한국경호경비학회 – 제59호(2019): 9–35
투고일 2019. 05. 01 심사일 2019. 05. 25 게재확정일 2019. 06. 05

중소기업의 기업경영 환경을 고려한 사이버 보안 관리

전 용 태

중소기업의 기업경영 환경을 고려한 사이버 보안 관리*

전 용 태**

〈요 약〉

지금까지 사이버보안에 대한 부분적인 연구는 많이 시도되었으나, 기업 내부적인 요인과 외부 요인의 관계를 총체적으로 분석한 연구는 국내뿐만 아니라 국외에서도 거의 없었다. 따라서, 본 연구에서는 중소기업의 내부 요소 뿐 아니라 기업경영 환경을 고려한 사이버보안 관리에 대하여 살펴보았다. 혼합적 연구방법론을 통하여 1차 질적 분석, 2차 양적 분석을 실시하였다. 질적 분석은 반구조적 인터뷰 방식을 통해 진행하였고 사이버보안 관리체계의 미비, 사이버보안에 대한 내부적인 비협조, 의사결정체계에 파생되는 문제점이라는 세 가지 주제를 발견하였다. 양적 분석은 설문 조사를 통해 확보한 데이터를 대상으로 다중회귀분석을 실시하였으며, 독립변수 중에 사이버위협에 대한 인식과 내부적인 지지가 종속변수인 사이버보안 관리체계에 (+)의 방향으로 영향을 미치며 통계적으로 유의미한 것으로 나타났다. 이 연구를 통해 중소기업의 사이버보안에 있어서는 외부적 환경 변수보다는 내부적인 변수가 사이버보안 관리체계에 인과적 영향이 있었으며, 이는 직원들의 인식 등 조직 문화와 관련되는 변수가 중요하다는 것을 말해준다. 이러한 결과는 중소기업에서 사이버보안 관리체계를 높이는데 실질적인 의의를 제공해 줄 것으로 기대된다.

주제어 : 중소기업, 혼합방법론, 사이버보안 관리, 기술적 · 인적 · 경영적 제어, 전체론적 접근

* 이 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2018S1A5A8027605)

** 경기대학교 시큐리티매니지먼트전공 조교수

목 차

Ⅰ. 도 입

기업의 사이버보안 관리에 대한 연구는 꾸준히 연구되어 온 분야이다. 하지만 기존의 연구 경향은 일정한 방향성을 띠고 있었으며, 이로 인해 제한된 집단에 대한 연구 및 특정한 분야에 대한 연구가 진행되어 왔다는 측면에서 편향된 결과를 가져왔다. 첫째로, 국내뿐만 아니라 전 세계적으로 기존 사이버보안 연구는 정부기관 및 대기업 중심으로 흘러왔다. 그 이유는 사이버테러에 대한 우려로 인해 국가 기반시설에 대한 보호가 화두가 되었기 때문이다. 국가 기반시설은 대부분 정부와 대기업이 운영하고 있어 자연스레 이들을 보호 대상으로 인식해왔던 것이다. 반면에 중소기업은 큰 주목을 받지 못하였다. 국내 중소기업의 사업체 수는 2016년 기준 394만 6,000여개로, 전체 사업체의 약 99.9%의 비중을 차지하고 있고, 중소기업 종사자 수는 약 1,820만 여명으로 전체 종사자 수의 85.7%를 차지하고 있다(통계청, 2017). 이러한 막중한 경제적 비중과는 달리 중소기업은 사이버 위협의 피해 대상으로 인식되고 있지 않아왔다는 문제점이 있다. 또한, 중소기업은 실제로 가장 큰 피해를 입고 있음에도 사이버 위협으로부터의 보호 대상이라는 인식이 상대적으로 적었다.

둘째로, 중소기업에 대한 선행연구들은 보통 중소기업의 보안 실태를 평가하는 수준에서 그쳤거나, 중소기업의 기술유출이라는 분야에 한정되어 중소기업 보호 대

책을 연구해 왔다(예: 강정헌, 2015; 김양훈, 2014; 남재성, 2012; 송봉규, 2014; 장항배, 2010: 전창욱, 유진호, 2016). 기존의 연구들이 중소기업의 기술 유출에 초점을 맞춘 이유는, 한국 경제가 기술주도형 수출에 의지하고 있기 때문이다. 최신 기술이 해외로 유출될 경우 한국 경제에 미치는 영향이 크다. 이러한 상황적 맥락에서 기술 유출에 대해 연구가 집중된 것은 충분히 이해할 수 있다. 하지만 기술 유출 일변도의 연구 경향은 중소기업이 다른 피해에도 노출되어 있다는 점을 간과하게 만든다. 가령, 이메일 무역사기, 고객 및 직원 정보 유출, 일반적인 사이버 범죄 등은 기술 유출 이외의 금전적, 기업 이미지 하락 등의 피해를 중소기업에 끼치고 있다.

셋째로, 기존 연구에서는 사이버보안에 대해서 컴퓨터 및 공학 등 기술적인 접근이 주를 이루었으며, 기업 내부 경영적 측면 및 외부적 경영 환경을 고려하지 않았다. 즉 조직 내부 차원에서 기술적인 해결책(예, 방화벽·침입탐지시스템·암호화·생체인식기술 등)을 통해 사이버보안을 해결하려는 노력이 그 동안 강조되어 왔다(Singh et al., 2013).

이러한 연구 부재를 고려하여, 이 연구에서는 기존의 중소기업의 기술유출 연구 경향을 벗어난 포괄적인 영역을 연구 대상으로 삼았다. 기술 유출이 사이버 위협으로 인한 다양한 피해결과 중의 한가지라는 점에서, 기술 유출이라는 피해결과에만 국한하지 않고 다양한 피해를 고려한 종합적 사이버보안 관리를 살펴보고자 하였다. 또한, 기술 일변도의 접근을 탈피하여 기업의 경영 환경을 고려하고자 하였다. 기술 중심의 사이버보안 대책은 의사결정자들 및 비IT직원들이 논의에서 소외되는 현상을 낳고 있어, 이들의 기술적인 이해 제고가 중요하다고 판단하였다. 이러한 연구 목적을 달성하기 위해서, 본 연구에서는 두 가지 연구 질문에 대한 답을 구하고자 한다.

중소기업이 사이버보안과 관련하여 전체론적 접근을 실시하고 있는가?

중소기업의 사이버보안 관리에 영향을 미치는 내부적 요인 및 외부적 경영 환경 요인은 무엇인가?

따라서, '중소기업의 사이버보안 관리'라는 주제를 '조직의 내부/외부적 요인을 포함한 전체론적 접근' 이라는 새로운 접근법으로 탐구하였다. 연구 방법은 탐색적 연구에 적합한 혼합방법론(mixed methods research)를 사용하였고, 이를 통해 질적 및 양적 연구를 각각 실시하여 유의미한 결과를 도출하였다.

Ⅱ. 이론적 배경

1. 사이버보안 관리의 조직 내부적 변수

중소기업의 사이버보안 관리는 단순히, 중소기업 내부 요인에 의해서 결정되는 사항이 아니라, 외부 환경적 요인들과 상호작용하는 메커니즘을 통해 운용된다. 따라서 중소기업의 시장 여건, 경쟁 관계, 동종 기업들과의 협력, 정부의 정책 등 외부 환경 요인에 대한 탐색이 중요하다. 하지만, 이에 대한 선행 연구는 지극히 적다. 대신에, 조직 내부적 변수의 영향에 대해 고찰한 연구는 다수 발견된다.

