Information Systems Review
Vol. 18, No. 1 March 2016
http://dx.doi.org/10.14329/isr.2016.18.1.001

조직의 정보보안 문화 형성이 조직 구성원의 보안 지식 및 준수의도에 미치는 영향 연구

Effect of Security Culture on Security Compliance and Knowledge of Employees

황 인 호 (Inho Hwang) (사)한국창업경영연구원 책임연구원
김 대 진 (Daejin Kim) 중앙대학교 경영경제대학 시간강사, 교신저자
김 태 하 (Taeha Kim) 중앙대학교 경영경제대학 경영학부 교수
김 진 수 (Jinsoo Kim) 중앙대학교 경영경제대학 경영학부 교수

요 약

본 연구는 정보보안 관리 영역 중 불확실성이 상대적으로 높고, 통제가 어려운 내부 조직 구성원에 의한 보안 위협 최소화를 위한 방안을 마련하고자 한다. 즉, 조직원의 정보보안 준수의도를 높이기 위하여, 조직의 보안 노력과 조직원의 보안 이해 간의 관계를 제시한다. 선행 연구를 기반으로 연구 모델 및 연구 가설을 제시하였으며, 정보보안 정책을 보유하고 있는 조직에서 근무하는 직장인 526명을 대상으로 설문을 실시하였다. 또한 구조방정식 모델링을 통하여 가설을 검증하였다. 가설 검증 결과, 조직원의 보안 준수의도를 높이기 위해서는 조직원의 정보보안 지식과 조직의 정보보안 문화가 긍정적인 영향을 미치는 것으로 나타났다. 또한 경영층의 지원, 보안 규정, 보안 가시성, 보안 교육 및 훈련이 보안 문화를 형성하는 선행 요인임을 찾았다. 본 연구는 조직원의 정보보안 준수를 위한 조직 차원의 정보보안 계획 수립 및 이행 측면에서 중요한 시사점을 가진다.

키워드 : 정보보안 준수의도, 정보보안 지식, 보안 문화

Ⅰ. 서 론

정보시스템이 조직의 환경 변화에 대응하기 위한 핵심 가치로 인식되면서, 조직의 정보시스템에 대한 의존도와 투자 비중이 높아지고 있다(Carr, 2003). 조직에서 정보시스템은 조직간의 업무 연계, 조직원간의 커뮤니케이션 및 노하우 전수 등을 보다 손쉽게 가능하도록 함으로써, 생산성을 높이고 있다. 하지만, 조직의 이해관계자간의 상호작용성과 공유의 가치를 제공하는 정보시스템 환경은 조직의 중요 정보에 대한 접근성을 손쉽게 만들어 조직의 정보보안 사고 위협을 높이는 원인이 되고 있다 (Bang *et al*., 2012). 전 세계적으로, 보안 사고의 14%가 조직 정보시스템에 접근이 가능한 내부자에 의해서 발생하고 있으며, 7%는 조직과 연관된 외부 파트너십에 의해 발생한 것으로 나타났다. 2012년에 비해 보안 위협 접근 방식을 비교 하면, 해킹 또는 네트워크 취약점에 의해 발생하는 피해

는 상대적으로 낮아졌지만, 정보에 대한 물리적 접근이나 자신의 특권을 오용 또는 남용함으로써 보안 사고를 일으킨 사례는 늘어나고 있다(Verizon, 2013). 또한 Verizon(2013) 보고서에 따르면, 내부자에 의한 보안 사고는 대외적으로 보고된 결과보다 실제로는 더 많을 것으로 판단하고 있다.

이러한 조직의 정보보안 사고는 단순히 기업의 물리적, 금전적 피해로만 끝나는 것이 아니라, 노출 정보와 관련되어 있는 이해관계자까지 2차 피해로 나타난다. 실제 국내 유수 기업들의 보안 사고로 인한 정보 노출 사고는 많은 고객들의 추가 피해로 나타났다. 따라서, 보안 사고의 잠재적 위협 요인이 될 수 있는 내부자 통제를 통한 정보보안 관리가 무엇보다 중요해지고 있다(Gordon and Loeb, 2002).

