KBR 제24권 제2호 2020년 5월 http://dx.doi.org/10.17287/kbr.2020.24.2.143

국내 사이버 침해사고의 경제적 피해금액 산정*

이 용 필**
김 태 성***
유 진 호****

본 논문은 기업들이 빈번한 사이버 침해사고를 당하고 있는 현실에서, 사이버 침해사고를 예방하기 위한 기업들의 적정한 정보보호 투자의사결정에 필요한 정보를 제공하기 위하여, 사이버 침해사고를 당한 기업들의 경제적 피해금액을 조사하기 위한 목적으로 작성되었다. 이를 위해 국내외 선행연구들을 참고하여 경제적 피해금액 산정모델을 개발하고, 최근 3년간 사이버 침해사고를 당한 국내 기업들을 대상으로 경제적 피해액을 산정하였다. 피해금액 산정모델은 정보보호 프로세스에 따라 탐지-사고조사-대응/복구-재발방지 과정별로 피해액 비용요소를 도출하되, Gordon & Loeb(2005) 모형을 참고하여 사고발생으로 직접적인 피해가 발생한 직접비용과 사고를 예방하고 탐지하는 과정에서 발생하는 간접비용으로 구분하였다. 피해를 당한 기업들을 대상으로 침해사고 분석 전문가와 함께 대면 인터뷰를 통해 침해사고 원인 및 피해상황을 재구성하고, 피해금액 항목을 도출하고, 피해금액을 산정하였다. 특히, 기업규모 및 산업 업종에 따라 정보보호 투자의사결정에 도움이 될 수 있도록 기업 규모별, 피해유형별, 산업 업종별 피해액을 산정하였다. 기업 규모별 침해사고의 경제적 피해액은 대기업(20.9억원), 중견기업(17.4억), 중소기업(4.4억원), 비영리재단(0.2억원) 순으로 기업규모가 클수록 커지는 것으로 조사되었다. 그러나, 직접적 피해액(직접비용)은 대기업(4.1억원)에 비해 중견기업(15.1억원)이 더 많은 것으로 나타났으며, 중소기업은 3.8억원이었다. 간접비용에 포함되는 침해사고 탐지, 재발방지 투자금액은 대기업은 16.8억원으로 직접적 피해액 대비 409%인 반면, 중견 및 중소기업은 각각 2.3억원, 0.6억원으로 직접적 피해액의 12%, 15%에 해당하였다. 이는 대기업이 예방 및 재발방지를 위해 노력한 결과 직접적 피해액은 상대적으로 적은데 비해, 중견 및 중소기업은 예방을 위한 투자가 적어 직접적 피해액이 큰 반면 재발방지를 위한 투자는 여전히 상대적으로 적게 되고 있음을 알 수 있었다. 중견기업, 중소기업 대상 가장 피해가 큰 피해유형은 랜섬웨어 공격으로 조사되어, 금전을 목적으로 랜섬웨어 공격을 하는 해커의 주요 타깃이 중견기업, 중소기업이 되고 있음을 확인할 수 있었으며, 중견기업 및 중소기업을 대상으로 정부의 후속 지원정책이 필요한 것으로 조사되었다.

주제어: 사이버 침해사고, 경제적 피해금액, 정보보호 투자의사결정

Ⅰ. 서 론

국내외적으로 많은 기업들이 사이버 침해사고를 당하고 있으나,[1] 랜섬웨어와 같이 일부 피해사례에 대해 보안기업들이 추정치를 제시하거나, 국가 차원으로 거시적으로 제시하고 있는 경우가 있지만, 구체적인 피해금액이 얼마인지 국내에서 조사되거나

논문접수일: 2020. 04. 24. 1차 수정본 접수일: 2020. 05. 10. 2차 수정본 접수일: 2020. 05. 20. 게재확정일: 2020. 05. 20.
* 본 사례는 과학기술정보통신부의 연구비 지원을 받아 수행되었음.
** 한국인터넷진흥원 융합보안단 단장(pals@kisa.or.kr), 제1저자
*** 충북대학교 경영대학 교수(kimts@cbnu.ac.kr), 교신저자
**** 상명대학교 경영경제대학 교수(jhyoo@smu.ac.kr)
1) 홈페이지 변조, DDoS 공격, 악성IP 차단 등 국내 사이버 침해사고로 한국인터넷진흥원에 신고되거나 탐지된 건은 45,000여 건(이용필, 2019)이며, 국내 기업들의 사이버 침해사고 경험률은 2.8%이다(과학기술정보통신부, 2020).

발표된 바가 없다. Gordon & Loeb(2002)의 정보보호 적정 투자모델에 따르면 정보보호 사고 발생시 기대 손실은 사이버 침해사고로 인한 피해금액, 공격발생률, 정보자산의 취약성에 의해 결정된다(서승우, 2008; 이용필, 2017). 개별 기업들은 기업의 피해금액, 공격발생률, 정보자산의 취약성이 얼마가 될지를 예측하고 이를 기반으로 정보보호 투자 의사결정을 하게 되는데, 피해금액이 얼마나 될지 파악하지 못하게 되면 이로 인해 과소 정보보호 투자가 발생할 가능성이 높아진다. 그동안 구체적인 피해금액을 조사하기가 어려웠던 이유는 사이버 침해사고의 특성상 피해기업들이 사이버 침해사고 피해정보를 공개하기 꺼려하는 경우가 대부분이어서, 외부인이 피해규모를 조사하거나 측정하기가 어려웠던 것이 현실이었다. 따라서 구체적인 사이버 침해사고의 피해금액을 조사하고 이를 개별 경제주체들이 인지할 수 있으면, 개별 기업들이 당면하고 있는 위험을 인식하고 이에 대해 적정한 정보보호 투자의사결정을 하는데 도움을 받을 수 있을 것이다.

한편 그동안 대부분의 사이버 침해사고 피해액 조사는 기업의 정보보호담당자를 대상으로 지난 일정기간에 기업이 입은 사이버 침해사고의 피해액 추정치에 대해 직접 설문조사나 인터뷰를 통해 조사하는 형태로 진행되거나 침해사고 정보가 공개되었을 경우 주식시장에 미치는 영향을 고려하여 간접적으로 측정하는 연구가 많았다. 개별기업 담당자를 대상으로 설문조사하는 경우는 침해사고의 피해범위를 어디까지 할지, 비용항목은 어느 것까지, 어떻게 산정할 것인지 개별 정보보호 담당자의 의견에 따라 많은 편차가 발생할 수 있다. 침해사고 정보가 주식시장에서 미치는 영향도 침해사고 정보의 공개가 극히 제한적인 상황에서 실증연구 결과도 제한적이었다. 또한 사이버 침해사고의 특성상 긴급히 정상화시켜야 하는 경영진 및 현업 담당자 입장에서 침해사고를 복구하기에 급급하므로 경제적 피해금액에 해당하는 항목들을 고려하여 경제적 피해금액이 얼마나 되는지 산정하고 있는 경우는 극히 드물며, 경우에 따라서는 장기적으로 대응해야하는 피해 후속 조치들이 있어 이를 고려하여 전체적인 비용을 고려해서 경제적 피해금액을 산정하는 경우는 더욱 힘들다.

이러한 상황에서 본고는 사이버 침해사고를 당한 기업들을 대상으로 경제적 피해금액을 산정할 수 있도록 모델을 설정하고, 정보보호 프로세스를 고려하여 비용항목들을 도출하였으며, 침해사고를 당해 신고한 기업들을 대상으로 침해사고 분석가와 함께 방문하여 침해사고 원인 및 피해현황을 재정리하고 항목별 비용금액을 계산하여, 업체별 비용항목 및 금액에 대한 응답 편차를 줄이고자 하였다. 이를 통해 사이버 침해사고의 피해유형, 기업 규모, 업종 등에 따라 피해액을 조사하였다. 기업에서는 재무적, 비고의적 의무위반 등 다양한 위험이 존재하며 이를 다루기 위한 위험관리 전략을 고려하고 있다(안중석 외, 2010; Park & Choi, 2014). 사이버 침해사고도 그러한 위험 관리 차원에서 접근이 필요하다.

2장에서는 사이버 침해사고의 정의를 살펴보고, 국내외 경제적 피해금액을 조사한 선행연구를 고찰한다. 국내외 소개된 경제적 피해금액 산정 모델을 살펴보고, 비용항목 등을 도출해 비교한다. 국내에서는 개인정보침해사고를 당한 기업 대상 설문조사를 통해 피해액 산정을 한 경우가 있었으며, 인터넷 침해사고의 경우 국가 전체적인 피해액을 산정한 경우가 있었다. 국외에서는 영국에서 사이버침해사고 종류별 피해액을 산정한 경우가 있었고, 설문조사를 통해 기업들의 피해액을 산정한 경우가 있었다.

3장에서는 국내・외 사례 조사를 바탕으로 설계한 모델을 소개하고, 구체적인 산출방식과 조사대상 및 조사방법을 제시한다.

4장에서는 본고에서 제시한 모형을 바탕으로 최근 3년간 침해사고를 당한 기업을 대상으로 실제 측정한 값을 기업 규모별, 피해유형별, 산업 업종별로 제

시하고 분석한다.

5장에서는 본고의 연구결과에 대한 평가와 이를 통한 시사점 분석, 연구의 한계점 및 향후 연구방향에 대해 정리한다.

Ⅱ. 선행연구 고찰

2.1 침해사고 피해 및 투자

사이버 상의 '침해사고'가 무엇인지에 대해 연구모델, 방법론에 따라 다르게 정의하고 있다. 국내 법적으로 정보통신망 이용촉진 및 정보보호등에 관한 법률(이하 정보통신망법) 제2조 제1항 제7호에 따르면, '해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.'고 정의하고 있다. 또한 정보통신망법 제48조 제1항에는 '누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니된다'고 해킹을 금지하고 있다. 예를 들어 DDoS 공격(서비스 거부 공격)에 의한 운영 서비스의 지연 또는 장애발생, 해킹 공격 및 악성코드 감염에 의한 정보 유출, 시스템 파괴, 공격 경유지 이용, 위변조 등 피해가 발생한 모든 사고를 침해사고로 볼 수 있다(한국인터넷진흥원, 2016; 장상수, 2019). 이러한 침해사고란 매우 광범위하고 공격 유형과 목적 또한 다양하다(유진호 외, 2008; 김승학 외, 2018).

