정보보안관리에 영향을 미치는 기업환경요소와 규제자 영향의 조절효과*

김상현** · 김근아**†

A Firm's Environmental Determinants Impacting the Information Security Management and the Moderating Effects of Regulatory Influence

Sanghyun Kim** · Geuna Kim**

■ Abstract ■

*According to the higher dependence of contemporary firms on data digitalization and the information technology, the role and importance of Information Security Management (ISM) is getting higher. Thus, there is a need to arrange proper procedure and a series of device within the organization in order to reduce diverse security risks, which take place from the inside and the outside of firm. In other words, prior examination for reinforcing recognition of ISM, and of a systematic performance method in the refined form is important. This study investigate the key variables influencing the ISM. Thus, this study suggests firm environmental factors that include four exogenous variables, market volatility, task interdependence, perceived benefits, and coordination mechanism affecting awareness of ISM. In addition, it proposes a concept of the ISM process with awareness, development, and performance, and examines the moderating effects of regulatory influence. The research model was tested by using Structural Equation Modeling, via SmartPLS 2.0 analysis on a sample collected from 186 employees in various industries. The research results provide the evidence that supports the tested hypotheses except significance of coordination mechanism. The implications of the findings suggest a new theoretical framework of the ISM and offers important solutions for the practical application guidelines.

Keyword : Information Security Management(ISM), Firm Environmental Factors, Regulatory Influence, ISM Process

논문접수일 : 2012년 07월 13일 논문게재확정일 : 2012년 08월 13일
논문수정일(1차 : 2012년 08월 08일)
* 이 논문은 2012학년도 경북대학교 학술연구비에 의하여 연구되었음.
** 경북대학교 경영학부
† 교신저자

1. 서 론

최근 기업들의 정보시스템 확대 및 네트워크 사용의 비중이 증가됨에 따라 정보보안관리(Information Security Management : ISM)의 중요성이 대두되고 있다[46]. 더욱이 급속한 변화로 인해 개인 및 기업 등의 정보자산에 대한 위협 및 취약성을 어느 때 보다 매우 심각한 문제로 인식하게 되었다[20]. 그 중 기업의 보안 실패는 피해를 입은 기업에 막대한 비용을 초래할 뿐만 아니라 신뢰와 명성에도 심각한 손상을 일으키고 심지어 파산에까지 이르게 하는 등 기업경영의 걸림돌이 되고 있다[32]. 이에 대한 적절한 정보보안관리 프로세스 개선활동과 이를 위한 기업 경쟁력을 강화하기 위한 수단으로 정보보안 관리체계 구축 및 운용에 지속적인 노력을 기울이고 있다. 따라서 정보보안관리는 기업 환경의 주요한 과제로 제기되고 있다[11, 23].

정보보안관리의 목표는 불확실한 사건들로부터의 보안 침해를 예방하고 통제함으로써 조직의 손상을 최소화하는 것이다[27]. 즉, 기업은 정보시스템 및 자산에 손해를 끼치는 위협의 원천들(예 : 자연재해, 의도적 · 비의도적 위협, 시스템 결함)로부터 관리적, 기술적, 물리적 보안의 관리를 통해 보안에 대한 성공적인 설명이 가능하다[10]. 한편, 기업들은 보안관리를 위해 기술기반의 솔루션에 상당한 투자를 하지만 이러한 물리적, 기술적 의존은 정보보안과 관련된 위험요소들을 제거하기에는 충분하지 않다[25]. 이전까지의 보안관리의 관심이 기술적 방법에 집중되어온 반면 정보의 이동성(mobility)이 증가함에 따라 관리적 측면에 대한 접근이 요구되고 있다[7]. 즉, 정보관리의 실패는 기술적 결함의 문제라기보다는 사회 및 경제적 동기에 의존하고, 조직 내 문화의 문제라는 인식의 전환이 필요하다[42].

하지만 이전의 정보보안관리에 관한 연구들은 조직이 보안성과를 얼마나 달성하였는지에 대한 효과적인 측정, 구체적 평가기준, 혹은 방법의 구축 및 실행은 미비하다. 기존 연구 결과에서 보여주는 단편적인 보안솔루션 도입이나 관련 정책 및 지침만으로는 기업 내의 성공적인 정보보안관리의 실현 가능성을 예측하기에는 역부족이라고 할 수 있다[48]. 즉, 구축된 기업의 보안체계는 형식적인 활동에 그치고 보안관리와 보안통제는 무너질 수 밖에 없다. 따라서 보안관리에 직접적인 원인이 되는 요인들에 대한 철저한 사전 분석과 지속족인 모니터링, 그리고 의식 수준 향상 등 다양한 수단과 도구를 적용한 적절한 예방책이 시행되어야만 하는 것이다[40]. 특히, 기업의 정보보안관리에 대한 필요성이 부각되고 있는 현시점에서 전체적인 조직의 유효성에 영향을 미칠 수 있는 보안 솔루션 조정에 대한 구체적 이해가 요구된다.

따라서 본 연구는 정보보안관리 구축으로 인한 기업에 미치는 가시적 효과의 측정을 돕고, 보안과제의 단순한 인식만으로는 예방책이 될 수 없을 뿐더러 기업의 이에 대한 실질적인 실행이 동반되어야만 그 효과를 측정할 수 있음을 실증적으로 증명하고자 한다. 또한, 기업의 보안관리에 대한 역할과 책임, 해결이 필수적이라는 사실을 강조하고 보안관리에 대한 절차 및 주체를 정의하고자 하였다. 이에 본 연구는 정보보안관리에 영향을 미치는 요인으로 기업환경특성을 고려한 총 4가지의 변수(시장불안정성, 업무 상호의존성, 보안관리 이점, 협력체계구축)와 규제자 영향의 조절효과, 즉 외부의 강압적 압력으로 인한 효과적인 보안관리의 설계를 주장하였다. 뿐만 아니라 정보보안관리 프로세스 개념(인식, 강화, 성과)을 적용하여 기업의 현 보안상태를 점검하고 내부 프로세스를 평가하고자 하였다. 즉, 본 연구는 정보보안관리 노력의 방향성과 성과향상을 찾기 위한 기준을 제시하고, 정보보안관리에 대한 기업의 인식제고 및 의사결정에 대한 이론적 바탕이 될 수 있다.

2. 문헌 연구

정보보안이란 조직 내 보호가 필요한 모든 정보자산을 유지 및 관리하기 위한 일련의 행위를 의미한다[16]. 이와 같은 정보보안에 대한 보편적 정의

는 조직의 정보자산을 보호하기 위한 제반 제도 및 도구에 의해 대책이 실현되며, 활동의 주체와 중심에는 사람이 존재한다[5]. Keller et al.[29]은 정보보안은 조직의 관찰이나 측정으로부터 수집된 자료들을 바탕으로 현실의 문제에 적용시킬 수 있도록 체계적으로 분석 및 정리된 정보들을 계속적으로 지켜나가는 과정이라고 정의하였다. 또한, Yeh and Chang [45]은 정보보안을 통해 조직에서 불가피하게 발생될 수 있는 보안사고를 미연에 방지하여 비즈니스의 지속성을 보장하고 그 피해 규모를 최소화시킬 수 있다고 주장하였다. 즉, 정보보안은 보호되어야 할 조직 내 모든 정보를 조직의 요구에 따라 안전한 환경에서 안전한 상태로 관리하는 일련의 보안대책이라고 요약할 수 있다[46].