조직의 정보보안 사고 예방을 위한 선행 연구를 살펴보면, 크게 조직의 취약한 보안 분야 문제 해결을 위한 기술적 접근과 조직 구성원의 정보보안 준수 동기를 개선하기 위한 연구로 진행되어 왔다. 시스템 개선 측면 연구는 대부분 알고리듬 및 시스템 접근 방법 개선, 보안 표준 정립 등을 통하여 시스템 신뢰성 및 무결성 확립을 위한 기술적 개선 연구 측면으로 이루어져왔다(Dhillon and Backhouse, 2000; Gordon and Loeb, 2002; Saint-Germain, 2005). 반면, 조직원의 정보보안 준수의도 및 행동을 높이기 위한 동기적 차원의 이론을 기반으로 한 연구들은 첫째, 조직원의 잠재적 이탈 행위와 처벌간의 관계를 기반으로 정보보안 위반을 설명한 이론인 억제 이론(D'Arcy *et al*., 2009; Herath and Rao, 2009), 둘째, 정보보안 사전 예방을 위하여 조직원의 태도 변화를 유발하는 요인을 설명한 보호 동기 이론(Ifinedo, 2011; Lee and Larsen, 2009), 마지막으로 개인의 정보보안 선택에 있어 비용, 혜택에 기반하여 합리적 선택을 한다는 합리적 선택 이론(Bulgurcu *et al*., 2010)이 대표적으로 진행되어 왔다. 제시된 이론들의 공통점은 조직의 정보보안 사고 원천 중 한 가지인 조직원의 태도에 대한 변화 및 접근 방법을 설명하고 있다는 것이다.

하지만, 조직원에 의한 정보보안 준수 행동은 단순히 개개인의 태도 변화에 의해서 나타나는 것이 아니라, 조직이 가지고 있는 고유 특성에 의해 영향을 받게 된다(Knapp *et al*., 2006). 더불어, 정보보안에 있어서 조직과 조직원은 상호 간에 교환관계가 성립한다(Emerson, 1976; Molm, 1990). 이에, 조직은 조직원에게 조직이 요구 수준에 맞는 정보보안 활동을 수행하길 바라고, 조직원은 자신의 제한된 정보를 기반으로 의사결정을 하게 된다(Hu *et al*., 2011; Sims, 2003). 또한, 조직원들의 정보보안에 대한 의사결정 및 행동에 따라서 조직의 정보보안 수준이 결정된다(Said *et al*., 2013). 즉, 조직은 조직을 구성하는 개개인의 집합이며, 하나의 사회성을 띄는 집단이기 때문에(Chang and Lin, 2007), 조직이 보유한 문화적 특성을 간과하고, 조직원에 대한 보안 행동을 중심으로 정보보안 억제 및 예방 관리 방안을 설명하는 것은 어려움이 많다.

따라서, 본 연구에서는 조직이 공유하고자 하는 보안 가치와 행동 방향을 설명하는 조직 보안 문화와 개인의 보안 지식 및 준수의도간의 관계를 찾고, 보다 체계적인 정보보안 준수 조직을 구성하기 위한 시사점을 제시하고자 한다.

이에 본 연구 목적은 첫째, 조직 보안 문화가 조직 구성원들의 정보보안 지식 형성 및 준수의도에 미치는 영향력을 찾고자 한다. 조직의 보안 문화는 조직이 조직원에게 제시하고자 하는 보안적 가치와 방향성이기 때문에, 확고한 보안 문화가 형성될 경우, 조직 구성원 개개인에게 자발적인 보안 지식 형성과 보안 준수의도가 발생할 것으로 판단된다.

둘째, 보안 문화를 결정하는 선행 요인을 찾고자 한다. 선행 연구를 기반으로 경영층 지원, 보안 규정, 보안 교육 및 훈련, 보안 가시성이 조직의 정보보안 문화 수준을 형성할 것으로 판단하였으며, 영향관계를 증명하고자 한다.

본 연구는 총 5개의 단락으로 구성되어 있다.

첫째, 연구의 배경 및 목적을 설명한다. 둘째, 선행 연구를 기반으로 관련 연구 및 연구 가설을 제시한다. 셋째, 연구 모델 및 연구 방법을 설명한다. 넷째, 연구 모델의 타당성과 신뢰성을 파악하고, 연구가설을 검증한다. 마지막으로 본 연구의 시사점과 향후 연구 방향을 제시한다.