이러한 사이버 침해사고의 위협으로부터 정보와 그러한 정보와 연관되는 정보자산을 보호하기 위한 활동이 '정보보호(또는 정보보안)'[2]이다(장상수, 2019). 정보보호는 권한 없는 자가 정보에 접근하지 못하도록 하는 기밀성(Confidentiality), 정보가 허가 없이는 수정될 수 없도록 하는 무결성(Integrity), 허가된 접근의 경우 정보에 대한 접근이 가능해야 하는 가용성(Availability)을 유지하기 위해 권한없는 접속, 이용, 공개, 방해, 변경 및 파괴로부터 정보, 정보시스템 및 정보통신망을 보호하는 활동을 말한다(이기혁 외, 2020). 예를 들어 해킹은 권한 없는 자가 정보통신망에 침입하여 정보를 획득하거나, 부여된 권한 이상의 권한을 획득하여 악성파일을 생성하는 등 기밀성, 무결성을 해하는 활동이다. 즉, 기밀성, 무결성, 가용성이 훼손된 경우 침해사고가 발생했다고 이해할 수 있으며, 침해사고의 정의에서 나열한 것들은 이러한 기밀성, 무결성, 가용성을 훼손하는 방법들 중 일부를 예를들어 제시한 것이다. 개인정보보호의 경우에도 정보통신망법 제28조에 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 기술적·관리적 조치를 하도록 하고 있는데, 사이버 침해사고로 인한 개인정보의 침해를 막기위한 조치를 포함하고 있다.

사이버 침해사고로 발생한 피해의 규모를 추정하거나 해당 피해의 규모를 고려한 투자의사결정 등 사이버보안 침해사고에 대한 경제적 관점에 관련된 연구는 20년 정도의 기간동안 수행되어왔다(강미화 외, 2015). 관련 연구는 1) 사이버보안 피해규모의 산정에 관한 연구, 2) 사이버보안 피해규모와 이를 감소시키기 위한 투자규모 사이의 관계에 대한 연구, 3) 다양한 정보보호 대안들로 구성된 투자 포트폴리오 의사결정에 대한 연구 등으로 구분할 수 있다.

사이버보안 피해규모의 산정에 관한 연구 분야에

2) 국가정보화기본법 제3조제6항, 정보보호 산업 진흥에 관한 법률 제2조 제1항 제1호 등에서 '정보보호'란 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하기 위한 관리적·기술적·물리적 수단을 마련하는 것으로 정의하고 있다.

서는 다시 사이버 침해사고의 피해금액을 직접 추정하는 방식과 주식시장 등을 통해 간접적으로 추정하는 방식으로 구분할 수 있다.

사이버 침해사고의 피해금액을 직접 추정하는 방식으로 유진호 외(2008)는 Gordon & Loeb 모형(2005)을 참조하여 피해액을 〈그림 1〉의 직접비용과 명시적비용 항목으로 한정하여 매출이익 손실, 생산효율 저하로 인한 손실, 복구비용, 영구히 손상된 데이터의 가치 4가지 항목으로 구분하였다. 이 모형으로 2003년 1.25 인터넷 침해사고의 가용성 상실로 인한 국내 피해액과 2005년도 국내 연간 민간기업 침해사고 피해액 추정에 적용하였다. 피해액 산정모형을 체계적으로 수립하고, 국가차원의 피해액을 산정한 연구로 의미가 있으나, 정보 수집의 한계로 정보보호 실태조사 등의 수치를 활용하여 간접적으로 국가 차원의 피해액을 추정하는데 그쳤다.

유진호 외(2009)는 개인정보 유노출 사고로 인한 기업의 손실비용을 Gordon & Loeb 모형을 참조하여 침해사고 대응비용(복구비용), 생산성 손실비용, 잠재적인 법적 책임비용으로 구분하여 조사하였다. 침해사고 대응비용, 생산성 손실비용은 실태조사 설문조사 결과를 주로 활용하였으며, 특히 잠재적인 법적 책임비용을 계산할 때, 소송을 제기하지 않은 모든 개인정보 피해자에게 손해배상을 한다는 가정하에 추정하여 총 손실의 99%가 잠재적인 손해배상금이 차지하였다. 이 연구는 국가 차원의 피해액을 제시하고 있으나, 개인정보 유노출 사고에 대해 피해액을 산정할 수 있는 비용항목을 도출하고 실무적으로 적용할 수 있도록 제시한 특징이 있다.

전용희 외(2009)는 DDoS 공격 대비를 위한 비용과 공격 발생시 서비스 중단으로 인한 경제손실 모델의 해외 사례연구를 정리하였다. 4가지 비용 모델 연구사례를 제시하고, 각 사례별로 DDoS 공격 관련 비용항목을 세부적으로 도출하였으며, 사례별 특성을 정리하고 있다. 현대경제연구원(2009)은 2009년 7.7 DDoS 공격의 피해액을 363억원~544억원으로 추정하였다, 이 연구는 7.7 DDoS 공격에 따른 피해시간, 피해업체 규모를 추정하고 GDP 비중을 고려하여 국가 차원의 피해액을 신속하게 계산하여 제시한 특징이 있다. 신영웅 외(2014)는 2013년 3.20 공격의 피해액을 8,672억원으로 산정하였다. Gordon & Loeb 모형을 적용하여 직접적인 피해액, 간접적인 피해액, 잠재적인 피해액으로 구분하였으며, 직접적인 피해액은 1,361억원, 간접적인 피해액은 6,600만원, 잠재적인 피해액은 주식시장 가치하락으로 7,310억원을 제시하여 잠재적 피해액을 강조한 특징이 있다. 한국마이크로소프트(2018)는 국내 대기업의 경우 직접적 손실이 32억원, 간접적 손실이 137억원, 추가손실이 130억원으로 국내 총 77조원의 피해액이 발생한다고 발표하였다. 아태지역 13개국 1,300명의 250인 이상의 대기업 인사를 인터뷰하여 조사하였고, 고객이탈, 평판 손실 등 간접적 손실과 일자리 손실 등의 추가손실을 더해 국가적인 총 피해액을 계산하여 제시한 특징이 있다. 임규건 외(2018)는 개인정보 유출에 따른 피해 비용 산출 모델을 실거래 평균값 기반, 개인 인식 가치 기반, 보상금액 기반, 타 국가 기반의 4가지 방식으로 제안하였으며, 2016년 개인정보 유출 피해비용을 방식별로 최소 74억에서 220조로 추산하였다. 이 연구는 개인정보 유출에 따른 피해액을 계산하기 위한 다양한 방식을 제시하였다는데 의미가 있다. 신진(2013)은 데이터 수집의 현실적인 제약을 인정하고 노턴 사이버범죄보고서(2011)의 계산방법을 원용하여 한국의 사이버 범죄의 피해금액을 GDP를 기준으로 산출하였으며 10조~40조원 정도 범위로 추정하였다. 자료의 정밀성을 확보하기 위해 업무담당 고위직원 인터뷰와 현장기반 연구가 필요함을 지적하였고, 사이버 공격에 의한 직간접 피해비용과 투자의 기회비용, 사후 대응 비용을 조사할 것을 제안하고 있다.

영국 Oxford Economics (2014)는 설문조사(9,973개 업체 대상, 427개 응답)를 통해 사이버 침해사고 피해액을 조사하였다. 피해기업별 피해액 평균을 삭제/치료, 생산성 손실, 조업중단, IT 피해/도난, 평판손실 항목으로 구분하여 조사하였는데, 사이버 공격에 의한 영국 내 기업들의 사이버 침해사고 경험을 다룬다는 좀 더 넓은 관점에서 조사하면서, 피해액 비용항목을 몇 가지만 선별하여 조사한 한계점이 있다.

UK Department for Digital, Culture, Media and Sport(2019, 영국 문화미디어체육부, 이하 영국 DCMS)는 사이버 침해사고로 인한 영향도 분석을 위해 자국 내 기업·단체 대상 침해사고로 인한 피해액 설문조사를 2016년도부터 실시하고 있다. 지난 12개월 중 가장 심각한 피해의 경우를 대상으로 피해액을 전체 피해액, 직접 비용, 복구비용, 장기비용으로 구분하여 설문하는 방식으로 진행하고 있다. 조사결과 피해 기업의 전체 평균 피해액은 635만원이며, 기업 규모별로는 대기업이 3,450만원, 중기업은 1,409만원, 소기업은 560만원, 비영리재단은 1,439만원 정도의 피해를 입은 것으로 조사되었다.[3] 정보보호 투자액은 대기업이 4.21억원, 중기업이 3,820만원, 소기업이 530만원, 비영리재단이 230만원 정도이며, 최초 조사가 이루어진 '16년 이후 사이버 침해사고에 의한 경제적 피해액은 지속적으로 증가하는 추세를 보였다. 이 연구는 피해액 비용항목을 체계적으로 정리하여 조사를 한 특징이 있으나 심층 인터뷰 대신 설문조사 방식을 이용하여 피해액 조사를 진행한 한계점이 존재한다. 한국과 영국의 사이버 침해사고를 경험한 비율은 한국 기업이 2.8%(과학기술정보통신부, 2020), 영국 기업은 32%(영국 DCMS, 2019)로 응답하고 있어 기업 환경, 문화적인 차이가 존재하고 있으나, 피해액 조사를 위한 연구에 영국 사례는 주요한 참고가 될 수 있다.

Accenture & Ponemon Institute(2019)에서는 미국, 영국, 일본 등 11개국(한국은 포함되지 않음)의 16개 산업 분야에서 355개의 기업 내의 IT 및 보안 전문가들을 대상으로 총 2,647개의 인터뷰를 실시하였다. 기업 내부에서 발생하는 사고를 탐지, 조사, 대응, 복구하기까지 내부적인 활동비용(Internal cost activity centers)과 사이버 공격의 결과로 나타난 비용(External consequence and costs)으로 구분하여 조사하였다. 미국은 기업별 평균 328억원, 영국은 138억원 정도 비용이 발생하는 것으로 조사되었다. 그러나 영국 Home Office(2018)에서 언급한 것과 같이 국내외 컨설팅업체나 보안업체 조사의 경우 간접비용, 평판손실 등의 비용이 크며 전체적인 피해액도 과대하게 부풀려지는 경향이 있다.