또한, 정보보안관리는 인적요소에 의한 정보 및 시스템이 제공하는 자료들에 대한 적절한 수준의 보안을 유지하는 과정으로 일반적인 관리주기를 따른다[40]. 즉, 기업 내 중요 자산과 이에 대한 위험의 존재 여부를 조사하고 만약 어떠한 위험이 발견된다면 대책을 강구하고 효율적으로 시행하는 등 모든 절차들을 보안관리라고 볼 수 있다. von Solms and von Solms[44]는 정보보안관리의 목표는 기업의 목적 달성을 위해 필요한 조직의 프로세스 및 협업관계를 지속하기 위한 제반 보안활동이라 하였으며, 위험분석, 정책, 준수, 통제를 관리의 기본적 원칙으로 제시하였다. Straub and Welke[41]는 보안관리에 대해 기업의 이윤을 돕는 경쟁력 강화 차원에서 위험 중심의 관리로 보았으며, 조직 내 전략과 정책의 결정을 지지하기 위해서는 첫째, 정보보안에 대한 문제와 필요성의 제기, 둘째, 위협의 식별, 그 크기와 빈도의 정확한 분석, 셋째, 보안관리를 위한 표준안 혹은 대안의 일반화 넷째, 계획의 결정 및 통합, 다섯째, 실질적 구현, 이와 같은 보안관리 단계와 피드백 루프(feedback loop)로 가능하다고 하였다. 특히, 관리의 효과를 위해서는 정보보안에 대한 인지수준 평가가 필요하다고 주장하였다.

보안관리에 대한 몇몇 실증연구들에서는 정보보안관리의 접근은 기업의 잠재된 변수들에 의해 그들의 경영 및 의사결정이 좌우될 수 있다고 하였다[33]. 즉, 기업 자산에 대한 공격과 방해를 발견하고 축소화하기 위해서는 세부적 검증 및 평가, 실증의 노력이 지속적으로 필요하다고 주장한다. 예를 들면, Hsu et al.[25]은 최근 기업과 공공기관의 정보노출사고가 급증하고 이에 대한 피해가 지속됨에 따라 조직 내 동료들의 관심과 더불어 관련법의 개정 등 기업의 관리와 사업자의 보안관리의 의무를 강제하기 위한 감독기관의 규제가 시행되어야 한다고 주장하였다. 이는 곧 정보관리에 대한 해당 기업의 책임과 의무를 크게 증가시키는 관리모형의 개발을 통해 기업의 정보보안관리를 위한 진단도구를 제시하고 있다. 한편, Babatunde and Selamat[5]는 정보보안관리에 대한 영향요인으로 기술 수준, 정보보안 정책, 정보보안 인식의 유의성을 조사하였다. 그들은 정보보안관리를 정확하게 평가하고 이를 토대로 개선방향을 제시함으로써 최적화된 보안관리체계의 수립 및 운영을 지원할 수 있는 개념적 모델을 제안하였다. 즉, 정보보안관리의 현실적 설명은 종업원들의 적극적인 참여와 의식으로부터 도출될 수 있다고 주장하였다. 또한, Chang and Ho [11]는 기업의 외부 비즈니스 환경(IT 능력, 환경 불확실성, 산업 유형, 기업 규모)을 우선적으로 고려한 정보관리에 대한 수준 평가 및 관련 평가를 통한 정보관리의 구현을 분석하였다. 이 연구에서는 경영성과 기여도 및 기업 전사적 차원에서 정보관리의 전략 수립을 위한 가이드라인을 제시하였는데, 기업의 보안기능을 강화시키기 위한 기본적 전제는 내부의 전략적 대처와 외부의 정확한 형태 파악에 의해서라고 하였다.

정보보안관리의 필요성이 제기되는 가장 큰 이유는 기업이 정보시스템과 네트워크로 구성된 조직의 정보자산을 활용하고 있는 한 정보보안에 대한 위험에 항상 노출되어 있고, 이러한 위험인자들을 모두 제거할 수 없을 뿐더러 미래의 모든 위협을 막기에는 엄연한 한계가 있을 수밖에 없기 때문이다[40, 41]. 또한, 이미 많은 기업들이 보안에 대한 어느 정도의 견제 장치 및 조치를 구현하고 있지만 보

안관리를 진단하기 위한 전제로는 충분하지 않다[26]. 즉, 기술적 수정에 과도하게 의존하는 대신 조직이 경계할 수 있는 적절한 규제 항목과 인식노력이 중요하다. 이에 Boss et al.[8]은 정보보안은 물리적 혹은 기술적 관리로부터 100% 완벽한 방어가 불가능할 뿐더러 절대적인 안전한 시스템의 구축은 존재할 수 없기 때문에 사람에 의한 끊임없는 관리가 필요하다고 주장하였다. 또한, Kankanhalli et al.[27]은 보안문제의 근본적 해결은 기술적, 물리적 보안의 측면과 나아가 문제를 직접적으로 대하는 행위 주체인 종업원에게 집중된 보안투자가 함께 유지될 때 현재의 보안 약점을 현저하게 줄일 수 있다고 하였다. 즉, 종업원들의 정보보안의 무관심과 무지, 혹은 무시 등에 의해 조직 전반의 평가가 절하될 수 있다고 강조하였다.

이 밖에도 보안에 관한 선행연구들은 기술적, 물리적 보안 설계 및 구축[32], 정보시스템 보안을 위한 투자의 효과 및 투자 결정[23], 정보보안지표 개발 및 계량화 연구[7], 정보보안정책의 역할 및 성숙도[8], 정보보안 및 위험 관리[40] 등과 같이 다양한 관점에서 정보보안의 필요성을 이해하게 해준다. 하지만 정보보안관리 및 요인에 관한 연구들은 프레임워크 중심의 연구에 한정하였기 때문에 발전된 모형의 제시와 요인들 간의 구조적 관계 해석에는 많은 제약이 뒤따른다. 또한, 정보보안관리의 연구가 시도되어 왔음에도 불구하고 기업이 이를 효과적으로 실천하고 설계하기에는 안정된 해결책이라고 할 수 없다. 왜냐하면 일련의 정책들을 실행하기 위한 중간단계로의 설명에 지나지 않고 기업의 보안 솔루션에 대한 합의점을 찾기에는 이론적 연구가 매우 한정되어 있기 때문이다. 따라서 기업의 실제적 보안관리의 노력으로 기업 전반의 영리를 추구하기 위해서는 당면한 문제에 대한 바람직한 시각과 해당 기업이 수용할 수 있는 허용 범위안의 보안관리 측정이 필요하다. 따라서 본 연구는 정보보안관리에 대한 기업 환경의 고유 특성을 반영한 실증적 검증을 통해 기존연구들의 한계점을 보완하고자 한다.

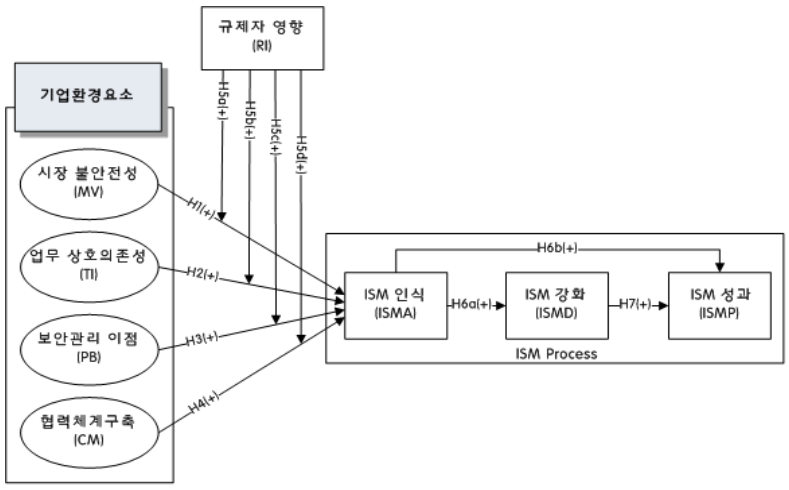
3. 연구모형 및 가설설정

3.1 연구모형

본 연구는 정보보안관리의 본질적 이해와 실효성을 강구하고 실현될 수 있는 제반사항들을 제시함으로써 기업의 정보보안 대책을 수립 및 적용하고자 하였다. 이는 기업의 정보보안을 현실적으로 관리하기 위한 동기를 찾고, 주요 연구질의인 '기업은 왜 정보보안관리를 위한 노력을 하는가?'에 대한 해답을 제공하는데 도움이 될 수 있다. 이와 같은 연구목적을 달성하기 위해 정보보안관리에 중요한 역할을 하는 기업환경요소를 제시하여 보안노력에 대한 잠재적 동기와 추진 효력을 결정할 수 있는 변수들(시장 불안정성, 업무 상호의존성, 보안관리 이점, 협력체계 구축)을 살펴보았다. 또한, 기업 외부의 정책적 및 사회적 제도의 의미의 중요성을 강조하고자 규제자 영향의 조절효과를 제안하였다. 나아가 효과적인 보안관리 과정을 설득하기 위한 단계적 접근(인식, 강화, 성과)을 포함시킴으로써 본 연구의 차별화를 확보하였다. [그림 1]은 본 연구에서 제안한 연구모형과 가설을 보여주고 있다.

