韓國IT서비스學會誌
第12卷 第1號
2013年 3月, pp.289-308
http://dx.doi.org/10.9716/KITS.2013.12.1.289

기업 보안 유형에 따른 보안사고 대응역량 : 사회기술시스템 이론 관점에서

이정환* · 정병호** · 김병초***

Incident Response Competence by The Security Types of Firms : Socio-Technical System Perspective

Jeonghwan Lee* · Byungho Jung** · Byungcho Kim***

■ Abstract ■

This study proceeded to examine the cause of the continuous secret information leakage in the firms. The purpose of this study is to find out what type of security among administrative, technological and physical security would have important influence on firm's security performance such as the security-incident response competence. We established the model that can empirically verify correlation between those three types of security and the security-incident response competence. In addition, We conducted another study to look at relation between developing department of security in the firms and reaction ability at the accidents.

According to the study, the administrative security is more important about dealing with the security-incident response competence than the rest. Furthermore, a group with department of security has better the security-incident response competence and shows higher competence in fixing or rebuilding the damage. Therefore, this study demonstrates that investing in administrative security will be effective for the firm security.

Keyword : Security, Administrative Security, Security-incident Response Competence, Security Organization

논문투고일 : 2012년 10월 27일 논문수정완료일 : 2013년 02월 15일 논문게재확정일 : 2013년 02월 20일

* 한국외국어대학교 경영정보학과 석사과정
** 한국외국어대학교 경영정보학과 박사과정
*** 한국외국어대학교 경영정보학과 교수, 교신저자

1. 서 론

최근 기업들은 기밀 정보 유출 사고로 신제품, 신기술 개발에 대한 재무적 또는 비재무적 손실이 발생한다고 토로한다. 산업기밀보호센터의 통계 자료를 보면 2005년부터 2011년간 국내 첨단기술을 국외로 불법유출하거나 유출을 시도한 사건이 총 264건이고 2005년 적발 건수가 29건에서 2011년 46건으로 증가하는 추세로 드러났다.[1] 이러한 증가에도 국내 기업들의 IT 예산 대비 정보보호 투자 비율이 저조한 실정이다. 2011년 한국인터넷진흥원에서 조사한 정보보호 실태조사에 따르면 대기업과 중견기업 900여 기업 중에서 249개 기업(27.7%)이 정보보호 투자 예산 중 물리적 보안, 기술적 보안에만 제한적으로 투자되었다[3].

기업들의 보안에 대한 투자는 일반적인 마케팅 활동 투자와는 다르게 기업 수익과의 직접적인 관계가 미흡하여 투자가 합리적으로 이행되지 않는다고 2012년 한국침해사고대응팀협의회[16]에서 밝혔다. 특히 최근의 e-biz 기업들은 보안에 관련된 사항들을 고객 유치를 통한 매출 증대에 집중하는 반면 정보보호 대책이 미흡하게 되면서 다양한 보안 사고로 사회적 주목을 받아왔다. 이러한 보안 사고가 발생한 기업들은 보안 대응 대책보다는 부정적 이미지를 막기 위한 투자에 집중하고 보안 투자에 집중하지 못하는 모습을 볼 수 있다. 특히 정보보호 사고 및 IT 관련 사고는 기업 가치를 떨어뜨릴 수 있고 또한 전통기업보다 인터넷을 기반으로 한 기업의 피해가 더 심각하다고 밝혔다[9, 22].

한편 보안사고가 발생한 기업의 공통적 특징을 살펴보면 수익만을 중요시하고 보안 관리에 대해 체계적으로 투자하지 않거나, 인적 보안 관리를 정책적으로 지원하지 못하고 있다[9, 22]. 즉, 기업들이 보안에 대한 중요성을 인지하고 있지만 보안의 실효성과 내부적 체계가 미흡하다고 볼 수 있는 것이다[31]. 따라서 기업들은 보안 관리 및 투자가 중요할 수도 있으며 보안 사고가 기업 내부만의 문제가 아닌 이해관계자에게 해당하는 중요한 문제임을 인지해야 한다. 그 이유는 국내외로 정보화시대를 맞아 기업이나 정부가 이전보다 많은 양의 정보를 입수 및 관리하고 있기 때문이다. 특히 기업은 이러한 정보를 활용하여 경제적 이득을 취하고 있으므로 보안 사고가 발생했을 시에 그에 따른 사회적 책임 역시 커질 수 있다는 점을 인지할 필요성이 있다. 각각의 기업은 고객 DB와 협력업체의 정보까지 포함한 방대한 자료를 소유하고 있기 때문에 현대의 보안은 한 기업의 사고로만 인식되기에는 부족하다. 이것은 대기업뿐 만이 아니라 중소기업에도 적용되는 사항이기에 회사의 크기와 관계없이 기업의 보안 문제는 기업 내부의 문제로 치부되기보다 보안사고로 인한 여러 부정적 여파가 기업의 이해관계자들에게도 영향을 준다는 점을 생각해야 한다[12]. 따라서 기업은 보안사고에 대해 사회적 의무로서 사회적 책임, 이해관계자들에 대한 의무로서 사회적 책임, 윤리적 의무로서 사회적 책임, 과정으로서 사회적 책임으로 생각해야 한다[6, 35, 42].

2011년 Ahnlab Report에 따르면 보안 사고에 있어 가장 중요한 원인이 관리적 대응조치 부재이다. 또한 이를 통제할 수 있는 보안 전담조직에 관련된 인적자원 투자가 미비하므로 보안사고 발생 확률이 높다고 밝혔다. 보안에 대한 국외의 연구에 따르면 보안은 사회적 가치(관리적 보안)와 기술적 가치(기술적 보안)가 더해질 때 조직 내에서 제 기능을 발휘한다고 언급하며 관리적 보안과 기술적, 물리적 보안의 관계에 따라 보안의 효과가 어떻게 달라지는지에 대한 연구가 활발히 이루어지고 있다[25]. 즉, 관리적 보안과 기술적, 물리적 보안이 함께 투자되어야 조직 내의 보안이 효과적일 수 있다. 하지만 국내 연구의 경우 가시적으로 기업보안 성과를 판단할 수 있는 기술적, 물리적 대응조치에 대한 기업의 투자와 관련된 연구가 대부분이었고, 관리적 대응력은 부재하다. 따라서 관

1) 산업기밀보호센터, “연도별 기술유출현황”, 2011. 12, http://service4.nis.go.kr/servlet/page?cmd = preservation&cd_code = outflow_1&menu = AAA00.

리적 보안에 대한 중요성과 실무적 검증이 필요하다. 이와 같은 내용을 토대로 하여 국내 기업의 관리적 보안에 대한 투자 미흡과 연구의 부족을 파악할 수 있었다.

본 연구에서 제시한 보안의 유형은 한국 정보보호진흥원의 정보보호 관리체계 인증제도에서 제시한 3가지 보안 유형이다[4]. 이는 기술적(Technical Security), 물리적(Physical Security), 관리적 보안(Administrative Security)으로 정의된다. 따라서 본 연구에서는 이러한 유형을 활용하여 각 보안 유형 간의 관계를 살펴보고 이에 따라 어떠한 보안 유형에 투자해야 가장 큰 실효성을 가질 수 있는지를 검증하고자 하였다. 또한 보안의 성과인 보안사고 대응역량에서 기술적 보안과 물리적 보안이 관리적 보안에 어떠한 영향을 미치는지를 살펴보고, 관리적 보안에서 중요한 부분을 차지하고 있는 보안전담조직의 유무에 따른 차이점 역시 살펴보고자 한다.

2. 이론적 배경

2.1 관리적 보안의 중요성

일반적으로 보안은 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 기준으로 위험을 관리(Risk Management)하여 발생할 수 있는 보안 사고를 최대한 줄이는 것을 목적 및 효과이다[49]. 즉, 통제를 기반으로 조직 내에서 보안이 운영되기 때문에 이익을 향상시키기 위한 기업의 목적과 비례하지 않는다는 점이 보안의 가장 큰 특징이다. 한국정보보호진흥원[4]의 정보보호 관리체계 인증제도를 살펴보면 보안의 유형을 관리적 보안(Administrative Security), 물리적 보안(Physical Security), 기술적 보안(Technical Security)으로 나누어 구분한다.

보안 관리에 관한 시대적 흐름은 미국을 중심으로 시작되었으며 이는 <표 1>에 제시하였다. 기업의 관리적 보안 연구의 흐름을 살펴보면 IT 기술의 발달과 함께 정보 보안의 관리 초점이 변화되었다. 1980년대 기술적 대응, 1990년대 관리적 대응, 2000년대 조직적 대응, 2006년 이후에는 보안 거버넌스라는 흐름으로 보안에 대한 초점이 맞추어졌고 집중되었던 시기이다.

〈표 1〉 시대별 보안 관리 흐름

시대별 구분	정의
1980년대	◦ 메인프레임 중심의 운영체제를 포함한 시스템 중심의 보안 기술
1990년대	◦ 정보 관리의 중요성이 대두 : 네트워크 확산과 시스템 분산화에 따라 정보시스템이 분산화 및 네트워크화
2000~2005년	◦ 조직구성원의 전반적인 참여와 보안 문화가 형성 ◦ 보안관리체계 인증제도 도입
2006년 이후	◦ 경영층의 책임이 강조 ◦ 보안을 통한 가치창출에 중점

주) Solms[48]의 일부 연구 내용을 재정의함.

