보안관리 인지 요인이 조직의 정보시스템 보안위험관리에 대한 인식 및 개발의지에 미치는 영향

The Impact of Cognitive Factors of IS Security Risk Management(ISM) on Awareness and Intention to Develop ISM

김 상 현 (Sanghyun Kim) 경북대학교 경상대학 경영학부 교수
송 영 미 (Youngmi Song) 경북대학교 경상대학 경영학부 박사과정, 교신저자

요 약

기술발달에 따라 기업들의 정보시스템에 대한 의존도가 높아지고 있는 만큼 보안위험에 노출될 확률도 더 높아져 보안위험관리에 대한 개발과 강화가 어느 때보다 요구되고 있다. 따라서 본 연구에서는 조직 내에서 자발적으로 보안위험관리 활동을 실행하고 있는 기업을 대상으로 보안관리 인지 요인의 6가지 변수가 보안위험관리 인지와 보안위험관리 개발의지에 어떤 영향을 주는지 나아가 이 두 가지 요소가 조직의 보안위험관리 실행에 어떤 영향을 미치는지를 실증적으로 증명하고자 하였다. 보안관리 인지 요인의 6가지 변수로는 조직원의 보안관리행동, 보안의무준수, 지각된 이득, 지각된 희생, 사회적 압력, 보안위험경험을 제안하고 이 변수들이 보안위험관리 인식과 개발의지에 나아가 보안위험관리 실행에 어떤 영향을 주는지에 대해 검증하였다. 가설검증을 위해 국내기업들을 대상으로 설문조사를 실시하여 237부의 데이터를 수집하여 PLS 방법으로 분석하였다. 그 결과 제안된 6가지 인지요인 중 지각된 희생을 제외한 모두가 보안위험관리 인식 및 개발의지에 유의한 영향을 미치는 것으로 나타났으며 보안위험관리 수행 역시 인식 및 개발의지와 상관관계를 형성하는 것으로 나타났다.

키워드 : 보안위험관리, 보안관리 인지요인, 보안위험관리 인식, 보안위험관리 개발의지, 보안위험관리 수행

Ⅰ. 서 론

광범위한 정보기술의 사용으로 인해 기업은 더 높은 생산성과 효율을 가질 수 있게 되었다. 그러나 정보기술에 대한 높은 의존성은 엄청난 손실을 끼치는 정보보안 사고와 보안실패에 대한 엄청난 증가를 이끌었다(Baker and Wallace, 2007). 또한 세계화, 더 높은 생산성 추구, 비용절감 등과 같은 경영 트렌드에 따라 기업들은 정보시스템과 인터넷 서비스에 점점 더 의지하게 되었다. 그로 인해 잠재적인 정보시스템의 공격과 붕괴의 가능성이 데이터, 서비스, 기업의 엄청난 운영손실을 야기할 수 있게 되었다. 조직의 정보시스템은 기술적 고장, 시스템의 취약함, 사람의 실수나 사기 또는 외부적 요인에 의해 보안위험에 노출된다. 따라서 정보 자산의 기밀성,

무결성, 유용성을 보호하기 위해 설계된 정보보안 위험관리에 대해 조직이 투자하고 인식하여야만 한다. 최근, 이러한 정보보안과 관련된 공격과 위반에 대한 잠재적인 위험에 관한 인식이 확대되면서 기업의 정보보안에 대한 투자가 증가하고 있으며 적용범위에 따라서 정보보안에 대한 다양한 접근이 시도되고 있다.

일반적으로 정보시스템 보안에 대한 조직의 노력은 하드웨어, 소프트웨어, 네트워킹과 같은 기술적 자산에 대한 약점에 중점을 두고 있다. 이는 사람, 정책, 프로세스, 문화와 같은 다른 원천에 대한 약점을 관리하는 비용을 희생한 결과이다(Halliday *et al*., 1996; Hu *et al*., 2006; Jahner and Krcmar, 2005; Straub and Welke, 1998; von Solms and von Solms, 2004). 더욱이 기술중심의 정보시스템 보안은 해커나 바이러스와 같은 외부적 위협에 중점을 두고 있어 조직이 내부로부터의 위반이나 위험에 노출되도록 하고 있다(Doherty and Fulford, 2005). 또한 최근 기업의 정보시스템에 대한 의존성이 높아짐에 따라 이와 관련한 위험에 대한 관리가 요구되고 있는데 그 중 보안위험이 기업에게 핵심 과제로 떠오르고 있다. 이는 보안위험이 기업의 브랜드 가치하락, 기업 신뢰성 추락, 금전적 손해 등의 물질적, 가치적으로 엄청난 피해를 입을 수 있는 결과를 초래할 잠재적 가능성이 높기 때문이다(Cavusoglu *et al*., 2009). 따라서 보안관리는 기업들에게 경영상 주요 사안 중 하나가 되고 있다(Brancheau *et al*., 1996; Lohmeyer *et al*., 2002; Ransbotham and Mitra, 2009). 일반적으로 정보보안에 대한 위험을 줄이기 위해 기업들은 기술기반의 해결책에 의존하는 경향이 있다. 하지만 이러한 기술적 해결책은 보안위험을 제거하는데 충분하지 않다(Cavusoglu *et al*., 2009; Dhillon and Backhous, 2001; Siponen, 2005).

기술발달에 따라 기업들의 정보시스템에 대한 의존도가 높아짐과 동시에 보안위험에 노출될 확률도 더 높아지고 따라서 기업의 보안위험관리에 대한 관심과 개발노력, 보안관리 강화가 더욱 강조되고 있다. 하지만 기업들의 보안위험관리에 대한 인식이나 투자가 미비한 현실에서 조직의 보안위험관리에 대한 의사결정이나 보안문제의 해결책 제시를 위한 이론적 연구가 필요하다고 판단된다. 기존의 보안관리에 관한 문헌연구들은 보안관리의 필요성을 강조하고 이에 대한 개념 정의나 기술적 강조, 보안관리 모델 제시, 필요자원에 중점을 둔 연구가 대부분이었다(Finne, 2000; Kotulic and Clark, 2004; Spears and Barki, 2010; Straub and Welke, 1998). 하지만 보안관리에 대한 기업의 인식과 투자에 대한 시각의 변화가 필요한 시점에서 기업의 내외부적 요인들을 모두 고려한 보안위험관리 인식 및 개발의지에 관한 실증 연구가 필요하다고 생각된다. 따라서 본 연구에서는 조직의 보안위험관리 인식과 개발의지에 어떤 결정적 영향 요인들이 보안관리 인지 요인으로 작용하는지를 살펴보고 조직에 보안위험관리의 필요성과 중요성을 강조하고자 한다. 이를 위해 보안관리 인지 요인의 6가지 변수로 조직원의 보안관리행동, 보안의무준수, 지각된 이득, 지각된 희생, 사회적 압력, 보안위험경험을 제안하였으며 이 변수들이 보안위험관리 인식과 개발의지와 어떤 영향 관계가 있는지 알아보고자 하였다. 또한, 조직의 보안위험관리 인식과 개발의지 간의 관계와 이 두 변수가 실제 보안위험관리 실행에 어떤 영향을 미치는 지에 대해 검증하고자 한다.

Ⅱ. 이론적 배경

2.1 보안위험관리

조직의 경영목표나 이념 수행을 어렵게 하는 대표적인 위험은 사기, 잘못된 의사결정, 생산성의 손실, 데이터의 부정확함, 승인되지 않은 데이터 폭로, 조직의 공신력을 잃게 되는 것 등이 있다(Fenz and Ekelhart, 2011). 위험은 조직의 자

산에 발생하는 사건의 결과 또는 가능한 영향으로 정의할 수 있다(Stoneburner *et al*., 2004). 위험은 정의되거나 크기와 같은 것으로 분류될 수 없으나 예상 가능한 결과와 예상치 못한 결과에 따라 분류될 수 있다. 위험관리의 목적은 보안을 위해 투자한 자금을 최대한 효과적으로 활용하고 손실을 최소화하기 위해 불확실한 사건을 규명하고 측정하고 관리하는 것이다(Caelli *et al*., 1989). 또한 위험관리는 기업의 재정적 수익에 대한 예기치 못한 가변성을 이해하고 비용을 치르고 효율적으로 관리하기 위한 일련의 과정을 이르는 것이다(Crouhy *et al*., 2006). 이는 수용 가능한 비용 안에서 수용 가능한 위험을 완화는 수단으로 위험관리를 선택하고 실행하는 활동을 포함하고 있다. 따라서 보안위험관리는 방어 활동이 아니라 보안관리 수행의 기회포착과 결과산출의 균형을 잡는 위험조절전략을 개발하는 과정이다. 위험관리는 IT 관리자에게 조직의 경영목표나 이념을 지원하는 IT 시스템과 데이터를 보호함으로써 경영목표 수행을 통해 이익을 얻고 보안보호 방책에 대한 운영비용과 실리비용의 균형을 유지할 수 있도록 하는 것이다(Stoneburner *et al*., 2004). 즉, 보안위험관리는 IT 시스템과 데이터로부터 발생하는 위험에 중점을 둔 것이다.

보안위험관리(Security Risk Management, SRM)는 정보시스템 보안위험을 식별하고 우선순위를 결정하고 이 같은 위험들에 대한 제어관리를 수행하고 모니터링 하는 계속적인 과정이다(Alberts and Dorofee, 2003). 보안위험관리는 조직이 노출되어 있는 위험을 규명하고, 분석하고, 기업에 끼칠 잠재적인 영향을 평가하고, 수용 가능한 수준에서 위험을 줄이거나 제거하기 위해 어떤 활동을 수행할 것인지 의사결정을 하는 전체 과정을 의미한다(NIST, 2002). 이 같은 보안위험관리는 조직의 정보 자산과 보안에 대한 사고발생 결과, 조직의 정보시스템에 대한 공격의 성공 가능성, 보안 투자에 따르는 비용과 이득에 대한 포괄적인 검증과 평가를 요구한다(Hoo, 2000).

정보시스템 보안은 정보시스템에 많이 의존을 하거나 높은 정보집약적 기업들에게 특히 매우 중요하다(Mohr, 1996). Goodhue and Straub(1991)는 금융회사들이 사업 운영을 위해 정보시스템에 더 많이 의존하고 정보시스템 오용으로 인한 손실이 엄청나게 커질 수 있으며 그들의 대중적 이미지가 그들의 경영에 매우 중요하기 때문에 다른 산업의 기업들 보다 더 많이 정보시스템의 보안에 투자한다고 주장하였다. Jung *et al*.(2001)은 정보의 가용성, 기밀성, 무결성을 유지하기 위한 조직의 필요성에 따라 산업별로 인터넷과 관련된 위협이 다양하게 존재한다고 하였다. 최근 기업의 정보시스템에 대한 의존성이 높아짐에 따라 이와 관련한 보안위험에 대한 관리가 요구되고 있다. 조직이 직면할 수 있는 다양한 보안관련 위협들은 조직의 명성, 책임 문제, 신뢰성 추락, 막대한 금전적 손실 등과 같은 결과를 초래하기에 보안위험관리가 기업들의 주요 화두로 떠오르고 있다(Cavusoglu *et al*., 2004). 하지만 지금까지 기업들은 정보보안에 대한 위험을 줄이고 정보보안을 지키기 위해서 기술기반의 해결책에만 의존하는 경향을 나타냈다(Ernst and Young, 2008). 기술적 기반의 해결책이 정보보안을 향상시키는데 도움을 준다 하더라도 이에 전적으로 또는 과도하게 의지하는 것은 보안위험을 제거하는데 충분치 않다(Cavusoglu *et al*., 2009; Dhillon and Backhous, 2001; Siponen, 2005). 따라서 기업의 정보보안에 대한 위험을 줄이고 대응 가능한 수준의 보안 상태를 유지하기 위해서는 기술적 자원과 사회-조직적 자원 모두에 투자하고 통합적이고 전문적인 보안관리가 필요할 것으로 보인다. 이에 본 연구에서는 기존의 연구들과의 차별성을 두어, 이러한 보안위험관리의 중요성을 강조하고 조직이 보안위험관리에 관한 인식과 보안위험관리에 대한 개발의지를 유발할 수 있는 요인들을 도출하여 보안위험관리 수행과의 관계를 알아보고자 연구 모형을 제시하였다.