간접적으로 측정하는 연구로는 기업의 침해사고 공개가 기업가치에 미치는 영향을 주식가치와 연계하여 평가하는 연구가 진행되었는데, Campbell 외(2003)는 단기적으로 기밀정보의 침해사건은 주식하락에 영향을 미치지만 다른 종류의 보안사고는 주가에 영향을 미치지 않았음을 보여주었고, Goel & Shawky(2009)에 따르면 침해사고를 당한 기업은 사고 후 2~3일에 걸쳐 주가가 -1.00% 하락하는 것으로 나타났다. 국내에서는 황해수 외(2015)가 침해사고가 기업가치에 미치는 영향을 Tobin's q의 분석기준으로 주가손실과 평판손실을 분석하였다. 보안사고로 인한 평판손실을 기업의 부채상황과 연관시켜 분석하였다는 데에 의미가 있다. 권홍 외(2012)는 개인정보 주권자인 서비스 이용자가 본인의 개인정보 침해에 대해 보상받기를 희망하는 경제적 가치를 CVM(Contingent Valuation Method)을 활용하여 측정하는 연구를 수행하였다. 전효정과 김태성(2016)은 차세대 전력 인프라인 스마트그리드에 발

3) 본 조사에서는 파운드(£) 단위로 조사되었으며, 환율에 따라 £1 = ₩1,520으로 산정

생하는 보안피해비용을 시나리오 기법을 이용하여 추정하는 연구를 수행하였다.

사이버보안 피해규모와 이를 감소시키기 위한 투자규모 사이의 관계에 대한 연구 분야에서는 취약점의 특성을 고려하여 피해 감소에 대한 비용대비 효과적인 투자 규모를 산정하는 Gordon & Loeb(2002)의 연구가 초기의 대표적인 성과이다. Anderson & Clayton(2009)의 사이버범죄의 경제적 유인에 대한 연구에서도 사이버범죄와 관련된 경제적 요인들이 고려되었다. Kong et al.(2012)은 정보보호 투자의 내부적 관점/외부적 관점, 재무적 관점/비재무적 관점, 단기적 관점/장기적 관점에서의 성과를 BSC(Balanced Score Card)를 이용하여 정보보호 관리자를 대상으로 실증분석하였다.

다양한 정보보호 대안들로 구성된 투자 포트폴리오 의사결정에 대한 연구 분야에서는 Kumar et al.(2008)이 사이버보안 침해사고로 인한 피해에 대비하는 정보보호 대안들로 구성되는 투자 포트폴리오의 효과를 개별 투자대안과 위협요인과의 관계, 투자효과의 세부단계 등을 고려하여 시뮬레이션 기법으로 실증분석하였다. 투자대안간의 포트폴리오 효과가 언제나 긍정적(+)이지만은 않다는 것을 실증했다는 점에서 의미가 있다. Zhao et al.(2013)은 정보보호 투자의 부(負)의 외부성(externality)이 있는 경우에는 기업간 상호협약을 통한 위험공유(risk pooling arrangement)가 사이버보험의 투자효율을 높이는데 도움이 되고, 보안관제서비스는 정보보호 투자의 외부성을 내부화 함으로서 정보보호 투자의 효율을 높인다는 결과를 보였다. Lam(2016)은 사이버보안 투자가 공격을 예방하기위한 목적 뿐만 아니라 피해감소를 목적으로 하는데, 소프트웨어업체는 충분히 검증되지 않은 소프트웨어를 조기에 출시함으로써 공격 예방을 위한 투자는 과소하게 투자하는 반면, 소프트웨어 결함으로 발생한 피해를 통제하는 데에는 과도하게 투자하는 경향이 있다는 것을 보였다. 예방적 사전투자와 대응적 사후투자 간의 균형이라는 보안경제학 분야의 오랜 주제와도 연결이 되는 연구결과이다. 김길환 외(2018)는 다양한 제품 및 서비스로 구성된 정보보호투자 포트폴리오의 최적 조합을 휴리스틱 방법론인 유전자 알고리즘을 적용하여 도출하였다.

2.2 침해사고 피해비용 구조

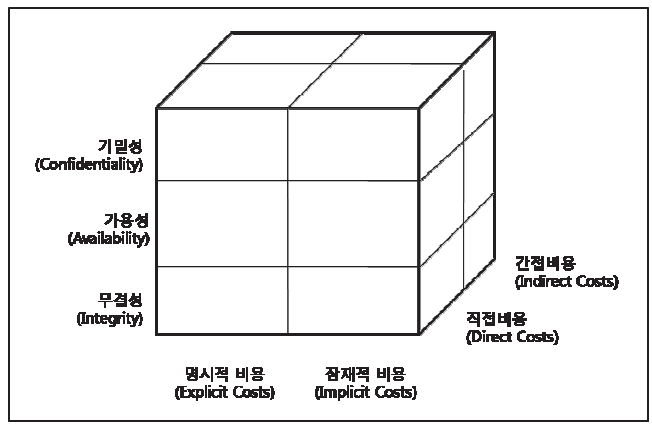
2.2.1 Gordon & Loeb 모형

Gordon & Loeb(2005)은 정보보호 침해사고에 의한 비용 산출에 활용하기 위해 사이버보안 비용구조(Cybersecurity Cost Grid)를 제시하였다. 이 연구는 특히 여러 가지 다양한 침해사고[4]로부터 발생하는 손실비용을 〈그림 1〉과 같이 직접비용(Direct Costs)과 간접비용(Indirect Costs), 명시적 비용(Explicit Costs)과 잠재적 비용(Implicit Costs)으로 구분하여 침해사고로 인한 손실비용을 산출할 수 있는 개념적인 분석 틀을 제시하였다.

직접비용은 특정 침해사고와 명확하게 연계할 수 있는 비용으로, 특정 침해사고를 예방하고, 탐지하고, 복구하는데 투입된 인력, 하드웨어, 소프트웨어와 관련된 비용이다. 간접비용은 특정 침해사고와 연계할 수 없는 비용으로 예를들어 수많은 침해사고를 탐지하기 위한 침입탐지시스템의 전반적인 비용을 포함한다. 간접비용을 계산할 때 특정 침해사고에 어떻게 할당할 것인지 절대적으로 올바른 방법은 없으며, 조직내 다양한 제품들과 서비스에 간접비용(overhead) 할당문제와 유사한 문제가 발생한다.

명시적 비용은 명확하게 침해사고 비용으로 측정

4) 다양한 침해사고는 기밀성(Confidentiality), 가용성(Availability), 무결성(Integrity)과 관련된 사고로 구분하였다.



〈그림 1〉 사이버 침해사고의 비용 구조

될 수 있는 것으로 예방, 탐지, 보안취약점 개선을 위한 활동과 정보보호 시스템 이용에서 발생한 비용, 인력 등 인건비를 포함한다. 또한, 사이버보안 정책과 매뉴얼 개발, 인식제고/훈련, 사이버보안 감사와 관련된 비용도 포함하고 있다. 잠재적 비용은 침해사고로 인한 기회비용으로 평판효과, 잠재적인 법적 배상비용 등 측정하기 애매한 비용을 말한다. 잠재적 비용은 침해사고의 실질적 비용에서 상당한 부분을 차지할 수 있기 때문에 명시적 비용과 잠재적 비용의 차이점을 구분하고 인식하는 것이 적정 정보보호 투자의사결정에서 중요한 의미를 가진다.

2.2.2 영국 Cyber Crime Working Group 모델

영국 정부(UK Home Office, 2018)는 사이버 범죄 피해액을 추정하기 위해 '사이버범죄 비용 워킹그룹[5]'을 구성하여 기존 추정 결과들('11~'16)을 분석하였다. 분석결과 기존 사이버 범죄 비용 추정 보고서들[6]의 데이터 신뢰성, 일관성, 분석 방법론 등의 문제점을 확인하고, 신규 분석 프레임워크를 제시하였다.

사이버 범죄가 영국 경제에 미치는 완전한 영향을 보여주기 위해 경제적 비용(기회비용) 개념을 이용하였는데, 이전비용(보조금, 벌금 등)은 국가 내 경제주체(국가 ↔기업) 간 이전에 해당하므로 영국 국가 차원에서는 비용에 해당하지 않으며, 피해자에게 제공되는 사이버 침해사고 보험금도 이전비용에 해당하므로 사이버 범죄 비용 프레임워크에서는 제외하였다. 다만, 보험사의 관리 비용(관리 인력, 부지, 장비 등)은 비용에 포함하였다. 사이버 범죄 비용 프레임워크의 사이버 범죄 비용 항목은 예상비용(Costs in anticipation), 결과비용(Costs as a consequence), 대응비용(Costs in response) 로 구분하였다.

2.2.3 Accenture & Ponemon Institute

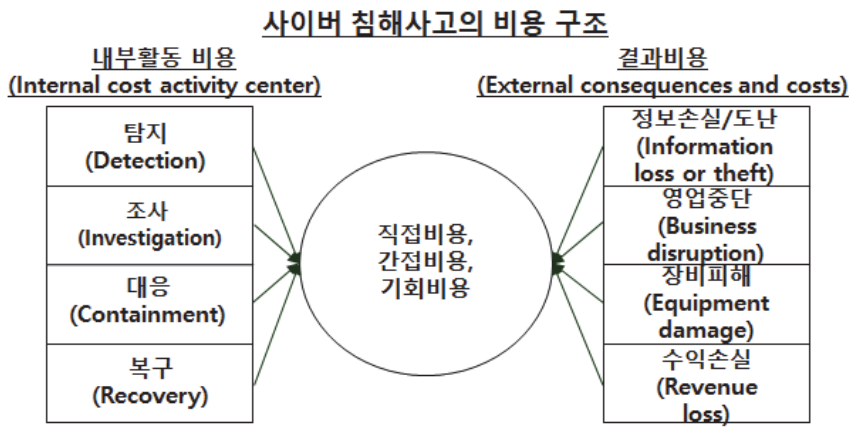
Accenture & Ponemon Institute(2019)는 기

5) 사이버 범죄 비용 워킹그룹은 다수의 정부부처, 학계, 경찰, 산업체 전문가들로 구성하여, 내무부 과학 자문 위원회(Home Office Science Advisory Council)가 주관이 되어 2014년 가을부터 2016년 봄(16개월)까지 활동하였다. 사이버 의존 범죄(악성코드, 해킹 등)와 사이버 활용 범죄(사기)를 다루었으며, 대상으로는 개인, 기업, 기관(공공) 까지 포함하였다.