해당 연구는 기술 중심의 보안 유형을 벗어나 조직 관점에서의 관리적 보안이 중요하게 되었다는 점을 설명한다[48]. 이러한 변화는 관리적 보안을 바탕으로 거버넌스 차원에서의 보안을 다루어야 더욱 효과적이고 효율적인 보안을 이룰 수 있다[49]. 또 다른 국외의 관리적 보안 연구 역시 관리적 보안이 기술적, 물리적 보안과 함께 고려해야 할 변수로써 연구되고 있고, 세 요소를 함께 고려해야 보안에 대한 효과가 상승할 것이라고 언급했다[8, 25]. 학술적 연구뿐만 아니라 실증적으로 국외에서는 이미 정보보호의 인증체계인 ISO27001를 통해 기업 내의 관리적 보안이 보안 체계에서 중요하다는 점을 언급하며 정보보호 인증을 통한 기업 가치 향상을 높이려는 움직임을 보인다. 미국 및 영국은 정보보호 관리체계를 통해 관리적 요소를 구체적, 체계적 지표로 제시한다. 또한 보안 관리 체계를 통한 목표를 보안을 통한 기업 가치 향상이라고 말한다[10, 22]. 반면 국내의 관리적 보안 연구를 살펴보면 첫째, 근래에 들어 관리적 보안 모델 수

립을 위한 연구가 대다수였고 둘째, 관리적 관점의 보안 연구는 CEO/CIO 관점에서의 보호 인지, 개인정보보호 등이 연구되고 있다. 그러나 최근 기업 보안 사고의 빈도가 높아지고 있는 반면[9, 22] 그와 관련된 실무적 관점에서의 관리적, 기술적, 물리적 보안 관계 및 보안 영역 성과 연구는 부족하다는 것을 알 수 있다. 또한 기업 및 정부의 관리적 보안에 대한 현황 역시 선진국보다 체계적이지 못함이 언론매체를 통해 언급되고 있고, 지속해서 발생하는 기업 보안 사고를 통해 관련 사항이 증명되고 있다. 보안 관련 전문가 인터뷰에 따르면 기업과 정부는 눈앞에 보이는 물리적, 기술적 보안에만 집중적으로 투자하고 가장 중요한 관리적 투자에는 관심이 부재하다고 언급하였다. 또한 2013년도에 발효될 정보통신망 이용촉진 및 정보보호 등에 관한 법률 개정 내용에서 정보보호 관련 항목 중 관리적 요소가 여러 면에서 부족하다고 보고 있으며 기업들이 보안 관리를 의무가 아닌 선택사항에 따라 적용할 수 있게 되어 있어 선진국과 비교하면 한계점을 가지고 있음을 지적하였다[1]. 이러한 원인을 살펴보면, 2012 한국침해사고대응팀협의회의 보고서에서 보안은 기업의 일반적인 성과 평가 기준과는 다르게, 투자 대비 매출이나 이익으로 그 성과를 판단하기 어렵다고 언급하였다. 이러한 불명확한 성과의 판단 기준이 기업들로 하여금 보안 강화 및 투자 증대에 부정적 요소로 작용하고 있음을 알 수 있는 대목이다. 즉, 선진국과 비교하면 국내는 최근까지도 기술적, 물리적 보안이 선행되어 집중적으로 투자되고 있기 때문에 상대적으로 관리적 보안이 미흡하다. 이처럼 최근 언론매체를 통해 관리적 보안이 보안성과에 중요한 영향을 미치고 있음이 지속적으로 언급되었다. 하지만 관리적 보안이 보안의 성과에 미치는 영향을 실증적으로 분석한 연구는 미흡한 실정이기 때문에 학술적 연구를 통해 이를 증명할 필요성이 있다.

기업의 관리적 보안 투자가 미흡한 원인을 살펴보기에 앞서, 기업 내의 관리적 보안과 같은 비가시적 투자에서 어떠한 의사결정을 내리는지 살펴봄으로써 관리적 보안이 투자되지 않은 이유를 살펴보고자 한다. 기업의 투자 의사결정은 목표의 선택과 의사결정의 과정이다[17]. 또한 의사결정을 과정 지향적 이론(process-oriented theory)으로 설명할 수 있으며, 기업 내 조직은 의사결정을 수행하는데 있어 제한된 합리성을 가지고 있다. 의사결정의 합리성을 제약하는 요인으로는 인식론적 제약, 환경 불확실성, 조직 유지에 따른 정치적 제약 및 조직 관리상의 제약으로 영향을 받는다. 즉, 기업 내외적 압력에 따라서 불완전한 의사결정이 진행되고 있다. 기업의 매출, 생산, 고객 관리를 위해 최고 경영자들은 의사결정 수행 시 제약된 의사결정을 수반하게 되고[44] 제약된 상황에서의 의사결정은 효율성 저하와 정보의 수집, 분석, 판단하는데 애로사항이 발생하게 된다[46]. 기업 경영자들은 이해관계자와의 관계와 대외적인 기업 성장에 따라 정치적 제약 및 조직 관리상의 제약을 받게 되는 때도 있다. 따라서 최고 경영자는 긍정적인 평가를 받기 위해 비가시적 성과보다는 가시적인 성과에 더욱 집중하는 때도 있다[32]. 같은 맥락에서 성과가 확연히 드러나는 물리적, 기술적 보안의 투자는 활발하지만 가시적이지 않은 관리적 보안 투자와 같은 비가시적 투자는 자산관리의 투자 의미보다는 비용 투자로의 인식으로 투자가 부족하다고 볼 수 있다. 특히 금융경제 위기와 산업 간 융합에 따른 기업들의 환경적 불확실성으로 보안과 같은 비가시적 투자가 더욱 위축되고 있다. 하지만 기업의 가시적 보안에 대한 투자만으로는 그 효과가 부족하므로 보다 효과적인 보안을 위해 투자되어야 할 비가시적 보안 즉, 관리적 보안 투자는 표준화된 절차나 계획에 따라 체계적으로 투자되어야 더욱 긍정적인 효과를 발휘한다[31].

2.2 사회기술 관점에서의 3가지 보안 요소와 보안사고 대응역량

앞서 설명한 관리적 보안의 중요성은 사회기술

시스템이론을 통해서도 살펴볼 수 있다. 사회기술시스템이론은 기술에 치중된 시스템의 문제점과 실패들을 살펴보기 위해 제기되어 사회적 시스템과 기술적 시스템의 요소 간 상호작용이 조직의 성과 또는 산출물에 영향을 줄 수도 있다는 점을 강조하고 있다. 사회적 시스템은 사람, 구조에 초점을 맞추어서 설명되어지며 기술적 시스템은 직무와 기술에 초점을 맞추어서 설명된다. 이는 기업 경영환경에 전반적으로 영향을 받는 요소로 정의된다[11, 50]. 이들 시스템에 포함되어 있는 기술, 직무, 사람, 구조의 4가지 요소는 다른 요소들과 상호작용하면서 시스템 전체의 작동에 기여하게 된다. 만약 어떤 구성요소의 특성이 변화한다면 시스템 내부의 다른 요소들도 바뀌어야 한다. 사회기술시스템이론에서 중요한 점은 기술적 요소에 사회적 요소를 투영시킴으로써 첫째, 기업의 생산성을 향상시킬 것이고 둘째, 신기술의 유연한 수용이 가능해진다는 점이다[34].

사회기술시스템이론이 기장 활발히 연구되고 있는 분야는 시스템 설계 분야이다. 따라서 많은 학자들이 해당 분야에 사회기술시스템이론을 접목시키기 위해 연구를 진행하고 있다. 그 흐름을 살펴보면 크게 두 가지로 구분된다. 첫째, Albert Cherns는 사회기술시스템이 시스템 설계의 고유 원칙을 보존해야 한다고 주장하였고 Chris Clegg는 Albert Cherns의 주장을 인터넷의 개념이 포함된 ICT 기반의 사회기술시스템이론으로 발전시켰다[15]. 둘째, Enid Mumford는 사회기술시스템의 원칙을 ETHICS라고 명명하고, 본인이 정의한 사회기술시스템이론에 근거한 IS 개발 방법론에 관련된 연구를 진행하였다[38]. 때론 시스템 설계에 관련된 두 이론이 충돌하기도 하였는데 첫째는 인본주의적인 원칙의 중요성이다. 시스템 설계자는 직원의 직무만족을 위해서는 생산성을 향상시키기 위한 목적을 취해야하지만, 직장생활에서의 가치를 향상시키기 위해서는 직원이 조직에서 업무 외에 추가적인 가치를 생산할 수 있도록 도와야 하기 때문이다. 둘째는 관리에 대한 가치에서 살펴볼 수 있다. 사회기술시스템이론의 원리는 경제적 목적을 성취하기 위한 도구이다. 따라서 인본주의적인 목적은 가치가 없는 것으로 판단하게 된다. 하지만 만약 인본주의적 가치가 직원으로부터 더욱 효과적으로 경제적 목적을 수행하게 할 수 있다면 이는 긍정적으로 바라볼 수 있다[33].

기업의 보안도 사회적, 기술적 관점에서 중요성을 강조할 수 있다. 보안은 사회기술시스템 이론의 4가지 요소의 중요성에 따라 개별적으로 관리적, 기술적, 물리적 요소를 집중하기보다 함께 고려해야 효과가 높아질 수 있다. 정보를 둘러싼 환경의 지속적 변화는 해당 정보를 풍부하게 만들기도 하지만 위협에 대한 노출을 더욱 상기시키는 결과를 가져올 수 있기 때문에 사회적, 기술적 관점을 통합적으로 운영할 수 있는 시각을 갖추어야 한다. 즉, 기존에 행해지던 기술적, 물리적 보안의 수준으로만 정보의 보안 사고를 예방하기에는 부족한 부분이 있으므로 특정 유형에 집중하는 것이 아닌 보안 유형 간의 상호보완적 활성화가 중요하다[5].