2.2 보안위험관리에 관한 연구 동향

지금까지의 보안위험관리에 관한 연구들은 위협과 취약성을 규명하거나 위험을 예측하는 것과 관련된 분야이거나 잠재적인 관리의 비용적 이익을 분석하는데 중점을 두었다(Bodin *et al*., 2008; Cavusoglu *et al*, 2004). 대부분의 보안위험관리와 관련된 연구들은 보안위험관리를 향상시키는데 그 목적을 두었으나 개발된 접근방법과 실제 수행에 대한 철저한 검증, 실증, 평가에 상당한 부족함이 나타난다. 보안위험관리의 가장 큰 문제 중 하나는 위험가능성에 대한 정확한 형태, 관리의 효율성, 산출된 손실 등이 정의될 수 없다는데 있다(Baskerville, 1991; Cybenko, 2006). 많은 잠재적 위협들은 드물게 나타나거나 또는 확실하게 발생하는 위험에 대한 데이터 제공을 불가능하게 하는 매우 많은 변수들에 의해 좌우된다. 더욱이 현재의 보안위험관리에 대한 접근은 이 같은 불확실한 입력 데이터를 기반으로 한 해결책을 제공한다(Fenz and Ekelhart, 2011). 이 같은 높은 불확실성 때문에 조직은 실제적 위협을 무시하거나 비효율적인 보안 대책에 투자해야 하는 위험에 처해 질 수 있다. 또한 조직은 보안대책의 결과의 부정확성과 보안위험이 가진 고유의 불확실성에 대해 인지하지 못하고 있다. 따라서 조직은 그들의 위험관리에 대한 의문점을 가지기 시작해야 할 것이다. 조직의 보안관리에 대한 검증, 실증, 평가의 결과는 조직이 적용하고 있는 보안위험관리에 대한 이해와 보안관리 수단에 중요한 역할을 한다.

보안위험관리에 관한 선행연구들은 보안위험관리의 개념 및 프로세스(Finne, 2000; Stoneburner *et al*., 2004), 보안위험관리 계획 및 전략(Humphreys, 2008; Paqiette *et al*., 2010; Straub and Welke, 1998; von Solms *et al*., 1994), 위험관리이론을 바탕으로 한 연구(Bojanc and Blazic, 2008; Feid and Floyd, 2001; Hong *et al*., 2003), 보안대책을 위해 필요한 자원 및 요소에 관한 연구(Hamill *et al*., 2005; Kankanhalli *et al*., 2003; Spears and Barki, 2010) 등과 같이 다양한 관점에서 보안위험관리를 이해할 수 있도록 해 준다. 하지만 보안위험관리의 중요성과 필요성이 강조되고 있는 것에 비해 보안관리 및 보안위험관리에 관한 연구는 아직 많이 부족하고 다양한 관점의 연구가 미미한 실정이다. 다음 <표 1>에서 보안위험관리의 선행연구들에 대해 나타내었다.

보안위험관리의 개념 및 프로세스에 관한 선행연구로는, Finne(2000)은 정보시스템 위험관리가 방대하고 복잡한 문제이므로 이에 대한 다양한 개념과 정의를 제안하여 위험관리에 대한 이해를 돕고자 하였다. 또한 정보시스템 위험관리를 위해 기업 프로세스와 내부적 관리의 중요성을 강조하였다. Stoneburner *et al*.(2004)는 정보시스템의 위험관리 이유로 조직 정보를 가공하는 더 나은 정보보안기술과 IT 자산의 개발에 대한 의사결정을 지원하기 위한 경영상의 필요한 정보를 제공을 위해, 마지막으로 조직의 위험에 대한 평가를 기반으로 한 정보기술의 인가 또는 승인을 지원하기 위해서라고 하였다.

보안위험관리 계획 및 전략에 관한 연구들은 다음과 같다. Humphreys(2008)는 보안관리 표준이 조직에 어떤 이득과 보안관리에 도움을 주었는지, 조직이 직면한 내부적 보안위험 문제를 보안관리 표준이 어떻게 유용한 해결책을 제시할 것인지에 대한 연구를 제안하였다. Paqiette *et al*.(2010)는 정부의 클라우드 컴퓨팅 사용에 따른 보안위험에 관해 정의하고 정부의 보안관리에 관한 사고나 문제 발생을 미연에 방지하기 위해서 가시적 위험 뿐 아니라 잠재적이고 비가시적인 위험에 대해서도 반드시 클라우드 컴퓨팅 기술의 특성에 맞는 국가적 차원의 보안위험관리 대책 및 정책이 필요하다고 강조하였다. Straub and Welke(1998)은 보안계획 모델을 기반으로 시스템 위험에 대처할 수 있는 경영상 가이드라인을 제안하여 보안에 대한 조직의 의사결정에 도움을 주고자 하였다. 그들이 제안한 경영상 보안위험

〈표 1〉 보안위험관리에 관한 선행연구

구 분	연구자	연구내용
보안위험관리 개념 및 프로세스	Finne(2000)	정보시스템 위험관리에 대한 개념 정의 및 기업 프로세스의 중요성 강조
	Stoneburner *et al.*(2004)	정보시스템 위험관리 정의 및 관리이유 제시
보안위험관리 계획 및 전략	Humphreys(2008)	조직의 보안관리의 표준 중요성 강조
	Paqiette *et al.*(2010)	클라우드 컴퓨팅 기술의 특성에 맞는 국가적 차원의 보안위험관리 대책 및 정책 필요성 강조
	Straub and Welke(1998)	보안위험에 대처할 수 있는 경영상 가이드라인 제안
	von Solms *et al.*(1994)	모든 정보시스템 자산과 위협에 대한 모든 대책 및 대안 마련 제안
위험관리 이론	Bojanc and Blazic(2008)	보안위험관리의 경제적 모델 제시
	Feid and Floyd(2001)	위험분석 흐름도를 제안하여 조직의 정보 자산에 대한 위협과 취약성 평가
	Hong *et al.*(2003)	통합된 시스템 이론을 바탕으로 기업의 보안관리를 이해하고 정보보안관리 전략과 예상되는 결과물에 대해 설명
보안대책을 위해 필요한 자원 및 요소에 관한 연구	Hamill *et al.*(2005)	효율적인 조직의 보안관리를 위한 3가지 요소(사람, 프로세스, 기술) 제안
	Kankanhalli *et al.*(2003)	조직의 정보시스템 보안을 위한 2가지 노력 요소(예방책, 억제책) 제안
	Spears and Barki(2010)	조직의 보안위험관리에 조직의 인적자원(조직원의 참여)의 역할강조

대처 전략 및 보안계획으로 우선 보안문제를 인지하고 다음으로 위험을 분석하여 대안을 생성하고 해결책에 대한 의사결정을 하고 마지막으로 보안대책에 관한 정보를 보급하여 피드백을 얻는 것이다. von Solms *et al.*(1994)은 보안의 기본은 모든 정보시스템 자산과 위협에 대한 모든 대책 및 대안을 추적하는 것이라고 하였다. 하지만 이러한 보안은 과도한 비용을 요구하고 기업의 생산성을 방해할 수 있다고 강조하였다.

보안위험관리 계획 및 전략에 관한 연구들은 다음과 같다. Humphreys(2008)는 보안관리 표준이 조직에 어떤 이득과 보안관리에 도움을 주었는지, 조직이 직면한 내부적 보안위험 문제를 보안관리 표준이 어떻게 유용한 해결책을 제시할 것인지에 대한 연구를 제안하였다. Paqiette *et al.*(2010)는 정부의 클라우드 컴퓨팅 사용에 따른 보안위험에 관해 정의하고 정부의 보안관리에 관한 사고나 문제 발생을 미연에 방지하기 위해서 가시적 위험 뿐 아니라 잠재적이고 비가시적인 위험에 대해서도 반드시 클라우드 컴퓨팅 기술의 특성에 맞는 국가적 차원의 보안위험관리 대책 및 정책이 필요하다고 강조하였다. Straub and Welke(1998)은 보안계획 모델을 기반으로 시스템위험에 대처할 수 있는 경영상 가이드라인을 제안하여 보안에 대한 조직의 의사결정에 도움을 주고자 하였다. 그들이 제안한 경영상 보안위험 대처 전략 및 보안계획으로 우선 보안문제를 인지하고 다음으로 위험을 분석하여 대안을 생성하고 해결책에 대한 의사결정을 하고 마지막으로 보안대책에 관한 정보를 보급하여 피드백

을 얻는 것이다. von Solms *et al.*(1994)은 보안의 기본은 모든 정보시스템 자산과 위협에 대한 모든 대책 및 대안을 추적하는 것이라고 하였다. 하지만 이러한 보안은 과도한 비용을 요구하고 기업의 생산성을 방해할 수 있다고 강조하였다.

또한, 위험관리 이론을 바탕으로 한 연구들을 살펴보면, Bojanc and Blazic(2008)은 보안위험관리의 경제적 모델을 제시하여 경제적 관점에서 보안기술 투자의 필요성을 평가하였다. 이 연구에서는 기업의 자산과 보안위협 요인, 정보통신 기술의 취약성 등을 고려하여 정보시스템의 가치를 계량적으로 산출하여 이를 기반으로 필요한 보안기술에 최적으로 투자할 수 있도록 하는 보안위험관리의 경제 모델을 제안하였다. Feid and Floyd(2001)는 위험분석 흐름도를 제안하여 조직의 정보 자산에 대한 위협과 취약성을 평가할 수 있도록 하였다. 조직적인 위험관리의 목적은 수용 가능한 수준의 더 낮은 위험을 도출하는 것이므로 위험평가와 위험관리의 상호작용은 조직의 보안위험을 수용 가능한 수준으로 낮추어 주고 보안위험관리 과정을 현실화시켜 준다고 주장하였다. Hong *et al.*(2003)은 통합된 시스템 이론을 바탕으로 기업의 보안관리를 이해하고 정보보안관리 전략과 예상되는 결과물에 대해 설명하였다. 즉, 보안위험관리는 조직적 위험 분석과 평가를 통해 정보보안의 취약성과 위협을 산출하고 판단할 수 있도록 하는 것이라 정의하였다. 따라서 평가결과는 정보보안 요구사항과 위험관리기준을 계획할 때 이용될 수 있으며 이 같은 위험관리의 목적은 조직이 수용할 수 있는 정도의 보안위험 수준에 있는 것이라고 하였다.