Ⅱ. 이론적 배경

2.1 조직과 조직원의 정보보안

정보시스템은 조직과 조직 구성원의 생산성, 협력, 그리고 성과에 영향을 주며, 경쟁 우위를 위한 조직차원의 노력이 강화될수록 정보보안 노력이 중요해진다(West, 2008).

조직의 정보보안 사고 원천 유형을 살펴보면, Loch *et al.*(1992)은 행위 주체(인간-비인간)와 침입 경로 관점(내부적-외부적)으로 구분하였다. 비인간-외부적 정보보안 사고 사례는 자연적 재해를 통해서 나타나는 보안 위협으로서 조직 차원의 사전 통제가 불가능하다. 비인간적-내부적 사고와 인간적-외부적 사고의 경우, 현재 조직의 보안 기술적 취약점에 대한 접근 경로를 통해 정보를 확보하는 유형의 위협으로서, 기술적 개선을 통해서 해결이 가능하다. 반면, 인간적-내부적 사고의 경우, 조직의 정보시스템에 접근이 가능한 내부자에 의한 사고 위협이다.

일반적으로 정보보안에 대한 조직의 노력은 기술적 취약점 개선에 중점을 두고 있는데, 통제에 대한 불확실성이 높은 영역인 내부자에 의한 보안 위협에 대한 통제 및 개선은 상대적으로 취약한 편이다(김상현, 송영미, 2012).

또한 정보 노출 사고를 일으킨 내부자의 직무를 살펴보면, 핵심 정보에 접근권한이 있는 보안이나 시스템 부서 조직원 이외에 일반 사무직, 임원, 기술직 등 조직의 정보시스템 관리 업무 유형과 무관한 것으로 나타나(Verizon, 2013), 조직원의 정보보안 사고 위협을 최소화하기 위한 노력을 통하여 조직원의 보안 준수 의식 및 행동을 변화시키도록 노력하는 것이 중요하다.

조직차원에서 체계적인 보안 관리를 위해서, Straub and Welke(1998)은 보안 계획 수립을 통한 접근의 중요성을 제시하였다. 그들은 내부자(조직원)에 의한 정보보안 위협 억제를 위해서는 억제(Deterrence)-예방(Prevention)-탐지(Detection)-개선(Remedy) 단계의 보안 행동 사이클을 고려하여, 조직원의 보안 준수 행동 수준을 조직에서 고려하는 수준까지 높이기 위한 계획적 접근이 필요하다고 하였다.

반면, 조직원은 조직이 요구하는 정보보안 수준에 대하여 무조건적인 참여 행동을 하지 않는다(West, 2008). 조직에서 조직원은 정보보안의 목표가 아닌 자신만의 고유한 업무 성과 목표를 가지고 있으며, 정보보안 준수 상황에 직면할 경우 자신을 둘러싼 환경과 보유한 정보를 기반으로 의사결정을 하게 된다(Bulgrucu *et al.*, 2010). 따라서 조직원의 정보보안 준수 행동 수준을 높이기 위해서는 정보보안과 관련된 조직의 환경과 조직원의 특성까지 고려해야 한다(Goodhue and Straub, 1991).

즉, 조직의 정보보안 준수 행동은 조직 구성원들의 행동 집합이며, 조직이 체계적인 정보보안 관리시스템을 보유하기 위해서는 조직원의 정보보안 준수 행동을 높이기 위한 사전적 노력을 하는 것이 중요하다.

2.2 조직원 정보보안 준수

2.2.1 정보보안 준수의도

조직의 정보보안 위협 중 내부 조직원에 의한 사건 발생가능성은 조직원의 보안 의지 수준에 따라서 변화한다(Loch *et al.*, 1992). 특히, 조직의 정보시스템에 접근이 가능한 조직원은 직무와 무관하게 정보시스템으로부터 직접적으로 정보 노출 사고를 발생시킬 수 있으며, 부주의로 조직의 정보자원을 타인에게 노출 시킬 수도 있다(D'Arcy *et al.*, 2009; Guo *et al.*, 2011). 즉, 조직원이 조직이

요구하는 정보보안 수준에 맞는 행동을 하도록 보안 전략적 측면에서 계획을 수립하고 이행하도록 유도하는 것이 필요하다(Straub and Welke, 1998).