따라서 앞서 관리적 보안의 중요성에서 언급하였듯이 변화된 환경을 전반적인 사회적, 기술적 관점으로 통제하고 관리할 수 있는 역량이 더욱 강조된다[5, 8, 25].

2.2.1 관리적 보안과 보안사고 대응역량의 관계

앞서 이론적 배경에서 투자 의사결정을 설명한 바와 같이 관리적 보안(Administrative Security)은 비가시적 자산의 투자요소이다. 그중에서도 인적자산, 정보자산, 정책 등은 기업의 비가시적 가치로서 보안 관리를 수행하는 중요한 통제 요소이며 관리적 보안의 투자 요소로서 정의된다[23]. 이러한 인적자산, 정보자산, 정책은 보안의 관리적 체계를 구축하여 기술적, 물리적 보안이 효과적으로 운영될 수 있도록 구성되어야 한다. 또한 기술적, 물리적 보안은 관리적 보안과의 관계에서 상호작용이 있고, 사회기술시스템이론에서도 기술적 요소와 기업의 인적 자산, 정책과 같은 사회적 요

소의 상호 작용을 강조하는 것이다[11].

이러한 관리적, 기술적, 물리적 보안 유형은 보안 사고가 발생하지 않도록 하는 방법인 보안사고 대응역량과 유의한 관계를 맺는다[49]. 각 조직은 보안사고 대응역량을 갖추어야 하고, 해당 대응역량은 물리적, 관리적, 기술적 보안의 유형에서 여러모로 접근하는 것이 효과적이다. 또한 보안사고 대응역량을 향상하기 위해서는 보안 체계 수립, 보안시스템 구축, 보안기술 개발, 투자 확대, 법 · 제도, 인력 등이 논의되어야 한다. 더욱 원활한 보안사고 대응역량을 키우기 위해서는 보안사고가 발생했을 시의 상황을 예측해보고 타당하면서 적절한 대응방안을 수립하는 것이 효과적이다[32].

사회기술시스템 이론에서 사회적 시스템을 통해 관리적 보안이 보안의 성과인 보안사고 대응역량과 관계가 있다. 사회적 시스템은 사람과 구조의 관점을 설명하고 있는데 실제 업무를 수행하는 사람 및 의사소통 체계와 권한 체계, 업무 흐름 체계를 의미하는 구조를 효과적으로 설계하면서 기업의 성과를 향상시킬 수 있다. 사회적 관점에서 보안을 보면 보안 전담조직과 같은 실제 업무를 수행하는 대상 및 정보보호 관리체계, 인적관리 등 제도적 운영과 같은 보안에 관한 체계적 구조로 설명될 수 있으며 이것은 보안의 성과를 향상시킨다는 점에서 보안사고 대응역량에 영향을 미친다[5, 50].

2.2.2 기술적 보안과 보안사고 대응역량의 관계

기술적 보안은 기업이 소유하거나 구현하려는 시스템, 네트워크, 서버, DB 및 단말기에 따라 기술적으로 활용 가능한 보호 대책을 의미한다. 기술적 보안의 영역을 살펴보면 파일 및 데이터 암호화, 시스템 접근 제어, 계정관리, 사용자 권한 관리, 바이러스 보안, DB 보안, SW 검사 등의 시스템 보안 영역과 조직 내의 네트워크 보안 솔루션으로 분류되는 방화벽 및 VPN, IPS, NAC와 관련된 영역을 네트워크 영역이라고 분류한다[43]. 또한 기술적 보안을 사용자 식별과 인증, 시스템 상 정보의 논리 접근 통제, 감사 증적 등을 기준으로 기술적 보안을 정의하여 총 5단계를 통해 해당 보안 사항을 통제하고 있다[39].

기술적 보안은 각 기업의 시스템 특성에 따라 설치 및 구현된다. 즉, 시스템이 구축된 환경적 특성에 따라 해당 기업이 구축하려 하는 시스템의 보안 실태가 결정된다. 따라서 시스템을 구축하는 업무를 담당하는 인력이나 기업의 정책 사항에 따라 관리적 보안의 수준이 결정될 것이고 이는 기업의 보안사고 대응역량에 유의한 영향을 미친다[49].

사회기술시스템 이론에서 기술적 시스템을 통해 기술적 보안과 보안사고 대응역량의 관계를 살펴볼 수 있다. 기술적 시스템은 기술과 직무의 관점을 설명하고 있는데 이는 조직의 성과 문제를 개인의 역량이 아닌 조직의 전체적인 해결책을 통해 해결하려는 방법 또는 도구를 의미한다. 기술적 시스템에서 기술적 보안은 시스템에서 발생할 수 있는 위험을 줄이기 위해 사용되는 신기술을 의미하고 이러한 것들이 적절히 구축되면 기업의 보안성과에 유의한 성과를 가진다[5, 50].

2.2.3 물리적 보안과 보안사고 대응역량의 관계

물리적 보안은 일반적으로 언급되고 있는 시설 및 출입보안 등에 적절한 보안 구역을 설정하여 관리하는 것을 말한다. 시스템을 구성하는 정보 자산에 가해질 수 있는 피해를 최소화하기 위해 기업은 1차적인 방어 수단인 물리적 보안에 투자하게 되고, 주요 시설물의 설계 및 접근 통제를 통해 해당 구역의 반출 · 입에 관련된 내용 및 인원에 관한 내용을 감시 및 통제할 필요성이 있다[47].

물리적 보안은 물리적 요소를 관리하고 통제하기 때문에 본 연구에서 제시된 보안 변수 중에서 가장 기초적인 변수이다. 또한 보안사고 대응역량에 있어 기업에 가시화해줄 수 있는 억제 기능이 있으므로 필요에 따라 큰 비용이 소요된다는 특징을 지니고 있다[49]. 따라서 관리적 보안과 맞지 않다고 해서 기존의 물리적 보안을 쉽게 변경하기가 어려울 수 있다. 즉, 더욱 효과적인 보안을 위

해서는 기업에 활용된 물리적 보안을 분석하여 가장 적절한 관리적 보안의 수준을 결정할 필요가 있으며 그 관계의 수준에 따라 보안사고 대응역량에 미치는 영향이 달라진다. 물리적 보안은 개인의 역량에 초점을 맞추기보다 기업 내 자산의 효과적 보호를 통해 보안성과를 향상시킨다는 점에서 기술적 시스템과 상충되는 의미를 찾을 수 있다[5, 50].

2.3 보안전담 조직과 보안사고 대응역량

기업의 보안 사고는 기업의 성장에 필요한 중요한 자산이 경쟁자 또는 제 3자에게로 유출되는 문제이다. 보안 사고는 기업 내부적으로 보안과 관련된 전문성, 담당인력 부족, 전담부서가 부재할 때 발생하게 된다[25]. 이는 보안 사고에 대한 예방 및 신속한 처리가 없으면 발생하게 되는데 특히 보안과 관련된 전담부서가 없는 경우, 신속하게 보안 사고에 대응할 수 없게 된다[36].

한 조직 내에서 성공적으로 보안을 관리하기 위해서는 보안 관리의 틀과 경영진의 확고한 지원이 필요하다. 보안 관리는 전체 조직에서 각 조직부문에 맞도록 책임과 권한 및 인력을 적절하게 배정하고 그에 해당하는 보안 전담 조직이 존재하면 더욱 긍정적인 효과가 발생한다. 이는 보안이라는 테두리 안에서 조직이 더욱 효과적으로 운영될 수 있도록 하는 전제조건이다[24]. 따라서 보안사고 대응역량에서 보안 전담부서의 유무는 중요한 변수가 된다. 또한 보안전담조직은 보안정책을 보다 효과적으로 실행할 수 있는 기반 조성에 도움을 준다[45]. 하지만 보안전담조직에 대한 기업의 반응은 아직도 냉소적이다. 2011년 금융위원회에서는 보안에 대한 중요성을 인식하고 금융회사 IT 보안강화 종합대책을 발표하여 금융회사로 하여금 보안 전담조직을 구성토록 유도하였지만, 23%가량이 보안 전담조직 계획이 없으며 68%가량이 IT 보안 관련 전담 인력을 채우지 못했다고 발표했다.

이는 일반적으로 보안 전담조직에 대한 중요성은 인지하고 있지만, 기업 내에 있어 그 성과에 대한 확신이 부족하여 투자에 소홀해지고 있음을 보여주는 지표라고 볼 수 있다. 금융위원회는 보안을 보다 효과적인 수준까지 끌어올릴 수 있는 수단으로 보안 전담조직을 선택하였음을 알 수 있다.

3. 연구 모형 및 가설 설정

본 연구는 한국중소기업청에서 2010년에 수집한 '기술보안역량 및 기술유출 실태조사표'에 기초하고 있으며 설문 문항은 국제 보안 표준규격인 ISO/IEC 27001를 바탕으로 국내 기업의 상황에 맞도록 재설정한 것이다[2]. 이 조사는 국내 기업을 대상으로 기업 유형별 단위 표본 조사를 하였으며 설문의 조사 기간은 2010년 10월 4일~2010년 11월 29일까지 진행되었다. 총 수집된 표본 수는 벤처, 중소, 대기업을 대상으로 1,500개이다.