효과적인 정보시스템 보안은 저장, 처리, 운송 중 승인되지 않은 정보에 대한 접근 또는 수정에 대비하거나 보안위협에 대한 추적하고 기록하고 대항할 필요성을 나타내는 승인된 사용자의 서비스를 거부하는 것을 방지하는 것이다(Yeh and Chaing, 2007). 따라서 정보시스템 보안대책을 위해 필요한 자원 및 요소에 관한 선행연구들은 다음과 같다. Hamill *et al.*(2005)은 효율적인 조직의 보안관리를 위해서는 사람, 프로세스, 기술의 3가지 요소에 의해 좌우된다고 하였다. Kankanhalli *et al.*(2003)은 조직의 정보시스템 보안을 위한 노력을 두 가지 관점에서 제시하였다. 우선, 예방책 노력은 높은 수준의 보안 소프트웨어를 알맞게 사용하거나 또는 높은 수준의 접근제어, 침입방지 시스템, 방화벽, 감시메커니즘, 예외보고서 생성 등과 같은 정보시스템 자산 보호를 위한 제어관리를 하는 것을 의미한다고 하였다. 억제 노력은 보안 정책과 가이드라인을 개발하고 사용자들(조직원들)을 교육하고 정보시스템 사용을 감시하는 숙련된 감사자를 양성하는 것을 포함한다고 하였다. 따라서 효과적인 정보시스템 보안을 위해서는 경영상의 규정을 정의하고 보안의 필요성과 정보시스템의 잘못된 사용의 결과를 이해하도록 조직원들을 교육하는 등 전체 IT 환경을 고려해야 한다. Spears and Barki (2010)는 조직의 보안위험 관리에 조직의 인적 자원인 조직원들의 참여가 보안관리 실행 향상 및 보안 유지, 보안위험관리 개발 등에 중요한 역할을 한다고 주장하였다.

기업은 자신들의 자신인 정보와 기술 자원을 보호하기 위해 기술적 수단의 활용, 조직 구성원들의 참여와 관리, 프로세스의 개발 등의 노력을 기울인다. 하지만 좀 더 체계적이고 전략적인 보안관리를 위해서는 보안위험관리에 대한 관심과 투자가 필요하다. 따라서 본 연구에서는 선행연구를 통해 조직 내외부적으로 보안위험관리에 대한 조직원들의 행동, 기업이 얻을 수 있는 이득, 외부환경 등의 인지적 요인들을 추출하여 기업의 보안위험관리 인식과 개발의지를 향상 시킬 수 있는 방안을 제시하고자 하였다. 기업차원에서 보안위험관리의 필요성을 인식을 하는데 요인들이 작용하는지에 관심을 가지고 보안위험관리 인식과 개발의지, 보안위험관리 실행을 이끄는 동기 요인들을 도출하고 이들의 영향 관계를 알아보고자 하였다.

Ⅲ. 연구모형 및 가설

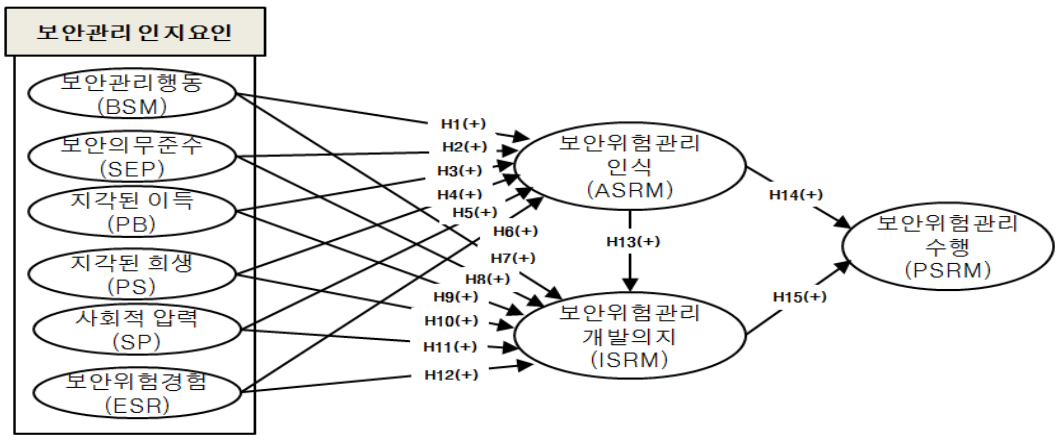
3.1 연구모형

본 연구는 조직 내에서 자발적으로 보안위험관리 활동을 실행하고 있는 기업을 대상으로 보안관리 인지요인의 6가지 변수가 보안위험관리 인지와 보안위험관리 개발의지에 어떤 영향을 주는지 나아가 이 두 가지 요소가 조직의 보안위험관리 실행에 어떤 영향을 미치는지를 실증적으로 증명하기 위해 선행연구들을 바탕으로 <그림 1>과 같은 연구모형을 도출하였다. 조직의 보안위험관리에 대한 인지요인으로 조직원의 보안관리행동, 보안의무준수, 지각된 이득, 지각된 희생, 사회적 압력, 보안위험경험을 제안하였다. 또한, 보안위험관리 인식과 보안위험관리 개발의지에 조직의 보안위험관리 수행에 긍정적인 영향을 미친다는 가설을 제안하였다.

3.2 가설설정

3.2.1 보안관리 인지 요인에 관한 가설설정

본 연구에서 제시한 인지 요인 중 조직원의 보안관리행동과 보안의무준수는 조직 내 보안위험관리를 실질적으로 실천하고 지킬 조직원들의 참여에 기인한 것이다. Spears and Barki(2010)는 조직원의 참여가 특정 보안 목적을 새롭게 창조하고 수정하는 역할을 한다고 주장하였다. 즉, 조직원의 참여가 조직 내 정보를 보호하기 위한 책임의 중심에 있다는 것이다. 따라서 조직원은 공식적으로 보안위험관리에 대한 책임을 할당 받았으며 조직원 개인이 조직 내 보안정책을 준수할 것이라는 조직적 기대를 가지고 있다는 것이다. 매입이론(Buy-In Theory)의 관점에서는 사용자의 참여가 정보시스템개발과 관련하여 사용자의 새로운 정보시스템 수용 및 수행에 영향을 미친다고 하였다. 즉, 조직의 정보시스템 개발에 사용자가 참여하면 그 시스템을 중요한 시스템으로 인지하고 더 중요하고 영향력이 높은 것으로 판단하여 그 시스템을 더 잘 수용하게 된다는 것이다(Markus and Mao, 2004). 이에 Spears and Barki, 2010)는 조직의 보안위험관리의 경우도 마찬가지로 이 매입이론을 적용하여 높은 규제 및 의무를 준수하는 조직에서의 보안위험관리가 더 잘 운영되는 것으로 나타났다고 하였다. 즉, 규제 및 의무 준수를 통해 보안위험관리에 조직원이 참



BSM: Behavior for Security Management, SEP: Compliance with Security Policy, PB: Perceived Benefits, PS: Perceived Sacrifice, SP: Social Pressure, ESR: Experience of Security Risks, ASRM: Awareness of SRM, ISRM: Intention to develop SRM, PSRM: Performance of SRM

〈그림 1〉 연구모형 및 가설설정

여하면 각각의 비즈니스 과정에 더 높은 수준의 정보시스템 보안이 나타난다고 하였다. 또한 조직원의 참여는 참여적 의사결정과 계획된 조직의 변화를 기반으로 하는 성공적인 정보시스템 수행에 대한 기회를 향상시킬 수 있다(Ives and Olson, 1984). 정보시스템 보안에 대한 인식은 조직원의 보안정책 준수의 향상으로 인해 높아질 있다(Goodhue and Straub, 1991; Straub and Welke, 1998). 정보시스템 보안에 대한 조직의 교육 및 정책의 목적은 정보시스템 보안에 대한 지속적인 점검과 조직원의 정책 미 준수에 대한 재제 등에 대해 조직원들과의 의사소통을 하기 위함이다. 또한 조직의 정보보안정책 준수를 위한 교육 및 조직원들의 보안행동을 장려하는 제도 및 장치들은 조직원들을 설득하고 조직원들의 생각 프로세서를 행동에 옮기도록 하는 동기요인이 된다. 즉, 이러한 조직 노력은 조직원들은 보안정책 준수의 중요성을 내면화하여 보안정책을 준수하고 보안행동을 행하게 한다는 것이다(Gardner, 2004). 조직의 보안에 대한 생각과 행동을 억제하고 제재함으로 인해 조직이 보안위험에 노출될 가능성이 줄어들고 조직원의 참여가 늘어나게 되는 것이다(Straub, 1990; Siponen *et al*., 2007). 따라서 본 연구에서는 조직원들의 보안위험관리의 참여 즉, 보안관리행동과 보안의무준수가 조직의 보안위험관리를 인식하고 개발하도록 이끄는 인지요인으로 판단하고 가설을 설정하였다.

가설 1: 조직원의 보안관리행동은 조직의 보안위험관리 인식에 정(+)의 영향을 줄 것이다.
가설 2: 조직원의 보안의무준수는 조직의 보안위험관리 인식에 정(+)의 영향을 줄 것이다.
가설 7: 조직원의 보안관리행동은 조직의 보안위험관리 개발의지에 정(+)의 영향을 줄 것이다.
가설 8: 조직원의 보안의무준수는 조직의 보안위험관리 개발의지에 정(+)의 영향을 줄 것이다.

가치는 이익과 희생이라는 두 가지 주요 구성요소를 포함하는 더 높은 수준의 복합 개념으로서 개념화할 수 있다(Gipp *et al*., 2008). 가치의 기본 특성은 표준, 기준, 이유, 규범, 목적, 이상 등과 관련한 결과적 판단에 의존하고 있는 분별력의 선호도를 의미한다(Holbrook, 1994). 대부분의 정의에서는 이러한 가치를 이득과 희생간의 지각된 상쇄(trade-off)로 나타낸다(Zeithaml, 1988; Anderson *et al*., 1993; Anderson and Narus, 1998; Kotler, 2000; Ulaga and Chacour, 2001). 따라서 가치는 상대적이다(Holbrook, 1994) 또한 가치는 개인 또는 조직의 지각, 기준, 기본적 가치 등을 기반으로 하거나 상황적 순간 또는 기회에 따른 다양한 구성요소로 구성된다(Ulaga and Chacour, 2001; Woodruff, 1997). 경영을 기본적으로 스스로에 대한 적절한 가치를 찾는 것이라고 가정하면, 경영상 여분의 가치를 창조하기 위한 여러 노력들에도 불구하고 공유하는 여분의 가치를 최대한으로 찾으려 할 때 피할 수 없는 갈등 영역이 존재하게 된다(Cox, 1999, 2004). 반대로 조직이 자신들의 전략과 목적을 달성하기 위해 적용하는 변수들과 조직이 혁신에 대한 적용, 적응, 통합의 의사결정들에 대한 이득들이 강조되기도 한다(Stern, 1969; Frazier and Summers, 1986). 그러므로 조직에 적합한 가치를 생성함으로써 얻는 이득과 마찬가지로 가치 생성을 제어하는 것으로부터 얻는 이득은 고려해야 할 잠재적 희생 요소로 나타난다. 이러한 가치는 제품/서비스 및 정보시스템의 도입의도, 구매 및 사용의지, 지속적 사용의 가능성 등에 주요한 영향을 미치는 것이 선행연구를 통해 증명되었다(Bolton and Drew, 1991; Brady and Robertson, 1999; Eggert and Ulaga, 2002; Zeithaml, 1988). 인지 요인 중 지각된 이득과 지각된 희생은 지각된 가치를 구성하는 것과 유사하게 희생과 이득의 누적된 효과가 고려된 계산의 결과이다(Zeithaml, 1988). 즉, 지각된 이득과 희생은 조직의 얻을 수 있는 이득과 발생할 불편함에 관한 인지를 기반으로 한 보안위험관리의 실용

성에 대한 조직의 전체적 평가라고 정의할 수 있다. 조직은 보안위험관리에 대한 의사결정을 통해 얻을 수 있는 잠재적 이득을 고려하여 어느 정도의 희생을 감수하는 것에 동의하는 것이다. 이득에 대한 지각을 확대하기 위해서 다양한 결과의 지각된 가치를 강화함으로써 선택적 행동의 방향을 제시할 수 있다. 따라서 더 높은 이득에 대한 기대는 조직의 보안위험관리에 대한 효용에 대한 평가를 더 강조해 줄 수 있을 것이다(Xu *et al.*, 2011). 지각된 희생은 조직이 보안위험관리를 수행하기 위해서 필요한 시간, 돈, 불편함, 이해력 등 물리적, 인지적 노력을 일컫는 것이다(Weinstein, 1993). 이러한 기대되는 노력들이 조직의 변화 동기보다 더 비중이 높아야 하며, 이러한 노력들이 기대되는 이득보다 더 많이 요구된다면 조직은 보안위험관리에 부정적 의사결정을 할 것이다. Samuelson and Zeckhauser(1988)은 의사결정과정에서 손실에 대한 반감은 가치관점에서 얻는 것 보다 잃는 것이 더 많을 때 나타난다고 하였다. 하지만 새로운 변화를 수용하는데 있어 따르는 비용이나 희생, 노력 등이 변화를 수용했을 때 얻을 수 있는 이점으로 상쇄될 정도의 수준일 때는 손실에 대한 반감을 가지기보다는 변화에 따른 비용 또는 희생이라고 인지하게 된다고 하였다. 따라서 본 연구에서는 조직이 보안위험관리의 가치를 인식하고 실행하기 위해서 지각된 이득과 지각된 희생이라는 두 가지의 요인을 함께 제안하여 측정하고자 하였다. 즉, 조직의 보안위험관리 도입 및 실행에 있어 조직의 그 가치에 대한 인식과 개발의지에 중요한 선행요인으로 판단하고 두 변수를 제시하여 그들과의 관계를 살펴보고자 하는 것이다.