정보보안 준수의도는 잠재적 보안 피해로부터 조직의 정보 및 기술 자원을 보호하기 위한 조직원의 의도로 정의된다(Bulgurcu *et al*., 2010; Vance *et al*., 2012). 즉, 조직원의 정보보안 준수의도는 자발적인 보안 활동을 위한 조직원의 의지이기 때문에, 조직이 요구하는 정보보안 수준을 달성하기 위해서는 조직원의 정보보안 준수의도를 지속적으로 높이기 위한 노력이 필요하다.

2.2.2 조직원 정보보안 지식과 준수의도

조직원에게 정보보안 행동을 요구하기 위해서는 조직이 요구하는 정보보안 행동 수칙 및 수준을 명확하게 제공하는 것이 필요하다(Herath and Roa, 2009; Siponen *et al*., 2010). 그리고 조직이 제공하는 정책 및 규정, 행동 방식 등을 조직원이 실천하기 위해서는 관련 지식을 명확하게 이해하고 있는 것이 필요하다(Nelson and Cooprider, 1996).

Desouza(2003)은 지식을 경험이나 가치로부터 유래되어 보유한 개인의 통찰력이나 노하우로서, 명시적이거나 암묵적인 형태의 지식으로 정의하고 있다. 조직에서 조직원이 관련된 지식을 명확하게 보유하지 못할 경우, 두려움, 압박, 불확실성, 그리고 걱정 등이 많아지기 때문에, 조직원의 계획 능력 향상, 업무 적합성 등을 높이기 위해서는 조직원의 지식 수준을 높이는 것이 중요하다(Cegarra-Navarro *et al*., 2011). 더불어, 조직의 지식 관리 체계를 사전에 구축하여 조직원들을 지원하는 것이 조직의 성과를 직접적으로 높일 수 있는 선행 조건이다(Tanriverdi, 2005).

조직의 정보보안 관점에서, 조직원의 정보보안에 대한 지식 수준은 정보보안 수용 의도를 높이는 선행 요인이다(Wang 2010). Wang(2010)은 조직원의 정보보안 지식 형성이 개인의 정보보안에 대한 인지와 조직에서의 경험 수준에 기인한다고 보았으며, 또한 정보보안 수용 의도를 높일 수 있다고 하였다. 더불어, Jiang *et al*.(2008)은 온라인 보안에 대한 사용자 지식은 판매자에 대한 태도를 형성한다고 하였으며, Neal *et al*.(2000)은 조직원의 지식 형성은 준수의도와 참여를 높이기 때문에, 조직은 조직원의 지식 보유를 위한 분위기를 형성하는 것이 중요하다고 하였다.

선행 연구를 기반으로, 본 연구에서는 정보보안 지식과 정보보안 준수의도와의 관계에 대하여 다음과 같은 가설을 제시한다.

H1: 조직원의 정보보안 지식 형성은 조직원의 정보보안 준수의도에 긍정적인(+) 영향을 미칠 것이다.

2.3 조직 정보보안 문화 형성

조직 문화는 조직체의 공유된 의미, 언어, 패러다임으로서, 조직의 다양한 환경에서 조직 구성원들이 공유하고 있는 가치판단의 틀이다(Adler and Jelinek, 1986). 조직 문화는 조직이 추구하는 가치의 공유를 통하여 조직 구성원들의 행동에 영향을 주는 핵심 가치를 의미하며, 조직의 다양한 이해관계자들에게 조직 환경의 특성과 개인의 업무 행동 사이의 관계를 제시 및 조절할 수 있기 때문에, 개인의 행동을 결정할 수 있는 중요한 요인이다(Chang and Lin, 2007).