우선, 중소기업의 경우 의사결정이 대부분 기업 대표에 의해 이루어진다(Blackburn, 2012). 큰 기업은 여러 단계의 경영자 층이 존재하며 자원이 풍부하여 위계서열에 따른 의사결정 단계를 거친다. 기능으로 구분된 부서에서 실질적인 의사결정을 하게 되며 최고 경영자층은 전략적인 측면의 의사결정을 담당하게 된다. 따라서, 대기업에서의 의사결정은 공식적인 위계적인 단계를 거친 과정으로 이루어지게 된다. 반면에, 중소기업의 경우 상당히 수평적인 조직 구조를 띠고 있어(Levy and Powell, 2005), 의사결정이 비공식적이고 비규칙적 과정으로 이루어지는 경우도 많다. 이러한 의사결정 구조는 유연함을 추구할 수 있다는 점에서 장점이지만, 자칫 수동적일수 있고 단기적인 현안 중심으로 이루어질 수 있다는 점이 단점으로 꼽힌다(Grant et al., 2014). 실제적으로, 중소기업의 의사결정은 소수의 사람들에 의해 이루어지고 있고 지극히 소유주 혹은 대표 중심으로 이루어지고 있어, 이들의 사이버보안에 대한 지식과 태도는 이와 관련된 의사결정에 있어서 매우 중요한 요소로 자리잡고 있다.

그 다음으로, 기업의 규모와 사이버보안의 여러 측면이 서로 연관되어 있다(Organ, 2015). 일반적으로, 기업의 규모는 직원의 수 혹은 자산 규모로 따지며, 직원이 많을수록 자산 규모도 증가하는 것과 같이 서로 긍정적으로 비례하는 성향을 보인다. 사이버보안 측면에서, 규모가 큰 회사일수록 위험 평가 툴을 사용하는 경향이 높거나 사이버보안 관리를 수용하는 경향이 나타난다(권장기, 김경일, 2017). 반면에, 중소기업의 경우는 인적·물적 지원이 충분하지 않기 때문에 사이버보안 위협에 적극적으로 대처하기 힘들다(Bauer and Dutton, 2015). 이로 인해 규모가 적은 회사들일수록 이러한 위협에 대비가 안 되어 있을 수밖에 없다. 대기업과 소기업이 사이버 위협에 대비하는 정도가 실질적으로 차이가 난다(Gupta and Hammond, 2005). 클라우드

컴퓨팅의 경우 대기업들은 이런 기술을 도입하는데 있어서 파생되는 위험을 관리할 능력이 되지만 중소기업들은 이러한 능력이 되지 않기 때문에 적극적으로 도입하는 것을 꺼려하는 경우도 많다. 사이버보안 위험 관리 능력 부족으로 인해 기업 경영에 도움이 될 만한 기술을 도입하지 못한다면 이로 인한 경영의 효율성, 수익 구조의 개선 등 장점도 향유 할 수 없기 때문에 장기적으로 기업의 생존에 영향을 줄 수 있다.

2. 사이버보안 관리의 기업환경 변수

사이버보안 연구에 기업의 외부적인 변수를 고려한 논문은 극히 드물었다. 관련 논문은 조직 내부에서 사이버보안에 긍정적인 문화를 조성한다든지 기술적·인적·경영적 제어를 균형적으로 통합해야 한다는 논지가 대부분이다. 예외적으로 기업 환경 변수가 언급된 논문 몇 개를 찾아볼 수 있었다. Chang and Ho(2006)는 사이버보안을 기업 경영적 관점에서 연구하였으며, 관리자들의 IT 능력, 불안정한 기업경영 환경, 업종, 및 기업 크기가 기업의 보안 강화에 긍정적인 영향을 미친다고 주장하였다. 기업들이 불안정한 기업경영 환경에 놓여 있다보면 외부적 불안정을 상쇄하기 위해 사이버보안 관리의 중요성을 느끼고 더욱 강화하게 된다는 것이다. 즉, 외부적 불안정성이 높을수록 사이버보안 관리가 강화된다는 주장이다. 그러나 이 연구에서 기업경영 환경이라는 외부적인 변수를 편입하였지만, 불안정한 기업환경이 구체적으로 어떤 개념이 조작화된 것인지 설명하지 않았다. 또한 상당히 큰 개념이기 때문에 상세한 추가 변수가 필요할 것으로 보이나, 구체적인 외부 변수 제시는 하지 않았다는 점에서 한계점이 있었다.

Hall, Sarkani, and Mazzuchi(2011)는 기업들의 외부적인 위협 환경에 대한 인식이 높아야 하고, 사이버보안 위협에 대응하기 위한 수단을 제대로 준비하는 능력이 있어야 전략 수립과 이행, 최종적으로 조직성과에 긍정적으로 영향을 미친다고 주장하였다. 즉, 기업의 대표 등 리더들이 조직 외부 환경에 대한 제대로 된 인식이 있어야 사이버보안 관리에 효과적이라는 논지이다. 이 논문도 구체적으로 위협 환경이 어떤 요소인지 어떠한 변수들로 구성이 되야하는지에 대한 내용은 제시하지 않았다는 점에서 제한적인 시사점을 주고 있다.

국내 논문으로, 박태형 외(2013)는 경기도의 사례를 통해 정부의 역할에 대해서

연구하였다. 경기도 내에서 중소기업의 산업보안 강화를 위해 도입한 정책에 대해서 중소기업 담당자들을 대상으로 분석하였다. 여기에서 산업보안 프로그램, 사이버안전 기업 구축 프로그램, 산업보안관리 센터 및 통합보안 관제센터 프로그램 등 외부적 변수로서 정부의 역할을 조명하였다. 하지만, 정부의 정책 및 전략이 기업 경영 및 사이버보안 관련 의사결정에 어떻게 영향을 줄 수 있는지와 그 인과관계가 제대로 논의되지 않았다.

이와 같이, 국내·외 연구에서 기업 환경에 대해서 연구한 논문은 있었으나, 구체적인 영향 메커니즘 및 인과관계를 집중으로 분석 및 평가한 논문은 찾아보기 어려웠다. 하지만, 기업이 외부 환경 속에서 생존하는 하나의 유기체로 볼 때 환경과 어떤 영향을 주고 받는지 또는 어떠한 작동 메커니즘이 있는지 알아보는 것은 중요하다 할 수 있다.

3. 기술적 · 인적 · 경영적 제어의 균형적 접근 필요성

앞에서 제시한바와 같이, 중소기업의 사이버보안에 대한 기존 연구는 기술적 제어에 치중한 채, 인적 제어 및 경영적 제어를 간과하고 기술적 제어에 치중하였으며, 이로 인해 균형적 접근이 부재했다.

기술 중심의 솔루션은 사이버보안 문제에서 가장 핵심적인 요소였고, 특히 강조되어 왔다(Singh et al., 2013). 컴퓨터 공학 분야의 연구자들을 중심으로 사이버 위협을 어떻게 발견하고 자산을 보호할지에 대한 논의는 기술 보안 솔루션을 중심으로 이루어졌다. 가령, 방화벽, 침입탐지시스템을 통한 네트워크 보안, 암호화를 통한 데이터 보호, 생체인식기술을 통한 접근 통제 등이 최근 논의가 되어온 기술들이다. 하지만, 이렇게 새로운 기술 중심의 솔루션을 도입해왔으나, 사이버보안 위협은 더 빈발해지고 심각해져왔다. 이에 따라, 인적 및 경영적 제어의 중요성 및 균형적 접근의 필요성을 주장하는 연구가 많아지고 있다.

