emanuel Kopp외 2명은 사이버 보안 현황, 금융시장에서 정보보호의 어려움, 위험 관리 방안 및 사이버 위험에 대한 대처 방안에 대해 연구하였으며 효율적인 정보보호 투자를 위해 정보공유가 중요하다고 하였다[14].

III. 정보보호 투자 대비 효과 측정 방법 분석

3.1 Gordon & Loeb 방법 분석

Gordon & Loeb 방법은 명시적 비용, 잠재적 비용, 직접 비용, 간접 비용의 4가지 요소에 의해 사이버사고 피해액을 계산한다. 세부 항목으로는 은 매출이익 감소액, 생산효율 저하 손실, 잠재적 책임 비용, 복구 비용, 복구 불능 정보자산가치, 예방 투자액, 이미지손상, 주가하락이 있다.

잠재적 비용이며 간접비용인 이미지손상은 정성적인 요인이므로 실제 계산이 어렵다. 또한, 주가 하락도 3•20 대란, 카드3사 개인정보 유출 사고 등 주요 사이버사고 사례를 볼 때 최소한 국내에서는 거의 발생하지 않는 피해이다.

사이버 사고 발생 시 과태료, 타 기관 또는 고객의 피해액 배상 등 법적 비용이 발생할 수 있으나 이러한 비용이 적절히 구분되지 않고 직접 비용에 포함되어 있다.

3.2 신진 방법 분석

GDP와 인터넷 보급률을 사이버피해액이 조사된 국가와 비교하여 국내 사이버피해액을 산출한 신진 방법은 스마트폰이 널리 보급되어 인터넷뱅킹, 간편결제를 이용하고 있는 최근의 상황을 적절히 반영하지 않는다.

또한, 신진 방법은 비교항목의 특성상 국가의 피해액 산출은 가능하나 기관의 피해액 산출은 불가능하다.

IV. 정보보호 투자 대비 효과 측정 방법 개선 방안

4.1 Gordon & Loeb 방법 개선

Gordon & Loeb 방법의 세부 항목 중 이미지손상은 실제 측정이 힘들고 이미지손상에 따라 매출이익이 감소할 가능성이 크므로 매출이익 감소액에 포함되어야 한다.

실제 사이버사고 시에는 주가하락 현상이 거의 발생하지 않으므로 사이버사고 피해액 계산 시 포함될 필요가 없다.

법적 비용은 사이버보험에서 피해액을 분류할 때 직접 피해와 제3자 피해로 분류하듯이 과태료 등 직접적으로 발생하는 비용과 타 기관 또는 고객에게 배상하는 간접 비용으로 분류가 가능하다.

정리하면, Gordon & Loeb 방법에서 잠재적 비용이며 간접 비용은 이미지 손상, 주가하락을 삭제하고 그대신 제3자 피해에 대한 법적 배상을 추가한다. 잠재적 비용 및 직접 비용인 잠재적 책임 비용은 과태료 등의 비용인 1차 법적 비용으로 변경하여 계산 방법을 명확히 한다.

4.2 신진 방법 개선

기존 신진 방법에 스마트폰을 이용한 인터넷뱅킹, 간편결제 등의 현상을 반영하기 위해 GDP, 인터넷보급율에 추가로 국가간 스마트폰 보급률을 비교하여 사이버피해액을 계산하는 것이 필요하다. 추가로 IoT기기의 보급이 증가함에 따라 IoT기기 수도 포함하여 계산하면 보다 정확한 사이버사고 계산이 가능할 것이다.

기관간 사이버피해액을 계산하기 위해서는 사이버사고 피해와 연관이 많은 해당 기관의 인터넷, 스마트폰, 클라우드 등을 이용한 사업의 매출액 및 순이익, 개인정보의 전자적 보유량을 이용하여 한다. 이러한 항목을 이용한 신진 방법으로 타 기관의 사이버사고 피해액을 이용해 다른 기관의 사이버피해액을 예상해 보는 것이 가능할 것이다.

V. 결 론

본 논문에서는 정보보호 투자 대비 효과 관련 연구들을 살펴보고 그러한 연구 중 사이버 피해액 계산에서 효과적이라고 생각되는 Gordon & Loeb 방법과 신진 방법을 분석한 후 그에 대한 개선 방법을 제시하였다.

향후에는 이러한 개선된 방법이 어느 정도의 개선 효과가 있었는지 실제 사이버사고 사례를 이용하여 측정해 보고 추가적인 개선 사항에 대해 연구하는 것이 필요하다.

참고문헌

[1] Scott Berinato, “Finally, a Real Return on Security Spending“, CIO FROM IDG, Feb. 2002, available: https://www.cio.com/article/2440999/metrics/finally—a-real-return-on-security-spending.html.

[2] Scott Berniato, “Calculated Risk: Return on Security Investment“, CSO FROM IDG, Dec. 2002, available: http://www.csoonline.com/article/2113094/metrics-budgets/calculated-risk-return-on-security-investment.html?page=2.

[3] J. D. Kim, J. E. Park, “Study of Return on Investment of TCO Based Information Security (ROSI)”, Proceedings of the 1st The Korea Society of Digital Policy and Management, pp. 251-261, 2003.

[4] Y. O. Kwon, B. D. Kim, “The Effect of Information Security Breach and Security Investment Announcement on the Market Value of Korean Firms”, Information Systems Review,

Vol. 9, No. 1, pp. 105-120, 2007.

[5] H. K. Kong, T. S. Kim, “An analysis on effects of information security investments: a BSC perspective”, Proceedings of Journal of Intelligent Manufacturing, pp. 669-679, 2008.

[6] Matthias Brecht and Thomas Nowey, “A Closer Look at Information Security Costs”, Workshop on the Economics of Information Security, 2012.

[7] “Introduction to Return on Security Investment”, ENISA, Dec. 2012.

[8] Lawrence A. Gordon, Martin P. Loeb, “Managing Cybersecurity Resources - A Cost-benefit Analysis”, McGraw-Hill Companies, Sep. 2005.

[9] J. Shin, “Economic Analysis on Effects of Cyber Information Security in Korea: Focused on Estimation of National Loss”, Journal of the Korea Institute of Information Security & Cryptology vol. 23, no. 1, Feb. 2013.

[10] Y. Y. Shin, S. H. Jeon, C. H. Lim et al., “Economic Damages Assessment for National Cyber Security Measures - Analysis of the March 20 Cyber Attack”, Journal of National Intelligence Studies vol. 6, no. 1, pp. 129-173, Oct. 2013..

[11] S. H. Jeong, J. S. Yoon, J. I. Lim et al., “Studies on the effect of Information Security Investment Executive”, Journal of the Korea Institute of Information Security & Cryptology vol. 24, no. 6, pp. 1271-1284 (14 pages), 2014.12.

[12] P. R. Kim, J. P. Hong, “Economic ripple effect and growth contribution of information security industry”, Journal of the Korea Institute of Information and Communication Engineering, vol. 19, no. 5, pp. 1031-1039, May 2015.

[13] W. P. Kim, “Analysis of Global Research Trend on Information Security,” Journal of the Korea Institute of Information and Communication Engineering, vol. 19, no. 5, pp.1110-1116, May 2015.

[14] Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson, “Cyber Risk, Market Failures, and Financial Stability”, International Monetary Fund, IMF Working Paper(WP/17/185), 2017.