3.2 가설설정

시장 불안정성은 산업 내 존재하는 시장의 변동성 및 기업에 가해지는 시장의 힘을 의미한다. 기업은 그들의 경영 및 업무 환경을 새롭게 구성하는데 있어 외부 시장의 압력을 고려한다[21]. Kearns and Lederer[28]는 조직변화 이유 중 하나가 글로벌 경쟁, 새로운 시장의 기회, 그리고 구성원의 니즈(needs)의 변화를 반영하는 시장의 힘에 의해서라고 주장하였다. 또한, Chang and Ho[11]은 정보보안관리의 기업의 재무적 및 비재무적, 손실과 이익의 측정에 있어서 외부 환경의 불확실 정도는 유의한 영향을 미친다고 제시하였다. 즉, 기존 연구들은 조직이 수행하고자 하는 기술 및 관리에 대해서 그들의 외부 지표에 의해 통제될 수 있음을 보고하고 있다[13, 25].



MV: Market Volatility, TI: Task Interdependence, PB: Perceived Benefits, CM: Coordination Mechanism, RI: Regulatory Influence, ISMA: ISM Awareness, ISMD: ISM Development, ISMP: ISM Performance

[그림 1] 연구모형 및 가설

다음으로 업무 상호의존성은 기업 내 업무의 관련성 및 자원 의존의 정도를 의미한다[39]. 많은 정보기술 분야의 연구에 따르면 조직 내 업무간의 의존도가 높을수록 많은 갈등이 발생될 수 있지만 이로 인해 더욱 혁신과 개선된 프로세스를 추구한다고 주장한다[38]. Sharma and Yetton[38] 독립적인 개별에 의해서는 지속적이고 일관된 조직 관리가 불가능하기 때문에 효과적인 조직 내 모델링을 구축하기 위해서는 상호 의존적일 수밖에 없다고 하였다. 즉, 조직 간의 업무에 대한 상호 의존성이 높을수록 많은 장벽에 부딪히지만 이러한 기존의 부정적 영향들을 제거하기 위해서는 새로운 프로세스의 지침과 개발이 불가피하다고 할 수 있다[9]. 뿐만 아니라 Guo et al.[22]은 조직의 업무성과와의 연계가 높을수록 조직의 자원 공유 및 보호를 위한 보안관리의 철저한 설계와 노력이 필요하다고 주장하였다.

보안관리 이점은 정보보안관리로부터 얻을 수 있는 상대적인 유·무형의 이익을 의미한다. 이는 기존의 연구에서 언급하고 있는 상대적 이점의 개념과 유사하다[31]. 조직은 새로운 프로세스를 채택할 때 이러한 노력으로부터 얻을 수 있는 경제적 인센티브와 혜택을 고려한다[13, 36]. 이미 많은 연구들에서 지각된 이익의 긍정적인 관계는 밝혀져 왔다[35]. Kuan and Chau[30]는 조직이 그들의 내부에 새로운 대응안을 제시하기 위해서는 이에 대한 직·간접적 이득에 대한 인식의 전환이 이루어져야만 성공적인 적용이 가능하다고 주장하였다. Anderson and Agarwal[4]은 보안의 심각성과 중요성을 인식하고 이에 대한 조직 내 올바른 태도를 구축하기 위해서는 조직원들에게 보안의 보호 및 관리 이득에 대한 충분한 설명이 이루어져야 한다고 강조하였다.

마지막으로 협력체계 구축은 동종 산업 내 기업간의 일치된 견해 및 합의된 의사결정을 의미한다. 기존의 연구에 의하면 경영활동의 상당 부분은 외부와 관련되어 있고, 또한 그들은 새로운 프로세스에 대한 가치나 역할에 대해 각기 다른 의견을 가지기 때문에 새로운 프로세스를 적용하기에 앞서 공식 및 비공식적인 협력체계의 구축이 이루어져야 한다고 주장한다[12]. Ho et al.[24]은 협력체계를 통해 정보와 위험에 대한 공유를 촉진하고 이로 인해 혁신의 기능 및 구현이 향상될 수 있다고 주장하였다. Bassellier and Benbasat[6] 역시 조직의 새로

운 도구를 효율적으로 활용할 수 있는 최선의 방법은 협력을 통한 관련 정보와 지식들을 통합하는 것이라고 제안하였으며, 이는 조직의 전반적인 개발을 돕고 시너지 효과를 유도한다고 하였다. 이와 같은 논의를 바탕으로 다음과 같은 가설을 제안한다.

가설 1 : 시장 불안정성은 ISM 인식에 정(+)의 영향을 미칠 것이다.
가설 2 : 업무 상호의존성은 ISM 인식에 정(+)의 영향을 미칠 것이다.
가설 3 : 보안관리 이점은 ISM 인식에 정(+)의 영향을 미칠 것이다.
가설 4 : 협력체계구축은 ISM 인식에 정(+)의 영향을 미칠 것이다.

많은 정보시스템 및 관리 분야에서 제도적 이론(institutional theory)이 연구에 적용되고 있다[18]. 기업은 그들이 속한 산업 범위 내에서 합법적이라고 이해되는 규범, 규율, 규정을 따르도록 강요받는다[30]. 특히, 정부의 규제나 법을 준수하도록 받는 압력을 강제적 제도적 압력(coercive institutional pressure)이라고 한다[43]. Hu et al.[26]은 제도화 이론을 바탕으로 조직의 정보보안 방침 및 정책에 대한 영향 메커니즘의 하나로 강제적 동형화(coercive isomorphism)를 제시하였다. 즉, 조직의 새로운 현상과 과정을 합리화시키기 위해서는 강제적인 제도적 압력을 통해 정치, 사회, 문화 등의 요구를 수용하고 이를 바탕으로 형성된 조직은 사회적 지지를 얻고 생존을 유지할 수 있다고 주장하였다. 따라서 이와 같은 외부의 힘으로부터 기업은 정보보안관리에 대한 산업 내 전반의 조건과 방법을 정의하고, 그들의 행동을 합법화, 혹은 통제가 가능하다[25, 33]. 본 연구는 이와 같은 정부 및 규제기관의 외부적 압력에 대해 규제자 영향으로 정의하고 다음과 같은 가설을 제안한다.

가설 5a : 규제자 영향은 시장 불안정성과 ISM 인식 사이의 관계를 더 강화시켜 줄 것이다.
가설 5b : 규제자 영향은 업무 상호의존성과 ISM 인식 사이의 관계를 더 강화시켜 줄 것이다.
가설 5c : 규제자 영향은 보안관리 이점과 ISM 인식 사이의 관계를 더 강화시켜 줄 것이다.
가설 5d : 규제자 영향은 협력체계구축과 ISM 인식 사이의 관계를 더 강화시켜 줄 것이다.