2010년 보안 실태 자료는 DDoS가 2009년 7월 7일 발생되면서 국가, 기업, 개인의 피해가 발생 후 복구하는 시점에서 조사된 연구 자료이다. 즉, 기업들이 보안에 대한 대책을 수립한 이후의 관리적 보안 운영 정보를 수집한 자료로서 기업들의 보안 역량에 관한 내용이 내포되었다. 또한 2010년 이후 동일 1,500개 기업군에 대한 추가적인 보안 운영 실태 조사가 이루어지지 못하여 현 시점에서 2010년 자료를 통해 관리적 보안의 중요성을 증명하려 한다.

본 연구의 목적은 보안 수준을 측정하기보다 보안 사고가 발생했을 때, 해당 기업에서 가지고 있는 보안사고 대응역량의 정도를 확인하고 보안 수준과 해당 기술적 물리적 관리적 보안과의 관계를 나타내고자 한다. 즉, 학문적 기여도와 함께 보안의 특성을 가시적으로 보여줌으로써 기업의 보안 투자의 방향성에 도움을 줄 수 있을 것이라 기대하고 있다. 따라서 연구 모형 설정은 기술적 보안과 물리적 보안으로 구분하고 이들이 보안사고 대응역량에서 관리적 보안에 매개 효과가 있는지 분석하고자 한다. 또한 관리적 보안과 보안사고 대응

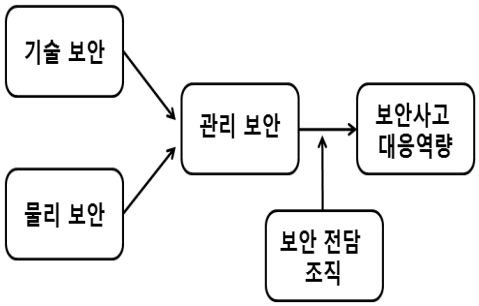
역량 간 보안 전담조직 여부의 조절 효과가 있는지를 분석하기 위해 연구 프로세스를 설정하였다.

앞서 이론적 배경을 통해 살펴본 바와 같이 기술적 보안과 물리적 보안이 관리적 보안에 영향을 미친다고 하였다. 또한 관리적 보안이 보안사고 대응역량에 영향을 미친다고 하였으며 보안 전담 조직 여부가 관리적 보안에서 중요하다고 언급했다. 이러한 내용을 토대로 [그림 1] 연구 모형과 가설을 설정하였다.

H1 : 관리적 보안(Administrative Security)은 기술적 보안(Technical Security)과 보안사고 대응역량의 관계에 긍정적이다.

H2 : 관리적 보안(Administrative Security)은 물리적 보안(Physical Security)과 보안사고 대응역량의 관계에 긍정적이다.

H3 : 기술/물리/관리보안과 대응역량간의 관계는 보안 전담조직 여부에 따라 달라진다.



[그림 1] 연구모형

본 연구의 분석 프로세스는 다음과 같다.

• 본 연구(주 목적)

(1) 매개 효과 분석 : 관리적 보안의 중요성을 확인하기 위해 독립변수인 기술적, 물리적 보안과 종속변수인 보안사고 대응역량에서 관리적 보안이 가진 매개효과를 분석하였다.

(2) 보안사고 대응역량 효과 분석 : 보안사고 대응역량에 대해 기술적, 물리적 보안 변수 중 어떠한 변수가 상대적으로 관리적 보안을 통해 긍정적인 효과가 도출되는지 분석하였다.

(3) 보안 전담조직 유무의 조절효과 분석 : 앞서 (2)번 보안사고 대응역량 효과를 분석한 후, 관리적 보안과 보안사고 대응역량 사이의 보안전담조직 유무가 보안사고 대응역량에 어떠한 영향을 주는지 조절효과 분석을 하였다.

이와 같은 3가지 연구 분석 프로세스를 통해 분석을 수행한 후 추가 연구로서 보안 전담조직 유무에 따른 보안사고 대응역량 차이 분석을 수행할 것이다.

즉, 본 연구는 기존 문헌에서 강조하는 관리적 보안을 실증적으로 증명하기 위한 연구이다. 추가 연구는 관리적 보안 내에서도 실제 보안을 수행하는 보안 전담조직 구성 여부에 따라 어떠한 차이가 존재하는지 살펴보고자 한다.

3.1 보안 유형 구분을 위한 기준 변수

본 연구에서는 앞서 이론적 배경에서 살펴본 선행 연구들을 토대로 시설관리를 물리적 통제, IT 관리를 기술적 통제로 조작적 정의 하였으며 보안 정책 및 자산 운영, 인적자원 교육은 관리적 보안으로 조작적 정의를 내렸다. 한국중소기업청에서는 '기술보안역량 및 기술유출 실태 조사표'를 수행하기 위하여 산업보안 역량 평가 framework에 따라서 조사를 진행하였다. 정책분야(정책관리), 적용분야(자산관리, 시설관리, 인적자원관리, IT 보안관리), 대응분야(재해 및 유출사고 발생 시 보안대응)로 구분하여 보안역량 평가를 수행하였다. 실태 조사표에 의거 각 영역 내 측정 항목은 1~3점까지의 점수로 부여되었으며, 이에 따른 점수를 통해 분석을 수행하였다.

한편 기업들이 보안사고 피해를 방지할 수 있는 요소 중 중요한 변수가 무엇인지 검증하는 연구 프로세스로서는 부재하였다. 그래서 3가지 보안 요

소 중 보안사고 대응역량에 영향을 미치는 변수가 무엇인지를 검증하기 위해 본 연구를 시행하였다. 즉, 기업들이 보안사고 대응역량 강화를 위해서 어떤 요소에 투자해야 하는지를 구분하여 보안사고 대응역량을 설명하는 것이 중요할 것으로 생각된다. 따라서 보안사고 대응역량의 수준을 검증하는 연구를 진행하기 위해서 물리적, 기술적 보안과 관리적 보안 차원에 따라 보안 유형을 구분하였고 기업이 응답한 항목별에 부여한 가중치 점수를 그대로 이용하여 분석을 수행하였다. 그 내용은 다음과 같이 <표 2>와 같다.

3.2 조작적 정의 및 변수 설명

본 연구는 기술적 보안과 물리적 보안이 보안사고 대응역량에서 관리적 보안의 중요성을 검증할

〈표 2〉 변수의 조작적 정의와 주요 측정 도구

요인	조작적정의	측정항목		관련 문헌
물리적 보안	건물의 중요시설 보안 강화를 위한 관리 수준 (시설관리)	PHY1	외부인 회사 내 출입절차 존재	NIST[39] Solms[47]
		PHY2	중요시설 출입통제 시스템 설치 및 운영	
		PHY3	외부인 식별을 위한 사원증 패용 의무화	
		PHY4	중요시설에 대한 카메라 등 장비반입 규정	
기술적 보안	IT에 따른 정보 유출 방지를 위한 관리 수준 (IT 관리)	ITM1	통신망 보안점검 실시	NIST[39] Post and Kagan[43] Yeh and Chang[51]
		ITM2	서버 및 DB 현황 보안점검 실시	
		ITM3	바이러스 침입, 해킹에 의한 대책 강구	
		ITM4	주요 정보 및 소프트웨어 백업 관리	
		ITM5	주요 시스템의 사용자 패스워드 관리	
		ITM6	정보시스템 사용 내용 로그 기록 관리	
		ITM7	주요 장애 발생 시 시정조치	
		ITM8	정보시스템에 대한 유지보수	
관리적 보안	정보유출 보안사고 방지를 위한 정책 및 인적, 정보자산 운영 수준	OPE1	보안 정책 및 관리 규정 보유	Bostrom and Heinen[11] Fred[23] Goel and Chengalur[25] Karyda et al.[31] NIST[39]
		OPE2	보안 정책, 지침, 절차 관련 공지	
		OPE3	보안업무 수행 공조체계 구성	
		OPE4	정기적 보안감사 실시	
		OPE5	정보자산 중요성에 따라 등급 구분	
		OPE6	정보자산 정기적 분류	
		OPE7	주요 기밀문서 관리 권한 설정	
		OPE8	자산 반출 사전 인가	
		OPE9	신입 입사자 보안교육 실시	
		OPE10	기존 임직원 보안교육 실시	
보안사고 대응역량	보안사고 발생 시 기업 대응방안 수준	PER1	기술유출 및 침해사고의 대응방안	Maigna and Ferrell[35] Hagen and Albrechtsen[28] NIST[39]
		PER2	기술유출 방지 관련 주요 법규 인지	
		PER3	스마트폰 보안사고 대응방안	

주) 각 변수 측정 점수는 1~3점 척도로 측정됨.

수 있도록 측정 항목을 선정하였다. 기업 보안 유형을 구분하기 위해 기존 문헌을 토대로 기술적 보안, 물리적 보안, 관리적 보안을 기업 보안 3가지 유형으로 구분하였다. 또한 추가 연구에서는 보안 전담조직 운영이 보안사고 대응역량에 어떠한 차이가 있는지 확인하기 위하여 보안 전담조직 구성과 미 구성으로 변수를 구분하였다.

기술적 보안은 기업이 소유하거나 구현하려는 시스템, 네트워크, 서버, DB 및 단말기에 따라 기술적으로 활용 가능한 보호 대책을 의미한다[43]. 이를 토대로 기술적 보안에 맞는 측정 항목을 '기술 보안역량 및 기술유출실태 조사표'에서 선정하였다.

물리적 보안은 일반적으로 언급되고 있는 시설 및 출입보안 등에 적절한 보안 구역을 설정하여 관리하는 것을 말한다[47]. 이를 토대로 물리적 보안에 맞는 측정 항목을 '기술보안역량 및 기술유출실태 조사표'에서 선정하였다.