인적 요소에 대한 기존의 연구를 우선 살펴보면, Safa et al. (2015)은 보안 인식, 정책, 경험, 태도, 주관적 규범, 위협 평가 등이 사용자 행동에 긍정적인 영향을 미친다고 주장하였고, Johnston and Warkentin(2010)은 관리자들이 위기감을 조성하는 대화방식을 시행하면 직원들이 긍정적인 행동으로 변화하는데 영향을 미친다고 설명하였다. 국내 연구에서도 인적 요인에 대한 연구가 있었다. 하지만 대부분 구성원들

의 정보보안 정책 준수·동기요인·정보보안 인식·정보보안 준수의도 등을 중심으로 연구하였다(예: 김상현, 송영미, 2011; 백민정, 손승희, 2011; 정재원, 이정훈, 김채리, 2016; 한진영, 유현선, 2016). 이처럼 국내외의 연구들은 구성원들의 인식 및 의도에만 치중하였고, 인적 요인에 대한 전체적인 조명이 아닌, 몇 가지 요인만을 연구하였다는 한계점이 있다.

경영적 요인에 대한 기존 연구는, 기업 내부의 문화·의사결정·문화 등 조직 행동이 사이버보안 관리에 미치는 영향을 탐구하였다(예: Chang and Ho, 2006; Singh et al., 2013; Soomro et al., 2016). 예를 들어, Kayworth and Whitten(2010)은 우수한 기술과 사회적·조직적 변수들이 조화되어야 효과적인 보안이 가능하다고 주장했고, Young and Windsor(2010)는 보안과 경영 기획 절차가 효율적으로 합쳐져야 자산을 성공적으로 보호할 수 있다고 말하였다. 국내 연구에서는 윤승영(2016)이 기업 경영진이 정보보안 리스크를 인지하고 관리하기 위해서는 기업 경영 전략이 중요하다고 제시하였다. 그러나 이 연구는 미국을 대상으로 한 연구로서 국내 기업에 대한 연구는 아니었고, 기업지배구조라는 측면에서만 정보보안을 살펴보았다. 또한, 한진영·유현선(2016)은 경영진의 정보보안 지능이 조직원들의 보안대책 인식에 미치는 영향을 살펴보았으나, 경영진의 리더십·의사결정 구조 등을 내부적 경영 구조를 고려하지 않고 한정적 영역만을 다루었다.

하지만 기술이 날로 복잡해짐에 따라 기업에서 의사결정을 하는 고위 관리자들이 관련 기술을 이해하기가 점점 어려워지고 있다(Werlinger, Hawkey, and Beznosov, 2009). 기술 일변도의 접근은 IT 직원들과 비IT직원들을 이분화 시키고 있다. 또한, 고위관리자들의 기술적인 이해가 뒷받침되지 않는 현실에서, 경영상의 의사결정에서 사이버보안에 대한 논의는 소외될 수밖에 없다. 따라서 사이버보안이 왜 기업 현장의 우선순위에서 밀려나는지, 내부 직원 및 관리자들이 과연 사이버보안 정책 및 규정을 수용하는지, 과연 어떠한 태도와 인식으로 접근하고 있는지 등에 대한 질문이 제기되었다. 또한, 회사의 고위 관리자들이 사이버보안에 적절한 지원을 하지 않고, 또 리더십·커뮤니케이션·의사결정 등과 같은 조직 행동이 고려되지 않는다면 단순한 기술적 제어 도입은 형식에 그치게 될 것이다. 이러한 문제점에 대한 인식으로, 최근의 연구(예: 권장기, 김경일, 2017; 나현대, 정현수, 2016; Parsons et al., 2014; Rhee, Ryu, and Kim, 2012; Safa et al., 2015; Safa, Von Solms, and Furnell, 2016)에서는 기술만으로 만족할 만한 해결책을 제시할 수 없다고 밝히고 있다. 이처럼,

기존의 연구들이 기술적인 제어 외에 경영상의 지원 혹은 인적 요인이 함께 고려되어야한다고 주장하고 있으나, 부분적인 연구였다는 점에서 한계를 노출하였다.

Ⅲ. 연구 방법

중소기업의 사이버보안 분야는 최근 부각된 사회적인 문제로서, 그동안 선행연구가 극히 적어, 유의미하게 제시된 변수나 개념이 많지 않다. 따라서 단순히 가설을 세우고 검증하는 양적 방법을 사용하기에는 적절하지 않다. 또한, 질적인 방법만 사용한다면, 실태에 대해서 파악만 하는데 그칠 뿐 모집단에 대한 유의미한 추정을 할 수 없게 된다. 따라서 연구 대상을 총괄적으로 탐색하는 연구가 필요하다. 이러한 탐색적 연구에는 혼합방법론이 가장 적합하다.

혼합방법론은 두 가지 이상의 연구 데이터 혹은 방법론을 사용하는 것으로, 양적과 질적인 방법론은 서로 배타적인 것이 아니라는 것에 근거한다(김은정, 2013). 따라서, 각각의 방법론에서 나온 결과를 서로 비교 및 대조하여 결과가 일치하는지 분석이 가능하다. 이러한 방식을 방법론적 다각화(triangulation)라고 하는데, 특히 질적 연구와 양적 연구의 한계를 상호 보완하는 효과를 이끌어 낼 수 있다(심준섭, 2008). 이 방법론은 연구자가 두 가지 연구에 능숙해야 하고 시간과 재원이 많이 소요되기 때문에, 연구자에게는 일종의 방법론적 도전으로 볼 수 있다.

혼합방법론 중 탐색 순차적 혼합 방법을 채택하였다. 연구자가 우선 질적 연구를 통해 개념이나 변수를 탐구하고 이를 후속 양적 연구에서 사용하는 유형이다. 즉, 질적 연구를 통해 내부적으로 사이버보안 관리, 외부적으로 기업 환경 요인 등 유의미한 변수를 탐색할 것이다. 그 후 사이버보안 관리에 영향을 주는 기업 내부/외부 요인들을 변수로 설정하고 적절한 가설을 세웠다. 이 연구에서 자료 수집 방법으로는 다음 두 가지를 사용하고자 한다. 첫째는 질적 자료 수집방법으로서 인터뷰 기법이고, 두 번째는 양적 자료 수집방법으로서 설문지 기법을 활용하였다.

1. 질적 인터뷰 방식

인터뷰는 반구조적 인터뷰 방식을 통해 인터뷰 대상의 응답을 폭넓게 확보하였다.

인터뷰 대상은 중소기업의 IT 관리자 혹은 대표이다. 중소기업 중에는 IT 담당자가 따로 없거나 IT 관련 기업의 경우 대표가 IT 영역을 담당하고 있는 경우가 많다. 또한, 기업 경영측면에서 볼 때 대표의 인식이 사이버보안에 중요한 영향을 미치기 때문에, 대표에 대한 인터뷰가 상당히 중요하다. 질적 연구에서는 일반적인 목적적 추출법을 사용하고자 한다. 이 샘플링 기법은 연구 목적에 적합하다고 생각되는 조사 대상을 표본으로 추출하는 것으로, 모집단 전체를 확인하는 것이 어려울 때 활용한다(김희경, 윤순진, 2011).