보편적으로 보안관리는 이들에 갖는 태도에서 사용의도, 그리고 실제 사용 및 구현으로 이어지는 과정을 거치게 된다[40]. 이러한 과정은 어떤 조직, 그리고 어떤 접근을 연구의 범위로 설정하는가에 따라 달라 질 수 있다[14]. 정보보안관리에 대한 실증적 연구는 보안과 관련된 많은 연구들에도 불구하고 미비할 뿐 아니라, 대부분 구체적 관리과정을 배제하고 외부요소에 의한 영향을 다루는 연구가 대부분이였다. 즉, 외생변수에 의해 관리의 실행을 살펴보고 있다. 하지만 어떠한 혁신이든 구체적인 단계에 의해 조직이 실행하고자하는 프로세스가 결정되기 마련이다[36]. 이는 단편적인 채택에서 발생되는 문제점 및 한계점들을 최소화할 수 있다. 또한, 단계적 접근을 강조하는 이유는 조직이 개선시키고 실천하고자 하는 목표의 달성은 한 시점에서 발생되는 것이 아니라 어느 정도의 시간을 필요로 하기 때문이다[15, 49]. 하지만 이에 대해 많은 정보기술 분야의 연구들에서는 사용자의 인식, 채택, 확산 등 세분화된 과정을 설명하고 있지만 정보보안관리의 측면에 적합한가를 재검토할 필요성이 있다. Spears and Barki[40]는 정보보안 위험관리 과정에 대해 user participation, organizational awareness, control development, control performance를 제안하고 조직원들의 보안관리의 합리적 의사결정 과정을 보여주었다. 정보보안관리의 과정은 여러 단계들로 정의될 수 있지만 본 연구는 정보보안관리 과정에 대해 인식, 강화, 성과의 세 단계로 구분하였다. 이를 요약해보면, 정보보안관리 의사를 묻는 인식, 실제 정보보안관리를 행하는 수준 정도를 의미하는 강화, 그리고 정보보안관리 실천으로 인한 기업의 재무적, 비재무적 이익의 발생정도를 의미하는 성

과로 정리할 수 있다. 이와 같은 논의를 바탕으로 다음과 같은 가설을 제안한다.

가설 6a : ISM 인식은 ISM 강화에 정(+)의 영향을 미칠 것이다.
가설 6b : ISM 인식은 ISM 성과에 정(+)의 영향을 미칠 것이다.
가설 7 : ISM 강화는 ISM 성과에 정(+)의 영향을 미칠 것이다.

4. 실증분석

4.1 연구대상 및 측정도구

본 연구는 현재 조직 내에서 정보보안관리와 관련된 정책과 활동을 실행 중인 국내 기업을 대상으로 기업이 가지고 있는 다양한 환경요소 중 정보보안관리와 관련된 4가지 요소가 정보보안관리(Information Security Management : ISM)인식 그리고 나아가 ISM 강화와 성과에 어떤 영향을 주는지를 실증적으로 증명하기 위해 조직을 분석의 단위(unit of analysis)로 설정하였다. 특히, 정보보안관리를 어떤 강압이 아니라 전략적 요소로 간주하여 실행하는 조직을 대상으로 데이터를 수집함으로써 본 연구에서 제안하는 연구모형에 대한 결과의 타당성을 더 높일 수 있었다.

먼저, 제안된 연구모형의 시장 불안정성, 업무 상호의존성, 보안관리 이점 및 협력체계구축의 영향과 규제자 영향의 효과를 실증적으로 검증하기 위한 데이터는 국내 여러 기관(예, 코스피, 코스닥, 한국외국인기업협회 등)에 등록된 기업을 대상으로 1차 데이터 수집을 실시하였다. 또한, 대구/경북지역의 유관기관(대구/경북 테크노파크 등)에 등록을 기업을 대상으로 2차 설문을 통해 데이터를 수집하였다. 데이터 수집 방법은 이메일, 직접방문 및 우편을 통해 이루어졌으며, 각 변수를 측정하기 위한 모든 설문 항목들은 (1) 강한 부정 에서부터 (7) 강한 긍정에 걸친 7점 리커트(seven-point Likert scale)로 측정하였다.

각 변수를 측정하는 항목 개발은 우선 기존 연구를 바탕으로 변수별 측정 항목을 찾아 본 연구의 내용과 목적에 적합하게 수정 및 보완을 하였다. 이렇게 개발된 항목들은 정보보안관리와 관련된 활동을 실행 중인 기업 종사자와 대학의 연구자를 대상으로 각 설문항목의 내용 타당성(content validity) 검증을 통해 각 항목에 대한 정교화 및 선별 과정을 실시하였다. <표 1>은 연구모형에서 제안하는 각 변수의 조작적 정의와 관련연구에 대해 보여주

〈표 1〉 연구변수의 조작적 정의 및 관련연구

연구변수	조작적 정의	관련 연구
시장 불안정성	기업의 정보보안관리에 대한 동종 산업 내 존재하는 시장의 변동성 및 기업에 가해지는 시장의 힘 정도	Chau and Tam[13])
업무 상호의존성	기업 내 업무의 상호 관련성 및 자원 의존의 정도	Sharma and Yetton[37]
보안관리 이점	기업이 정보보안관리로부터 얻을 수 있는 유·무형 이익에 대한 인식 정도	Chau and Tam[13]
협력체계구축	기업의 제휴기업과의 의사결정 및 활동의 관계 구축 정도	Chatterjee et al.[12]
규제자 영향	동종 산업 내 감독기구(정부기관 및 규제기관)의 정보보안관리에 대한 압력 및 규제의 정도	Hsu et al.[25]
ISM 인식	기업 내 정보보안관리의 중요성 및 필요성을 인식하는 정도	Spears and Barki[40]
ISM 강화	기업의 정보보안관리와 관련된 활동의 통제 및 실행 정도	Hsu et al.[25]
ISM 성과	기업의 정보보안관리를 통해 얻을 수 있는 재무적/비재무적 성과의 정도(예 : 업무오류감소, 기업 내 자산보호, 영리추구 등)	Spears and Barki[40]

고 있다.

연구모형을 실증적으로 검증하기 위해 총 1,000부의 설문지가 무작위로 배포되어 이 중 224부(회수율 22.4%)가 회수 되었다. 하지만 응답이 불성실하거나 본 연구의 내용과 맞지 않은 총 38부의 설문지를 제외한 186부가 본 연구의 연구모형 분석을 위해 최종 사용되었다. 설문에 응답한 응답자 특성과 응답자가 종사 중인 조직의 특성은 <표 2>와 <표 3>에서 보여주고 있다.

〈표 2〉 응답자 특성

분류		빈도	응답비율(%)
성별	남자	134	72.0%
	여자	52	28.0%
연령	20~29세	18	9.7%
	30~39세	65	34.9%
	40~49세	84	45.2%
	50세 이상	19	10.2%
최종 학력	고졸	15	8.1%
	대학교졸	115	61.8%
	대학원(재)	28	15.1%
	대학원졸	28	15.1%
근무 연수	3년 미만	17	9.1%
	3~5년	64	34.4%
	5~10년	58	31.2%
	10~15년	25	13.4%
	15년 이상	22	11.8%
응답자 직위	이사급 이상	64	34.4%
	부장/차장	77	41.4%
	과장/대리	28	15.1%
	기타	17	9.1%
합계		186	100.0%

우선, 응답자의 특성을 살펴보면, 응답 연령은 40대(45.2%), 30대(34.9%)가 가장 많았으며, 직위로는 부장/차장급이(41.4%), 그 다음으로 이사급 이상이(34.4%), 과장/대리(15.1%)의 순으로 나타났다. 근무연수로는 3~5년(34.4%), 5~10년(31.2%), 10~15년(13.4%)의 순의 분포를 보였다. 응답 조직의 특성을