6) Detica (2011), National Fraud Authority (2013), Oxford Economics(2014), McAfee/Intel(2014), Ponemon(2015)

〈표 1〉 피해비용 항목 구분

구분	내용
예상비용	기술적 비용(보안제품), 교육훈련, 보안절차 추가로 인한 사용자 영향, 정부활동(정부 규제, 인식 제고활동), 사이버보험관리 등
결과비용	복구비용(장비 피해, 데이터 복구), 재정손실(업무중단, 사기, 지적재산권 손실 가치, 평판 손해, 거래중단)
대응비용	수사기관 활동, 사이버 형사재판, 구금 및 교정시설 운영비용 등



〈그림 2〉 사이버 침해사고의 비용 구조

업 내부에서 침해사고를 탐지, 조사, 대응, 복구하는 정보보호 내부 프로세스에 따라 업무를 수행하면서 발생하는 비용(Internal cost activity centers)과 사이버 공격의 결과로서 나타난 결과비용(External consequence and costs)으로 구분하여 〈그림 2〉와 같이 사이버 침해사고 비용 구조를 수립하였다. '직접비용'은 주어진 활동을 수행하기 위한 직접 지출된 비용으로, '간접비용'은 직접 현금 지출은 아니지만 투입된 시간, 노력 등 조직차원의 자원 투입, '기회비용'은 사고 이후 평판 저하의 결과로 상실된 영업 기회로부터 발생한 비용으로 계산하고 있다.

2.3 침해사고 피해비용 선행연구 시사점

사이버 침해사고의 특성상 구체적인 피해금액과 정보보호 투자와 관련한 정보는 기업들이 공개하지 않는 특성이 있어 경제적 피해금액을 조사하는데 한계가 있다(Kotulic and Clark, 2004; 신일순, 2013). 국내외 연구사례들은 이러한 한계로 인해 특정 사고에 대한 국가적인 피해액을 추정(유진호 외, 2008)하거나, 실태조사를 기반으로 답변한 자료를 기반으로 추정(유진호 외, 2009; 신일순 2013)하거나, DDoS와 같은 특정 침해사고에 한정된 사고금액을 산정(전영희, 2009)하거나, 기업 실무자 대상 피해액 설문조사 답변 자료를 근거로 피해액을 산정하되 피해액이 과소하게 계산되거나(UK DCMS, 2019; 황해수 외, 2015), 간접적 손실, 추가손실 등을 직접적 손실의 몇 배로 제시하여 피해액을 과도하게 추정하는(한국마이크로소프트, 2018) 문제점이 있었다.

기업들의 정보보호 투자의사결정에 활용하기 위해서는 개별 기업의 규모 및 피해유형, 업종 등 기업의 처한 다양한 상황에서 적용할 수 있도록 다차원의 피해액이 조사되어 공개될 필요성이 있다. 또한 기업 담당자 대상 설문조사를 실시하는 경우에도 피해금액 범위 및 항목이 답변자들마다 상이할 수 있는 문제점을 해소할 수 있도록 전체적인 피해비용을 직접 질문하기 보다는 개별 기업의 특정 피해상황을 정리하고, 정보보호 프로세스에 따른 비용항목들을 도출하고 조사대상자별 비용항목 산정에 차이가 나는 부분을 최소화시키기 위한 산정모델 적용이 필요하다.

본 연구에서는 특정 침해사고에 한정하지 않고 다양한 침해사고에 적용될 수 있도록 최근 3년 내 실제 침해사고를 당해 한국인터넷진흥원에 신고한 기업을 대상으로 개별 기업의 경제적 피해금액을 도출하고자 하였다. 신고한 기업들 전체를 대상으로 피해사고 유형별로 조사를 하여 특정 사고 유형에 한정하지 않았다. 또한 구체적인 피해금액 항목이 답변자들마다 상이할 수 있는 문제점을 해소하기 위해 정보보호 프로세스에 따른 피해산정 모델을 수립하고, 사고조사 전문가가 인터뷰에 참여하여 반구조화된 설문지를 활용하여 침해사고의 범위, 사고 수습과정 등 침해사고 경과 및 대응 과정을 전체적으로 재정리하고 구체적인 비용항목에 해당하는 요소들을 도출하여 피해기업별로 피해항목이 누락되지 않도록 진행하였다.

피해산정 모델과 관련해서는 Gordon & Loeb (2005)의 모형은 사고 종류에 따라 기밀성, 가용성, 무결성 피해가 발생하고 각 피해유형별로 발생하는 비용을 구조화하는 것인데, 실제 사고현장에서는 하나의 침해사고에서 기밀성, 가용성, 무결성 피해가 복합적으로 발생하게 되므로 사고 피해 유형별로 비용항목을 계산하는 것은 구분 의미가 약하다. 예를들어 기업을 대상으로 랜섬웨어 공격을 하는 해커의 경우, 해킹 이후 공격 대상이 되는 기업인지를 탐색하는 과정을 거치는 동안 악성코드를 설치하고 기업 내부 서버 및 네트워크 구성을 조사한 후 최후에 랜섬웨어 실행을 통해 가용성을 침해한다. 이 경우 가용성 이외에도 해킹 과정에서 기밀성, 무결성의 피해도 동시에 발생하게 된다. 또한, 침해사고를 탐지, 조사, 대응, 복구하는 정보보호 과정에서 발생하는 비용을 모델에 반영하기가 어려운 한계가 있다.

영국 Cyber Crime Working Group의 모델은 기회비용(Opportunity Cost)이라는 경제적 비용 관점에 충실한 반면, 보안절차 추가로 인한 사용자 비용, 수사기관의 비용, 보험사 운영 비용 등 국가차원의 경제적 비용을 계산하는데 이론적으로 적합할 수 있으나, 개별 기업 차원의 정보보호 투자의사결정에 활용될 수 있는 피해비용을 산정하는 목적으로는 한계가 있다. 영국 정부에서 운영하는 정보보호 실태조사에서도 이러한 모형을 실제 적용하고 있지 못하다.

Accenture & Ponemon Institute(2019)는 침해사고 대응 프로세스 관점에서 탐지, 사고조사, 대응, 복구 과정에 따라 발생하는 내부활동 비용을 계산하였는데, 이렇게 프로세스를 기반으로 하는 경우 내부 활동 기준의 비용항목을 누락하지 않고 전체를 포괄할 수 있게 된다. 그러나, 직접비용, 간접비용을 산정하는 구분 기준이 침해사고와 직접적인 관련성 여부로 구분하지 아니하고 내부활동과 관련된 비용인지 여부로 판단함으로써 침해사고와 연관된 비용인지 측정하기 어려운 한계가 존재하고, 객관적인 비용으로 측정하기 어려운 기회비용을 추가하여 과다하게 추정될 수 있는 여지가 있게 되는 문제점이 있을 수 있다.

비용항목과 관련해서는 영국 DCMS, Oxford Economics, Accenture & Ponemon Institute (2019)의 비용항목들을 비교하여 보면 〈표 2〉와 같다. Oxford Economics는 사이버 공격의 직접적인 결과로서 나타나는 설문만을 질문하였고, 영국 DCMS

〈표 2〉 해외 침해사고 경제적 피해 모델들의 비용요소 분류

구분	Oxford Economics	영국 DCMS 설문지 비용 항목	Accenture & Ponemon Institute
정보보호 투자	-	사이버 공격을 예방하기 위해서 사용된 각종 소프트웨어, 하드웨어, 직원 인건비, 아웃소싱, 교육 관련 비용	내부비용(탐지)
직접비용	침해사고의 발생으로 업무가 중단되어 발생한 비용	업무 중단이 된 직원이 입은 피해	결과비용(업무 중단)
	침해사고로 인하여 IT 자산과 인프라가 파손된 비용	잃어버리거나, 손상, 도난 당한 데이터/자산/기밀정보/IP	결과비용(정보손실/도난)
	직원들의 생산성 손실 비용	사람들이 온라인 서비스에 접속하지 못해서 발생한 손해	결과비용(수익 손실)
복구비용	침해사고로 인한 피해를 복구하는데 사용한 비용	발생한 사이버 공격을 대응 혹은 수습하기 위해 추가적으로 투입된 직원	내부비용(대응)
			내부비용(복구)
		고객, 주주 등에게 관련 상황을 통지하기 위해 들어간 비용	결과비용(업무 중단)
		장비나 인프라를 수리하기 위해 들어간 비용	결과비용(장비 피해)
		그 외 관련된 수리/복구 비용	내부비용(복구)
장기비용	평판과 이미지 타격으로 인한 비용	주주가치 손실, 미래 투자자로부터의 투자액 손실	결과비용(수익 손실)
		신규 고객이 들어오지 않음으로서 발생하는 장기적 이익 손실	결과비용(수익 손실)
	-	고객 불만 대응 비용	결과비용(업무 중단)
	-	과태료/손해배상 비용	결과비용(업무 중단)

설문지는 직접, 복구, 장기비용 금액을 구간별로 대략 선택하도록 하면서, 구체적인 비용항목리스트를 참고하여 피해금액을 선택하도록 하였다. 정보보호 투자금액 설문은 피해액이 아닌 별도의 정보보호 투자부문에서 질문하였고, 피해액에 반영되는 비용과 중복되지 않도록 조사하였다.