질적 연구에서 표본의 크기에는 연구마다 큰 차이가 있다. 적절한 표본 크기를 선택하는 데 필요한 숫자 기준을 가진 양적 연구와는 달리, 질적 연구에서 표본 크기의 선택은 주로 연구자가 결정하지만 완전히 주관적이지는 않다. 질적 인터뷰에서 샘플 수를 정하는 기준은 이론적 혹은 데이터 포화이다(Bryman, 2016). 즉 인터뷰 대상자로부터 추가적으로 의미 있는 내용이나 개념을 더 이상 끌어낼 수 없다고 판단되는 경우, 포화상태라고 판단하는 것이다. 또한, 연구 질문에 충분한 대답이 이루어졌다면 데이터 포화 상태에 이르렀다고 할 수 있다. 이 연구에서도 정확한 인터뷰 대상자 수는 인터뷰 도중에 정해졌으며, 최종 16명의 중소기업 IT 관리자 혹은 대표를 인터뷰하였다. 인터뷰는 30분에서 1시간 정도로 진행되었다.

질적 연구 결과의 분석을 위해서는 주제 분석(thematic analysis)기법(Boyatzis, 1998)을 통해 질적 데이터의 패턴과 주제를 파악하였다. 이 기법은 질적 연구에서 가장 많이 활용되는 방식 중의 하나이다.

2. 양적 설문조사

여기에서 사용된 질적 연구와 양적 연구는 밀접히 연결되어야 한다. 연구의 순서를 고려해 볼 때, 설문지의 질문 내용은 질적 연구의 결과에 영향을 크게 받을 것이다. 질적 연구에서 도출된 결과를 바탕으로 내부적으로 사이버보안 관리, 외부적으로 기업 환경 요인 등의 변수를 발견하였다. 그 후, 양적 연구에서 사이버보안 관리에 영향을 주는 기업 내부/외부 요인들을 변수로 설정하고 적절한 가설을 세워 검증하였다.

설문지 기법은 편의 표본추출법을 사용하였다. 약 5백만 개의 중소기업이 전국적으로 분산되어 있음을 고려할 때, 무작위 추출법은 사실상 불가능하다. 하지만 편의

표본추출은 연구자 편의대로 표본을 수집하는 방식으로, 가령 학교, 관공서, 교육원 등 표본 대상자들이 다른 목적으로 모집되어 있는 기회를 활용하여 다수의 표본을 수집할 수 있다는 장점이 있다. 이 연구에서는 중소기업의 IT 관리자 혹은 대표들이 한국인터넷진흥원 또는 한국산업기술보호협회 등에서 교육을 받을 경우를 활용하여, 설문에 대한 설명을 하고, 동의하는 사람들만을 대상으로 설문을 배포하여, 170개 중소기업(100개 소기업, 70개 중기업)의 샘플을 확보하였다. 이 자료 수집 방식은 확률표집은 아니나, 전국의 중소기업들을 대상으로 무작위 추출이 현실적으로 불가능하다는 점 등을 고려할 때, 연구목적을 달성하는데 큰 무리는 없는 것으로 판단된다.

설문 문항은 대부분은 5점 리커트 척도를 통해 측정되었고, 자료는 통계 프로그램인 RStudio를 통해 분석하였다. 설문의 변수는 기존의 선행 연구에서 차용한 변수(가령, 업종, 조직 규모 등) 이외에, 질적 인터뷰 자료에서 발견한 주제(theme)를 조작화하여 변수로 포함하였다. 통계 분석 방법은 기술통계, 신뢰도 분석, 다중회귀분석 등을 사용하였다. 전체 설문은 170부가 회수되었으나, 이 중 결측치를 포함하고 있는 샘플 4개를 제외한 후, 추가로 회귀모델에서 이상치가 발견되었던 샘플 4개를 추가로 제외하여 총 162개의 샘플이 다중회귀분석에 실제적으로 활용되었다.

Ⅳ. 연구 결과 및 분석

1. 다각화(triangulation) 방식을 통한 조사 결과 분석

1) 질적 인터뷰 결과 분석

전체 16명의 면담자 중에, 10명은 중소기업의 대표였고, 6명은 IT 관련 부분의 중간관리자였다. 이들의 프로필은 다음과 같다.

〈표 1〉 면담자 관련 기초사항

	업종	기업 분류	직위
기업1	교육서비스	중기업	과장
기업2	건강 및 사회복지서비스	소기업	대표
기업3	금융 및 보험서비스	중기업	대표
기업4	건강 및 사회복지서비스	소기업	부장

	업종	기업 분류	직위
기업5	교육서비스	중기업	대표
기업6	제조업	중기업	부장
기업7	건설업	소기업	대표
기업8	정보 및 통신서비스	중기업	대표
기업9	전문, 과학 및 기술서비스	소기업	부장
기업10	제조업	소기업	대표
기업11	도/소매	중기업	대표
기업12	제조업	중기업	대표
기업13	건설업	중기업	과장
기업14	정보 및 통신서비스	중기업	대표
기업15	전문, 과학 및 기술서비스	중기업	부장
기업16	도/소매	소기업	대표

심층 인터뷰를 통해 의미가 있는 그리고 반복되는 문구를 중심으로 코딩을 하였으며, 1차로 설명적 코드를 추상화하여 2차로 분석적 코드를 산출하였으며, 3차로 소주제(sub-theme)를 선별하였다. 그리고 최종적으로 주제(theme)를 찾아냈다. 결과적으로 '사이버보안 관리체계의 미비', '사이버보안에 대한 내부적인 비협조', '의사결정체계에서 파생되는 문제점'이라는 세 가지 주제가 드러났다. 주제와 소주제의 체계는 다음과 같다.

(1) 사이버보안 관리체계의 미비

① 사이버 위협에 대한 낮은 인식
② 사이버 범죄에 대한 준비 부족
③ 사고 발생 시 대응 시스템 구축 미비
④ 인적·금전적 지원 체계 부족

(2) 사이버보안에 대한 내부적인 비협조

① 기업 경영과 상충하는 문제
② 비IT 관련 직원들과의 소통문제
③ 타 기능과 내부적 경쟁체제

(3) 의사결정체계에 파생되는 문제점

① 대표 리더십의 강한 영향력

② 수평적 기능간 대화채널 부족

첫째로, 사이버보안 관리체계의 미비이다. 중소기업의 대부분이 사이버보안 관리체계를 구축하고 있지 않은 것으로 드러났다. 70% 이상이 사이버보안 관리체계에 대한 인식조차도 없었으며, 인식하고 있더라고 실제적으로 도입하여 관리하고 있는 곳은 드물었다. 대부분의 업종에서 공통적인 현상이었으나, 예외적으로 금융 및 보험서비스를 제공하는 기업 3과 정보 및 통신서비스를 제공하는 기업 8 및 14에서는 사이버보안 관리체계를 구축하고 운용 중이었는데, 이것은 이들의 업종이 금융 및 정보·통신 시스템 관련이기 때문에 그 중요성을 인식하고 있었다고 보인다.