〈표 3〉 조직 특성

분류		빈도	응답비율(%)
산업분야	제조	29	15.6%
	물류/유통	61	32.8%
	전기 · 전자/정보통신업	54	29.0%
	금융/보험/서비스	35	18.8%
	기타	7	3.8%
종업원 수	100명 미만	21	11.3%
	100명~300명 미만	43	23.1%
	300명~500명 미만	55	29.6%
	500명~1,000명 미만	37	19.9%
	1,000명 이상	30	16.1%
매출액	10억 미만	7	3.8%
	10억~50억 미만	25	13.4%
	50억~100억 미만	49	26.3%
	100억~500억 미만	76	40.9%
	500억 이상	29	15.6%
보안관리에 대한 정책적 패널티 강도 (복수응답)	정해진 공식적 제재 없음	16	8.6%
	경영진 견책	109	58.6%
	직무 정지	73	39.2%
	직무 해임	41	22.0%
	법적 행동	34	18.3%
	기타	8	4.3%
정보보안 관리 노력 (복수응답)	강력한 보안정책(패널티/보상정책)제시	165	88.7%
	사용자 접근제어 및 주의/감시 시스템 유지	59	31.7%
	보안 취약성의 지속적인 점검	51	27.4%
	바이러스 백신, 방화벽, 고급 OS 등 강력한 HW/SW 사용	150	80.6%
	정보보안위험에 대한 유연한 대처능력 훈련	18	9.7%
	정보보안관리에 대한 투자 및 인력배치	37	19.9%
	정보보안관리에 대한 지속적 교육	101	54.3%
	기타	12	6.5%
합계		186	100.0%

살펴보면, 산업분야의 경우 물류/유통업이 32.8%로 가장 높은 분포를 보였으며, 그 다음으로 전기・전자/정보통신업 29.0%, 금융/보험/서비스가 18.8%, 제조업이 15.6%의 순으로 많았다. 설문에 응답한 기업들의 보안관리에 대한 실행되고 있는 정책적 패널티 강도는 경영진 견책이 58.6%, 직무 정지가 39.2%, 직무 해임이 22.0%, 법적 행동이 18.3%의 순으로 나타났다. 이는 곧 설문에 참여한 대부분의 기업들이 정보보안관리를 위해 다양한 조치가 이루어지고 있다는 것을 알 수 있다. 또한, 이러한 기업들의 정보보안관리에 대한 노력은 강력한 보안정책(패널티/보상정책)이 88.7%로 가장 많은 것으로 나타나 이와 같은 사실을 뒷받침해주고 있다. 그 밖에도 바이러스 백신, 방화벽, 고급 OS 등 강력한 HW/SW 사용(80.6%), 정보보안에 대한 지속적 교육(54.3%), 사용자 접근제어 및 주의/감시 시스템 유지(31.7%) 등 다양한 정보보안관리의 노력이 이루어지고 있다는 것을 알 수 있다.

4.2 측정모형 검증

수집된 데이터는 우선 측정모형 검증 후 구조모형 분석을 통해 가설을 검증하는 2가지 단계를 거쳐 분석되었다. 측정모형 검증은 구조방정식 접근 방법인 편최소제곱법(Partial Least Square : PLS) 방법을 사용하여 확인적 요인분석(confirmatory factor analysis : CFA)을 실시하였다. 구조방정식 분석 도구로는 SmartPLS2.0를 사용하였다. 본 연구에서 다른 종류(예 : Lisrel, Amos 등)의 구조방정식보다 PLS 접근방법을 사용한 주요 이유는 크게 두 가지가 있다. 첫째 PLS는 연구 표본이 작거나 비정규분표 일 경우에도 잠재변수(latent variable)들에 대한 모델 검증이 가능하다[47]. 둘째는 본 연구의 주요 목적이 최상의 인과관계를 생산하기 보다는 특정 경로의 예측 타당성을 증명하는 것이기 때문에 PLS 접근 방법이 적합하다.

측정모형 검증은 신뢰성 검증, 판별타당성(discriminant validity) 및 수렴타당성(convergent validity) 총 3가지 요소를 검증 하였다. 측정모형 검증은 최종 수집된 데이터(n = 186)를 사용하였다. 우선 신뢰성은 일반적으로 가장 많이 사용하는 Cronbach's Alphs 값을 사용하였으며, Alpha 값이 0.7 이상이면 신뢰성에 문제가 없는 것으로 판단된다[34]. 둘째로 판별타당성에 대한 평가는 Fornell and Larcker[19])이 제안한 평균분산추출(Average Variance Extracted : AVE)의 제곱근(square root) 값과 구성개념들 간의 상관관계분석 방법을 사용하였다. 각 구성개념의 AVE 제곱근 값이 다른 구성개념 간의 종과 횡의 상관계수 값을 초과하면 판별타당성이 존재하는 것으로 본다. 마지막으로 수렴 타당성에 대한 평가는 각 요인의 요인적재값(factor loading), 구성신뢰도(composite reliability) 및 AVE 값을 사용하였다. 각 요인적재값은 0.6 이상이고, 구성신뢰도 지수는 0.7 이상 그리고 각 잠재변수의 AVE 값이 0.5 이상이어야 수렴타당성이 존재한다고 할 수 있다[19].

〈표 4〉 신뢰도 및 타당성 분석 결과

잠재변수	측정 항목수	AVE	구성 신뢰도	Cronbach's Alpha
시장 불안전성	4	0.678	0.894	0.769
업무 상호의존성	4	0.599	0.856	0.814
보안관리 이점	4	0.627	0.870	0.853
협력체계구축	4	0.640	0.877	0.790
규제자 영향	4	0.672	0.891	0.826
ISM 인식	4	0.677	0.893	0.855
ISM 강화	4	0.605	0.859	0.839
ISM 성과	4	0.713	0.908	0.910

측정모형 분석 결과는 <표 4>~<표 6>에서 보여주고 있다. 우선 연구모형의 모든 잠재변수의 Cronbach's Alpha 계수값은 0.769에서 0.910으로 나타나 신뢰성에는 문제가 없는 것으로 나타났다. 또한, 각 요인의 요인적재값은 모두 0.6 이상이고, 구성신뢰도와 AVE 역시 기준값 이상으로 나타나 수렴타당성이 확보된 것으로 나타났다. 마지막으로

〈표 5〉 구성개념의 요인적재값과 교차요인 적재값

구성개념 (변수)	시장 불안전성	업무 상호 의존성	보안관리 이점	협력체계 구축	규제자 영향	ISM 인식	ISM 강화	ISM 성과
mv1	0.855	0.154	0.378	0.158	0.204	0.146	-0.094	0.147
mv2	0.845	0.230	0.158	0.107	0.196	0.171	0.089	0.084
mv3	0.814	0.211	0.250	0.094	0.170	0.061	0.081	0.031
mv4	0.778	0.214	0.180	0.087	0.170	0.071	0.111	0.158
ti1	0.224	0.777	0.236	0.054	0.153	0.131	0.148	0.088
ti2	0.130	0.723	0.301	0.174	0.034	-0.121	0.060	0.048
ti3	0.436	0.738	0.322	0.068	0.114	-0.430	0.016	0.142
ti4	0.244	0.852	0.153	0.119	0.052	0.103	0.086	0.139
pb1	0.125	0.145	0.840	0.167	0.072	0.490	0.137	-0.030
pb2	0.289	0.223	0.795	0.115	-0.016	0.018	0.127	0.063
pb3	0.270	0.103	0.781	0.088	0.224	0.387	0.150	0.091
pb4	0.287	0.039	0.748	0.178	-0.083	0.313	0.131	0.087
cm1	0.332	0.156	0.077	0.744	0.018	-0.173	0.016	0.136
cm2	0.211	0.163	0.212	0.786	0.129	0.134	-0.159	-0.021
cm3	0.259	0.223	0.325	0.822	0.224	0.152	0.385	-0.009
cm4	0.414	0.392	0.122	0.845	0.108	-0.213	0.162	0.039
ri1	0.261	0.233	0.310	0.104	0.889	0.196	-0.142	0.140
ri2	0.490	0.418	0.493	0.118	0.858	0.387	0.122	0.094
ri3	0.143	0.137	0.068	0.289	0.754	-0.120	-0.106	-0.013
ri4	0.180	0.159	0.071	0.158	0.769	0.030	0.040	0.147
ISMa1	0.045	0.106	0.190	0.845	0.084	0.858	0.032	0.033
ISMa2	0.303	0.102	0.021	0.100	0.005	0.843	-0.057	0.091
ISMa3	0.295	0.086	0.118	0.094	0.129	0.760	0.020	0.120
ISMa4	0.117	-0.086	0.247	-0.046	0.038	0.828	-0.057	-0.027
ISMd1	0.056	-0.022	0.210	0.205	-0.039	0.377	0.727	0.071
ISMd2	-0.115	0.115	0.322	0.281	-0.395	0.332	0.824	-0.193
ISMd3	-0.245	-0.090	0.358	0.089	0.146	0.099	0.745	-0.064
ISMd4	0.046	0.189	0.261	0.356	0.326	-0.126	0.810	0.053
ISMp1	-0.116	0.123	0.210	0.245	0.012	0.263	0.458	0.860
ISMp2	0.167	-0.003	0.303	0.145	0.186	0.180	-0.135	0.818
ISMp3	0.290	0.309	0.296	0.038	0.088	-0.131	0.017	0.784
ISMp4	0.128	0.149	0.071	0.125	0.028	-0.095	0.243	0.910

<표 6>에서 보여주듯이 연구모형에 포함된 각 구성개념의 AVE 제곱근 값이 인접하고 있는 종과 횡의 구성개념들 간의 상관계수보다 높게 나타나 측정도구의 판별타당성을 가지고 있는 것으로 나타났다.