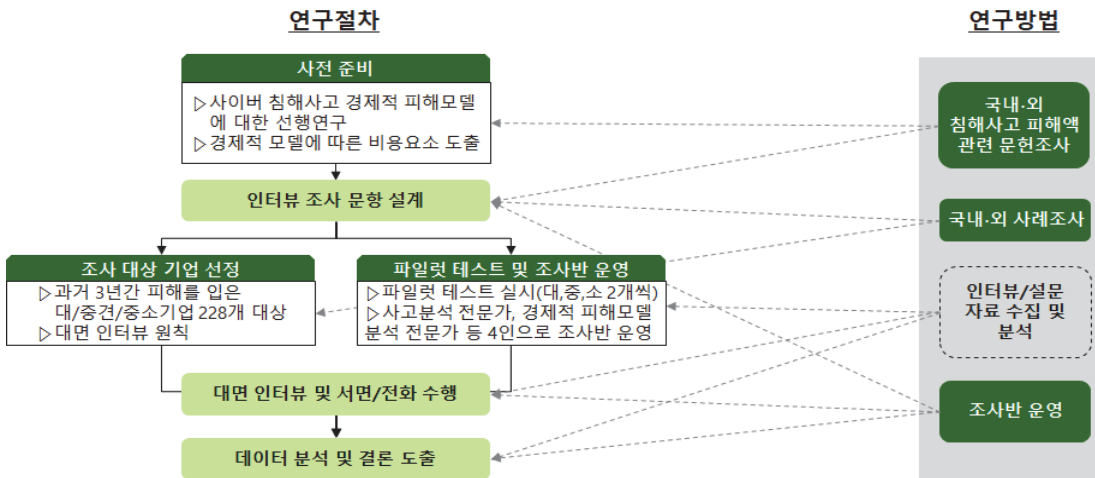
Ⅲ. 연구모델 및 조사방법

3.1 연구절차 및 방법

본 연구는 국내외 사이버 침해사고의 경제적 피해 모델 관련 문헌 및 비용항목, 비용요소 등 사례 조사 및 분석을 하여 피해산정 모델을 도출하였다. 이어서 인터뷰 질의서 문항 설계 및 파일럿 조사를 수행하였다. 조사대상은 과거 3년간 사이버 침해사고 피해를 입은 기업을 대상으로 하였으며, 경제적 피해액 산정 전문가를 포함한 조사반을 구성하여 실제 인터뷰 및 데이터 분석을 수행하였다. 연구절차 및 방법은 〈그림 3〉과 같다.

3.2 피해금액 산정 모델

본 연구에서는 비용항목 도출을 위해 Gordon & Loeb(2005)의 모형을 기본으로 하고, 조사과정에서 인터뷰에 활용하는 반구조화된 설문구조는 Accenture



〈그림 3〉 연구절차 및 방법

& Ponemon Institute(2019)의 정보보호 활동 과정에서의 내부 비용과 침해사고로 인한 결과 비용을 참고하여 〈그림 4〉와 같이 모델을 설계하였다.

침해사고 대응 프로세스는 한국인터넷진흥원(2016)에 따르면 '사고 전 준비 - 사고탐지 - 초기대응 - 대응전략 체계화 - 사고조사(데이터 수집, 데이터 분석) - 보고서 작성 - 해결(재발방지 대책)'의 7단계로 제시하고 있으며, 미국 국립표준 기술연구소(NIST, 2012)에서 발표한 모델에 따르면 '대응준비 - 탐지/분석 - 대응/근절/복구 - 사후 활동'으로 4단계로 제시하고 있다. 김승학 외(2018)는 '사전준비 - 탐지/초기 대응 - 수집/분석 - 감염제거/복구'의 4단계로 프로세스를 제시하고 있다.

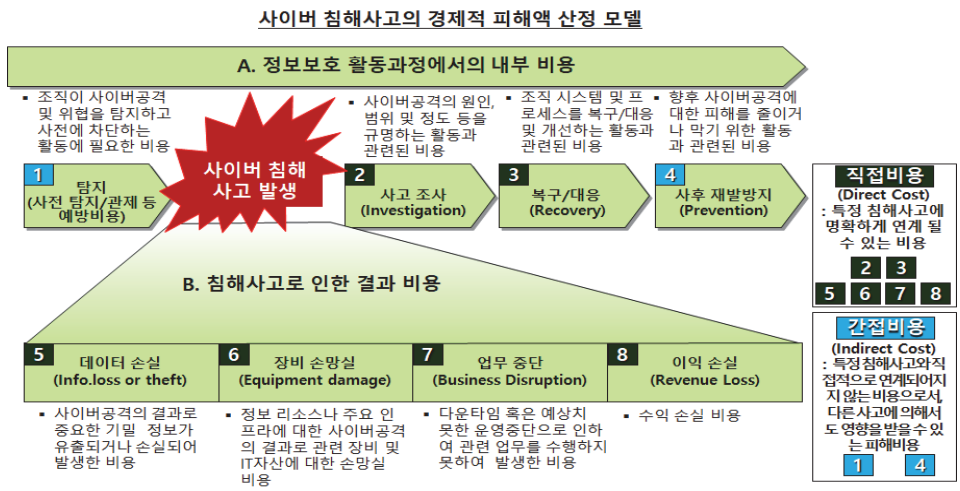
본 연구에서 침해사고 대응을 위한 프로세스는 탐지 - 사고조사 - 대응/복구 - 사후 재발방지 과정으로 분류하였다.

먼저 탐지의 경우 지속적인 모니터링을 통한 이상징후 탐지, 침해사고 식별과 같은 침해사고 탐지 및 랜섬웨어와 같은 사고 대비를 위한 백업 등 예방단계이고, 사고 조사단계의 경우 데이터 수집 및 분석을 통한 명확한 사고원인과 피해 범위를 분석하는 과정이다. 대응/복구 단계는 초기 조사 수행 내용을 바탕으로 피해 확산 방지를 위한 차단, 신고, 소집, 침해사고 관련 부서 통지 등의 절차를 이행하며, 백업 데이터의 복원, 해킹으로 인해 감염된 웹서버, DB 서버, 인증서버, 네트워크 장비, 보안 솔루션, PC 등 전산장비의 초기화 및 프로그램 재설치, 업무 프로세스 정상화를 위한 복구 활동 등을 이행한다. 사후 재발 방지는 추후 유사 공격 대응과 식별을 위한 보안 정책의 수립, 절차변경, 보안 솔루션 등의 재정비, 인력 보충 계획 수립 및 이행이 포함된다.

이러한 프로세스를 고려하여 내부비용 카테고리와 비용항목을 구분하였고, 결과비용은 침해사고로 인해 데이터 손실, 장비 손망실, 업무중단, 이익 손실 등으로 구성하였다. 구체적인 비용 카테고리 및 비용항목과 항목에 대한 설명은 〈표 3〉과 같다.

이들 각 비용항목을 조사한 후 특정 침해사고와 명확하게 연계될 수 있는 비용인 직접비용과 그렇지 않은 간접비용으로 구분하여 집계하는 방식을 이용하였다.

평판비용, 이미지 손상, 주가 하락, 고객 이탈로 인한 손실 같은 비용항목도 설계에 반영하여 조사하



〈그림 4〉 사이버 침해사고의 경제적 피해액 산정 모델

였으나, 현실적으로 측정하기 어려움이 있었고, 실제 유의미한 값이 나오지 않아 결과분석에는 반영하지 않았다. 이는 황해수 외(2015)의 연구에서도 조사된 바와 같이 주가가 사고 이후 단기간 내 하락하였으나 곧 회복한다는 것을 확인할 수 있었다.

3.3 피해액 산정 조사

3.3.1 대상 및 응답자

정보통신망법 제48조의3에 따르면 정보통신서비스 제공자, 직접 정보통신서비스 제공자(IDC 운영자)는 침해사고가 발생하면 그 사실을 과학기술정보통신부나 한국인터넷진흥원에 즉시 신고하도록 되어 있고, 동법 제76조의 제3항에 따라 신고하지 않을 경우 1천만원 이하의 과태료를 부과하도록 하고 있다. 신고의무대상은 영리를 목적으로 인터넷 서비스를 운영하는 모든 사업자(기업)가 해당된다(한국인터넷진흥원, 2016). 최근 3년간 한국인터넷진흥원에 침해사고를 신고하여 사고조사 지원을 받은 전체 기업 중 피해액이 발생한 228개를 대상으로 2019년 9월부터 11월까지 3개월간 조사가 실시되었다. 49개의 기업이 응답했는데, 대기업 7개, 중견기업 8개, 중소기업 31개, 비영리기관 3개가 포함되었다. 개인정보침해사고의 경우 정부의 과태료 등 행정처분이 완료된 기업들을 대상으로 하여 피해금액에 반영될 수 있도록 하였다. 기업별로 정보보호최고책임자, 정보보호 담당자들이 참석하였고, 중소기업의 경우 대표가 직접 참여하여 응답하였다.

응답한 기업을 산업별로 분류하면 정보통신업 18개, 제조업 14개, 도소매업 9개, 전문서비스업 2개, 비영리조직 3개, 금융 및 보험업 1개, 시설관리업 1개, 음식점업 1개가 포함되어 있었다. 이들의 사고유형으로는 랜섬웨어 21개, DDos공격 6개, 비정상 SMS발송 6개, 개인정보 유출 7개, DB변삭제 4개, 홈페이지 변조 2개, 악성코드유포 1개, 코드서명 유출 1개, 게시글 스팸 1개 등 9개 유형으로 분류할 수 있었다.