관리적 보안은 비가시적 자산의 투자요소이다. 그중에서도 인적자산, 정보자산, 정책 등은 기업의 무형적 가치로서 보안 관리를 수행하는데 중요한 통제 요소이다. 즉, 인적보안, 자산통제, 정책 통제를 관리적 보안의 세 가지 투자 유형으로서 정의된다[23]. 첫째, 보안에서 정책관리는 조직 내 보안을 통해 도출하고 싶어 하는 기대사항들과 의무사항들이 기술된 문서를 기초하여 조직원들이 따라야 하는 의무를 말한다[25]. 따라서 조직원들의 보안 정책 준수 여부는 조직이 보안 사항에 대해 얼마나 준수하는지를 판단할 수 있는 수단이 될 수 있고, 정책 준수 여부는 보안에 대한 성과에도 영향을 미침을 추측해 볼 수 있다. 또한 보안정책의 포괄성은 조직 보안 수준이 얼마나 준수되고 있는지를 가늠해 볼 수 있다. 보안 정책을 지속해서 준수시키기 위해서는 정책에 대한 이해와 지속적인 교육을 통해 정책의 실효성을 높일 수 있다. 정책관리는 기업의 보안사고 대응의 출발점이다. 따라서 각 기업의 사항에 맞는 정책을 물리적, 기술적, 관리적 보안에 맞게 구성되어 있어야 보안에 대한 효과가 높다[27, 31]. 둘째, 기업 내 사용되고 있는 정보자산은 하드웨어와 소프트웨어로 구분되고 기업의 비즈니스 목표를 달성하도록 지원하는 도구이다. 하드웨어 종류를 분류 시, 용도별 관점에서 생산에 사용되는 장비, 사무용 장비 및 설계에 사용되는 장비로 구분할 수 있고, 장비별 관점에서는 PC, 프린트 장비, 서버장비 등으로 구분된다. 소프트웨어 분류 시 용도별 관점에서 생산, 시스템, 정보통신 소프트웨어로 구분할 수 있고, 제품별 관점에서는 운영체제, 오피스, DBMS, 백업 및 복구 도구, 기업용 솔루션(ERP) 등으로 나눌 수 있다[51]. 보안에서 자산관리는 위의 나열된 자산들을 기업 내 보안 정책에 맞게 관리하는 것이다[37]. 셋째, 인적관리는 조직의 구성원이나 협업관계의 인원이 조직의 보안 정책에 맞게 업무를 실시하도록 관리하는 것을 의미한다[19, 26]. 정보보호의 흐름은 지속해서 변하고 있다. 하지만 그 근본을 살펴보면 결국 조직 내의 사람이 보안을 통제하고 있다. 따라서 보안에 관련된 이슈 대부분에는 사람이 존재한다[14, 26]. 그 근거로 IDC와 Deloitte의 보고서를 살펴보면 각각 59%와 79%의 확률로 조직 내의 인원에 의해 보안사고가 발생한다고 발표했다[18, 30]. 이러한 인적관리로 발생하는 위험을 해결하기 위해서는 인적관리의 지속적인 역량 강화와 조직원의 자발적인 참여가 필요하다[13, 36]. 따라서 관리적 보안에서 특히 인적 통제를 강화함으로 인해 보안사고 발생을 줄이고 조직과 개인의 정보에 대한 침해와 같은 정보보호 효과를 달성할 수 있을 것이고[20, 47], 인적 보안의 부족 말미암은 통제의 실패는 곧 정보보호의 실패로 이어진다[40]. 이러한 보안 사고가 발생하지 않도록 하는 방법들이 보안사고 대응역량이다[49]. 이를 토대로 관리적 보안에 맞는 측정 항목을 '기술보안역량 및 기술유출실태 조사표'에서 선정하였다.

기업의 정보보안 실패는 기밀 유출로 이어진[40]. 이러한 보안 사고가 발생하지 않기 위해서는 기업들의 기술유출 및 침해사고와 관련된 대응방안이 수립되어야 하나 법규 인지 부족, 그리고 최

근의 스마트폰을 이용한 정보 유출의 빈도수가 높아지면서 첨단기술의 유출이 발생하고 있다[3]. 이를 토대로 보안사고 대응역량에 맞는 측정 항목을 '기술보안역량 및 기술유출실태 조사표'에서 선정하였다.

앞서 문헌에서 설명하였듯이 관리적 보안을 더욱 효율적으로 운영하기 위해서는 보안 전담조직이 필요함을 언급하였다. 보안 전담조직이 관리적 보안에 영향을 준다는 의미는 조직 내 보안 관련 업무에 대한 책임과 역할을 맡고 있다. 또한 보안 전담조직은 보안 사고가 발생했을 시에 적절한 대응 프로세스를 구축 및 실행하는 역할도 맡고 있다. 따라서 보안 사고에 대해 더욱 효과적인 대응을 위해서는 보안 전담조직을 강화해야 하고 해당 인력을 체계적으로 육성·확충하는 것이 효과적이다[31]. 또한 그들로 하여금 다양한 사고 예측 시나리오를 마련토록 하여 정기적인 검토 제도를 구축하는 것이 보안 사고에 긍정적이다. 조직의 대응역량에서 전담조직이 효과적이라는 주장은 비단 보안 영역에서만 있는 것이 아니다. 다양한 종류의 범죄에서도 해당 범죄에 특화된 전담조직은 그 성과가 뛰어난 것으로 나타났다[25]. 이를 토대로 보안 전담조직의 역할을 구분할 수 있는 측정 항목을 '기술보안역량 및 기술유출실태 조사표'에서 선정하였다.

4. 연구 분석 및 결과

4.1 표본의 특성

기밀유출 사고 대응역량 조사 대상 기업의 표본 특성을 알아보기 위하여 빈도 분석을 한 결과를 <표 3>에 제시하였다. 표본의 특성은 기업 규모, 사업 유형, 지역을 조사하였으며 특징적인 것은 기업 규모에서 중소기업이 702개(46.8%)로 제일 높았으며, 사업 유형으로는 기계소재 411개(27.4%)가 가장 많았다. 지역으로는 경기 552개(34.8%)를 차지하였다.

〈표 3〉 표본의 특성

구 분		빈도수	구성비율(%)
기업 규모	대기업	150	10.0
	벤처기업	648	43.2
	중소기업	702	46.8
사업 유형	기계소재	411	27.4
	전기전자	262	17.5
	정보통신	245	16.3
	화학섬유	251	16.7
	기타	331	22.1
지역	경기	552	34.8
	서울	430	28.7
	영남	290	19.3
	충청	156	10.4
	기타	102	6.8

4.2 신뢰성 및 타당성 분석

본 연구의 신뢰성과 타당성을 검증하기 위해서 Cronbach's α계수를 사용하였다. 각 문항 점수는 조사 결과에 나타난 문항별 가중치 점수를 이용하였다. 신뢰도 검증은 일반적인 연구에서 계수 값이 0.6 이상이면 측정 도구의 신뢰성에 문제가 없는 것으로 보고 있으며[41], <표 4>에 나타난 바와 같이 대부분의 변수가 높은 신뢰도를 보였다. 그리고 분석 표본의 타당성을 검증하고 자료에 대한 가치 있는 정보를 얻기 위해 요인분석을 하였다. 즉, 단일 차원성을 확보하기 위해 구성 단위별로 주성분 분석(principal component analysis)을 실시한 후 요인 적재량(factor loading)을 단순화시키기 위해 직각 회전 방식(orthogonal rotation) 중에서 베리맥스(varimax) 방식을 적용해 요인 분석을 실시하였다. 주성분 분석은 관찰된 여러 변수들 중 서로 연관성이 있는 변수들끼리 선형 결합 형태로 묶어 몇 개의 잠재 변수로 변수를 축약하는 것을 말하며 베리맥스 방법은 Kaiser가 제안한 것으로 요인 행렬의 각 열 내의 부하 제곱의 분산 합을 이용하여 분산을 최대화시키는 회전 방법이다.

표본자료의 적합성을 나타내는 KMO(Kaiser-Meyer-Olkin) 검정은 요인분석을 위해 변수 간 상

〈표 4〉 변수의 타당성 및 신뢰도 분석 결과

요인	측정 항목	표준화 요인 적재량	공통성	신뢰도
물리적 보안	PHY1	.718	.631	.709
	PHY2	.688	.553	
	PHY3	.672	.499	
	PHY4	.579	.466	
기술적 보안	ITM1	.692	.645	.876
	ITM2	.758	.711	
	ITM3	.674	.567	
	ITM4	.685	.481	
	ITM5	.516	.435	
	ITM6	.609	.578	
	ITM7	.615	.473	
	ITM8	.638	.509	
관리적 보안	OPE1	.676	.522	.879
	OPE2	.662	.477	
	OPE3	.626	.470	
	OPE4	.646	.592	
	OPE5	.655	.487	
	OPE6	.518	.413	
	OPE7	.701	.558	
	OPE8	.680	.565	
	OPE9	.652	.488	
	OPE10	.654	.540	
보안사고 대응역량	PER1	.836	.698	.689
	PER2	.795	.632	
	PER3	.744	.553	

주) 요인추출방법 : 주성분분석.
회전방법 : 베리맥스(varimax) 방식.