가설 3: 지각된 이득은 조직의 보안위험관리 인식에 정(+)의 영향을 줄 것이다.

가설 4: 지각된 희생은 조직의 보안위험관리 인식에 정(+)의 영향을 줄 것이다.

가설 9: 지각된 이득은 조직의 보안위험관리 개발의지에 정(+)의 영향을 줄 것이다.

가설 10: 지각된 희생은 조직의 보안위험관리 개발의지에 정(+)의 영향을 줄 것이다.

사회적 환경은 조직이 정보위험관리를 평가할 수 있는 정보를 제공한다. 특히 보안위험관리에 대한 경험이나 지식이 부족할 시 더욱 중요하게 느껴진다. 사회적 영향은 한 구성원의 사회적 네트워크가 다른 구성원의 행동에 영향을 미치는 정도를 나타내는 것으로 특정활동 또는 행동에 대한 가치를 지각시키는데 도움을 주는 메시지와 신호를 통해 전달된다(Venkatesh and Brown, 2001). 또한 개인은 기대에 대한 메시지와 다른 사람들의 관찰된 행동 두 가지 모두에 영향을 받는다. 사회적 영향은 특정 행동 또는 활동에 대한 수용을 사회적 구성원이 행하면 이 행동은 승인 되거나 규정 되고 그 후 다른 사회 구성원들은 다른 생각 없이 이 행동을 수용하게 되는 것이다(Lieberman and Asaba, 2006). 조직의 경우도 마찬가지로 산업 내 다른 조직의 의사결정이나 활동이 조직의 의사결정 또는 활동에 미치는 경우를 사회적 영향 또는 사회적 압력으로 볼 수 있다. 정보기술에 대한 투자는 높은 전략적 의사결정으로 조직의 경쟁적 우위를 선점할 수 있도록 해 준다. 따라서 이 같은 의사결정은 다른 조직 특히 경쟁기업의 의사결정에 직접적으로, 상당한 영향을 미치게 된다(Kim *et al.*, 2009). 이 같은 현상은 의사결정의 결과물에 대한 불확실성이 높을수록 더 현저하게 나타난다(Cyert and March, 1963). 전략적 의사결정에 대한 압력과 경쟁적 환경은 내재된 위험에 조직이 덜 민감할 수 있도록 하기 위해 다른 조직과 일치하는 의사결정을 하는 경우가 많다(Swanson and Ramiller, 2004). 또한, 정보기술 보급의 증가로 조직의 경계가 엷어지고 컴퓨터 네트워크와 소프트웨어 어플리케이션을 통한 다양한 기업과의 연결이 가능해지고 비즈니스 프로세스의 병합 현상이 나타나고 있다(Basu and Blanning 2003; Hammer, 2001; Mukho-

padhyay and Kekre, 2002; Straub and Watson, 2001). 그 결과 기업에게 정보기술 경영의 가치 생성에 거래 파트너의 영향력이 증가하게 되었다(Bakos and Nault, 1997; Chatfield and Yetton, 2000; Clemons and Row, 1993). 예를 들면 파트너 기업간의 비능률적인 경영 프로세스와 뒤처진 기술은 기업의 내부적 시스템의 정보시스템 가치에 대한 목표 달성을 저지할 것이다. 따라서 조직은 파트너 기업과 함께 정보기술 향상을 위해 협력하는 것이 동기요인이 될 수 있다(Williams and Frolick, 2001). 또한 산업 내 경쟁정도나 파트너 의존도 등의 사회적 압력이 조직의 혁신이나 기술 도입에 중요한 역할을 하는 것으로 나타났다(Chwelos *et al*., 2001; Iacovou *et al*., 1995; Kraemer *et al*., 2002; Tornatzky and Fleischer, 1990). 따라서 전략적으로 중요한 의사결정 중 하나인 보안위험관리에 대한 기업의 의사결정은 지각된 다른 조직의 보안위험관리 정도에 따라 영향을 받게 될 것이다.

개인의 믿음과 기술수용은 개인의 경험과 특성에 많은 영향을 받는다는 것은 많은 선행 연구를 통해 검증되었다(Xu, 2007; Phelps *et al*., 2000). 또한 이전의 경험은 자신의 능력에 대한 믿음과 관련이 있다(Bandura, 1986). 조직의 경우도 마찬가지로 보안 위험에 노출되어 본 경험이 있거나 보안 위협에 피해를 본 경험이 있는 조직은 경우 조직의 보안관리에 더 많은 노력과 투자를 하게 될 것이다(Smith *et al*., 1996). 과거의 서비스 품질에 대한 만족 경험은 미래의 사용의도에 긍정적인 영향을 미친다(Ganesan, 1994). 과거의 긍정적인 경험은 위험에 대한 지각을 줄여준다 반대로 나쁜 경험은 위험의 가능성을 느끼게 한다. 즉, 부정적 경험은 위험에 대해 높게 인식하게 하고 위험에 대한 인식으로 인해 미래의 의사결정에 영향을 미치게 되는 것이다(Pavlou and Gefen, 2004). 조직의 보안위험관리의 경우 과거의 보안에 관한 경험 또는 보안위험에 대한 경험은 조직에게 위험을 인지하게 하고 이러한 위험을 줄이기 위해 보안위험관리에 대한 필요성 및 중요성을 인식하고 개발의지가 생성될 수 있다. 이러한 선행연구들을 바탕으로 본 연구에서는 사회적 압력과 보안위험경험이 조직의 보안위험관리 인식과 보안위험관리 개발의지에 미치는 영향에 대해 알아보기 위해 다음과 같은 연구가설을 설정하였다.

가설 5: 사회적 압력은 조직의 보안위험관리 인식에 정(+)의 영향을 줄 것이다.

가설 6: 보안위험경험은 조직의 보안위험관리 인식에 정(+)의 영향을 줄 것이다.

가설 11: 사회적 압력은 조직의 보안위험관리 개발의지에 정(+)의 영향을 줄 것이다.

가설 12: 보안위험경험은 조직의 보안위험관리 개발의지에 정(+)의 영향을 줄 것이다.

3.2.2 보안위험관리 인식 및 개발의지, 수행에 관한 가설설정

정보시스템 보안과 관련된 선행연구들은 지각된 의식에 대한 인식과 보안정책 및 보안대책 수용을 강화하는데 중점을 둔 연구들이 많다(Dinev and Hu, 2007; Tsohou *et al*., 2008). 조직의 보안위험관리에 대한 인식은 조직원, 정보시스템 전문가, 관리자 등의 다양한 특정 그룹에서의 조직의 보안정책, 보안절차, 보호되어야 할 민감한 정보의 존재에 대한 인식이 나타나는 것을 의미한다(Sipinen, 2001). 따라서 보안위험관리에 대한 조직의 인식은 조직 내 조직원, 정보시스템 전문가, 관리자 등의 다양한 특정 그룹의 행동을 반영하는 것이라고 할 수 있다. 또한 보안위험관리 인식은 특정그룹에 포함된 조직원의 행동을 수정하여 조직의 표준에 따른 조직원의 보안위험관리 실행을 의미한다(Whiteman, 2008). 다양한 인지요인과 조직원들의 참여를 통해 조직은 보안위험관리에 대한 인식을 가지게 되고 이러한 보안위험관리에 대한 인식은 조직에 실제 적용할 수 있는 새로운 정보보안관리 전략을 도출할 수 있게 해 준다. 보안위험관리

에 대한 개발은 정보시스템 보안관리에 대한 디자인과 실행을 포함하는 것이다(Spears and Barki, 2010). 즉, 보안위험관리 개발은 접근제어, 보안의무 구분, 보안정책 등을 정의하거나 실행함에 있어서의 더 나은 향상을 꾀하려는 의지가 보안위험관리 개발의지인 것이다. 보안정책은 조직의 법률로서 수용 가능한 행동과 수용 불가능한 행동에 대한 규제를 포함하고 있으며 데이터 구별, 위험 허용범위 등과 같은 조직의 보안정책을 정의하는 조직의 경영에 참여하는 관리자와 영향관계가 있다(Whitman, 2008). 즉, 보안위험관리에 대한 경영관리자의 관심과 더 나은 수행을 위한 노력은 결과적으로 기업의 보안위험관리에 대한 개발 의지로 이어지고 이는 조직의 보안위험관리 수행에 긍정적 영향을 미칠 것이다.

마지막으로, 향상된 디자인과 더 나은 수행의 필요성 인식 등은 보안위험관리를 결과적으로 적은 오류와 정보시스템의 효율성의 향상을 야기시켜 더 나은 보안위험관리가 수행될 수 있도록 해 준다(Spears and Barki, 2010). 조직의 보안위험관리 개발을 통해 향상된 보안관리가 수행되면 오류의 수와 그 영향을 줄여주고 보안위험으로부터 조직의 정보시스템이 보호받음으로 시스템관리의 효율성이 증가한다. 따라서 보안위험관리 인식과 보안위험관리 개발의지와 보안위험관리 수행과의 관계 가설을 다음과 같이 설정하였다.

가설 13: 조직의 보안위험관리 인식은 보안위험관리 개발의지에 정(+)의 영향을 줄 것이다.

가설 14: 조직의 보안위험관리인식은 조직의 보안위험관리 수행에 정(+)의 영향을 줄 것이다.

가설 15: 조직의 보안위험관리 개발의지는 조직의 보안위험관리 수행에 정(+)의 영향을 줄 것이다.

Ⅳ. 연구방법 및 실증분석

4.1 연구대상 및 측정방법

본 연구는 조직 내에서 자발적으로 보안위험관리 활동을 실행하고 있는 기업을 대상으로 보안관리 인지요인의 6가지 변수가 보안위험관리 인지와 보안위험관리 개발의지에 어떤 영향을 주는지 나아가 이 두 가지 요소가 조직의 보안위험관리 실행에 어떤 영향을 미치는지를 실증적으로 증명하기 위해 기업 단위의 행동에 대한 설명을 연구 범위로 설정하였다. 이는 곧 조직의 보안위험에 대한 행동이 조직 내 또는 그 조직이 속한 산업 내에서 자발적인 필요에 의해서가 아니라 거래기업과 경영활동을 위해 어쩔 수 없이 비자발적으로 보안위험 관리를 실행하는 경우가 있기 때문이다. 따라서 비자발적으로 보안위험관리를 실행하는 기업들은 보안위험관리 실행에 있어 다른 요소로서의 설명이 필요하다. 이에 연구의 목적과 결과의 타당성을 높이기 위해 본 연구에서는 자발적으로 보안위험관리를 하는 기업만 연구대상으로 포함 하고 있다.