조직 문화는 복합적, 포괄적, 애매한 요인들의 집합이며, '당연시 여기는' 조직 구성원들의 공유된 가정 및 가치에 근거하기 때문에 객관적인 평가가 어렵다(Cameron and Freeman, 1991). 즉, 다문화적 현상으로 설명되기 때문에 조직 문화를 진단하고 분석하기가 쉽지 않다(최성욱, 2005). 이에 Cameron and Quinn(1999)은 조직 문화 진단 및 분석을 위하여 경쟁가치모형(Competing Value Model)을 제시하였다. 그들은 일반적인 조직 문화유형을 신축성과 역동성, 그리고 내부지향성과 외부지향성을 기반으로 네 가지 유형 즉, 관계지향문화, 혁신지향문화, 위계지향문화, 시장지향

문화로 구분하였다. 관계지향문화는 조직원에게 인간미를 기반으로 가족으로 느끼게 하여 조직에 대한 몰입을 높이며, 혁신지향 문화는 역동적, 진취적이기 때문에 조직원들은 위험을 감수하려는 성향을 보인다. 위계지향문화는 조직원에게 통제적으로 구조화하여 원만한 행동을 요구한다. 마지막으로 시장지향문화는 결과 중심적이기 때문에, 업적과 목표달성을 중점적으로 고려한다. 조직 문화가 구성되면, 조직원의 목표, 행동, 성과에 영향을 미치기 때문에, 조직 특성에 맞는 문화를 형성하고 조직원 행동 전환을 위한 전략적 노력을 하는 것이 중요하다.

사회 정체성 이론(Social Identity Theory)에 따르면, 집단화되어 있는 조직 문화의 창출은 조직원의 업무 및 행동에 영향을 미친다(Trice and Beyer, 1993). 직원들은 집단에서 성공과 실패를 공유하고 소속감을 가지게 되며(Campbell and Goritz, 2014), 이렇게 얻어진 소속감을 기반으로 조직원들은 조직 몰입을 높일 뿐만 아니라, 성과 창출을 위한 노력, 조직의 규칙에 반하는 행동 최소화 등 조직의 목표와 비전을 자신의 일상 업무에 적용하기 위한 노력을 한다(Chang and Lai, 2002). 더불어 Campbell and Goritz(2014)은 조직 문화 개발을 위한 목표 및 규범을 설정하고, 행동에 대한 가치를 제공할 경우 조직원의 성과를 높일 수 있다고 하였다. 즉, 바람직한 조직 문화 정립은 조직원의 정체성을 확립시켜 조직의 목적에 적합한 행동을 하게하는 기반 요인이다.

조직 문화 중 정보보안 문화에 대한 개념을 살펴보면, Knapp *et al.*(2006)은 조직원의 활동과 의식에 조직이 요구하는 보안 수준을 내재하여 올바르게 이루어지는 정도로 정의하고 있으며, 김혜정, 안중호(2012)는 조직 환경의 객관적 특성(규정, 정책, 절차 등)을 조직원들에게 인식될 수 있도록 하는 조직의 정보보안 상황으로 정의하고 있다. Chang and Lin(2007)은 조직의 정보보안 문화는 조직의 정보보안 관리 수준을 높인다고 하였다. 또한, Chan *et al.*(2005)은 조직의 정보보안 사회화 및 그룹간의 보안 분위기 형성이 개인의 보안 준수행동에 영향을 준다고 하였다. 즉, 정보보안 문화는 조직의 보안 환경에 맞게 조직원들의 보안 수준을 결정하며, 보안 문화가 체계적으로 정립될수록 조직원의 정보보안 의식이 높아진다(Knapp *et al.*, 2006).

보안 문화 형성이 조직원의 보안 지식 형성에 영향을 미치는 선행연구를 살펴보면, Van Niekerk and Von Solms(2010)는 조직원에 대한 정보보안 관리는 보안 문화 형성을 통해 접근해야 한다고 주장하였다. 정보보안 문화는 조직 문화의 핵심 요인인 조직의 가시적인 구조와 프로세스, 목표와 철학, 그리고 믿음과 느낌 외에 정보보안 행동에 필요한 지식을 함께 고려해야 한다고 하였다. Said *et al.*(2013)은 정보보안 지식 관리는 조직이 가지고 있는 특성에 기반하며, 정보보안 문화가 주요 특성임을 증명하였다. Harnesk and Lindstrom(2011)은 조직 문화를 민첩성과 규정 수준에 따라 4단계로 구분하였으며, 조직 문화 수준이 높을수록 조직원들의 정보보안 공유 행동을 통한 지식 전이 및 준수행동이 높게 나타난다고 하였다. 선행 연구를 기반으로, 본 연구에서는 조직 보안 문화 형성과 조직원의 정보보안 지식 형성과의 관계에 대하여 다음과 같은 가설을 제시한다.