4.3 구조모형 검증

측정모형을 검증 한 후 본 연구에서 제안하는 가설, 즉 연구모형 변수들 간의 영향 관계를 검증하기

〈표 6〉 잠재변수의 상관계수 및 판별타당성 분석 결과

변수	1	2	3	4	5	6	7	9
1. 시장 불안전성	.824							
2. 업무 상호의존성	.355	.774						
3. 보안관리 이점	.384	.296	.792					
4. 협력체계 구축	.187	.312	.202	.800				
5. 규제자 영향	.121	.170	.090	.316	.820			
6. ISM 인식	.116	.250	.202	.333	.283	.823		
7. ISM 강화	.125	.239	.184	.367	.284	.230	.778	
8. ISM 성과	.247	.339	.373	.302	.451	.302	.273	.844

주) 진하게 표시된 대각선 값은 AVE의 제곱근 값임.

위한 구조모형 분석을 실시하였다. 구조모형 역시 SmartPLS2.0를 사용하였으며, 구조모형 분석을 통해 연구모형의 변수들 간의 영향(인과) 관계를 알 수 있는 경로계수(β)와 내생변수(또는 의존변수)에 대한 결정계수(R^2) 결과 값을 알 수 있다. R^2 값은 예측변수(내생변수)가 가지고 있는 총 변동 중에서 회귀선 즉, 외생변수(예 : 설명변수, 독립변수)에 의해 설명되는 비율을 의미한다. SmartPLS2.0에서 제공하는 부스트랩 리샘플링 방법(bootstrap resampling method)으로 500번 리샘플링한 뒤 연구모형의 각 경로를 분석하였다.

분석 결과를 살펴보면, 우선 기업환경요소의 네 가지 변수 중 세 변수, 시장 불안정성(β = 0.196, p < 0.05), 업무 상호의존성(β = 0.337, p < 0.01), 보안관리 이점(β = 0.211, p < 0.01)은 ISM 인식에 통계적으로 유의한 결과를 보였다. 따라서 가설 1~가설 3은 채택되었다. 이는 곧 기업이 속한 산업 내 시장의 변화, 기업 내 업무의 상호 관련성, 기업이 지각하는 보안관리에 대한 전반적 이득과 같은 기업 내·외부에서 발생되는 요소들에 의해 정보보안관리에 대한 인식이 더욱 강화되고 높아질 수 있다는 것을 의미한다. 하지만 협력체계구축은 경로계수 0.021로 ISM 인식에 통계적으로 유의하지 않은 것으로 나타나 가설 4는 기각되었다. 즉, 기업과 기업 간의 관련성 및 의존은 정보보안관리 인식에 중요한 역할을 하지 못한다는 것을 의미한다. 또한, 외생변수별 영향정도를 살펴보면, 보안관리 이점(β = 0.211)이 ISM 인식에 가장 큰 영향을 미치는 것으로 나타났다.

다음으로 규제자 영향의 조절효과에 대한 가설 5a (β = 0.291, p < 0.05), 가설 5b(β = 0.360, p < 0.01), 가설 5c(β = 0.216, p < 0.01)는 모두 채택되었다. 이는 기업은 그들 외부의 사회·정치적 압력과 같은 규제화에 의해 실제 정보보안관리는 더욱 강화될 수 있다는 것을 의미한다. 하지만 가설 5d는 경로계수 0.073으로 통계적 유의성이 없는 것으로 나타났다. 이는 곧 협력체계구축의 외생변수별 영향과 일치하는 결과이다.

마지막으로 ISM 프로세스에 대한 변수, 즉 인식, 강화, 성과의 변수들 간 인과관계를 살펴보면, 인식과 강화(β = 0.629, p < 0.01), 강화와 성과(β = 0.560, p < 0.01)는 통계적으로 유의한 것으로 나타났으나 인식과 성과는 경로계수 0.007로 유의하지 않은 것으로 나타났다. ISM 인식이 ISM 성과에 미치는 직접효과(direct effect)는 0.007이며, 간접효과(indirect effect)는 ISM 인식 → ISM 강화의 경로계수(0.629)×ISM 강화 → ISM 성과의 경로계수(0.560) = 0.352이다. 따라서 총효과(total effect)는 0.359이다. 이러한 결과는 ISM 강화가 ISM 성과에 가장 큰 영향을 미치며, ISM 인식이 ISM 성과에 미치는 영향은 이에 비해 상대적으로 작다고 할 수 있다.

또한, PLS를 통한 구조모형의 신뢰성 측정을 위한 지표로 내생변수의 R^2 값이 가장 일반적인 방법

이며, R^2 기준값은 0.10 이상이 되어야 한다[17]. <그림 2>에서 보여주듯이 내생변수(ISM 인식, ISM 강화, ISM 성과)에 대한 R^2 값은 모두 0.10 이상의 값을 나타냈으며, 각 내생변수에 대해서 ISM 인식은 31.6%, ISM 강화는 39.6%, 그리고 ISM 성과는 31.4%의 분산, 즉 설명력을 보여주고 있다. <표 7>은 가설검정 최종결과 및 채택 유·무에 대한 요약을 보여 주고 있다.

Ⅴ. 토의 및 결론

현대의 기업 환경은 정보시스템에 대한 의존도와 비중이 높아짐에 따라 정보보안의 역할과 중요도가 확장 및 재설정 될 필요성이 증가하고 있다. 따라서 본 연구는 정보보안관리의 실질적인 효과를 거두기 위한 요건과 근거를 제시함으로써 기업의 정보보안 관리 실천방안을 유형화하고자 하였다. 이는 이전 연구의 비판적 고찰을 통해 기업의 정보보안관리에 대한 예방 도구를 제시하여 그 의미가 크다고 할 수 있다. 따라서 기업의 내·외부 환경과 관련된 요소들(시장 불안정성, 업무 상호의존성, 보안관리 이점, 협력체계구축)을 포괄적으로 제안하고, 이들 변수가 세분화된 정보보안관리 프로세스(인식, 강화, 성과)에 미치는 영향을 살펴보았다 또한, 제도적 실효성 확보의 중요한 역할을 검증하기 위해 규제자 영향의 조절효과를 살펴보았다. 본 연구의 결과를 종합하면 아래와 같다.