관관계가 어느 정도 존재하고 있는가를 검증하는 것으로 0.5 이상이면 요인분석에서 적합하다. 본 연구에서는 물리적 보안 요인의 KMO 값은 0.746로 나타났고, 기술적 보안 요인의 KMO 값은 0.899로 나타났으며, 관리적 보안 요인의 KMO 값은 0.903 및 보안사고 대응역량의 KMO는 0.654로 나타났다. 각 변수의 공통성은 추출된 요인에 의해 설명되는 비율로서 일반적으로 공통성이 0.4 이하이면 낮다고 판정하여 요인분석에서 제외하게 되어 있으나 본 연구에서는 제외대상에 해당하는 변수 는 없었다. 나머지 측정치는 <표 4>에 제시하였다.

4.3 가설 검증

4.3.1 매개효과 검증

앞서 제시된 가설들을 검증하기 위해 기술적 보안과 보안사고 대응역량, 물리적 보안과 보안사고 대응역량에서 관리적 보안이 매개역할을 하는지를 알아보고자 한다. 따라서 산업 유형과 기업 규모를 통제 변수로, 관리적 보안을 매개 변수로, 보안사고 대응역량을 종속변수로 간주하여 회귀 분석을 이용한 매개 효과의 검증을 시행하였다. 매개효과 분석은 단계 1에서 독립변수와 매개변수와의 유의한 인과관계가 있어야 하며 단계 2에서 독립변수와 종속변수 간의 유의한 인과관계가 있어야 한다. 단계 3에서는 독립변수와 매개변수가 종속변수에 미치는 유의한 영향관계가 있어야 하며, 2단계에서 도출된 독립변수의 회귀계수 값은 제 3단계에서 도출된 독립변수의 회귀계수 값보다 커야한다[21, 29].

관리적 보안의 매개효과 분석 결과는 <표 5>에 제시하였다. 기술적 보안과 물리적 보안이 기업 관리적 보안에 중요하다는 가설을 검증하기 위해 회귀분석을 시행하였다.

구체적으로 기술적 보안이 보안사고 대응역량에 미치는 영향관계에서 관리적 보안의 매개 역할을 분석한 결과는 다음과 같다. 1단계 회귀계수는 .660으로 정(+)의 영향을 미치고 있고, 2단계에서는 .631, 3단계에서는 독립변수가 .329, 매개변수가 .458의 값을 나타내고 있다. 유의수준을 가늠할 수 있는 t값과 p값은 1단계, 2단계, 3단계 모두 유의한 결과를 보여주고 있다. 또한 2단계에서의 독립변수의 효과도 3단계에서의 독립변수 효과보다 크게 나타나고 있음을 알 수 있다. 설명력을 나타내는 R^2 값은 1단계에서는 44.8%의 설명력을 나타내고 있으며, 2단계에서는 41.1%, 그리고 3단계에서는 52.7%의 설명력을 제시하고 있다. 즉, 가설 H1

은 채택되었으며 기술적 보안이 보안사고 대응역량과의 직접적 관계보다 관리적 보안과의 관계가 더 높게 나타나고 있음을 알 수 있다. 이는 기술적 관리가 보안 사고를 방지할 수 있도록 관리적 보안에 영향을 제공하고 있는 것으로 풀이된다. 관리적 보안은 기술적 보안에 따라서 통제된 행동을 하게 되므로 보안사고 대응역량에 긍정적 영향을 미친다고 판단할 수 있다.

물리적 보안이 보안사고 대응역량에 미치는 영향관계에서 관리적 보안의 매개 역할을 분석한 결과는 다음과 같다. 1단계 회귀계수는 .530으로 정(+)의 영향을 미치고 있고, 2단계에서는 .503, 3단계에서는 독립변수가 .206, 매개변수가 .560의 값을 나타내고 있다. 기술적 보안과 마찬가지로 유의수준을 가늠할 수 있는 t값과 p값은 1단계, 2단계, 3단계 모두 유의한 결과를 보여주고 있다. 또한 2단계에서의 독립 변수의 효과도 3단계에서의 독립변수 효과보다 크게 나타나고 있다. 설명력을 나타내는 R^2 값은 1단계에서는 31.0%의 설명력을 나타내고 있으며, 2단계에서는 28.2%, 그리고 3단계에서는 49.8%의 설명력을 제시하고 있다. 즉, 가설 H2는 채택되었으며 물리적 보안이 보안사고 대응역량에 직접적 영향을 주기보다는 관리적 보안을 통해 효율적인 통제가 필요한 것으로 풀이된다. 기술적 보안도 관리적 보안에 따라서 통제된 행동을 하게 되므로 보안사고 대응역량에 긍정적 영향을 미친다.

한편, 보안과 관련된 관리적 보안을 수행하는데

〈표 5〉 기술적/물리적 보안과 보안사고 대응역량 간 관리적 보안 회귀분석 매개효과 결과

독립/매개/종속변수	매개효과 검정단계	표준화된 베타값	t값	p값	R^2
기술적 보안/ 관리적 보안/ 보안사고 대응역량	단계 1(기술적 보안 → 관리적 보안)	.660	32.947	.000*	.448
	단계 2(기술적 보안 → 대응역량)	.631	30.490	.000*	.411
	단계 3(기술적 보안 → 대응역량) 단계 3(관리적 보안 → 대응역량)	.329 .458	13.486 19.119	.000* .000*	.527
물리적 보안/ 관리적 보안/ 보안사고 대응역량	단계 1(물리적 보안 → 관리적 보안)	.530	23.891	.000*	.310
	단계 2(물리적 보안 → 대응역량)	.503	22.212	.000*	.282
	단계 3(물리적 보안 → 대응역량) 단계 3(관리적 보안 → 대응역량)	.206 .560	9.263 25.369	.000* .000*	.498

주) 통제변수 : 기업규모, 산업유형.
* $p < 0.001$.

〈표 6〉 관리적 보안과 보안 전담조직 구성 여부에 대한 회귀분석 조절효과 결과

단계	독립변수	R 제곱	R 제곱 변화량	Beta	F값	t값(p값)
1	관리적 보안	.464	.464	.681	1295.288**	35.990(.000)
2	관리적 보안 보안 전담조직 구성	.467	.003	.635 .073	655.777**	26.280(.000) 3.031(.002)
3	관리적 보안 보안 전담조직 구성 관리적 보안×보안 전담조직 구성	.471	.004	.525 .175 .335	443.957**	12.942(.000) 2.254(.024) 3.361(.001)

주) 종속변수 : 보안사고 대응역량.
* $p < 0.05$, ** $p < 0.001$.

있어 물리적 보안보다는 기술적 보안의 영향이 더 크게 나타났다. 이는 기업의 기밀문서 및 정보 교류를 IT와 네트워크 망을 통해 교환하고 있기 때문에 기술적 보안의 통제가 관리적 보안과 보안사고 대응역량에서 중요하게 나타났다고 판단할 수 있다. 따라서 기술적 보안과 관리적 보안을 통합 관리할 수 있는 역량이 필요하다.

4.3.2 보안 전담조직의 조절효과 검증

관리적 보안과 보안사고 대응역량 간 관계에서 보안 전담조직 구성 여부는 앞서 문헌 연구에서 설명하였듯이 보안 전담조직이 보안사고 대응역량 강화에 중요한 요소로 강조되고 있다. 따라서 관리적 보안과 보안사고 대응역량에서 “보안 전담조직 구성이 대응역량을 높일 것이다”에 대한 검정을 시행하였다. 이는 <표 6>에 제시하였다. ‘관리적 보안과 보안사고 대응역량 간 보안 전담 조직 여부에 따라 역량 효과가 다를 것이다’라는 가설을 검증하기 위하여 회귀분석을 통해 조절 효과를 분석하였다.

조절효과 분석은 단계 1에서 독립변수와 종속변수 간의 유의한 인과관계를 맺고 있어야 하며 단계 2에서 독립변수와 조절변수가 종속변수와의 유의한 인과관계가 있어야 한다. 또한 단계 3에서 독립변수와 조절변수, 상호작용 항(독립변수×조절변수)이 종속변수와 유의한 인과관계가 있어야 한다. 그리고 단계별 설명력(R^2)이 유의수준 하에서 유의하게 증가하였다면 조절효과가 있다고 해석될 수 있다[7].

검정 결과 R 제곱은 모형 1은 46.4%, 모형 2는 46.7%, 모형 3은 47.1%로 점점 더 증가하고 있는 것으로 나타났다. 유의확률 역시 $p < 0.05$ 이하로 나타나면서 조절효과가 있다고 해석할 수 있으며 가설 H3는 채택되었다. 최종적으로 보안전담조직 구성은 관리적 보안과 보안사고 대응역량 간의 영향관계에서 조절작용을 하는 것으로 나타났다. 이는 관리적 보안을 통제할 수 있는 전담조직 역량에 기인한 것으로 풀이된다. 즉, 기업의 보안전담조직이 보안사고 대응역량에서 피해 예방과 피해 발생 시 보안전담조직이 없는 기업보다 신속한 대처 역량을 갖출 수 있다.

보안 전담조직의 조절 효과에 대한 유의한 결과는 기업 보안역량을 강화하는데 긍정적인 효과를 가져다준다.

회귀분석 조절효과의 분석 결과는 보안 전담조직이 구성되어 있을수록 보안 피해를 예방할 수 있는 역량이 높다고 말할 수 있다. 이러한 결과에 따라서 추가 연구로 보안 전담 조직 구성 여부에 따라 어떠한 차이가 있는지를 확인하고자 한다. 즉, 기업의 보안 관리를 수행하고자 할 때 보안전담 조직 구성 여부에 따라서 보안 보안사고 대응역량이 차이가 난다고 볼 수 있기 때문에 추가적인 연구를 수행하여 검증하였다.