H2: 조직의 보안 문화 형성은 조직원의 정보보안 지식 형성에 긍정적인(+) 영향을 미칠 것이다.

또한, 보안 문화 형성이 조직원의 보안 준수의도에 영향을 미치는 연구결과를 살펴보면, Dugo (2007)는 내부자에 의한 조직의 정보보안 피해 의도에 영향을 미치는 선행 변수로 보안 문화를 제시하였다. 그는 정보보안 문화 수준이 낮을수록 주관적 규범과 조직원의 정보보안 준수 태도를 낮추고 나아가 정보보안 피해 의도를 높인다고 하였다. Li *et al.*(2010)은 조직 정보보안 정책의 동일시 노력이 개인의 정보보안 규범의식을 높인다고 하였다. Herath and Ra(2009)는 조직 차원의 압력이

조직원의 정보보안 정책 준수의도를 높이는 요인이라고 하였으며, D'Arcy and Greene(2014)는 정보보안 문화 수준이 높을수록 조직원의 정보보안 준수의도를 높인다고 하였다. 선행 연구를 기반으로, 본 연구에서는 조직 보안 문화 형성과 조직원의 정보보안 준수의도와의 관계에 대하여 다음과 같은 가설을 제시한다.

H3: 조직의 보안 문화 형성은 조직원의 정보보안 준수의도에 긍정적인(+) 영향을 미칠 것이다.

2.4 조직 정보보안 문화 형성 선행 요인

조직 문화는 단일 문화가 아닌 가치의 조합(combination of values)이며, 해당조직에 문화적 특성을 부여하고 조직 구성원의 의식이나 상징 등으로 반영된다(Quinn and Spreitzer, 1991). 즉, 조직이 요구하는 가치 수준을 조직원에게 바람직하게 제시하고 이끌어 내는 것이 중요한 문화 형성의 조건이다(Campbell and Goritz, 2014).

Campbell and Goritz(2014)는 조직 문화 형성을 위해서는 보안 목표 설정 및 실제 행동을 위한 지원이 무엇보다 중요하다고 하였다. 또한 Crossan *et al.*(2008)은 조직 리더는 조직 문화를 조정하고 변화를 주는 주체라고 하였다. 즉, 조직 경영층의 문화에 대한 방향과 관심, 목표 설정, 그리고 목표 행동을 위한 가치 형성 및 지원은 문화 형성의 중요 선행 요인이다.

본 연구에서는 보안 문화 형성을 위하여 조직의 방향성 정립을 위한 경영층의 지원, 보안 목표 설정을 위한 보안 규정 정립, 그리고 조직 구성원들이 조직이 요구하는 보안 행동에 대하여 가치를 부여하고 바람직한 방향으로 행동할 수 있도록 지속적인 홍보 등 가시성 확보 노력과 교육 및 훈련을 선행 요인으로 제시한다.

2.4.1 경영층 지원

조직원에 대한 경영층의 관심 및 지원은 조직원의 행동에 영향을 주는 중요 요인이다(Sail *et al.*, 2014). 특히, 정보시스템 분야의 경우 경영층의 관심과 지원은 조직원의 새로운 정보시스템에 대한 수용의지를 높이고, 목표 성과를 달성할 수 있는 성공요인으로 제시되고 있다(Liang *et al.*, 2007; Mitchell, 2006).

정보보안 분야의 경영층의 지원에 대한 정의를 살펴보면, Kankanhalli *et al.*(2003)은 정보보안을 위한 경영층의 참여 및 활동, 그리고 보안 문화 활성화를 위한 지원 정도로 정의하였다. 그들은 정보보안 효과성을 높이기 위해서는 사전 예방을 위한 조직 차원의 통합적 노력이 필요하다고 보았으며, 이중 최고경영층의 지원이 중요한 선행 변수임을 증명하였다. 즉, 최고 경영층 주최하에 정보보안 회의 및 관리시스템 운영, 최고 경영층의 자발적인 정보보안 활동 준수, 그리고 최고경영층 차원에서 정보보안 필요성 및 관련 정보 제공 등은 조직원들의 정보보안 행동에 긍정적인 영향을 미친다고 할 수 있다.