3.3.2 조사방법

모델설계 후 대·중·소 각 2개씩을 선정하여 파

〈표 3〉 피해액 비용 카테고리 및 비용항목 분류

구분	비용 카테고리	비용항목	비용항목 설명	직접/간접
내부 비용	탐지	보안관제 비용	외부 보안관제 서비스 아웃소싱 비용, 방화벽과 같은 하드웨어, 침입탐지 솔루션 비용, 내부 보안관제 관리 비용 등을 포함	간접비용
	사고조사	사고조사 비용	침해사고 발생 원인 규명 등 조사 비용	직접비용
		법률 자문 비용	사고 발생 후 발생 시 조직 차원의 대응방안 등에 관하여 변호사와 법률 상담으로 발생한 비용	
	대응/복구	사고통지비용	사이버 침해사고 발생 후 침해사고 발생 사실에 대하여 공지 또는 사과의 목적으로 고객들과 내부 직원들에게 통지하는데 들어간 비용(SMS, 우편 비용, 신문, 웹페이지 공지 비용 등 포함)	직접비용
		고객대응 비용	침해사고로 인하여 발생한 고객들의 피해에 대응하기 위하여 조직 내부에서 수행한 재발급, 추가적인 상담 등의 활동으로부터 발생한 비용	
		고객피해보상비용	침해사고로 인하여 발생한 고객들에 대해 피해를 보상하는데 발생한 비용	
		위기대응팀 관리 비용	사이버 침해사고로 인한 피해들을 복구하는데 투입된 조직 내부 혹은 외부 인력들의 인건비	
		과태료/과징금/손해배상금	위반 사실로 인하여 행정기관이나 법에 의하여 조직에 부과된 비용	
		법률 소송 비용	사이버 침해사고가 발생함으로써 발생한 여러 가지 법적 소송에 대응하기 위해서 지출한 비용	
	사후 재발방지	보안장비/솔루션 구입비	방화벽 등 침해사고 재발방지를 위하여 각종 보안장비, 보안 솔루션을 구입하여 발생한 비용	간접비용
		보안컨설팅 등 서비스 이용 비용	침해사고 발생 이후 보안컨설팅, 취약점검 등 보안 강화를 위한 서비스를 이용함으로써 발생한 비용	
		교육 및 모의훈련 비용	조직 내의 구성원들을 대상으로 재발 방지를 위하여 실시하는 교육 및 모의훈련 수행 비용	
		정책, 운영개선 비용	조직 내부에 정보보안 관련 인력을 추가적으로 충원하는 등 조직 내부 보안을 강화하기 위해서 정책 및 업무 프로세스를 개선하는데 발생한 비용	
결과 비용	데이터 손실	복구 불가능한 데이터 가치	사이버 침해사고의 결과로 중요 기밀정보가 유출되어 발생한 피해액이나 데이터가 손실되어서 복구가 불가능하게 된 데이터의 가치	직접비용
	장비 손망실	인프라 피해금액	사이버 침해사고의 결과로 피해를 입은 하드웨어나 소프트웨어를 교체하거나 신규 구입 비용	
	업무 중단	영업 중단으로 인한 이익 손실	사이버 침해사고 결과로 운영중단, 다운타임(Downtime) 등이 발생하여 조직의 구성원들이 맡은 업무를 수행하는데 지연되거나 처리하지 못하여 발생한 피해액	
	이익 손실	직접 피해액	랜섬웨어 협상 비용, 해커에 의한 SMS발송 비용 등 사이버 침해사고로부터 발생하게 된 직접적인 피해액	
		이미지 손상	사이버 침해사고의 결과 조직의 대외적인 이미지나 평판(Reputation)이 손상을 입어 조직의 이익 혹은 매출액이 하락하여 발생한 손해액	
		주가하락	사이버 침해사고의 결과로 조직의 평판 등이 나빠져 주가가 하락하여 입은 손해비용	
		정신적 피해	사이버 침해사고의 결과로 고객들의 불만에 대응하고 침해사고 피해를 복구하는 과정에서 내부 구성원들이 받은 스트레스 등 정신적으로 고통받은 피해	
		고객 이탈로 인한 손실	사이버 침해사고를 당한 사실이 외부에 알려져 신뢰도가 하락하여 보유하고 있는 고객들이 이탈함으로서 기업의 이익 혹은 매출액이 하락하여 발생한 손실액	
		영업 기회 손실	계획 중이었거나 진행 중이었던 프로젝트가 사이버 침해사고 대응 및 복구 작업으로 인하여 지연되거나 취소되면서 잃어버리게 된 영업 이익	

일럿 테스트를 진행하였다. 파일럿 테스트를 통해 모델 및 설문문항의 적절성을 검토하였다. 이후 전체 신고기업 대상 연락 후 방문 또는 전화 면접을 하여 반구조화된 설문으로 피해유형 및 범위, 대응내용 등을 확인하고, 내부 비용 및 결과비용에 해당하는 항목별 금액을 산정하였다. 인터뷰는 먼저 침해사고 경위를 전체적으로 설명을 듣고, 침해사고 발생 경로와 실제 피해의 범위를 산정할 수 있도록 침해사고 분석 전문가와 경제적 피해액 산정을 위한 전문가가 별도로 인터뷰에 동행하였다.

3.3.3 조사내용

피해기업을 대상으로 피해유형별로 랜섬웨어 감염, DDoS 공격, 개인정보 유출 등 피해를 당한 상황 및 복구 과정을 전체적으로 정리하였다. 사고를 당한 기업의 경우 복구 및 정상화에 전념하기 때문에, 실제 투입된 인력 및 비용을 파악하는데 우선 순위를 두지 않는 경향이 있다(영국 DCMS, 2019). 랜섬웨어의 경우 직접 지급한 비용, 복구전문가 비용 등은 알고 있지만, 인력투입, 업무 중단에 따른 비용 산정 등은 비용으로 별도로 산정해 보지 않은 경우가 대부분이어서 이를 일정한 기준으로 산정하였다.

침해사고 대응을 위한 내부비용과 사고로 인한 결과비용을 조사한 후 이를 직접비용과 간접비용으로 구분하여 비용을 집계하였다.

Ⅳ. 연구결과분석

4.1 기업 규모별, 항목별 피해액

침해사고의 경제적 피해액은 기업규모별로 〈표 4〉와 같이 대기업(20.9억원), 중견기업(17.4억), 중소기업(4.4억원), 비영리재단(0.2억원) 등으로 기업규모가 클수록 커지는 것으로 나타났다.

직접적 피해액은 대기업(4.1억원)에 비해 중견기업(15.1억원)이 더 많은 것으로 나타났으며, 직접비 중 업무중단에 따른 피해액이 가장 큰 요소를 차지하였다(대기업 2.7억, 중견기업 13.4억, 중소기업 2.9억).

〈표 4〉 기업규모별, 항목별 평균피해액

(단위 : 백만원)

기업 규모(n)		대기업(n=7)	중견기업(n=8)	중소기업(n=31)	비영리재단(n=3)
직접비용	2.사고조사	40.8	23.1	24.3	7.0
	3.대응/복구	75.0	98.0	43.5	2.2
	5.데이터 손실			10.7	
	6.장비 손망실		5.2	3.6	2.0
	7.업무중단	273.8	1,337.8	285.7	1.7
	8.이익손실	21.4	43.5	17.7	
직접비용 합계		411.1	1,507.6	385.6	12.8
간접비용	1.탐지	610.0	53.9	25.9	0.6
	4.재발방지	1,073.0	174.0	32.2	2.4
간접비용 합계		1,683.0	227.9	58.1	3.0
평균 피해액		2,094.0	1,735.4	443.7	15.8

간접비용에 해당하는 침해사고 탐지, 재발방지 투자를 대기업은 16.8억원(직접피해액의 409%)을 하는 반면, 중견 및 중소기업은 각각 2.3억원, 0.6억원(간접비용 비율이 직접피해액의 12%, 15%에 불과)으로 상대적으로 적었다.

4.2 피해 유형별 피해액

〈표 5〉와 같이 유형별로는 랜섬웨어(13.8억원), DDoS(12.9억원), 개인정보유출(4.9억원), 홈페이지 변조(0.8억원), DB 변삭제(0.6억원) 등으로 조사되었다.

직접적 피해액은 랜섬웨어감염에 의한 업무중단 등으로 10.3억원, DDoS 공격으로 5.1억원, 개인정보유출 조사 등으로 2.0억원 발생하였다.

간접비용으로 예방 및 재발방지를 위해 DDoS 공격(7.7억원), 코드서명 유출(6.7억원), 랜섬웨어(3.5억원) 비용 순서이다.

피해건수는 랜섬웨어가 가장 많았으며, 개인정보유출, DDoS 공격 순이었다. 해커가 기업들 대상으로 랜섬웨어 공격을 통해 이익을 창출하고 있음을 확인할 수 있었다. 악성코드 유포, 코드서명 유출은 Supply Chain 공격에 해당하는 것으로 Supply Chain의 약한 중간 공급자를 공격하여 다수에게 공격을 하기 위한 것으로 대비가 필요한 부분이다.

4.3 산업 업종별 피해액

업종별 피해액은 〈표 6〉과 같이 전문서비스업 26.1억원, 도소매업 16.7억원, 제조업 11.0억원, 정보통신업 3.1억원 순으로 조사되었다. 직접비용 피해액은 전문서비스업이 23.9억원, 제조업이 10.1억원, 도소매업이 5.3억원, 정보통신업이 1.6억원 순으로 조사되었다. 간접비용으로 도소매업 11.4억원, 전문서비스업이 2.2억원, 정보통신업이 1.5억원, 제조업이 0.9억원 순이었다[7].

4.4 기업 규모별, 피해유형별 피해액

대기업은 〈표 7〉과 같이 피해유형으로 DDoS, 랜

〈표 5〉 피해 유형별 평균피해액

(단위 : 백만원)

피해유형		랜섬웨어 (n=21)	DDoS공격 (n=6)	개인정보 유출(n=7)	홈페이지 변조(n=2)	비정상SMS 발송(n=6)	DB변삭제 (n=4)	악성코드 유포(n=1)	코드서명 유출(n=1)
	직접비용 합계	1,025	512	201	20	21	16	278	394
	간접비용 합계	353	773	287	62	56	45	20	666
평균피해액		1,379	1,286	489	82	77	59	298	1,060

〈표 6〉 업종별 평균피해액

(단위 : 백만원)

업종*		전문서비스업(n=2)	도소매업(n=9)	제조업(n=14)	정보통신업(n=18)
	직접비용 합계	2,388	530	1,014	162
	간접비용 합계	217	1,140	86	151
평균 피해액		2,605	1,671	1,100	313

7) * 기타(3) : 음식점업(1), 시설관리업(1), 금융 및 보험업(1)

〈표 7〉 대기업의 피해유형별 평균피해액

(단위 : 백만원)

기업규모	피해유형(n)	직접비용 합계	간접비용 합계	평균 피해액
대기업	DDoS (n=1)	1,797	4,512	6,309
	랜섬웨어 (n=2)	203	2,441	2,645
	코드서명유출 (n=1)	394	666	1,060
	개인정보유출 (n=3)	93	573	667

〈표 8〉 중견기업의 피해유형별 평균피해액

(단위 : 백만원)

기업규모	피해유형(n)	직접비용 합계	간접비용 합계	평균 피해액
중견기업	랜섬웨어(n=5)	2,334	266	2,600
	개인정보유출(n=1)	338	185	523
	비정상SMS발송(n=1)	25	185	210
	홈페이지변조 (n=1)	28	121	149

〈표 9〉 중소기업의 피해유형별 평균피해액

(단위 : 백만원)

기업규모	피해유형	직접비용 합계	간접비용 합계	평균 피해액
중소기업	랜섬웨어(n=13)	727	93	820
	DDos (n=4)	319	31	350
	개인정보유출 (n=3)	263	34	297
	악성코드유포(n=1)	278	20	298
	DB변삭제 (n=3)	8	59	67
	비정상SMS발송(n=5)	20	30	50
	게시글 스팸(n=1)	2	20	22
	홈페이지변조(n=1)	12	3	15

섬웨어, 코드서명 유출, 개인정보유출의 경우가 있었다. DDoS 공격으로 인한 피해가 가장 컸으며, 직접적인 피해액은 18억원이었으며, 탐지 및 재발방지를 위한 간접비용이 45.1억원을 차지하였다. 다음으로 랜섬웨어 감염피해로 직접비용은 2억원이었으나, 탐지 및 재발방지를 위한 간접비용으로 24.4억원의 피해액이 조사되었다.