실제적으로, 사이버 위협이 얼마나 심각한지, 기업에 얼마나 타격을 줄 수 있는지 이에 대한 인식이 부족하였다. 또한, 사이버 위협은 대기업들이 겪는 문제이지 중소기업에서 겪는 문제는 아니라고 생각하고 있었으며, 이에 따라 사전 대응 시스템을 갖추고 있지 않았다. 물론, 사이버 위협 사건이 발생하였을 경우에 어떻게 대처를 할 것인지, 경찰 혹은 인터넷 진흥원에 신고를 할 것인지 등에 대한 내부 지침이 제대로 준비되어 있지 않았다. 이러한 대응 시스템 부족인 기본적으로 사이버보안 담당 부서에 인적·금전적 지원이 상당히 부족하다는데 있다. 이는 특히, 중간 관리자들이 지적한 내용으로 경영·홍보·물자구입 등 다른 기능에 우선적으로 내부적 지원이 이루어지고 사이버보안 관련 지원은 후순위로 지정되는 경우가 많았다. 이를 통해서 볼 때, 사이버보안 관리체계의 미비는 낮은 인식, 내부적 지원이 부족 등으로 인해 사실상 관리체계가 제대로 작동하고 있지 않음을 알 수 있다.

둘째로, 사이버보안에 대한 내부적인 비협조이다. 기업 경영자의 입장에 보면 기업의 수익을 늘리는 것이 중요하고, 이와 관련된 기업의 수익·업무 편의성·효율성 등의 가치가 중요하게 여겨졌고 이러한 가치와 사이버보안이 상충하는 경우가 많았다. 가장 흔한 경우가 자료나 시스템 접근 권한 강화·외부 자료 유출 금지 등 사이버보안을 강화하는 경우로서, 이로 인해 직원들이 업무 효율성이 떨어진다는 불평이 많이 내부적으로 지지를 받지 못하였다. 특히, 건강 및 사회복지서비스와 교육서비스를 제공하는 중소기업들(기업 1, 2, 4, 5)의 경우 외부 고객 및 업체들과 자료를 공유하고 협력해야 할 사안이 많아 사이버보안을 강조하는 것에 대한 부정적인 분위기가 팽배하였다. 내부적으로, IT 직원들은 비IT직원들과 융합되지 못하게 되는 의사소통의 문제가 있었다. 비IT직원들은 컴퓨터 및 전산 용어를 대부분 이해하지 못

하고 운용되는 시스템의 메커니즘을 모르기 때문에 도입하려는 정책에 대한 이해도가 현저히 낮았다. 이로 인해서 내부적인 반발이 있더라도 이를 이해시킬 수 있는 대화가 제대로 진행되기가 어려웠다. 끝으로, 기업 내부적으로 다른 기능과 경쟁 체제에 있었다. 내부의 한정된 인력과 예산을 두고 서로 경쟁하는 분위기에서 기업의 수익과 직결되는 현안 중심으로 지원이 이루어졌다. 이에 따라, 사이버보안 영역은 큰 관심을 받지 못하였고, 대부분 의사결정에서 후순위로 밀리게 되었다. 기업의 규모와 업종을 불문하고 이러한 내부적인 비협조 분위기는 팽배하였으나, 서비스 제공을 하는 기업들의 경우, 특히 금융 및 보험서비스, 정보·통신서비스 관련 기업의 경우 상대적으로 비협조 정도가 낮았다.

셋째로, 의사결정체계에 파생되는 문제점이다. 여기에는 수직적 의사결정체계와 수평적 의사결정체계로 나누어볼 수 있다. 선행연구에서 제시했듯이, 규모가 작은 기업일수록 기업 대표의 리더십의 영향력이 강하다. 면담자들의 절대 다수도 비슷한 응답을 하였으며, 대부분의 의사결정 하나하나가 대표에 의해 결정되고 혹은 순식간에 번복되기도 했다. 이러한 강한 영향력을 가진 대표가 사이버보안에 호의적이고 중요성을 인지할 경우에는 도움이 될 수도 있지만, 대부분 사이버보안에 대한 인식이 낮기 때문에 부정적인 영향을 주는 것으로 나타났다. 사이버보안에 중요성을 인지하고 있었던 대표들(기업 3, 8, 9, 12, 14)은 금융 및 보험회사와 영업비밀 혹은 특허기술 등을 갖고 기업들이었다. 기업의 자산인 지적재산을 보호하는 것이 기업의 생존과 직결된다는 것을 알고 있었기 때문에 사이버보안에 대한 내부적인 강조를 하고 있었다. 다음으로, 수평적 의사결정체계는 기능간의 대화채널로서 이들 간의 대화·토론·의사결정체계는 거의 찾아보기가 힘들었다. 즉, 중소기업의 의사결정은 수직적 구조에 의해서 이루어졌으며, 수평적 대화의 부족은 중요한 안건이 있을 때 다양한 부서의 공감대를 확보하는 것이 어렵다는 것을 의미한다. 특히, 사이버보안의 경우 이러한 공감대 형성이 상당히 중요하다고 볼 수 있는데, 수직적으로 의사결정이 이루어지다보니, 내부적인 지지를 받기가 더욱 힘들어졌다.

2) 양적 설문조사 결과 분석

(1) 연구가설 및 설문의 구성

위의 질적 인터뷰 결과를 바탕으로 하여 양적 설문조사를 위한 연구 가설 네 개를

수립하였다. 질적인 연구 결과에서 상충되는 결과는 제외하고 80% 이상의 면담자들이 비슷한 것을 주장한 내용을 중심으로 변수를 선택하고 가설을 만들었다. 여기에서는 사이버보안 관리체계를 종속변수로 하고, 독립변수로는 사이버 위협에 대한 인식, 내부적인 지지 정도, 대표의 리더십, 외부 환경 요소를 선정하였다. 즉, 이러한 내·외부 변수가 사이버보안 관리체계에 긍정적 혹은 부정적 영향을 미치는지 평가하고자 하였다. 또한, 기업의 설립연도, 직원 수, 매출액은 통제변수로 포함시켰다. 이 네 가지 가설 중에서 앞의 세 개는 기업 내부적인 요소를 변수화하였고, 마지막 가설은 외부 환경적 요소를 변수화하여 측정하였다.

가설 1: 사이버 위협에 대한 인식이 낮을수록 사이버보안 관리체계가 미비하다.
가설 2: 사이버보안에 대해서 내부적인 지지가 낮을수록 사이버보안 관리체계가 낮다.
가설 3: 기업 대표의 리더십이 강력할수록 사이버보안 관리체계 구축에 부정적인 영향을 미친다.
가설 4: 기업의 외부 환경이 불안정할수록 사이버보안 관리체계에 부정적인 영향을 미친다.