이러한 최고경영층의 지원은 조직의 정보보안 분위기를 형성하고 긍정적인 정보보안 문화를 형성하는 요인이다(MacNeil, 2004). 더불어 조직에서 분위기가 형성되면, 조직원의 지식 형성을 돕고, 준수의도 및 참여를 높인다(Neal *et al.*, 2000). Knapp *et al.*(2006)은 정보보안 분야는 조직의 특성을 반영한 정보보안 활동 및 조직원 관리가 필수적이기 때문에, 조직 정보보안 정책 개발 및 조직 정보보안 문화를 활성화시키기 위해서는 최고경영층의 자발적 참여가 우선적으로 고려되어야 됨을 증명하였다. D'Arcy and Greene(2014)는 최고경영층의 지원이 정보보안 문화를 정립시킨다고 하였으며, 김영춘, 정민숙(2012)은 경영진의 리더십이 조직 문화에 긍정적인 영향을 준다고 하였다. 선행 연구를 기반으로, 본 연구에서는 경영층 지원과 정보보안 문화와의 관계에 대하여 다음과 같은 가설을 제시한다.

H4: 경영층 지원은 조직의 정보보안 문화 형성에 긍정적인(+) 영향을 미칠 것이다.

2.4.2 정보보안 규정 확립

정보보안 규정은 조직의 정보시스템 자원의 적절한 사용에 대한 규칙 또는 가이드라인으로 정의된다(Whitman *et al*., 2001). 정보보안 규정에는 조직의 정보보안 목표, 표준 및 규정 준수 요구사항에 대한 설명, 보안 행동에 대한 책임, 그리고 보안 사고 보고 절차 및 진술 방법 등에 대한 설명 등이 포함된다(Kwok and Longley, 1999). 즉, 보안 규정은 조직의 임무, 정보시스템 종류, 규모, 역할, 운영 방식 등 조직의 목표와 특성에 맞는 규정을 말한다.

조직의 현실에 맞게 잘 정의되고 검증된 보안 규정은 조직원로부터 신뢰성을 확보할 수 있다(von Solm, 1999). 따라서 조직의 외부 영향 요인(기술 변화, 산업 표준, 법적 요구사항, 외부 위협 등)과 내부 영향 요인(비즈니스 목표, 문화, 기술 아키텍쳐, 내부 위협 등)을 함께 고려하여 보안 규정을 구성하는 것이 필요하다(Knapp *et al*., 2009).

조직의 체계적인 보안 규정은 보안 문화를 형성하는데 도움이 된다. Griffin and Neal(2000)은 조직 차원의 안전 규정 및 프랙티스 제공이 조직의 안전 분위기를 형성한다고 하였으며, 조직의 분위기는 조직 문화를 형성하는데 핵심적인 요인이 된다(Marcoulides and Heck, 1993). 또한, Faily and Flechais(2010)는 조직에서 원하는 수준의 보안 문화를 달성하기 위해서는 조직의 규정을 조직원에게 인지시킴으로써 가능하다고 보았다. Ruighaver *et al*.(2007)은 조직원 관점에서 정보보안 문화를 살펴보았으며, 보안 정책과 절차의 수준이 조직원들의 구성체인 조직 차원의 정보보안 문화 수준을 결정한다고 하였다. 선행 연구를 기반으로, 본 연구에서는 조직의 정보보안 규정과 정보보안 문화와의 관계에 대하여 다음과 같은 가설을 제시한다.

H5: 정보보안 규정 확립은 조직의 정보보안 문화 형성에 긍정적인(+) 영향을 미칠 것이다.

2.4.3 정보보안 가시성 확보

조직의 정보보안 규정은 조직 내·외부 환경 변화에 따라 지속적으로 변화한다. 새로운 기술의 도입 및 시스템 활용 방식의 변화 등은 조직의 정보보안 목표를 변화시킨다(West, 2008). 조직 정보보안 관리 및 행동 방식을 정확하게 조직원에게 전달하기 위해서는 가시적인 형태로 제공하는 것이 필요하다(Siponen *et al*., 2010).