〈표 8〉과 같이 중견기업은 랜섬웨어, 개인정보유출, 비정상SMS발송, 홈페이지변조, 악성코드 유포의 피해유형이 있었다. 랜섬웨어 공격으로 인한 피해가 가장 컸으며, 직접적인 피해액은 23.3억원이었고, 탐지 및 재발방지를 위한 간접비용이 2.7억원을 차지하였다. 다음으로 개인정보 유출피해로 직접비용은 3.4억원이었으며, 탐지 및 재발방지를 위한 간접비용으로 1.9억원의 피해액이 조사되었다.

〈표 9〉와 같이 중소기업은 DDoS, 랜섬웨어, 개인정보유출, 악성코드유포, DB변삭제, 비정상SMS발송, 게시글 스팸, 홈페이지변조의 피해유형이 있었다. 랜섬웨어 공격으로 인한 피해가 가장 크고 많았으며, 직접적인 피해액은 7.3억원이었고, 탐지 및

〈표 10〉 비영리조직의 피해유형별 평균피해액

(단위 : 백만원)

기업규모	피해유형	직접비용 합계	간접비용 합계	평균 피해액
비영리조직	랜섬웨어(n=1)	5	2	7
	DB변삭제(n=1)	31	4	35
	DDoS (n=1)	3	3	6

재발방지를 위한 간접비용이 0.9억원을 차지하였다. 다음으로 DDoS 피해로 직접비용은 3.2억원이었으며, 탐지 및 재발방지를 위한 간접비용으로 0.3억원의 피해액이 조사되었다.

비영리재단은 〈표 10〉가 같이 랜섬웨어, DB변삭제, DDoS 공격의 피해유형이 있었다. DB변삭제 공격으로 인한 피해가 가장 컸으며, 직접적인 피해액은 31백만원이었고, 탐지 및 재발방지를 위한 간접비용이 4백만원을 차지하였다. 다음은 랜섬웨어로 직접비용은 5백만원이었으며, 탐지 및 재발방지를 위한 간접비용으로 2백만원의 피해액이 조사되었다.

Ⅴ. 결 론

5.1 주요 결과 및 시사점

본 논문에서는 정보보호 특성상 기업들의 사고 피해액 정보가 공개되지 않는 상황에서 기업들의 정보보호 투자의사결정에 도움을 주기위해 실제 피해를 받은 기업들을 대상으로 경제적 피해액을 계산하여 제시하는 국내 최초의 연구를 시도하였다.

기업 규모별 침해사고의 경제적 피해액은 대기업(20.9억원), 중견기업(17.4억), 중소기업(4.4억원), 비영리재단(0.2억원) 순으로 기업규모가 클수록 커지는 것으로 조사되었으나, 직접적 피해액은 대기업(4.1억원)에 비해 중견기업(15.1억원)이 더 많은 것으로 나타나, 대기업이 예방 및 재발방지를 위해 노력한 결과 직접적 피해액은 상대적으로 적은데 비해 중견 및 중소기업은 예방을 위한 투자가 적어 직접적인 피해액이 컸음을 확인할 수 있었다. 그러나 재발방지를 위한 투자는 중견기업, 중소기업이 여전히 상대적으로 적은 것으로 파악되어 사고를 당한 기업 대상으로 보안투자를 지원하는 정부정책이 필요하다는 점을 확인하였다. 대기업은 정보보호 관련 규제의 대상이 되는 경우가 많고 자발적인 정보보호 투자를 할 수 있는 여력을 보유하고 있다고 판단되고, 중소기업은 정보보호 관련 지원 대상이 되는 경우가 많고 보유한 정보자산의 가치가 상대적으로 작기 때문에 피해규모가 적게 나타난 것으로 판단된다. 하지만, 정보보호의 규제와 지원의 사각지대에 위치한 중견기업은 대기업에 비해서는 투자 여력이 부족하고 중소기업에 비해서는 정보자산의 규모가 크기 때문에 직접적인 피해액이 크게 나타난 것으로 판단된다. 중견기업이 사이버보안 침해사고로 겪을 수 있는 피해를 축소할 수 있는 특화된 정보보호 정책의 개발이 필요하다. 현재는 기업들에게 침해사고 신고를 하도록 하고 사고조사를 지원해 주고 있지만, 재발방지를 위해 후속으로 정보보호 대책 수립 및 보안솔루션 구입비 지원 등의 정부지원 사업이 필요하다.

피해 유형별 피해액은 랜섬웨어(13.8억원), DDoS(12.9억원), 개인정보유출(4.9억원), 홈페이지 변조(0.8억원), DB 변삭제(0.6억원) 등으로 조사되었다. 피해건수는 랜섬웨어가 가장 많았으며, 개인정보 유출, DDoS 공격 순으로, 기업들이 랜섬웨어 등 기술적으로 고도화된 신종 위협에 대한 대비가 충분하지

않은 것으로 판단된다. 산업 업종별 피해액은 전문서비스업 26.1억원, 도소매업 16.7억원, 제조업 11.0억원, 정보통신업 3.1억원으로 조사되었다. ICT 업종에 속하지 않으면서 지식서비스를 제공하는 전문서비스업의 피해규모가 매우 크고, ICT업종인 정보통신업의 피해규모가 상대적으로 작은 것은, 정부의 규제가 ICT업종에 집중된 영향인 것으로 판단된다. 전통적인 ICT업종에 대한 정보보호 관련 규제는 꾸준하게 강화되었지만, 실질적으로 정보보호가 중요한 업무를 취급하고 있는 전문서비스업 등의 비 ICT업종에 대한 규제는 상대적으로 균형을 잃은 것이 업종별 피해규모의 차이에 영향을 미친 것으로 해석될 수 있다. 정보화가 ICT산업 뿐만 아니라 전통산업에까지 확산되면서 각종 정보가 기업활동의 중요한 대상이나 수단이 되고 있는 최근의 상황을 고려하여 전체 산업에 보편적으로 적용될 수 있는 정보보호 정책 뿐만 아니라 산업별로 특화된 정보보호 정책의 개발이 필요하다.

사이버 침해사고로 인한 경제적 피해에 대해 국가, 기업, 개인 등 피해주체에 따라 분류하여 수행한 연구도 있었고, 직접적인 피해, 간접적인 피해 등 피해유형으로 분류하여 수행한 연구도 있었다.

기존의 연구들과 달리 본 연구는 사이버 침해사고 피해액 조사를 위해 기본적으로 Gordon & Loeb 모형을 사용하면서도, 정보보호 프로세스에 따라 탐지 - 사고조사 - 대응/복구 - 사후 재발방지 과정별로 내부 비용항목들을 도출하고, 침해사고로 인한 결과비용을 도출하여 비용항목을 직접비용과 간접비용으로 재구성하였다. 또한, 기존의 연구들은 사이버 침해사고의 특성 상 정보수집의 한계로 실제 침해사고를 당한 기업을 특정화하여 피해액을 조사하는데 한계가 있었다면, 본 연구는 침해사고를 당해 신고한 다양한 기업을 대상으로 기업 규모별, 피해유형별, 업종별로 유형화하여 피해액을 조사할 수 있었다. 영국 DCMS 등의 조사 사례와 같이 피해액 조사 과정에서 응답자에게 피해액을 직접 질문하는 대신, 반구조화된 설문지로 침해사고 상황을 재정리하여 응답자별로 피해범위, 피해액 산정내용이 차이가 나는 것을 피하고 동일한 기준으로 피해액을 산정할 수 있도록 하였다.

본 연구의 의미는 개별 침해사고 기업을 대상으로 사이버 침해사고의 경제적 피해금액을 기업규모별/피해유형별/업종별 피해액을 산정하여 경영진 및 실무자들이 인식할 수 있도록 정보를 제공함으로써, 개별 기업들이 당면하는 사이버 침해사고 Risk를 관리하기 위해 정보보호 투자의사결정에 도움이 될 수 있을 뿐만 아니라 기업 규모별, 산업분야별 정보보호 정책을 결정하는 정책결정자에게도 차별적인 정보보호 정책 수립에 활용 가능할 것이다.

5.2 연구의 한계 및 추후 연구 과제

본 연구는 전체 피해를 받은 기업 중 일부만 인터뷰에 응하여 대표성에 일정한 한계가 있으며, 침해사고로 인한 피해가 상대적으로 적은 기업만 인터뷰에 응하고 개인정보유출피해를 입은 기업의 경우 피해금액 산정을 회피하는 경향이 강해 경제적 피해액이 실제 피해보다 과소 추정되었을 가능성이 있다. 또한 사전예방비용으로 기업별 정보보호 투자액에 대한 조사와 브랜드이미지 손실, 고객이탈 손실 등 장기적 비용은 기업들이 인식하는 피해액에 반영되지 않아 고려되지 않았다는 점은 연구의 한계로 남을 수 있다.