〈표 2〉 설문지 구성내용

변인	변수	질문 사항	문항수
배경변인	기업의 특성	설립연도, 직원 수, 매출액	3개
독립변인	사이버 위협에 대한 인식	사이버 위협 존재 정도	17개
		사이버 사건의 경험	
		사이버 위협에 노출 정도	
	내부적인 지지	다른 기능에서의 지원	
		경영층의 IT 지식 및 관심	
		대표의 관심	
		가치 충돌 시 우선적 지원 여부	
		보안 제어 추진 시 협조 정도	
	대표의 강한 리더십	대표의 리더십이 권위적인지	
		의사결정의 수직화 여부	
		민주적 의견제시 가능성	
		대표의 권한 위임 여부	

변인	변수	질문 사항	문항수
	불안정한 외부 환경	타 기업들과 경쟁 심화 여부	
		소속된 시장이 성장하는지	
		매출액 및 기업 가치 상승 여부	
		정부의 관심과 지지	
		관련 기업의 지지 및 협력	
종속변인	사이버보안 관리체계	인적 · 금전적 지원체계	5개
		사고 발생 시 대응체계	
		위험 관리체계	
		경영진의 관심도	
		내부 직원 교육체계	

(2) 변수의 기초통계량 및 측정도구의 타당성 · 신뢰도 분석

〈표 3〉 독립 · 종속 · 통제 변수의 기초통계량

	최소값	최대값	평균	표준편차
사이버 위협에 대한 인식	1	5	3.667	0.939
내부적인 지지	1	5	2.835	0.805
대표의 강한 리더십	1	5	2.91	1.068
불안정한 외부 환경	1	5	3.193	0.648
설립연도	1945	2016	1999	13.724
직원 수	10	297	76.51	87.773
매출액(억원)	0.95	580	117.05	147.555
사이버보안 관리체계	1	4.6	2.383	0.762

독립변수인 사이버 위협에 대한 인식, 내부적인 지지, 대표의 강한 리더십, 불안정한 외부 환경에 대해 요인분석을 실시하였고, 4개의 요인으로 각각 묶였다. 또한, 4개의 요인 모두의 Cronbach's Alpha값이 0.6이상으로 나와 측정도구에 문제가 없음을 보여준다. 종속변수의 사이버보안 관리체계 설문문항 5개 모두 1개의 요인으로 묶였으며, Cronbach's Alpha값이 0.87로 높게 나와, 이 연구에 사용된 척도의 신뢰도는 인정될 수 있다.

〈표 4〉 독립변수의 요인분석 및 신뢰도 검사

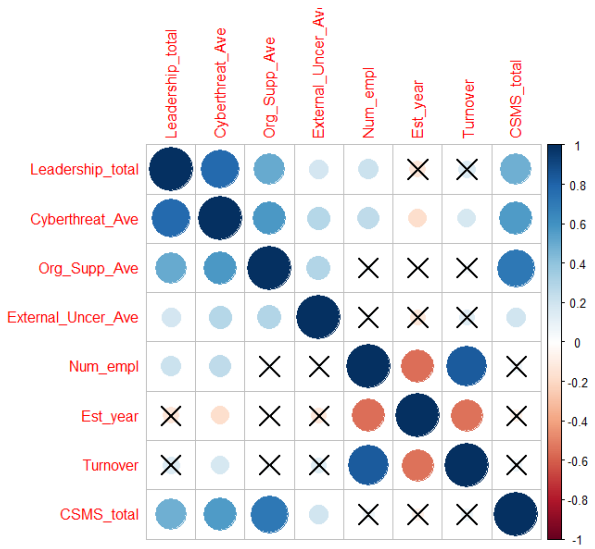
설문 항목	요인명			
	1	2	3	4
사이버 위협1	0.76			
사이버 위협2	0.69			
사이버 위협3	0.81			
내부적인 지지1		0.55		
내부적인 지지2		0.80		
내부적인 지지3		0.87		
내부적인 지지4		0.88		
내부적인 지지5		0.87		
대표의 강한 리더십1			0.87	
대표의 강한 리더십2			0.90	
대표의 강한 리더십3			0.88	
대표의 강한 리더십4			0.84	
불안정한 외부 환경1				0.79
불안정한 외부 환경2				0.82
불안정한 외부 환경3				0.51
불안정한 외부 환경4				0.60
불안정한 외부 환경5				0.70
SS loadings	5.19	3.68	2.14	1.84
설명분산	0.31	0.22	0.13	0.11
누적분산	0.31	0.52	0.65	0.76
Cronbach's Alpha	0.88	0.91	0.94	0.75

〈표 5〉 종속변수의 요인분석 및 신뢰도 검사

설문 항목	요인명
	1
사이버보안 관리체계1	0.65
사이버보안 관리체계2	0.91
사이버보안 관리체계3	0.83
사이버보안 관리체계4	0.88
사이버보안 관리체계5	0.79
SS loadings	3.35
설명분산	0.67
Cronbach's Alpha	0.87

(3) 변수들간의 상관관계

변수들간의 상관관계를 분석한 결과, 상당한 변수들이 유의수준 0.05를 기준으로 통계적으로 유의미한 관계를 가지는 것으로 확인되었다. 종속변수인 사이버보안 관리체계와의 상관관계를 살펴보면, 통제변수인 직원 수, 설립연도, 매출액만 제외한 모든 독립변수들은 통계적으로 유의미한 관계를 가지는 것으로 나타났다. 사이버 위협에 대한 인식(0.56)·내부적지지(0.72)·대표의 강한 리더십(0.49)·불안정한 외부 환경(0.2)과 사이버보안 관리체계는 모두 (+)의 상관관계를 가지는 것으로 나타났는데, 이는 가령 사이버 위협이 높다고 인식할 경우 사이버보안 관리체계 정도가 높다는 것을 의미한다.



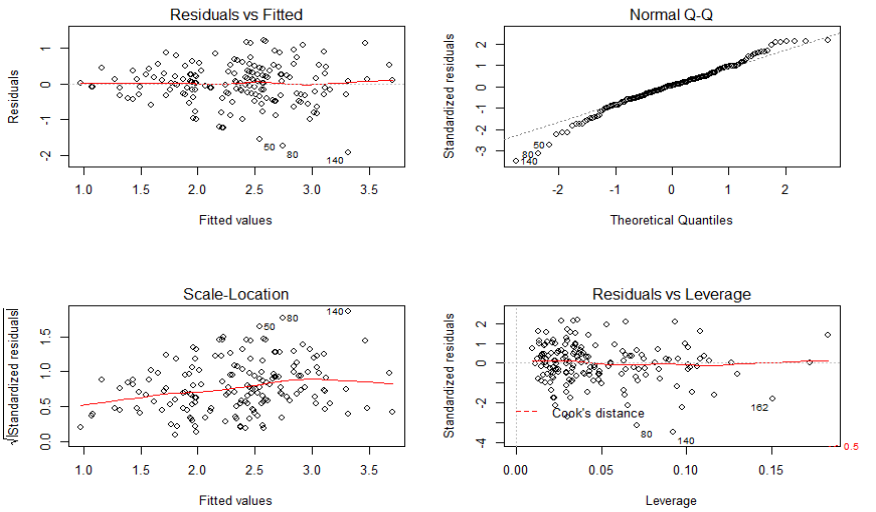
〈그림 1〉 변수들간 상관관계[1)]

(4) 인과관계 분석

결측치가 있는 샘플 4개를 제외한 166개 샘플에 대해 사이버보안 관리체계에 영

1) Corrplot 패키지를 사용하여, 시각화한 그림으로 X는 통계적으로 유의미하지 않다는 것이고, 파란색은 (+)의 방향으로 붉은색은 (–)의 방향의 관계라는 것이며, 색이 진하고 원이 클수록 관계 정도가 큰 것을 나타낸다.