먼저, 본 연구에서 제안한 연구모형을 실증적으로 검증하기 위한 데이터 수집은 우선 코스피와 코스닥에 등록된 기업뿐 아니라 한국외국기업협회에 등록된 기업을 대상으로 1차 설문을 실시하였다. 또한 대구/경북지역의 유관기관에 등록을 기업을 대상으로 2차 설문을 통해 데이터를 수집하였다. 설문 방법은 이메일, 전화, 직접방문 및 우편을 통한 다차원적인 방법을 사용 하였으며, 연구모형의 각 변수를 측정하기 위한 설문의 모든 항목들은 (1) 강한 긍정에서부터 (5) 강한 부정에 걸친 5점 리커트(five-point Likert scale)의 항목으로 측정하였다.

측정항목은 일차적으로 기존의 연구를 바탕으로 본 연구의 목적에 맞게 수정·보완 한 후, 정보보안위험관리를 실행 중인 기업 및 경영정보관련 연구자를 대상으로 설문항목의 내용 타

당성(content validity)을 검증을 통해 각 항목에 대한 정교화 및 선별 과정을 실시하였다. <표 2>은 연구모형에서 제안하는 각 변수의 조작적 정의와 관련연구에 대해 보여주고 있다.

본 연구의 연구모형을 실증적으로 검증하기 위해, 총 2,000부의 설문지가 배포되어 이 중 251(회수율 12.6%)개의 설문지만 회수되었고, 응답이 불성실한 설문지 14개를 제거한 총 237부를 본 연구의 연구모형 분석을 위해 사용하였다. 응답자의 직위, 산업분류, 매출액 등에 대한 응답자 특성은 <표 3>에서 보여주고 있다.

설문 응답기업의 인구통계학적 특성을 살펴보면, 응답기업의 산업분야는 금융/보험(39.7%), 전기전자/정보통신(29.5%)업이 과반수이상을 차지하였으며, 설문응답자의 직위는 부장/차장(35.9%), 이사급 이상(30.0%), 과장/대리(26.6%) 순으로 기업의 관리자 그룹의 응답을 수거하여 설문의 유효성을 높였다. 응답 기업의 규모는 매출액 기준으로 100억~500억 미만(30.4%), 500억 이상(29.5%)의 기업들이 과반수 이상을 차지하였으며 다음으로 50억~100억 미만(24.9%), 10억~50억 미만(10.5%). 10억 미만(4.6%) 순으로 나타났다. 응답 기업들의 보안관리위험을 위한 노력으로는 사용자 접근제어 및 주의/감시 시스템 유지(79.3%), 정보보안에 대한 지속적인 교육(69.6%), 정보보안위험관리에 대한 투자 및 인력배치(51.9%) 등이 높은 비율을 보였다.

4.2 측정모형검증

수집된 데이터는 2가지 단계를 거쳐 분석 되었다. 우선 측정모형의 신뢰성과 타당성 검증 후 구조모형 접근 방식을 통해 연구모형에서 제안하는 가설을 검증하였다. 데이터 분석 방법은 구조방정식 접근 방법 중 연구의 특성상 편최소제곱법(Partial Least Square: PLS) 방법을 사용하였으며,

〈표 2〉 연구변수에 대한 조작적 정의 및 관련연구

변수	조작적 정의	관련 연구
보안관리행동	조직구성원들의 정보보안관련 행동 및 보안실천의 정도	Karahanna *et al.*(1999), Spears and Barki(2010)
보안의무준수	조직구성원이 조직의 보안정책 및 지침을 지키고 따르는 정도	Chan *et al.*(2005), Pahnila *et al.*(2007)
지각된 이득	조직구성원들이 보안위험관리를 통해 얻을 수 있는 유/무형의 이득에 대한 인식의 정도	Pee *et al.*(2008)
지각된 희생	조직구성원들이 보안위험관리를 위해 감수해야 하는 유/무형의 불이익의 가치에 대한 인식의 정도	Sirdeshmukh *et al.*(2002)
사회적 압력	동종 산업 내 보안위험관리에 대한 의사결정 및 인식의 정도	Teo *et al.*(2003), Son and Benbasat(2007)
보안위험경험	조직의 보안문제 및 보안위험의 직·간접적인 노출 및 과거 경험의 정도	Rhee *et al.*(2009)
보안위험관리 인식	조직구성원들이 보안위험관리의 중요성과 필요성에 대해 인식 정도	Spears and Barki(2010)
보안위험관리 개발의지	조직의 보안위험관리 강화를 위해 필요한 요인들에 대한 의사결정 및 도입 의지 정도	Spears and Barki(2010)
보안위험관리 수행	조직이 보안위험관리와 관련된 활동의 실행 정도	Spears and Barki(2010)

〈표 3〉 표본의 일반적 특성

분류		빈도	응답비율(%)
산업분야	제조	35	14.8%
	물류/유통	28	11.8%
	전기・전자/정보통신	70	29.5%
	금융/보험	94	39.7%
	기타	10	4.2%
성별	남자	179	75.5%
	여자	58	24.5%
응답자 직위	이사급 이상	71	30.0%
	부장/차장	85	35.9%
	과장/대리	63	26.6%
	기타	18	7.6%
종업원 수	50명 미만	24	10.1%
	50명~100명 미만	41	17.3%
	100명~500명 미만	55	23.2%
	500명~1,000명 미만	68	28.7%
	1,000명~3,000명 미만	33	13.9%
	3,000명 이상	16	6.8%
매출액	10억 미만	11	4.6%
	10억~50억 미만	25	10.5%
	50억~100억 미만	59	24.9%
	100억~500억 미만	72	30.4%
	500억 이상	70	29.5%
정보보안관리 빈도	연 1회	21	8.9%
	연 4회(분기별)	68	28.7%
	연 6회	50	21.1%
	연 6회 이상	98	41.4%
보안위험관리 노력(복수응답)	강력한 보안정책(패널티/보상정책)제시	89	37.6%
	사용자 접근제어 및 주의/감시 시스템 유지	188	79.3%
	정보보안위험에 대한 유연한 대처능력 훈련	94	39.7%
	정보보안위험관리에 대한 투자 및 인력배치	123	51.9%
	정보보안에 대한 지속적 교육	165	69.6%
	기타	18	7.6%
합계		237	100.0%

분석 도구로는 SmartPLS를 사용하였다. PLS를 사용한 주요 이유는 크게 두 가가 있다. 첫째 본 연구의 주요 목적이 최상의 인과관계를 생산하기 보다는 특정 경로의 예측 타당성을 증명하는 것

이다. 둘째, 보안위험관리에 영향을 미치는 구성요소에 대한 분석은 비교적 새로운 연구 분야로 이론적 정립이 미약하고, 신뢰성과 타당성이 높은 측정기법에 관한 선행연구 또한 부족하기 때문이다. 이는 곧 본 연구의 성격이 확인적이기 보다는 탐색적 성향이 강하다고 할 수 있다. 이에 AMOS 또는 과 같은 공분산구조 모형 보다는 PLS와 같은 분산구조 모형 접근방법이 더 적합하다.

구조모형 검증을 하기 전에 최종 수집된 데이터(n = 237)로 측정항목에 대한 타당성 검증을 실시하였다. 측정항목의 타당성은 개발항목 신뢰도(individual item reliability), 내적 일관성(internal consistency)과 판별타당성(discriminant validity) 검증을 통해 증명 하였다. 우선 개별항목 신뢰도는 각 변수와 관련된 측정항목의 개별항목 요인적재값을 사용할 수 있으며, 요인 적재값은 최소 0.7 이상이어야 개별항목 신뢰도에 문제가 없는 것으로(Carmines and Zeller, 1979). 다음으로 내적 일관성 검증은 일반적으로 가장 많이 사용되는 Cronbach's Alpha 계수를 이용하였으며, Alpha값이 0.7 이상이면 신뢰성이 확보되었다고 할 수 있다(Nunnally, 1967). 마지막으로 판별타당성은 잠재변수들 간의 개념이 뚜렷이 구별되는 정도를 검증하며, Fornell and Larcker(1981)이 제안한 평균분산추출(Average Variance Extracted: AVE)과 잠재변수들 간의 상관관계분석 방법을 사용하였다. 각 잠재변수의 AVE 제곱근 값이 해당 그 잠재변수와 다른 잠재변수간의 종과 회의 상관계수 값을 초과하면 판별타당성이 존재하는 것으로 본다.

측정모형의 타당성 검증 결과는 <표 4>과 <표 5>에서 보여 준다. 개별항목 신뢰도 검증에서 3개 항목(sep3, sp3, aSRM2)이 기준값(0.7) 이하로 나타나 이 세 항목을 제외한 후 개별항목 신뢰도를 다시 검증하였다. 그 결과 개별항목 신뢰도를 저해하는 항목은 없었다. 또한 Cronbach's Alpha 값을 사용한 내적 일관성 검증 결과 Alpha값은 0.830에서 0.938로 분포되어 권장치(0.7 이상) 이상으로 나타나 내적 일관성에는 문제가 없는 것으로 판단된다. 마지막으로 판별타당성 검증 결과는 <표 5>에서 나타나듯이 각 잠재변수의 AVE 제곱근 값이 인접하고 있는 종과 횡의 변수들 간의 상관계수들보다 크게 나타나 측정도구의 판별타당성 역시 확보된 것으로 나타났다. 측정모형에 대한 검증결과는 본 연구에 사용된 측정항목의 내적 일관성 및 타당성을 통계적으로 증명하고 있다.

4.3 구조모형 분석

본 연구에서 제안한 가설들 검증하기 위해 총 366개의 데이터로 SmartPLS를 사용하여 구조방정식 분석을 실시하였다. 구조방정식 분석을 측정모형의 타당성 검증 후 연구모형에서 제시한 변수들 간의 관계를 검증하기 위해 SmartPLS를 사용하여 구조방정식 분석을 실시하였다. PLS에서 제공하는 부스트랩 리샘플링 방법(bootstrap resampling method)으로 500번 리샘플링한 뒤 연구모형의 각 경로를 분석하였다.