보안 전담조직 구성 여부에 따른 차이 검정 결

〈표 7〉 보안전담조직 구성 여부에 따른 보안역량 차이 분석 결과

구 분	평균		표준편차		t값	p값
	전담조직 미구성(n = 623)	전담조직 구성(n = 877)	전담조직 미구성	전담조직 구성		
대응역량	1.34	1.78	.34	.44	-21.526	.000*
기술적 보안	1.81	2.31	.42	.45	-21.834	.000*
물리적 보안	1.52	2.03	.50	.66	-17.005	.000*
관리적 보안	1.56	2.35	.44	.51	-31.685	.000*

주) * $p < 0.001$.

과는 <표 7>에 제시하였다. 보안 전담조직 구성에 따라 물리적 보안, 기술적 보안, 관리적 보안, 보안사고 대응역량에서 차이가 나타났다. 살펴보면 대응역량은 -21.526, 기술적 보안은 -21.834, 물리보안은 -17.005, 관리적 보안은 -31.685로 나타났다. 구체적으로 전담조직이 구성된 기업과 미 구성된 기업의 차이는 기술적 보안에서 가장 높게 차이가 나타났다. 보안 전담조직이 있는 기업이 전담 조직이 없는 기업보다 보안 피해대응역량이 높다.

한편, 보안사고 대응방안의 수에 대한 질문으로 총 6가지의 복수응답을 분석한 결과 전담 조직 구성 여부에 따라 대응방안 역량 수에서 차이가 발생한다는 것을 확인하였다. 피해발생 시 대응방안 질문으로는 '① 비상시 따라야 할 절차와 관련자의 책임 규정 ② 유관기관과의 연락체계 구성여부 ③ 필수업무 및 지원서비스를 대체장소로 이전하여 운영하기 위한 절차 ④ 정상적인 사업 활동으로 복귀하기 위한 원상복귀 절차 ⑤ 위기관리를 포함한 비상절차 및 프로세스에 대한 임직원 교육 ⑥ 시스템 오작동 시 시스템의 재시작 및 복구절차 준수'이다.

<표 8>에서 보듯이 보안사고 발생 시 대응방안의 수에 대해 전담조직이 미 구성된 조직은 대응방안이 없다는 빈도수가 308로 가장 높게 나타났으며 보안 전담조직이 없는 경우 보안사고 대응방안 역량이 0~2개 정도 내외로 보안 강화 역량이 부재하다는 것을 확인할 수 있다. 전담조직이 있는 기업은 2개 정도의 피해대응 역량 방안을 가지고 있는 기업이 가장 높게 나타났으며 보안사고 대응방안 역량이 1~3개 정도 내외로 보안사고 발생에 대비한 보안 대응방안의 역량을 갖추고 있다고 응답하여 전담조직 구성 유무에 따른 보안사고 대응방안의 차이를 확인하였다.

따라서 체계적인 관리적 보안을 위해서는 보안 전담조직의 구성이 중요하고, 보안전담조직의 유무에 따른 대응방안 개수의 차이는 기업의 보안사고 대응 수준을 나타낸다는 점에서 기업이 보안전담조직을 구성해야 한다는 점을 <표 8>을 통해 중요성을 강조할 수 있다.

〈표 8〉 보안사고 대응방안 수에 대한 빈도분석

대응방안 갯수	전담조직 구성				계
	미구성		구성		
	기업수	순위	기업수	순위	
0	**308**	**1**	123	4	431
1	**151**	**2**	**150**	**2**	301
2	**84**	**3**	**183**	**1**	267
3	42	4	**140**	**3**	182
4	20	5	104	6	124
5	8	7	66	7	74
6	10	6	111	5	121
계	**623**		**877**		1500

5. 결 론

5.1 연구 결론

본 연구의 출발점은 기업의 관리적 보안 관점에서 관련된 연구가 부재함에 따라, 관리적 보안의 중요성을 강조하고자 시작하였다. 대다수의 기업은 가시적으로 검증할 수 있는 물리적 보안과 기술적 보안에 상당한 투자를 하고 있지만 체계적인 보안 관리적 보안의 부재에 인하여 보안사고 유출이 발생할 수 있다는 점을 간과하고 있었다. 따라서 물리적 보안, 기술적 보안이 관리적 보안에 영향을 미치며 관리적 보안이 보안사고 대응역량에 어떤 영향을 미치는지를 실증 분석하여 관리적 보안의 중요성을 강조하였다. 연구 결과에서도 보안사고 및 기밀 유출을 방지하기 위해서는 관리적 보안의 중요성은 강조될 수밖에 없다는 점이 밝혀졌으며, 보안 전담조직이 구성될수록 보안사고 대응역량을 강화할 수 있음을 알 수 있었고 이러한 인식을 심어주고자 하였다. 이에 따른 실증연구 결과를 요약하면 다음과 같다.

첫째, 물리적 보안과 기술적 보안이 보안사고 대응역량에 직접 영향을 제공하기보다는 관리적

보안을 통해 보안사고 대응역량이 강조됨을 밝혀냈다. 물리적 보안과 기술적 보안은 기업의 정책, 제도, 자산운영, 인적자원 관리에 따라 물리적 보안과 기술적 보안이 보안사고 대응역량에 긍정적 효과를 제공할 수 있다는 결과이다.

둘째, 관리적 보안을 체계적이고 규범화된 프로세스로 운영하기 위해서는 보안 전담조직이 필요하다고 나타났다. 보안 전담조직은 보안사고 발생 전후로 기밀 유출 예방 및 사고 후 신속한 응급처치에 일련의 프로세스로 대응할 수 있다고 밝혀졌다. 따라서 정보자산의 보안사고를 방지하기 위한 교육 및 정책 수립, 감사 역할을 수행하게 되면서 내부적/외부적으로 발생할 수 있는 보안 사고를 감독 및 감시할 수 역할자의 역할을 할 수 있을 것으로 기대된다.

끝으로, 보안 전담조직이 구성된 기업이 구성되어 있지 않은 기업보다 보안사고 대응역량, 기술적 보안, 물리적 보안, 관리적 보안에서 역량이 높다는 차이를 밝혀냈다.

5.2 연구 의의

본 연구는 기업들의 보안 투자가 보안사고 대응역량에 미치는 연구를 통하여 이론적 부분과 실무적인 부분으로 다음과 같은 의의를 가진다.

본 연구를 통해 기대할 수 있는 이론적 성과로는 기존의 보안 연구들이 보안 시스템 관련 구축의 기술 관련 연구 및 내부 감시, 보안 행위의도 등과 관련된 관리 관련 연구가 중점을 이루고 있었다. 반면 본 연구는 보안 조직 운영 관점에서 물리적, 기술적, 관리적 보안 유형의 관계를 제공하여 이론적 기반을 마련하였다.

첫째, 인적보안, 정보자산, 정책과 같은 무형적 투자의 중요성을 투자 의사결정 이론을 통해서 설명하였으며 관리적 보안이 보안사고 대응역량에 중요한 점임을 규명하였다. 따라서 본 연구는 이를 살펴봄으로써 관리적 보안과 보안사고 대응역량과 관련된 연구에 이바지할 것으로 기대된다.

둘째, 보안사고 대응역량에 더욱 큰 효과를 발휘하기 위해서는 3가지 보안 요소인 기술적, 물리적, 관리적 보안이 함께 투자될 수 있도록 고려해야 한다는 점을 사회기술시스템이론과 실증적 검증을 통해 설명하였다. 따라서 보안과 관련된 3가지 보안 요소에 관련된 보안 투자 의사결정 연구에도 도움을 줄 것으로 기대된다.

셋째, 관리적 보안 및 보안 전담조직이 구성되어 있을 때, 보안사고 대응역량에 긍정적인 영향을 줄 것이라는 점을 규명하였다. 또한 보안 전담조직이 미 구성된 기업에 있어서 보안사고 대응방안 수가 미흡하다는 것은 기업의 피해가 기업 이해관계자에게 부정적 영향을 미칠 수 있다고 볼 수 있다. 따라서 보안사고 대응역량 방안으로서 논의된 기술유출 및 침해사고, 기술유출 방지 관련 주요 법규 및 제도 인지, 스마트폰 관련 기술유출 대응방안은 사회적 이해관계자의 피해를 최소화하기 위한 대응책으로 설명할 수 있다. 이는 CSR에서 기업의 사회적 책임 강조를 설명하였듯이 기업의 보안사고가 이해관계자의 재무적, 비재무적 피해로 영향을 미칠 수 있다는 점을 의미한다. 이러한 연구 결과는 사회적 책임과 기업 보안사고 피해와 관련된 연구에 도움을 줄 것으로 기대된다.

본 연구를 통해 기술적 보안, 물리적 보안, 관리적 보안과 보안사고 대응역량과의 관계 연구에 대한 실증적인 검증을 통하여 실무적 의의를 찾았다.

첫째, 물리적, 기술적 보안 요소에서 무형적 투자로 분류되는 관리적 보안이 기업의 보안사고 대응역량을 향상할 수 있다는 점을 인지시켰다는데 실무적 의의가 있다.

둘째, 보안 전담조직이 존재하는 기업이 보안사고 대응역량에 높은 효과를 발휘하여 보안 피해사고를 예방할 수 있다는 점을 인지시켰다는데 실무적 의의가 있다.

셋째, 기술적 보안이 물리적 보안보다 중요한 점은 언론 매체에서 언급하였듯이 정보시스템 또는 이동저장장치를 통한 보안사고의 빈도수가 높다는 점에서 기업들의 물리적 보안 투자보다 기술

적 보안과 관리적 보안의 투자가 중요하다는 점을 인지시켰다는 점에서 실무적 의의를 찾을 수 있다.