후속적인 연구가 매년 반복적으로 진행하면서 기업 규모별, 피해유형별, 산업 업종별 응답 데이터를 확대할 필요가 있다. 사이버보안 침해사고로 인한 경제적 피해의 규모뿐만 아니라 피해요소의 도출 및 추정에 대해서는 연구자들의 관심이 상대적으로 적었는데, 관련 연구가 지속적으로 수행될 필요가 있다고 판단된다. 정부의 정책이 개별적인 피해요소를

조절하기 위한 직접적인 지원의 형태가 될 것인지, 아니면 전반적인 기업의 정보보호에 대한 관심을 제고하기 위한 유인체계의 설계 등의 간접적인 형태가 될 것인지에 대한 시사점을 얻을 수 있는 연구도 필요할 것이다. 그동안 수행된 정부의 정책에 대한 종적 성과 분석, 국가간 비교연구 등의 방법을 적용한다면 상대적으로 부족했던 관련 분야 정책 수행의 근거를 확보하는데 도움이 될 것이다.

REFERENCES

Accenture & Ponemon Institute(2019), *Ninth Annual Cost of Cybercrime Study*.

Anderson, R., Clayton, R. , and Moore, T. (2009), "The economics of online crime," *Journal of Economic Perspectives*, 23(3), 3-20.

Campbell, K., Gordon, L.A., Loeb, M.P and Zhou, L. (2003), "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *Journal of Computer Security*, 11(3), 431-448.

Detica(2011), *The Cost of Cyber Crime*. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943 /the-cost-of-cyber-crime-full-report.pdf

Goel, Sanjay and Shawky, Hany A. (2009), "Estimating the market impact of security breach announcements on firm values," *Information & Management*, 46(7), 404-410.

Gordon, L. A. and Loeb, M. P. (2002, Nov), "The economics of information security investment," *ACM Transactions on Information and System Security*, 5(4), 438-457.

_____ (2005, Sep), *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, McGraw-Hill Companies, Inc.

Kong, H. K., Kim, T. S., and Kim, J. D. (2012), "Evaluation of information security investments: A BSC perspective," *Journal of Intelligent Manufacturing*, 23(4), 941-953.

Kotulic, A. G. and Clark, J. G. (2004, May), "Why there aren't more information security research studies," *Information & Management*, 41, 597-607.

Kumar, Ram L., Park, S., and Subramaniam, C. (2008), "Understanding the value of countermeasure portfolios in information systems security," *Journal of Management Information Systems*, 25(2), 241-280.

McAfee/Intel(2014), *Net Losses: Estimating the Global Cost of Cyber Crime*. Economic Impact of Cyber Crime II. Center for Strategic and International Studies. Available at: http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf Last accessed: 1st December 2016.

National Fraud Authority(2013), *Annual Fraud Indicator*. Available at: https://www.gov.uk/government/publications/annual-fraud-indicator--2 Last accessed: 1st December 2016.

National Institute of Standards and Technology (2012), *Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide*

Oxford Economics(2014), *Cyber-attacks: Effects on UK Companies*. A Report for the Centre for the Protection of National Infrastructure.

Park, J,. Choi, Y. (2014). "Economic Recession and Hyundai Heavy Industries." *Korea Business Review*, 18(4), 81-104.

Ponemon Institute(2016), *Flipping the Economics of Attacks*. Available at: http://www.ponemon.org/library/flipping-the-economics-of-attacks

Last accessed: 1st December 2016.

UK Department for Digital, Culture, Media and Sport(2019), *Cyber Security Breaches Survey 2019*.

UK Home Office(2008), *Understanding the Costs of Cyber Crime*, Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf.

Wynne Lam, W. M.(2016), "Attack-prevention and damage-control investments in cybersecurity," *Information Economics and Policy*, 37, 42-51.

Zhao, X., Xue, L. and Whinston, A. B. (2013), "Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements," *Journal of Management Information Systems*, 30(1), 123-152.

국내참고문헌

강미화, 김태성(2015), "보안경제성 연구동향 분석: WEIS 발표 논문을 중심으로," **정보보호학회논문지**, 25(6), 1561-1570.

과학기술정보통신부(2020), 2019년 정보보호 실태조사 결과 발표, 2020.2.26. 보도자료, https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=_policycom2&artId=2650308

권홍, 이은주, 김태성, 전효정(2012), "CVM을 이용한 국내 개인정보 침해사고의 위자료 산정," **정보보호학회논문지**, 22(2), 367-377.

김길환, 양원석, 김태성(2018), "유전자 알고리즘을 이용한 정보보호 대책 투자 포트폴리오의 최적화," **한국통신학회논문지**, 43(2), 439-451.

김민정, 허남길, 유진호(2016), "개인정보 유출 사고 시 정보보호 기업의 주가 변동에 관한 연구," **정보보호학회논문지**, 26(1), 275-283.

김승학, 윤창민, 김대유, 정기현. (2018.6). "침해사고 대응을 위한 최적화 모델 연구," **대한전자공학회 학술대회**, 1210-1213.

김태성, 유혜원, 권홍, 전효정(2009), "사이버 침해사고 발생에 의한 사회적 비용 및 정보보호 적정예산 산출," **한국인터넷진흥원 연구보고서**

방송통신위원회(2017), "개인정보의 기술적, 관리적 보호조치 해설서," https://www.kisa.or.kr/jsp/common/down.jsp?folder=uploadfile&filename=%EC%A0%9C2010-31%ED%98%B8-%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EC%9D%98%EA%B8%B0%EC%88%A0%EC%A0%81%EA%B4%80%EB%A6%AC%EC%A0%81%EB%B3%B4%ED%98%B8%EC%A1%B0%EC%B9%98%EA%B8%B0%EC%A4%80%ED%95%B4%EC%84%A4%EC%84%9C.pdf

법제처, http://www.law.go.kr/

서승우(2008), 보안경제학, **서울대학교출판부**

신영웅, 전상훈, 임채호, 김명철(2013), "국가 사이버보안 피해금액 분석과 대안-3·20 사이버 침해사건을 중심으로," **국가정보화연구**, 6(1), 129-173.

신일순, 장원창, 박희영(2013), "정보보호 투자와 침해사고의 인과관계에 대한 실증분석," **정보보호학회논문지**, 23(6), 1207-1217.

신진(2013), "사이버정보보호의 경제적 효과분석: 국가적 피해액 산정을 중심으로," **정보보호학회논문지**, 23(1), 89-96.

안중석, 이준행, 고영희(2010). 자산운용산업의 운영위험 관리 전략에 관한 사례연구. **Korea Business Review**, 14(2), 27-51.

유진호, 지상호, 송혜인, 정경호, 임종인(2008), "인터넷 침해사고에 의한 피해손실 측정," **정보화정책**, 15(1), 3-18.

유진호, 지상호, 임종인(2009), "개인정보 유·노출 사고로 인한 기업의 손실비용 추정," **정보보호학회논문지**, 19(4), 63-75.

이기혁, 강선준(2020), ICT 융합보안의 이해, **진한엠앤비**

이용필(2017), "불완전 정보 하의 정보보호 투자모델 및 투자 수준," **정보보호학회논문지**, 27(4), 855-862.

_____(2019), "사이버 침해사고의 경제적 피해금액 산정," **한국정책학회 추계학술대회 발표자료**

임규건, 류미나, 이정미(2018), "개인정보유출 피해 비용 산출 모델에 관한 연구," **정보보호학회논문지**, 28(1), 215-227.

장상수(2019), "4차 산업혁명의 정보보호개론," **배움터**

전용희(2009), "DDoS 공격의 경제손실 모델 사례 연구," **정보보호학회논문지**, 19(3), 58-68.

전효정, 김태성(2016), "AMI 공격 시나리오에 기반한 스마트그리드 보안피해비용 산정 사례," **정보보호학회논문지**, 26(3), 809-820.

한국마이크로소프트(2018), "한국마이크로소프트, '사이버 보안 위협 보고서' 발표," 2018.8.10. 보도자료, https://news.microsoft.com/ko-kr/2018/06/18/cybersecurity-report/

한국인터넷진흥원(2016), "민간부문 침해사고 대응 안내서," https://www.boho.or.kr/filedownload.do?attach_file_seq=970&attach_file_id=EpF970.pdf

_____(2019), 2019 국가정보보호백서, https://www.kisa.or.kr/jsp/common/libraryDown.jsp?folder=0012001

현대경제연구원(2009), "사이버테러의 상시 감시 체제를 구축하자!-디도스 사이버 테러의 피해와 대책," **현대경제연구원 현안참고자료**, 2009. 7. 23.

황해수, 이희상(2015), "정보보안 사고가 기업가치에 미치는 영향 분석: 한국 상장기업 중심으로," **정보보호학회논문지**, 25(3), 649-664.

Measurement of Economic Costs of Cybersecurity Breaches in South Korea

Yong-Pil Lee* · Tae-Sung Kim** · Jinho Yoo***

Abstract

To help companies make cybersecurity investment decisions, we conducted a survey to estimate the costs of cyber incidents by company size, incidents type, and industry type for the first in South Korea. According to the survey, it was found that the costs of cyber incidents by company size increased in the order of size, large companies (20.9 billion won), medium-sized enterprises (17.4 billion won), small and medium-sized enterprises (4.4 billion won), and non-profit foundations (0.2 billion won). However, the direct costs was higher in mid-sized enterprises (15.1 billion won) than in large enterprises (4.1 billion won), and SMEs were 3.8 billion won. The amount of investment in detecting incidents and preventing recurrence included in indirect costs was 16.8 billion won, which was 409% of the direct costs, while mid-sized and small and medium-sized companies were 2.3 billion won and 0.6 billion won, respectively, accounting for 12% and 15% of the direct costs. As a result of the efforts of large companies to prevent and prevent recurrence, direct costs was relatively small, whereas small and medium-sized enterprises and small and medium-sized enterprises had little investment in prevention, and the direct costs was large, while the investment to prevent recurrence was still relatively small. The most damaging attack types for medium-sized companies and small and medium-sized enterprises were surveyed as ransomware attacks. It was confirmed that the main targets of hackers attacking ransomware for the purpose of money are medium-sized companies and small and medium-sized enterprises. It was found that the government's follow-up support policy was needed for medium-sized enterprises and SMEs.

Key Words: Cybersecurity breaches, Economic costs, Decision of Cybersecurity investment

* Director, Korea Internet & Security Agency, First Author
** Professor, College of Business, Chungbuk National University, Corresponding Author
*** Professor, College of Business and Economics, Sangmyung University