본 연구에서 제안한 기업환경요소의 세 변수, 시장 불안정성, 업무 상호의존성, 보안관리 이점은 정보보안관리 인식에 긍정적인 영향을 미치는 것으로 나타났다. 또한, 규제자 영향의 조절효과 역시 협력체계구축과의 유의성을 제외한 다른 외생변수와 정보보안관리 인식 간의 사이에서 중요한 역할을 한다는 것을 알 수 있었다. 이러한 결과는 보안관리를 기업 내에 구체적으로 적용하기 위해서는 정보보안은 개별 보안 솔루션이나 특정요소보다는 정부·기업·개인의 다양한 주체들을 통해 위험들을 감소시키기 위한 일련의 노력이 필요하다고 해석할 수 있다. 또한, 기업이 가지는 본질적 문제 및 니즈(needs), 그리고 내·외부 패턴의 발견이 중요하다는 것을 의미한다. 하지만 협력체계구축은 정보보안관리 인식에 영향을 미치지 않는 것으로 나타나 제휴기업과의 관계가 보안강화나 보안관리에 대한 인식 및 의지에 영향을 준다기 보다는 기업의 핵심 전략과

〈표 7〉 가설검증 결과

가설	경로	표준화된 경로계수	t 값	채택 유·무
가설 1	시장 불안전성 → ISM 인식	0.196*	2.394	채택
가설 2	업무 상호의존성 → ISM 인식	0.337**	4.250	채택
가설 3	보안관리 이점 → ISM 인식	0.211**	2.814	채택
가설 4	협력체계구축 → ISM 인식	0.021	0.268	기각
가설 5a	시장 불안전성×규제자 영향 → ISM 인식	0.291*	3.521	채택
가설 5b	업무 상호의존성×규제자 영향 → ISM 인식	0.360**	4.976	채택
가설 5c	보안관리 이점×규제자 영향 → ISM 인식	0.216**	3.064	채택
가설 5d	협력체계구축×규제자 영향 → ISM 인식	0.073	0.803	기각
가설 6a	ISM 인식 → ISM 강화	0.629**	8.786	채택
가설 6b	ISM 인식 → ISM 성과	0.007	0.029	기각
가설 7	ISM 강화 → ISM 성과	0.560**	6.452	채택

주) * $p < 0.05$, ** $p < 0.01$.

기술을 보호하기 위한 자구노력이 보안관리에 더 집중되고 있다는 것을 알 수 있었다. 다음으로 본 연구에서 개념화한 정보보안관리 프로세스의 세 단계, 인식, 강화, 성과 간의 유의성 검증결과, 인식은 강화에 그리고 강화는 성과에 긍정적인 영향을 미치는 것으로 나타났으나 인식은 성과에 영향을 미치지 않는 것으로 나타났다. 즉, 효과적인 보안관리를 위해서는 기업이 이를 현실적으로 관리를 할 수 있는 인식 및 능력의 속도가 어느 정도 확보되고 일치될 때 기업의 전반적 질적 향상과 경제적 이득이 발생될 수 있는 것으로 해석할 수 있다.

본 연구는 실증적 검증을 통해 정보보안관리에 대한 관리 기준을 제시하였다. 이는 곧 많은 정보보안 연구들에도 불구하고 정보보안관리에 대한 연구가 부진한 점을 지적하고, 기업의 실질적인 보안관리 실행에 필요한 이론적 바탕과 실용적 지침의 결과물을 제안한데 그 의의가 있다. 본 연구결과에 기초하여 몇 가지 기대효과와 활용방안을 제시하면 다음과 같다. 우선 학문적 시사점으로는 어느 조직에서나 실행 가능한 보안관리의 기준을 이론적 연구를 시행하여 정립하였다. 이는 곧 정보보안관리의 필요성이 강조되는 반면 학문적 전제가 미흡한 상황에서 시의적절한 연구 모델을 제시하였을 뿐 아니라 기업 및 개인의 보안관리 행동을 설명하는 연구에 좋은 시발점이 될 수 있다. 또한, 이전의 보안관리 연구에서 찾아 볼 수 없었던 기업환경요소와 규제자 영향의 조절변수를 이론화하여 그 시사점이 크다고 할 수 있다. 더불어 정보보안관리 프로세스를 세 단계로 정리하고 이에 대한 인과관계를 증명하여 논리적 기틀을 마련하였다. 즉, 본 연구에서 제안한 보안관리와 관련된 변수를 측정하기 위한 새로운 측정변수를 이전 연구로부터 개발하여 타당성을 검증한다는 시사점이 있다.

아울러 실무적으로도 중요한 의미를 가진다. 상당수의 기업들은 보안관리로부터 발생되는 갈등 해결의 수단으로 기술적, 물리적 도구에 의존하고 있다. 따라서 이들만으로 보안환경이 충분히 구축되었다는 오해를 일깨우고 현재의 기업차원의 보안조치는 많은 제약과 한계가 있다는 것을 알 수 있다. 즉, 현재의 보안관리 수준을 향상시키기 위한 통합적인 방법을 제공하고 바람직한 해결책에 대한 조언과 도움이 될 수 있다. 또한, 실제 기업들이 보안 비즈니스 및 프로세스에 적용할 수 있는 기회와 동기를 제공하고 정보보안관리 체계를 정비함에 있어 이견을 좁히고 강한 설득력을 얻을 수 있다. 만약 기업들이 그들 환경에 도출된 지표를 활용한다면 상당부분의 가치 평가에 유용한 결과를 제시하고 기존의 역기능들을 최소화할 수 있을 것이다.

하지만 본 연구에서도 마찬가지로 몇 가지 한계점이 있다. 이전의 정보보안관리에 대한 연구의 시도는 상당히 제한되어 왔다. 이는 곧 보안관리에 대한 선행연구의 미비함으로 인해 구체적인 참고자료를 통한 기업관리 현상을 설명하기에는 제약이 있을 수 있다. 따라서 본 연구에서 사용된 측정도구는 하나의 시안으로 연구변수 조작화(operationalization)에 보다 엄격한 개념타당성과 신뢰성 검증을 추가적 연구를 통해 개선 및 개발될 필요가 있다. 또한, 본 연구의 이론적 모델에서 포함한 요인 외의 실제 기업 사례에 적용되기 위한 실무적 관점의 의미있는 요소들을 더 분석할 필요가 있다. 뿐만 아니라 정보보안관리를 효과적으로 설계하기 위한 또 다른 과정으로써의 접근이 필요하다. 이는 곧 한정된 변수에 의존할 수 있다는 한계가 있기 때문이다. 마지막으로 한정된 자료의 보편성 및 일반성을 확보하기 위해서는 설문조사의 표본에 대해 다양한 기업의 특성과 참여를 포함시킬 필요가 있다. 즉, 향후 연구에서는 기업들의 정보보안관리에 대한 단편적 범위를 탈피한 개발과 응용이 필요하다는 것을 의미한다.

참 고 문 헌

[1] 박용재, 임명환, “RFID 기술의 인식, 채택, 실행별 영향요인 분석,”「한국경영과학회지」, 제26권, 제3호(2009), pp.205-221.

[2] 이수열, “협력적 공급사슬관리가 참여기업 성

과에 미치는 영향에 대한 연구,"「한국경영과학회지」, 제34권, 제3호(2009), pp.85-104.

[3] 이웅규, 권정일, "기술수용 모형과 전환비용의 관계 분석,"「한국경영과학회지」, 제37권, 제1호(2012), pp.89-104.

[4] Anderson, D.L. and R. Agarwal, "Practicing Safe Computing : A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly*, Vol.34, No.3(2010), pp.613-643.

[5] Babatunde, D.A. and M.H. Selamat, "Investigating Information Security Management and Its Influencing Factors in the Nigerian Banking Industry : A Conceptual Model," *International Journal on Social Science, Economics and Art*, Vol.2, No.2(2012), pp.55-59.

[6] Bassellier, G. and I. Benbasat, "Business Competence of Information Technology Professionals : Conceptual Development and Influence on IT-Business Partnerships," *MIS Quarterly*, Vol.28, No.4(2004), pp.673-694.

[7] Baker, W.H. and L. Wallace, "Is Information Security Under Control?," *IEEE Security and Privacy*, Vol.5, No.1(2007), pp.36-44.

[8] Boss, S.R., L.J. Kirsch, I. Angermmeier, R.A. Shingler, and R.W. Boss, "If Someone is Watching, I'll Do What I'm Asked : Mandatoriness, Control, and Information Security," *European Journal of Information Systems*, Vol.18, No.2(2009), pp.151-164.