향을 미치는 변수들의 인과관계에 대한 OLS 모형 분석을 실시하고, 해당 방정식을 바탕으로 잔차의 분포를 살펴보았다. 아래의 그림에서와 같이 샘플 50, 80, 140, 162 번이 이상치로 판정되어 분석에서 제거하고 다중회귀분석을 다시 실시하였다.



〈그림 2〉 잔차의 분포 및 이상치 검사

〈표 6〉 독립 · 종속 변수의 인과관계(OLS)

변수명	비표준화 계수	*t*
(Constant)	8.925	7.410
사이버 위협에 대한 인식	0.173	2.305*
내부적인 지지	0.562	8.762***
대표의 강한 리더십	0.030	0.485
불안정한 외부 환경	-0.064	-0.943
설립연도	-0.004	-1.151
직원 수	-0.001	-1.041
매출액	0.000	0.544
F	27.76***	
R^2	0.558	
Adjusted R^2	0.538	

* p<.05, ** p<.01, *** p<.001

이 모델의 설명력은 약 55.8%로 포함된 변수들이 종속변수를 비교적 높게 설명하고 있으며, 방정식의 F 값이 유의수준 0.001 수준에서 통계적으로 유의미했고, 이는 모델에 포함된 변수 중 적어도 하나는 종속변수에 영향을 미칠 수 있다는 것을 의미한다. 또한 독립변수 4가지 변수간에 다중공선성이 존재하는지를 확인하기 위해 VIF 측정법을 이용해 확인한 결과 모두 분산팽창계수가 3.0 이하로 나타났기 때문에 다중공선성 문제는 없는 것으로 확인되었다. 통제변수 세 개는 그 어떤 것도 유의미한 결과를 나타내지 못하였고, 독립변수 중에 사이버 위협에 대한 인식(p<0.05)과 기업 내부적인 지지(p<0.001)라는 두 가지 변수만 통계적으로 유의미한 결과를 나타냈다. 계수를 보면, 내부적인 지지는 (+)의 방향으로 지지 정도가 1단위가 높아질 경우 사이버보안 관리체계 정도 0.56이 높았고, 사이버 위협에 대한 인식은 (+)의 방향으로 인식 정도가 1단위 높아질 경우 사이버보안 관리체계 정도가 0.17 높았다. 상대적으로 보면, 내부적인 지지가 사이버 위협에 대한 인식보다는 종속변수에 대한 영향력이 크다고 볼 수 있다. 반면에, 대표의 강한 리더십과 불안정한 외부 환경은 사이버 보안 관리체계에 통계적으로 유의미한 영향을 주지 못하는 것으로 나타났다. 분석결과, 가설 1과 가설 2를 지지하였다. 이러한 결과를 방정식으로 나타내면 다음과 같다.

사이버보안 관리체계 = 0.03*대표의 강한 리더십 + 0.17*사이버위협 +
0.56*내부적 지지 − 0.06*불안정한 외부 환경 + 8.93

이 결과를 통해 볼 때, 중소기업에서 사이버보안에 대한 내부적인 지지가 가장 중요한 것으로 나타났다. 이는 다른 부서 그리고 비IT직원들이 사이버보안에 대해 호의적으로 평가를 하고 필요한 업무라고 인정해주어야 사이버보안 관리체계가 도입되고 제대로 작동할 수 있다는 것을 말한다. 내부적인 지지는 기업의 문화와도 관련되는 것으로 조직 문화가 사이버보안의 가치를 인정해주고 다른 경영적 가치와 배치되지 않는다는 것을 공유해야 한다. 둘째로, 자신의 회사가 사이버 위협에 노출되어 있거나 혹은 노출될 가능성이 있다라고 인식하는 것이 중요하다. 이러한 인식은 사이버보안 관리체계를 높일 수 있는 기본 바탕으로 작용할 것으로 보이며, 이것을 바탕으로 다른 변수들이 매개변수로 작용할 가능성도 있어 보인다. 통계적으로 유의미한 내부적인 지지와 사이버 위협에 대한 인식이라는 독립변수는 기업 내부에

서 사이버보안을 어떻게 바라보는지, 내부적으로 중요성을 인식하는지 그리고 공감대가 있는지와 같은 조직 분위기 내지 조직 문화의 형성과도 관련된다. 반면에, 기업의 불안정한 외부 환경은 사이버보안 관리에 유의미한 영향을 주지 못한 것으로 나타났으나, 이는 현실을 정확히 반영한 결과일 수도 있겠으나 이 모델의 한계 혹은 샘플링의 문제 등에 기인할 수도 있기 때문에 향후 연구에서 지속적으로 연구될 필요는 있어 보인다. 향후 연구에서 내부 요인과 외부 환경을 고려한 다각도의 심도 깊은 연구가 실시되기를 바란다.

V. 결 론

그 동안, 국내 및 해외에서도 이 주제와 관련해서 중소기업에 대한 연구는 많지 않았다. 국내에서는 중소기업에 대한 연구는 있으나, 기술유출이라는 분야에 한정되어 왔다. 그리고 기업 내부적으로 기술적, 인적, 경영적 요소를 포함한 사이버보안 관리를 살펴보고, 기업 외부적인 환경 변수가 미치는 영향까지 고려한 연구는 국내외를 막론하고 거의 없었다. 이러한 연구 공백을 고려할 때, 이 연구는 중소기업 사이버보안 관리 분야에 새로운 지식을 제공할 수 있을 것이다.

이 연구에도 몇 가지 한계점이 보인다. 첫째로, 질적 인터뷰 면담자들을 충분히 확보하지 못하였다. 그 이유는 사이버보안에 대해서 외부로 공개한다는 것에 대한 거부감 혹은 두려움 때문으로 보인다. 인터뷰가 오직 학술적인 연구 목적이라고 설명을 했음에도 인터뷰 자체 혹은 인터뷰 녹음을 하는 것이 불편하다는 답변이 많았다. 둘째로, 모든 중소기업에 연구 결과를 적용하기 어렵다는 것이다. 질적 연구는 연구 목적상 목적적 추출법을 사용해서 특별히 관계가 없지만, 양적 설문조사 방식에서는 샘플에 접근이 어려워 무작위성을 바탕으로 샘플을 확보하지 못했다. 이로 인해 연구 결과를 바탕으로 모집단 전체의 특성을 유추하기에는 한계가 있어, 확대 적용하기는 어려울 것으로 보인다.

하지만, 사이버보안 분야에서 혼합방법론을 도전적으로 시도함으로써 관련 개념 및 변수를 발견하고, 이를 바탕으로 만든 가설을 검증함으로써, 이론적인 함의를 제공하였다. 양적 연구 결과에서 중소기업의 사이버보안 관리가 기업 외부적 환경 관련 변수보다는 내부적 조직 문화와 관련된 변수인 내부적인지지 및 사이버보안 위협

에 대한 인식이 영향을 미친다는 것이 밝혀졌다.

물론, 국내에 한정된 내용이기 때문에 한국이 아닌 외국에 그대로 적용하기는 어렵다. 하지만 다른 환경적 맥락에도 불구하고, 이 연구는 국제적으로도 의의를 가질 수 있다. 특히, 사이버 위협은 국경을 넘어서는 위험이기 때문에, 다른 나라들도 비슷한 문제에 직면해 있을 가능성이 크다. 연구를 통해 발견한 개념 및 변수는 다른 나라를 배경으로 하는 연구에서도 적용 가능하거나 다른 나라의 환경적 맥락에서도 참고할 수 있을 것으로 보인다.