분석 결과, 첫째, 본 연구에서 제안하는 인지요인 변수인 보안관리행동, 보안의무준수, 지각된 이득, 사회적 압력, 보안위험 경험은 보안위험관리 인식에 경로계수 0.269, 0.362, 0.357, 0.536, 0.398로 유의수준 0.05, 0.01, 0.001에서 지지되었다. 따라서 가설 1~가설 3, 가설 5, 가설 6은 채택되었다. 또한 보안관리행동, 보안의무준수, 지각된 이득, 사회적 압력, 보안위험 경험은 보안위험관리 개발의지에 각각 경로계수 0.375, 0.323, 0.299, 0.461, 0.537로 유의수준 0.01, 0.001에서 지지되어 가설 7~가설 9, 가설 11, 가설 12는 채택되었다. 하지만 지각된 희생은 보안위험관리 인식과 개발의지와의 영향관계에서 각각 경로계수 -0.025, 0.098로 유의한 영향을 미치지 않는 것으로 나타나 가설 4와 가설 10은 기각되었다. 또한 총 6개의 외생변수 중 변수별 영향 정도를 살펴보면, 사회적 압력(β = 0.536)이 보안위험관

〈표 4〉 측정변수의 신뢰성 및 타당성 분석 결과

변수	항목	초기 측정모형			수정된 측정모형		
		가중치	요인값	크론바하 알파	가중치	요인값	크론바하 알파
보안관리행동 (Behavior for Security Management)	bsm1	0.257	0.729	0.883	0.242	0.743	0.883
	bsm2	0.324	0.726		0.348	0.729	
	bsm3	0.119	0.855		0.127	0.860	
	bsm4	0.245	0.795		0.213	0.796	
보안의무준수 (Compliance with Security Policy)	sep1	0.694	0.862	0.829	0.514	0.862	0.875
	sep2	0.258	0.820		0.288	0.838	
	sep3	0.357	0.348		삭제		
	sep4	0.195	0.791		0.200	0.810	
지각된 이득 (Perceived Benefits)	pb1	0.394	0.910	0.854	0.351	0.899	0.854
	pb2	0.458	0.845		0.399	0.857	
	pb3	0.099	0.883		0.107	0.860	
	pb4	0.678	0.817		0.664	0.805	
지각된 희생 (Perceived Sacrifice)	ps1	0.394	0.789	0.849	0.326	0.767	0.849
	ps2	0.552	0.855		0.547	0.884	
	ps3	0.428	0.849		0.420	0.857	
	ps4	0.246	0.816		0.269	0.825	
사회적 압력 (Social Pressure)	sp1	0.281	0.830	0.847	0.266	0.838	0.860
	sp2	0.089	0.782		0.110	0.797	
	sp3	0.356	0.442		삭제		
	sp4	0.245	0.769		0.284	0.779	
보안위험경험 (Experience of Security Risks)	esr1	0.546	0.832	0.830	0.586	0.844	0.830
	esr2	0.327	0.817		0.360	0.820	
	esr3	0.290	0.810		0.320	0.833	
	esr4	0.200	0.768		0.258	0.800	
보안위험관리 인식 (Awareness of SRM)	aSRM1	0.348	0.804	0.880	0.388	0.799	0.896
	aSRM2	0.315	0.886		삭제		
	aSRM3	0.299	0.485		0.247	0.842	
	aSRM4	0.259	0.859		0.288	0.847	
	aSRM5	0.138	0.802		0.210	0.869	
보안위험관리 개발의지 (Intention to develop SRM)	iSRM1	0.301	0.795	0.922	0.322	0.810	0.922
	iSRM2	0.371	0.824		0.358	0.827	
	iSRM3	0.244	0.873		0.261	0.873	
	iSRM4	0.348	0.861		0.300	0.866	
	iSRM5	0.094	0.900		0.210	0.915	
보안위험 관리수행 (Performance of SRM)	pSRM1	0.148	0.859	0.938	0.177	0.869	0.938
	pSRM2	0.225	0.887		0.295	0.915	
	pSRM3	0.250	0.913		0.342	0.927	

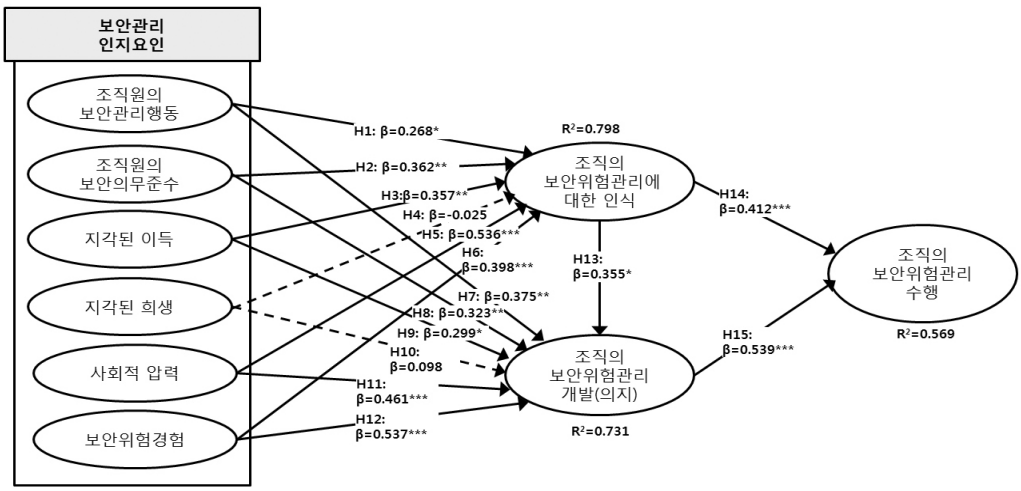
〈표 5〉 잠재변수의 판별타당성 분석결과

변수	1	2	3	4	5	6	7	8	9
1. 보안관리 행동	**0.78**								
2. 보안의무준수	0.21	**0.84**							
3. 지각된 이득	0.18	0.20	**0.86**						
4. 지각된 희생	0.24	0.38	0.41	**0.83**					
5. 사회적 압력	0.33	0.49	0.29	0.28	**0.81**				
6. 보안위험경험	0.12	0.30	0.18	0.25	0.29	**0.82**			
7. 보안위험관리인식	0.35	0.28	0.22	0.38	0.37	0.33	**0.84**		
8. 보안위험관리개발의지	0.31	0.25	0.26	0.45	0.56	0.37	0.28	**0.86**	
9. 보안위험관리수행	0.28	0.27	0.23	0.41	0.25	0.30	0.31	0.46	**0.90**

주) 진하게 표시된 대각선 값은 AVE의 제곱근 값임.

리 인식에 가장 큰 영향을 주는 것으로 나타났으며 보안위험경험(β = 0.537)이 보안위험관리 개발의지에 가장 큰 영향을 미치는 것으로 나타났다. 또한 보안위험관리 인식과 보안위험관리 개발의지 사이의 정(+)의 관계를 나타내는 가설 13은 경로계수 0.355, 유의수준 0.05에서 지지되었다. 마지막으로 보안위험관리 인식 및 개발의지와 보안위험관리 실행 간의 영향관계는 각각 경로계수 0.412와 0.539로 유의수준 0.001에서 지지되어 가설 14, 가설 15 또한 채택되었다.

연구모형에서 제안한 보안관리 인지 요인의 총 6개 변수 중 지각된 희생을 제외한 나머지 5개 변수는 보안위험관리 인식과 보안위험관리 개발의지를 설명하는 분산의 79.8%와 73.1%를 설명하고 있다. 이는 곧 내생변수인 보안위험관리 인식과 보안위험관리 개발의지가 가지고 있는 정보 중 79.8%와 73.1%는 보안관리 인지 요인의 5개 외생 변수의 변동으로 설명할 수 있다는 것을



주) *: p < 0.05, **: p < 0.01, ***: p < 0.001.

〈그림 2〉 구조모형 분석결과

〈표 6〉 가설검증 결과요약

가설	경로	표준화된 경로계수	t-값	채택 유·무
가설 1	보안관리행동 → 보안위험관리 인식	0.269*	3.867	채택
가설 2	보안의무준수 → 보안위험관리 인식	0.362**	4.780	채택
가설 3	지각된 이득 → 보안위험관리 인식	0.357**	6.054	채택
가설 4	지각된 희생 → 보안위험관리 인식	-0.025	-1.084	기각
가설 5	사회적 압력 → 보안위험관리 인식	0.536***	8.994	채택
가설 6	보안위험경험 → 보안위험관리 인식	0.398***	5.948	채택
가설 7	보안관리행동 → 보안위험관리 개발의지	0.375**	5.128	채택
가설 8	보안의무준수 → 보안위험관리 개발의지	0.323**	4.488	채택
가설 9	지각된 이득 → 보안위험관리 개발의지	0.299**	4.377	채택
가설 10	지각된 희생 → 보안위험관리 개발의지	0.098	1.167	기각
가설 11	사회적 압력 → 보안위험관리 개발의지	0.461***	6.775	채택
가설 12	보안위험경험 → 보안위험관리 개발의지	0.537***	9.280	채택
가설 13	보안위험관리 인식 → 보안위험관리 개발의지	0.355*	4.228	채택
가설 14	보안위험관리 인식 → 보안위험관리 수행	0.412***	5.803	채택
가설 15	보안위험관리 개발의지 → 보안위험관리 수행	0.539***	9.182	채택

주) *: $p < 0.05$, **: $p < 0.01$, ***: $p < 0.001$.

의미한다. 또한, 보안위험관리 인식은 보안위험관리 개발의지의 총 62.6%의 분산을 보안위험관리 인식과 보안위험관리 개발의지는 보안위험관리 수행의 총 56.9%의 분산을 설명하고 있다. 다음 <그림 2>와 <표 6>는 가설검정 결과와 채택 유무 결과를 보여 주고 있다.

V. 결 론

5.1 연구결과 요약

정보기술에 의존하는 경영환경에서 조직의 정보시스템 보안위험관리의 필요성과 중요성이 강조되고 있지만 기업들의 보안위험관리에 대한 인식이나 대비가 아직은 미미한 실정이다. 본 연구에서는 기업들의 보안위험관리에 대한 관심을 이끌고 이에 대한 중요성을 강조하기 위해 보안위험관리 활동을 하고 있는 기업들을 대상으로 보안위험관리 인식과 개발의지, 실질적 수행에 영향을 주는 요인들에 대한 실증적 연구를 하였다. 기술발달에 따라 기업들의 정보시스템에 대한 의존도가 높아지고 있는 만큼 보안위험에 노출될 확률도 더 높아져 있으므로 보안위험관리에 대한 개발과 강화가 어느 때보다 요구되고 있다. 따라서 본 연구를 통해 조직의 보안위험관리 인식과 개발의지에 어떤 결정적 영향 요인들이 작용하는지에 대한 이해를 높이고 조직의 보안위험관리 실행을 장려하고자 한다. 또한 기업의 보안관리 관련 실무자들이 보안위험관리에 대한 의사결정을 하는데 중요한 학문적 바탕이 되고자 한다.

이러한 목적을 달성하기 위해 본 연구에서 제시하는 주요 연구 질의는 “조직의 보안위험관리 실행을 이끄는 조직의 내외부적 인지요인들이 보안위험관리 인식과 개발의지에 어떤 영향을 미치는가?”이다. 이러한 연구 질의에 대한 실증

적 증명을 위해서 보안관리 인지요인의 6가지 변수로 조직원의 보안관리행동, 보안의무준수, 지각된 이득, 지각된 희생, 사회적 압력, 보안위험경험을 제안하여 이 변수들이 보안위험관리 인식과 개발의지 나아가 보안위험관리 실행에 어떤 영향을 주는지에 대해 검증하였다.

연구결과를 요약하면 다음과 같다. 첫째, 보안관리 인지요인인 여섯 변수 중 다섯 변수 즉, 조직원의 보안관리행동, 보안의무준수, 지각된 이득, 사회적 압력, 보안위험경험은 보안위험관리 인식과 보안위험관리 개발의지에 긍정적 영향을 미치는 것으로 나타났다. 따라서 조직 내의 조직원들의 보안관리가 조직의 보안위험관리에 중요한 역할을 하는 것을 알 수 있으며 기업의 경영환경이나 보안위험의 노출도 또한 조직이 보안위험관리의 중요성을 인식시켜주는 요인인 것으로 나타났다. 마찬가지로 보안관리를 통해 얻을 수 있는 이득에 대한 기업차원의 이해 또한 조직의 보안위험관리 실행에 도움을 줄 것임을 알 수 있었다. 하지만, 지각된 희생은 보안위험관리 인식 및 개발의지에 유의한 영향을 미치지 않는 것으로 나타났다. 이는 아직은 기업의 보안위험관리에 대한 인식이 미흡하고 기업의 이익이나 성과에 즉각적인 영향을 미치지 못하기 때문에 보안위험관리의 필요성을 인식하거나 개발하고자 하는 의지에 영향을 미치지 않는 것으로 생각된다. 마지막으로 보안위험관리 인식과 보안위험관리 개발의지는 보안위험관리에 대한 실질적 수행에 긍정적 영향을 미치는 것으로 나타났다.