[9] Brandon, D.P. and A.B. Hollingshead, "Transactive Memory Systems in Organizations : Matching Tasks, Expertise, and People," *Organization Science*, Vol.15, No.6(2004), pp.633-644.

[10] Cavusoglu, H., B. Mishra, and S. Raghunathan, "A Model for Evaluating IT Security Investments," *Communications of the ACM*, Vol.47, No.7(2004), pp.87-92.

[11] Chang, S.E. and C.B. Ho, "Organizational Factors to the Effectiveness of Implementing Information Security Management," *Industrial Management and Data Systems*, Vol.106, No.3(2006), pp.345-361.

[12] Chatterjee, D., R. Grewal, and V. Sambamurthy, "Shaping Up for E-Commerce : Institutional Enablers of the Organizational Assimilation of Web Technologies," *MIS Quarterly*, Vol.26, No.2(2002), pp.65-89.

[13] Chau, P.Y.K. and K.Y. Tam, "Organizational Adoption of Open Systems : A 'Technology-Push, Need-Pull' Perspective," *Information and Management*, Vol.37, No.5(2000), pp.229-239.

[14] Cooper, R. and R. Zmud, "Information Technology Implementation Research : A Technological Diffusion Approach," *Management Science*, Vol.36, No.2(1990), pp.123-139.

[15] Damanpour, F. and M. Schneider, "Phases of the Adoption of Innovation in Organizations : Effects of Environment, Organization and Top Managers," *British Journal of Management*, Vol.17, No.3(2006), pp.215-236.

[16] Dhillon, G. and J. Backhouse, "Information System Security Management in the New Millennium," *Communications of the ACM*, Vol.43(2000), pp.125-128.

[17] Doz, Y.L., P.M. Olk, and P.S. Ring, "Formation Processes of R&D Consortia : Which Path to Take? Where Does it Lead?," *Strategic Management Journal*, Vol.21, No.3(2000), pp.239-266.

[18] Flanagin, A.J., "Social Pressures on Organizational Website Adoption," *Human Communication Research*, Vol.26, No.4(2000), pp.618-646.

[19] Fornell, C. and D. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, Vol.18, No.1(1981), pp. 39-50.

[20] Goodhue, D.L. and E.W. Straub, "Security Concerns of System Users : A Study of Perceptions of the Adequacy of Security," *Information and Management*, Vol.20, No.1(1991), pp.13-27.

[21] Grover, V. and K.A. Saeed, "The Impact of Product, Market, and Relationship Characteristics on Interorganizational System Integration in Manufacturer-Supplier Dyads," *Journal of Management Information Systems*, Vol.23, No.4(2007), pp.185-216.

[22] Guo, K.H., Y. Yuan, N.P. Archer, and C.E. Connelly, "Understanding Nomnalicious Security Violations in the Workplace : A Composite Behavior Model," *Journal of Management Information Systems*, Vol.28, No.2(2011), pp.203-236.

[23] Gupta, A. and R. Hammond, "Information Systems Security Issues and Decisions for Small Business : An Empirical Examination," *Information Management and Computer Security*, Vol.13, No.4(2005), pp.297-310.

[24] Ho, C.R., Y.P. Chi, and Y.M. Tai, "A Structural Approach to Measuring Uncertainty in Supply Chains," *International Journal of Electronic Commerce*, Vol.9, No.3(2005), pp.91-114.

[25] Hsu, C., J.N. Lee, and D.W. Straub, "Institutional Influences on Information Systems Security Innovations," *Information Systems Research*, Vol.23, No.1(2012), pp.1-22.

[26] Hu, Q., P. Hart, and D. Cooke, "The Role of External and Internal Influences on Information Systems Security-A Neo-Institutional Perspective," *The Journal of Strategic Information Systems*, Vol.16, No.2(2007), pp.153-172.

[27] Kankanhalli, A., H.H. Teo, B.C.Y. Tan, and K.K. Wei, "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management*, Vol.23, No.2(2003), pp.139-154.

[28] Kearns, G.S. and A.L. Lederer, "The Impact of Industry Contextual Factors on IT Focus and the Use of IT for Competitive Advantage," *Information and Management*, Vol.41, No.7(2004), pp.899-919.

[29] Keller, S., A. Powell, B. Horstmann, C. Predmore, and M. Crawford, "Information Security Threats and Practices in Small Business," *Information System Management*, Vol.22, No.2(2005), pp.7-19.

[30] Kuan, K.K.Y. and P.Y.K. Chau, "A Perception-Based Model for EDI Adoption in Small Businesses Using a Technology-Organization-Environment Framework," *Information and Management*, Vol.38, No.8(2001), pp.507-521.

[31] Lee, Y. and K.A. Kozar, "An Empirical Investigation of Anti-Spyware Software Adoption : A Multitheoretical Perspective," *Information and Management*, Vol.45, No.2(2008), pp.109-119.

[32] Lee, Y. and K.R. Larsen, "Threat of Coping Appraisal : Determinants of SMB Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems*, Vol.18, No.2(2009), pp.177-187.

[33] Ma, Q. and P. Ratnasingam, "Factors Affecting the Objectives of Information Security Management," International Conference on In-

formation Resources Management 2008 Proceedings, 2008.

[34] Nunnally, J.C., *Psychometric theory*, 2nd ed., New York : McGraw Hill, 1978.

[35] Pee, L.G., I.M.Y. Woon, and A. Kankanhalli, "Explaining Non-Work-Related Computing in the Workplace : A Comparison of Alternative Models," *Information and Management*, Vol.45, No.2(2008), pp.120-130.

[36] Rogers, E.M., *Diffusion of Innovations*, 5th ed., The Free Press, New York, 2003.

[37] Sharma, R. and P. Yetton, "The Contigent Effects of Management Support and Task Interdependence on Successful Information Systems Implementation," *MIS Quarterly*, Vol.27, No.4(2003), pp.533-556.

[38] Sharma, R. and P. Yetton, "The Contingent Effects of Training, Technical Complexity, and Task Interdependence on Successful Information Systems Implementation," *MIS Quarterly*, Vol.31, No.2(2007), pp.219-238.

[39] Shih, H.P., "Technology-Push and Communication-Pull Forces Driving Message-Based Coordination Performance," *Journal of Strategic Information Systems*, Vol.15, No.2(2006), pp.105-123.

[40] Spears, J.L. and H. Barki, "User Participation in Information Systems Security Risk Management," *MIS Quarterly*, Vol.34, No.3(2010), pp.503-522.

[41] Straub, D.W., "Effective IS Security : An Empirical Study," *Information Systems Research*, Vol.1, No.3(1990), pp.255-276.

[42] Straub, D.W. and R.J. Welke, "Coping with Systems Risk : Security Planning Models for Management Decision Making," *MIS Quarterly*, Vol.22, No.4(1998), pp.441-469.

[43] Teo, H.H., K.K. Wei, and I. Benbasat, "Predicting Intention to Adopt Interorganizational Linkages : An Institutional Perspective," *MIS Quarterly*, Vol.27, No.1(2003), pp.19-49.

[44] von Solms, B. and R. von Solms, "The 10 Deadly Sins of Information Security Management," *Computers and Security*, Vol.23, No.5(2004), pp.371-376.

[45] 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.

[46] Yildirim, E.Y., G. Akalp, S. Aytac, and N. Bayram, "Factors Influencing Information Security Management in Small-and Medium-Sized Enterprises : A Case Study From Turkey," *International Journal of Information Management*, Vol.31, No.4(2011), pp.360-365.

[47] Yoo, Y. and M. Alavi, "Media and group cohesion : Relative influences on social presence, task participation, and group consensus," *MIS Quarterly*, Vol.25, No.3(2001), pp. 371-390.

[48] Zhang, J., B.J. Reithel, and H. Li, "Impact of Perceived Technical Protection on Security Behaviors," I*nformation Management and Computer Security*, Vol.17, No.4(2009), pp. 330-340.

[49] Zumd, R.W., "Diffusion of Modern Software Practices : Influence of Centralization and Formalization," *Management Science*, Vol.28, No.12(1982), pp.1421-1431.