중소기업의 사이버보안을 둘러싼 정부의 규제 제도 및 정책에 대해서 기존과 달리 전체론적으로 살펴봄으로써, 현재의 정책에 대한 평가를 하는 동시에 향후 바람직한 정책 방향을 제시하였다. 여기에서 더욱 중요한 것은 기업의 경영 환경을 고려했다는 것이다. 물론, 유의미한 결과값이 산출되지 않았지만, 향후 연구에서 더욱 많은 샘플과 정제된 모델을 사용하여 추가의 검증이 필요할 것으로 보인다. 이러한 측면에서 이 연구는 정부 정책과 제도 발전에 활용될 가능성이 크다. 그동안 중소기업의 사이버보안에 대해서 정밀한 현장 중심의 연구 없이 파편적인 정책이 도입되어 온 것이 사실이다. 또한, 중소기업의 사이버보안은 기술유출의 분야에 한정되어서 주도되어 왔다. 이제는 기술유출 분야를 아우르는 사이버보안이라는 틀 안에서 정부 정책과 기업 환경을 고려한 거시적인 접근이 필요하다. 이 연구를 통해 밝혀진 연구 결과는 실효성 있는 정책 및 제도의 도입에 적절한 근거를 제시할 것으로 보인다.

참고문헌

1. 국내문헌

강정헌 (2015). 국내 중소기업 산업보안 증진 방안 제시-통합 기술보호증진센터 설립과 단계별 지원 방안을 중심으로. **한국산업보안연구**, 5(1), 113-144.

권장기, 김경일 (2017). 자원 제약하의 중소기업 정보보안계획 수립방안 연구. **융합정보논문지**, 7(2), 119-124.

김상현, 송영미 (2011). 조직 구성원들의 정보보안 정책 준수 동기요인에 관한 연구. **e-비즈니스연구**, 12(3), 327-349.

김양훈 (2014). 핵심기술 유출과 보안수준 상관관계 연구: 중소기업 기술유출을 중심으로. **한국산업보안연구**, 4(1), 97-108.

김은정 (2013). 경호· 경비 연구방법론에서 질적 연구의 활용. **한국경호경비학회지**, 34, 33-55.

김희경, 윤순진 (2011). 에코맘의 삶과 의미에 관한 질적 사례 연구. **교육인류학연구**, 14(2), 91-127.

나현대, 정현수 (2016) 국내 · 외 정보보호 관리체계기반의 인적보안의 이론적 비교연구. **융합정보논문지**, 6(3), 13-19.

남재성 (2012). 중소기업의 산업기밀 유출범죄 피해실태와 대책. **한국공안행정학회보**, 21, 44-75.

박태형, 임채홍, 이기오, 임종인 (2013). 중소기업 산업보안 강화를 위한 지방정부의 역할 분석연구-경기도 사례에 대한 실증분석을 중심으로. **디지털융복합연구**, 11(10), 1-16.

백민정, 손승희 (2011). 중소규모 조직구성원의 정보보안인식과 행동이 정보보안성과에 미치는 영향에 관한 연구. **중소기업연구**, 33(2), 113-132.

송봉규 (2014). 중소기업 영업비밀 보안수준 인식과 보안 관리체계의 차이에 관한 연구. **한국테러학회보**, 77, 31-62.

심준섭 (2008). 행정학 연구의 대안적 방법으로서 의 방법론적 다각화(Triangulation) : 질적 방법과 양적 방법의 결합. **한국행정연구**, 17(2), 3-31.

윤승영 (2016). 기업지배구조 관점에서 바라본 내부통제와 기업의 정보보안. **기업법연구**, 30(1), 9-37.

장항배 (2010). 중소기업 산업기술 유출방지를 위한 정보보호 관리체계 설계. **멀티미디어학회논문지**, 13(1), 111-121.

전창욱, 유진호 (2017). 중소기업에서 산업보안을 위한 디지털포렌식 활용방안 연구-이미징

처리시간 비교분석을 중심으로. **한국산업보안연구, 6(2),** 169-193.
정재원, 이정훈, 김채리 (2016). 기업의 정보보안 활동이 구성원의 정보보안 준수의도에 미치는 영향 연구. **정보 · 보안논문지, 16(7),** 51-59.
통계청 (2017). **2016 시도 · 산업 · 종사자규모별 전국 사업체 조사.**
한진영, 유현선 (2016). 경영진의 정보보안 지능이 조직원의 보안대책 인식에 미치는 영향. Information Systems Review, 18(3), 137-153.

2. 국외문헌

Bauer, J. M., & Dutton, W. H. (2015). *The New Cyber security Agenda: Economic and Social Challenges to a Secure Internet* (World Bank's World Development Report n.102965).

Blackburn, R. (2012). *Segmenting the SME market and implications for service provision: A literature review* (Research Paper Ref: 9/12). London: Advisory, Conciliation and Arbitration Service.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. Sage.

Bryman, A. (2016). *Social research methods*. Oxford: Oxford university press.

Chang, E. S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106(3)*, 345-361.

Grant, K., Edgar, D., Sukumar, A., & Meyer, M. (2014). 'Risky business': Perceptions of e-business risk by UK small and medium sized enterprises (SMEs). *International Journal of Information Management, 34(2)*, 99-122.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for SMEs: An empirical examination. *Information Management & Computer Security, 13(4)*, 297–310.

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security, 19(3)*, 155-176.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly, 34(3)*, 549-566.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive, 9(3)*, 2012-2052.

Levy, M., & Powell, P. (2005). *Strategies for growth in SMEs: The role of information and information systems*. Oxford: Butterworth Heinemann.

Organ, D. (2015). Trust through certification in SME Cloud adoption. In P. R. J. Trim, & H.Y. Youm (Eds.), *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership* (pp. 32-46), Seoul: British Embassy in South Korea.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire.

Computers & Security, 42, 165-176.

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security, 31(2)*, 221-232.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations, *Computers & Security, 56*, 70-82.

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ISM) Practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management, 14(4)*, 225-239.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36(2)*, 215-225.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17(1)*, 4-19.

Young, R. F., & Windsor, J. (2010). Empirical evaluation of information security planning and integration. *Communications of the Association for Information Systems, 26(1)*, 245-266.

【Abstract】

Cyber Security Management of Small and Medium-sized Enterprises with Consideration of Business Management Environment

Chun, Yong-Tae

Until now, a lot of research on cyber security have been tried, but there have been few studies on overall relationships, including internal factors and external factors. Therefore, this study examined cyber security management considering not only internal elements of SMEs but also corporate management environment. The first qualitative analysis and the second quantitative analysis were conducted through mixed method research. Qualitative analysis was conducted through a semi-structured interview method, and three themes were found: insufficient cyber security management system, internal noncooperation for cyber security, and problems derived from decision-making system. In the quantitative analysis, multiple regression analysis was conducted on the data obtained through the questionnaire. The perception of cyber threats and internal support among independent variables positively influenced the cyber security management system or the dependent variable. Through this study, internal variables had a causal impact on the cyber security management system rather than external environment variables. This implies that the variables related to the organizational culture such as employees' perception are important. These results are expected to provide practical significance for enhancing the cyber security management system in SMEs.

Keywords: Small and medium-sized enterprises, Mixed methods, Cyber security management, Technical · human · managerial controls, Holistic approach