5.2 연구의 시사점

조직의 보안위험관리에 대한 인식과 개발의지를 향상시킬 수 있는 방안이나 보안관리와 관련한 의사결정에 해결책을 제시해 줄 수 있는 연구의 필요성이 대두되고 있는 현실에서 본 연구의 학문적, 실무적 시사점은 다음과 같다. 우선, 보안위험관리에 대한 이해와 지식이 부족한 현실에서 보안관리와 관련된 인지 요인들에 대한 이론적 기반을 제공하였다. 기존의 보안관리에 관한 연구들은 보안위험에 기술적 접근이나 조직원들의 행동에 대한 연구가 대부분이며 이 또한 미미한 실정이다. 따라서 기업의 보안위험관리 인지 요인들을 도출하여 이를 실증적으로 검증한 본 연구는 기업의 보안위험에 대한 인식을 일깨우고 조직의 보안위험관리에 대한 개발 의지를 높일 수 있는 영향 요인에 관한 실증적 연구를 제안하였다는데 그 의미가 있다. 또한 이 같은 인지 요인들의 유효성을 검증하여 조직의 보안 관리자들에게 보안위험관리에 대한 의사결정시 이론적 바탕이 되었다는데 본 연구의 의의가 있다. 이전의 연구들에서 실증적으로 연구되지 않은 요인 및 인과관계 등을 이론화하여 증명했다는데도 시사점이 있다. 이러한 시도는 향후 기업의 보안위험관리에 있어 인식 및 개발 의지 나아가 실질적인 실행을 이끄는 영향관계를 설명하는 이론적 배경이 될 것이며 실무적으로는 기업의 보안위험관리에 대한 의사결정 및 강화, 정책수립 등에 이론적 기반이 될 수 있을 것이다.

실무적으로는 조직의 경쟁력과 위험에 대한 대비와 인식을 이끌기 위해 조직들이 활용하고 적용할 수 있는 보안위험관리에 대해 기업이 실질적으로 어떤 변화와 정책이 필요한지에 대해 알 수 있는 근거를 제시 하였다. 이에 실무적인 기대효과와 활용방안은 크게 두 가지로 제시할 수 있다. 첫째, 본 연구의 실증적 결과를 바탕으로 보안위험관리의 성공적인 수행을 위해 조직에서는 내부적으로 어떤 변화가 필요한지에 대해서 알 수 있다. 이는 곧 급변하는 정보기술 환경 속에서 좀 더 효과적인 보안위험관리 전략이 필요하다는 것을 조직에게 일깨워준다. 또한 보안위험관리 전략을 수립하는데 있어서도 조직은 내부적으로 어떤 변화가 필요하며, 이러한 변화 속에서 조직은 어떤 필요성에 의해 보안위험관리에 대해 인지하게 되는지 실증적으로 증명하였다. 따라서 조직은 변화에 대한 사고와 필요성에

대해 더 많은 지각을 할 수 있는 기회를 가지게 되고 정보보안이라는 이슈에 대한 성공적인 전략을 수립할 수 있을 것이며 이를 통한 기업의 경쟁력 향상과 보안위험에 대한 대비책을 수립할 수 있을 것이다. 본 연구 결과를 통한 두 번째 기대효과와 활용방안은 보안위험관리를 통한 기업의 경쟁력 강화와 위험관리에 대한 체계적인 시스템 확립을 위해서 기업이 어떠한 형태의 접근과 지원을 제공해야 하는지에 대한 정보를 제공한다. 즉 보안위험관리 책임자 및 관련 부서 및 기업의 중역들이 조직의 보안위험관리 개발과 실행을 위해 어떠한 노력과 접근이 필요한지에 대한 정보를 제공한다. 특히 기업 내부 조직원 관리의 중요성뿐 아니라 외부 환경적 요인들에 대한 전략 수립과 대책을 위한 방향을 제시할 수 있는 기반이 될 것이다. 또한 보안위험관리의 필요성에 대한 인식 확산과 개발을 위해서 기업이 더 많은 투자와 노력이 필요 할 것이라는 점도 시사한다.

5.3 연구의 한계점 및 향후 연구방향

본 연구의 한계점은 제안한 보안위험관리에 인지요인들 이외에 기술적, 환경적, 사회적, 자원적 관점 등 다양한 관점의 보안위험관리에 인식 및 의지, 실행에 영향요인들에 대한 이론화와 실증연구가 더 필요할 것으로 보인다. 또한 본 연구에서는 분석대상 기업들의 산업적 특성 등의 환경적 특성에 따른 차이를 고려하지 않고 연구결과를 도출하였다. 따라서 산업의 특징을 세분화하고 다양한 특성에 따른 차이점에 따라 보안위험관리에 대한 조직의 인식 및 개발의지가 달라질 수 있는지에 관한 후속 연구가 필요할 것으로 보인다.

참 고 문 헌

Anderson, J. C., D. C. Jain, and P. K. Chintagunta, "Customer Value Assessment in Business Markets: A State-of-Practice Study", *Journal of Business-to-Business Marketing*, Vol.1, No.1, 1993, pp. 3-29.

Anderson, J. C. and J. A. Narus, "Business Marketing: Understand What Customers Value", *Harvard Business Review*, Vol.76, No.6, 1998, pp. 53-65.

Baker, W. and L. Wallace, "Is Information Security Under Control? Investigating Quality in Information Security Management", *IEEE Security and Privacy*, Vol.5, No.1, 2007, pp. 36-44.

Bakos, J. Y. and B.R. Naultm, "Ownership and Investment in Electronic Networks", *Information Systems Research*, Vol.8, No.4, 1997, pp. 321-341.

Bandura, A., *Social Foundations of Thoughts and Action: A Social Cognitive Theory*, Englewood Cliffs, NJ: Prentice Hall, 1986.

Baskerville, R., "Risk Analysis as a Source of Professional Knowledge", *Computers and Security*, Vol.10, No.9, 1991, pp. 749-764.

Basu, A. and R. W. Blamming, "Synthesis and Decomposition of Processes in Organizations", *Information Systems Research*, Vol.14, No.4, 2003, pp. 337-355.

Bodin, L., L. Gordon, and M. Loeb, "Information Security and Risk Management", *Comm. ACM*, Vol.51, No.4, 2008, pp. 64-68.

Bojanc, R. and J. B. Blazic, "An Economic Modelling Approach to Information Security Risk Management", *International Journal of Information Management*, Vol.28, No.5, 2008, pp. 413-422.

Bolton, R. N. and J. H. Drew, "A Multistage Model of Customers' Assessments of Service Quality and Value", *Journal of Consumer Research*, Vol.17, No.4, 1991, pp. 375-384.

Brady, M. K. and C. J. Robertson, "An Exploratory Study of Service Value in the USA and Ecuador", *International Journal of Service Industry Management*, Vol.10, No.5, 1999, pp. 469-486.

Brancheau, J. C., B. D. Janz, and J. C. Wetherbe, "Key Issues in Information Systems Management: 1994～1995 SIM Delphi Results", *MIS Quarterly*, Vol.20, No.2, 1996, pp. 225-242.

Caelli, W. J., D. Longley, and M. Shain, *Information Security for Managers*, Stockton Press, UK., 1989.

Carmines, E. G. and R. A. Zeller, *Reliability and Validity Assessment*, Newbury Park, CA: Sage Publications, 1979.

Cavusoglu, H., B. Mishra, and S. Raghunathan, "A Model for Evaluating IT Security Investments", *Comm. ACM*, Vol.47, No.3, 2004, pp. 87-92.

Cavusoglu, H., H. Cavusoglu, J. Y. Son, and I. Benbasat, *Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers*, Working paper, Sauder School of Business, University of British Columbia, 2009.

Chan, M., I. Woon, and A. Kankanhalli, "Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior", *Journal of Information Privacy and Security*, Vol.1, No.3, 2005, pp. 18-41.

Chatfield, A. T. and P. Yetton, "Strategic Payoff from EDI as a Function of EDI Embeddedness", *Journal of Management Information Systems*, Vol.16, No.4, 2000, pp. 195-224.

Chwelos, P., I. Benbasat, and A. S. Dexter, "Research Report: Empirical Test of an EDI Adoption Model", *Information Systems Research*, Vol.12, No.3, 2001, pp. 304-321.

Clemins, E. K. and M. C. Row, "Limits to Interfirm Coordination through Information Technology: Results of a Field Study in Consumer Packaged Goods Distribution", *Journal of Management Information Systems*, Vol.10, No.1, 1993, pp. 73-95.

Cox, A., "Power, Value, and Supply Chain Management", *Supply Chain Management: An International Journal*, Vol.4, No.4, 1999, pp. 167-175.

Cox, A., "Business Relationship Alignment: On the Commensurability of Value Capture and Mutuality in Buyer and Supplier Exchange", *Supply Chain Management: An International Journal*, Vol.9, No.5, 2004, pp. 410-420.

Crouhy, M., D. Galai, and R. Mark, *The Essentials fo Risk Management*, McGraw-Hill, Toronto, 2006.

Cybenko, C., "Why Johnny Can't Evaluate Security Risk", *IEEE Security and Privacy*, Vol.4, No.1, 2006, p. 5.

Cyert, R. M. and J. G. March, *A Behavioral Theory of the Firm*, Englewood Cliffs, NJ: Prentice-Hall, 1963.

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.

Dinev, T. and Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies", *Journal of the Association for Information Systems*, Vol.8, No.7, 2007, pp. 386-408.

Doherty, N. F. and H. Fulford, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory analysis", *Information Resources Management Journal*, Vol.18, No.4, 2005, pp. 21-39.

Eggert, A. and W. Ulaga, "Customer Perceived Value: A Substitute for Satisfaction in Business Market?", *Journal of Business and Industrial Marketing*, Vol.7, No.2/3, 2002, pp. 107-118.

Ernst and Young, Moving Beyond Compliance: Ernst and Young's 2008 Global Information Security Survey(available online at http://www.ey.com/Publication/vwLUAssets/2008_Global_Information_Security_Survey_english/$FILE/2008_GISS_ingles.pdf).

Fenz, S. and A. Ekelhart, "Verification, Validation, and Evaluation in Information Security Risk Management", *IEEE Security and Privacy*, Vol.9, No.2, 2011, pp. 58-65.

Finne, T., "Information Systems Risk Management: Key Concepts and Business Processes", *Computer and Security*, Vol.19, No.3, 2000, pp. 234-242.

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

Ganesan, S., "Determinants of Long-term Orientation in Buyerseller Relationships", *J. Marketing*, Vol.58, No.1, 1994, pp. 1-19.

Gipp, N., S. P. Kalafatis, and L. Ledden, "Perceived Value of Corporate Donations: An Empirical Investigation", *International Journal of Nonprofit and Voluntary Sector Marketing*, Vol.13, No.4, 2008, pp. 327-346.

Goodhue, D. L. and D. 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. 13-22.

Halliday, S., K. Badenhorst, and R. von solms, "A Business Approach to Effective Information Technology Risk Analysis and Management", *Information Management and Computer Security*, Vol.4, No.1, 1996, pp. 19-31.

Holbrook, M. B., *The Nature of Customer Value: An Axiology of Services in the Consumption Experience*, Service Quality: New Directions in Theory and Practice Rust R. T. and Oliver R. L.(eds), Sage Publications: Thousand Oaks, CA; 1994, pp. 21-71.

Hammer, M., "The Superefficient Company", *Harvard Business Review*", Vol.79, No.8, 2001, pp. 82-91.