참 고 문 헌

[1] 미래포럼, "정보보호의 다음 단계는?", 「전자신문」, 2011.

[2] 중소기업청, "보안 컨설턴트용 실무가이드북", 「중소기업기술정보진흥원」, 2007.

[3] 한국인터넷진흥원, "2011년 정보보호 실태조사 : 기업편", 2012.

[4] 한국정보보호진흥원, "정보보호 관리체계 관리과정 가이드", 2004.

[5] Anderson E. E. and C. Joobin, "Enterprise information security strategies", *Computers and Security*, Vol.27, No.1/2,(2008), pp.22-29.

[6] Barnea, A. and A, Rubin, "Corporate Social Responsibility as a Conflict Between Shareholders", *Journal of Business Ethics*, Vol. 97, No.1(2010), pp.71-86.

[7] Baron, R. M. and D. A. Kenny, "The moderator variable distintion in social psychological research : Conceptual, strategic, and statistical considerations", *Journal of Personality and Social Psychology*, Vol.51(1986), pp.1173-1182.

[8] Baskerville and R. M. Siponen, "An information security meta-policy for emergent organizations", *Journal of Enterprise Information Management*, Vol.15, No.5/6(2002), pp.337-346.

[9] Bharadwaj, A. and M. Keil, "The Effect of Information Technology Failures on the Market Value of Firms : An Empirical Examination", *The Journal of Strategic Information Systems*, Vol.18, No.2(2001).

[10] Boehmer, W., "Appraisal of the eectiveness and eciency of an Information Security Management System based on ISO 27001", *Emerging Security Information, Systems and Technologies*, SECURWARE, Second International Conference on, (2008), pp.224-231.

[11] Bostrom, R. P. and J. S. Heinen, "MIS Problems and Failures : A Socio-Technical Perspective", *MIS Quarterly*, Vol.1, No.4(1977), pp.11-28.

[12] Bowen, H., Social Responsibilities of the Businessman, New York, *Haper and Row*, 1953.

[13] Caralli, R. A., "Managing for Enterprise Security", *Carnegie Mellon Software Engineering Institute*, 2004.

[14] Caylor, J., M. E. Withman, P. Fendler, and D. Baker, "Rebuilding Human Firewall", *ACM*, InfoSecCD Proceedings of the 2nd annual conference on Information security curriculum development, (2005), p.1.

[15] Clegg, C. W., "Sociotechnical Principles for Systems Design", *Applied Ergonomics*, Vol.31(2000), pp.463-477.

[16] CONsortium of CERT, "CONCERT SECURITY FORECAST 2012", 2012.

[17] Cyert, R. M. and J. G. March, "A behavioral theory of organizational objectives", *Modern Organization Theory*, (1996), pp.138-148.

[18] Deloitte, "Global Security Survey", 2008.

[19] Department of the Army, "Information Security Program", Vol.1, No.5200.01(2012).

[20] Dhillon, G. and J. Backhouse, "Current directions in IS security research : towards socio-organizational perspectives", *Information Systems Journal*, Vol.11, No.2(2001), pp.127-153.

[21] Dyne, L. V., J. W. Graham, and R. M. Dienesch, "Organizational Citizenship Behavior

: Construct Redefinition, Measurement, and Validation", *The Academy of Management Journal*, Vol.37, No.4(1994), pp.765-802.

[22] Ettredge, M. and V. Richardson, "Assessing the Risk of in E commerce", *System Sciences*, HICSS. Proceedings of the 35th Annual Hawaii International Conference on, (2002), p.11.

[23] Fred, C., "Managing network security-Part 5 : Risk management or risk analysis", *Network Security*, Vol.1997, No.4(1997), pp.15-19.

[24] Gerber, M. and V. R. Solms, "From risk analysis to security requirements", *Computers and Security*, Vol.20, No.7(2001), pp. 577-584.

[25] Goel, S. and S. I. N. Chengalur, "Metrics for Characterizing the Form of Security Policies", *Journal of Strategic Information Systems*, Vol.19(2010), pp.281-295.

[26] Goh, R., The Importance of the Human Element, *Doctorial Dissertation*, 2003.

[27] Gordon, L. A. and M. P. Loeb, "The economics of information security investment", *ACM Transactions on Information and System Security*, Vol.5, No.4(2002), pp.438-457.

[28] Hagen, J. M. and E. Albrechtsen, "Implementation and effectiveness of organizational information security measures", *Information Management and Computer Security*, Vol. 16, No.4(2008).

[29] Hair, J. F., C. B. William, B. J. Babin, and R. E. Anderson, Multivariate Data Analysis (7th Edition), *PEARSON*, 2009.

[30] IDC, "2007 Global Security Survey", 2008.

[31] Karyda, M., E. Kiountouzis, and S. Kokolakis, "Information systems security policies : acontextual perspective", *Computers and Security*, Vol.24, No.3(2005), pp.246-260.

[32] Kotulic, A. G. and J. G. Clark, "Why there aren't more information security research studies", *Information and Management*, Vol. 41, No.5(2004), pp.597-607.

[33] Land, F. F., Evaluation in a Socio-Technical Context, in Basskerville, R., Stage, J., and DeGross, J. I., Organizational and Social Perspectives on Information Technology, Boston, *Kluwer Academic Publishers*, (2000), pp.115-126.

[34] Leavitt, H. J., Applied Organisational Change in industry : Structural, Technological and Humanistic Approaches, Carnegie Institute of Technology, *Graduate School of Industrial Administration*, 1965.

[35] Maignan, I. and O. C. Ferrell, "Corporate Social Responsibility and Marketing : An Integrative Framework", *Journal of the Academy of Marketing Science*, Vol.32(2004), pp.3-19.

[36] Mattord, H. and M. Whitman, "Regulatory Compliance in Information Technology and Information Security", *AMCIS* Proceedings, (2007), p.357.

[37] Michael, R., Grimaila, and L. W. Fortson, "Towards an Information Asset-Based Defensive Cyber Damage Assessment Process", *Computational Intelligence in Security and Defense Applications*, CISDA IEE, (2007), pp.203-212.

[38] Mumford, E., "A socio-technical approach to systems design", *Requirements Engineering*, (2000), pp.59-77.

[39] NIST, Information Security Handbook : A Guide for Managers, 2006.

[40] Nosworthy, J. D., "Implementing informa-

tion security in the 21 super(st) Century-do you have the balancing factors?", *Computers and Security*, Vol.19, No.4(2000), pp. 337-347.

[41] Nunnally. J. C., Psychometric Theory 2th Edition, *Mcgraw Hill*, NewYork, 1978.

[42] Porter, M. E. and M. R. Kramer, "Creating Shared Value", *Harvard Business Review*, 2011.

[43] Post, G. and A. Kagan, "Management trade-offs in anti-virus strategies", *Information and Management*, Vol.37(2000), pp.13-24.

[44] Pugh, D. S. and D. J. Hickson, Writers on Organizations, *Beverly Hills*, Cal. : SAGE, 2007.

[45] Shin, S. C. and H. J. Wen, "Building E-enterprise security : a business view", *Information Systems Security*, Vol.13, No.4(2003), pp.44-56.

[46] Simon, H. A., "Rationality as Process and as Product of Thought", *The American Economic Review*, apers and Proceedings of the Ninetieth Annual Meeting of the American Economic Association, Vol.68, No.2 (1978), pp.1-16.

[47] Solms, B., "Corporate Governance and Information Security", *Computers and Security*, Vol.20(2001), pp.215-218.

[48] Solms, B., "Information Security-The Fourth Wave?", *Computers and Security*, Vol.25 (2006), pp.165-168.

[49] Stoneburner, G., A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems", *NIST special publication*, 2002.

[50] Trist, E., "The evolution of socio-technical systems", a conceptual framework and an action research program, *Occasional paper*, No.2(1981).

[51] Yeh, Q. J. and A. J. T. Chang, "Threats and countermeasures for information system security : a cross-industry study", *Information and Management*, Vol.44, No.5(2007), pp.480-491.

◈ 저 자 소 개 ◈

이 정 환 (wcrtv.jhl@gmail.com)

한국외국어대학교 경영정보 전공으로 경영학 석사 과정으로 재학 중이다. 주요 관심분야로 IT Alignment, Information Security, E-Business Strategy, 상생 경영 등이다. KISA 사전점검 경제적 효과분석 프로젝트 팀에 참여 수행한 바 있다.

정 병 호 (jung.hmis@gmail.com)

한국외국어대학교에서 경영정보 전공으로 경영학 석사학위를 취득하였으며 현재 동 대학에서 경영정보 박사 과정으로 재학 중이다. 주요 관심분야로 정보 보안, e비즈니스 전략, IT 투자 평가, IT 생산성, IT 아웃소싱, 상생 경영 등이다. SKT Business Partnership Happiness의(파트너 상생경영 프로젝트) 프로젝트 팀에 참여 수행한 바 있다.

김 병 초 (bckim@hufs.ac.kr)

영화회계법인(Ernst and Young)에서 공인회계사를 거쳐 미국 Purdue University에서 경영정보학으로 박사학위를 받았다. 현재 한국외국어대학교 경영정보학과 교수로 재직 중이며 최근 진행하고 있는 연구 분야는 기업 IT 투자 성과평가와 가치평가, 망중립성(Network Neutrality), 정보보호관리, 기업윤리와 사회적 책임 등이다.