Hong, K. S., Y. P. Chi, L. R. Chao, and J. H. Tang, "An Integrated System Theory of Information Security Management", *Information Management and Computer Security*, Vol.11, No.5, 2003, pp. 243-248.

Hoo, S., *How Much Is Enough? A Risk-Management Approach to Computer Security*, Center for International Security and Cooperation (CISAC), Stanford, 2000.

Hu, Q., P. Hart, and D. Cooke, *The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective*, in Proceedings of the 39th Annual Hawaii International Conference on System Sciences, Washington DC, CA: IEEE Computer Society Press, Vol.6, 2006.

Humphreys, E., "Information Security Management Standards: Compliance, Governance and Risk Management", *Information Security Technical Report*, Vol.13, No.4, 2008, pp. 247-255.

Iacovou, C. L., I Bennasat, and A. S. Dexter, "Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology", *MIS Quarterly*, No.19, No.4, 1995, pp. 465-485.

Ives, B. and M. Olson, "User Involvement and MIS Success: A Review of Research", *Management Science*, Vol.30, No.5, 1984, pp. 586-603.

Jahner, S. and H. Krcmar, *Beyond Technical As-*

pects of Information Security: Risk Culture as a Success Factor for IT Risk Management, in Proceedings of the 11th AMCIS, Omaha, NE, 2005.

Jung, B., I. Han, and S. Lee, "Security Threats to Internet: A Korean Multi-Industry Investigation", *Information and Management*, Vol.38, No.8, 2001, pp. 487-498.

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.

Karahanna, E., D. W. Straun, and N. L. Chervany, "Information Technology Adoption across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs", *MIS Quarterly*, Vol.23, No.3, 1999, pp. 183-213.

Kim, E., S. Shim, and B. Lee, *Rival Precedence and IT Platform Migration: An Empirical Analysis of Network Effects*, *Information Spillover Effects*, *and Mimetic Pressure*, Working Paper, Korea Advanced Institute of Science and Technology, 2009.

Kotler, P., *Marketing Management* (millennium edn), Upper Saddle River, NJ: Prentice Hall, 2000.

Kotulic, A. C. and J. G. Clark, "Why There Aren't More Information Security Research Studies", *Information and Management*, Vol.41, No.5, 2004, pp. 597-607.

Kraemer, K., J. Gibbs, and J. Dedrick, "Environment and Policy Facilitators Shaping e-Commerce Diffusion: A Cross-Country Comparison", In: Applegate, L., Degross, J. I., R. G.(Eds.), Proceedings of the 23rd International Conference on Information System, Wiley Barcelona, Spain, 2002.

Lieberman, M. B. and S. Asaba, "Why Do Firms Imitate Each Other?", *Academy of Management Review*, Vol.31, No.2, 2006, pp. 366-385.

Lohmeyer, D. F., J. McCrory, and S. Pogreb, "Managing Information Security", *The McKinsey Quarterly*, *Special Edition: Risk and Resilience*, Vol.2, 2002, pp. 12-16.

Markus, M. L. and J. Y. Mao, "Participation in Development and Implementation-Updating an Old Tired Concept for Today's IS Contexts", *Journal of the Association for Information systems*, Vol.5, No.11/12, 2004, pp. 514-544.

Mohr, J. J., "The Management and Control of Information in High-Technology Firms", *The Journal of High Technology Management Research*, Vol.7, No.2, 1996, pp. 254-268.

Mukhopadhyay, T. and S. Kekre, "Strategic and Operational Benefits of Electronic Integration in B2B Procurement Processes", *Management Science*, Vol.48, No.10, 2002, pp. 1301-1313.

NIST, *Risk Management Guide for Information Technology System to Security Categories*, National Institute of Standards and Technology (NIST) Special Publication 800-30, 2002.

Nunnally, J. C., *Psychometric theory*, New York: McGraw Hil, 1978l.

Pahnila, S., M. Siponen, and A. Mahmood, *Employees' Behavior towards IS Security Policy Compliance*, 40th Hawaii International Conference on System Sciences, 2007.

Paquette, S., P. T. Jaeger, and S. C. Wilson, "Identifying the Security Risks Associated with Governmental Use of Cloud Computing", *Government Information Quarterly*, Vol.27, No.3, 2010, pp. 245-253.

Pavlou, P. A. and D. Gefen, "Building Effective Online Marketplaces with Institution-Based Trust", *Information Systems Research*, Vol.15, No.1, 2004, pp. 37-59.

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.

Phelps, J., G. Nowak, and E. Ferrell, "Privacy Concerns and Consumer Willingness to Provide Personal Information", *Journal of Public Policy and Marketing*, Vol.19, No.1, 2000, pp. 27-41.

Ransbotham, S. and S. Mitra, "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise", *Information Systems Research*, Vol.20, No.1, 2009, pp. 121-139.

Rhee, H. S., C. Kim, Y. U. Ryu, "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior", *Computers and Security*, Vol.28, No.8, 2009, pp. 816-826.

Samuelson, W. and R. Zeckhauser, "Status Quo Bias in Decision Making", *Journal of Risk and Uncertainty*, Vol.1, No.1, 1988, pp. 7-59.

Siponen, M. T., "Five Dimensions of Information Security Awareness", C*omputers and Society*, Vol.31, No.2, 2001, pp. 24-29.

Siponen, M. T., "Analysis of Modern IS Security Development Approaches: Towards the Next Generation of Social And Adaptable ISS Methods", *Information and Organization*, Vol.15, No.4, 2005, pp. 339-375.

Siponen, M. T., S. Pahnila, and A. Mahmood, "Employees' Adherence to Information Security Policies: An Empirical Study", *in New Approaches for Security, Privacy and Trust in Complex Environments(Proceedings of the 22nd IFIP (International Federation for Information Processing)*), Vol.232, 2007, pp. 133-144.

Sirdeshmukh, D., J. Singh, and B. Sabol, "Consumer Trust, Value and Loyalty in Relational Exchange", *Journal of Marketing*, Vol.66, No.1, 2002, pp. 15-37.

Smith, H. J., J. S. Milberg, and J. S. Burke, "Information Privacy: Measuring Individuals' Concerns About Organizational Practices", *MIS Quarterly,* Vol.20, No.2, 1996, pp. 167-196.

Son, J. Y. and I. Benbasat, "Organizational Buyers' Adoption and Use of B2B Electronic Marketplaces: Efficiency and Legitimacy-Oriented Perspectives", *Journal of Management Information Systems*, Vol.24, No.1, 2007, pp. 55-99.

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

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

Straub, D. W. and R. T. Watson, "Transformational Issues in Researching IS and Net-Enabled Organizations", *Information systems Research*, Vol.12, No.4, 2001, pp. 337-345.

Stoneburner, G., A. Goguen, and A. Feringa, *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology(NIST) Special Publication, Washington D. C., 2004.

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.

Tornatzky, L. G. and M. Fleischer, *The Processes of Technological Innovation*, Lexington Books, Lexington, MA, 1990.

Tsohou, A., S. Kokolakis, M. Karyda, and E. Kiountouzis, "Process-Variance Models in Information Security Awareness Research", *Infor-*

mation Management and Computer Security, Vol.16, No.3, 2008, pp. 271-287.

Ulaga, W. and S. Chacour, "Measuring Customer Perceived Value in Business Markets: A Prerequisite for Marketing Strategy Development and Implementation", *Industrial Marketing Management*, Vol.30, No.6, 2001, pp. 525-540.

Venkatesh, V. and S. Brown, "A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges", *MIS Quarterly*, Vol.25, No.1, 2001, pp. 71-102.

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.

von Solms, B., H. van de Haar, S. H. von Solms, and W. J. Caelli, "A Framework for Information Security Evaluation", *Information and Management*, Vol.26, No.3, 1994, pp. 143-153.

Wanson, E. B. and N. C. Ramiller, "Innovating Mindfully with Information Technology", *MIS Quarterly*, Vol.28, No.4, 2004, pp. 553-583.

Weinstein, N. D., "Testing Four Competing Theories of Health-Protective Behavior", *Health Psychology*, Vol.12, No.4, 1993, pp. 324-333.

Whitman, M. E., "*Security Policy: From Design to Maintenance*", in Information Security: Policy, Processes, and Practices, Starub, D. W., Goodman, S. and Baskerville, R. L.(eds.), Armonk, NY: M. E. Sharpe, Inc, 2008, pp. 123-151.

Williams, M. L. and M. N. Frolick, "The Evolution of EDI for Competitive Advantage: The FedEx Case", *Information Systems Management*, Vol. 18, No.2, 2001, pp. 47-53.

Wixom, B. and H. Watson, "An Empirical Investigation of the Factors Affecting Data Warehousing Success", *MIS Quarterly*, Vol.21, No.2, 2001, pp. 17-41.

Woodruff, R. B., "Customer Value: The Next source of Competitive Advantage", *Journal of the Academy of Marketing Science*, Vol.25, No.2, 1997, pp. 139-153.

Xu, H., "*The Effects of Self-Construal and Perceived Control of Privacy Concerns*", in: Proceedings of the 28th Annual International Conference on Information Systems, Canada, 2007.

Xu, H., X. R. Luo, J. M. Carroll, and M. B. Rosson, "The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing", *Decision Support Systems*, Vol.51, No.1, 2011, pp. 42-52.

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.

Zeithaml, V. A., "Consumer Perceptions of Price, Quality, and Value: A Means-End Model and Synthesis of Evidence", *Journal of Marketing*, Vol.52, 1988, pp. 2-22.

Information Systems Review
Volume 14 Number 2
August 2012

The Impact of Cognitive Factors of IS Security Risk Management(ISM) on Awareness and Intention to Develop ISM

Sanghyun Kim* · Youngmi Song**

Abstract

Organizations that make widely use of information technologies can be more efficient. But, the dependence of information technologies leads to an increase in threat of security. This is the reason why organizations are investing in security risk management (SRM) which is designed to protect of information assets. Noting a lack of empirical research in SRM, we investigate the key factors having a direct effect on performance of SRM. Particularly, this study focused on identifying factors influencing awareness of SRM and Intention to develop SRM in Organization. Based on relevant literature review, six motivating factors, including Behavior for Security Management, Compliance with Security Policy, perceived Benefits, Perceived Sacrifice, Social Pressure, Experience of Security Risks, were initially identified. The results indicated that most perception factors were positively related to Organization's intention to develop SRM and awareness of SRM, which then had positive impact on performance of SRM. But Perceived Sacrifice was not significantly related to two variables which is Organization's intention to develop SRM and awareness of SRM.

Keywords: Security Risk Management(SRM), Organizational Awareness, Intention to Develop SRM, Performance of SRM

* Associate Professor, School of Bus. Admin., Kyungpook National University
** Doctoral Student, School of Bus. Admin., Kyungpook National University

◐ 저 자 소 개 ◑

김 상 현 (ksh@knu.ac.kr)

미국 Washington State University에서 호텔경영학 및 경영학 학사와 MBA를 취득하였으며, University of Mississippi에서 경영학박사학위를 취득하였다. 현재 경북대학교 경영학부에 재직 중이며, 주요 연구 관심분야는 공개소프트웨어, RFID, 유비쿼터스 기술 등이 있다. Information and Management, Information Systems Frontiers, DATABASE, International Journal of Information Management 등에 논문을 발표하였다.

송 영 미 (goodsky@knu.ac.kr)

경북대학교 경영학부에서 석사학위를 취득하였으며 현재 동 대학원 박사과정 중에 있다. 주요 연구 관심분야는 웹 2.0, OSS, 포탈, 모바일 서비스 등이 있다.

논문접수일 : 2012년 04월 11일 **게재확정일 : 2012년 08월 06일**
1차 수정일 : 2012년 07월 02일