가시성은 조직에 새로운 정보 및 규칙 등을 적용하는데 있어서 발생할 수 있는 불확실성 및 애로사항 등을 줄이는 중요한 요인이다(Moore and Benbasat, 1991). 가시성은 조직 내 시스템 활용을 다양한 방식으로 보여주는 정도로 정의된다(Venkatesh *et al*., 2003). Venkatesh *et al*.(2003)은 조직원의 IT 수용에 있어서 시스템 활용성에 대한 가시적 정보를 제공하는 것이 실제 개인의 시스템 수용에 영향을 준다고 하였다.

조직의 정보보안 문화를 형성하기 위해서는 보안 준수의 중요성에 대한 메시지가 가시적으로 조직원들에게 제공되는 것이 중요하다. 정보보안 가시성을 확보하는 방법으로 정보 보안 캠페인, 포스터 그리고 머그컵과 같이 쉽게 눈에 보이는 부분에 정보보안 관리 방법 등을 제시하는 것이 필요하다(Siponen *et al*., 2010). Faily and Flechais (2010)는 효과적인 보안 문화 구축은 조직에서 필요한 기술, 절차, 통제 방법 등을 가시적으로 보여줌으로써 가능하다고 하였다. Lacey(2010)은 조직에서 발생할 수 있는 다양한 보안 사건에 대하여 원인을 파악하고 해결 방법들을 조직원에게 가시적으로 제공함으로써, 조직의 보안 문화를 정립시킬 수 있다고 하였다. 선행연구를 기반으로, 본 연구에서는 조직의 정보보안 가시성 확보와 정보보안 문화와의 관계에 대하여 다음과 같은 가설을 제시한다.

H6: 정보보안 가시성 확보는 조직의 정보보안 문화 형성에 긍정적인(+) 영향을 미칠 것이다.

2.4.4 정보보안 교육 및 훈련

조직원의 정보시스템에 대한 접근 가능성은 언제든 조직에서 정보보안 사고가 발생할 수 있음을 의미한다. 따라서, 조직원의 정보보안에 대한 인식을 높이기 위한 조직 차원의 사전 예방 노력이 중요하다(Whitman *et al*., 2001). Thomson and van Niekerk(2012)는 조직의 정보보안 정책에 대한 정보보안 교육 및 훈련은 조직원에게 보안 목적을 정립시키고, 나아가서는 정보보안 협력 문화를 정립할 수 있다고 하였다.

정보보안 교육은 조직의 정보보안 환경, 정책, 행동 규정 등을 조직원이 인식하기 위하여 제공하는 방식 또는 프로그램을 지칭한다(D'Arcy *et al*., 2009). 조직의 체계적인 정보보안 교육 프로그램은 조직원들에게 조직의 정보보안 정책 이해, 보안 사고의 위험에 따른 비용 그리고 정보 자원에 대한 조직원의 책임을 인식시켜 정보보안 활동을 사전에 하도록 유도하며(Straub and Welke, 1998), 나아가 정보시스템의 오용을 감소시킴으로써 생산성 향상을 유도 한다(Lee and Lee, 2002).

반면 정보보안 교육 부족으로 발생한 조직원의 정보보안 정책 및 절차에 대한 인식 결핍은 보안 사고의 원인이 된다(Mitnick, 2003). D'Arcy *et al*.(2009)은 조직의 보안 교육 훈련 프로그램은 조직원의 보안 미준수 행동에 대한 이해와 조직 차원의 엄격한 대응을 이해시키기 때문에, 시스템 오용 의도를 막을 수 있다고 하였다.

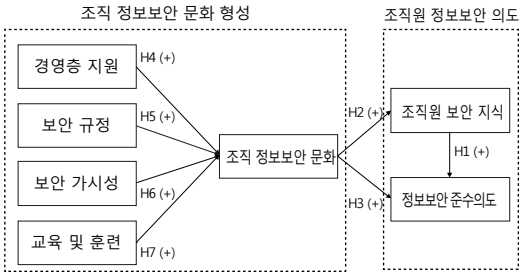
효과적인 정보보안 교육 체계는 조직의 정보보안 문화 수준을 높일 수 있다. Dhillon(1999)은 사용자 교육 프로그램은 조직원들이 보안 이슈를 인식할 수 있도록 도움을 줄 수 있는 효과적인 통제 방식이라고 하였으며, 교육 프로그램은 보안 인식에 대한 조직의 세부적인 문화를 결정할 수 있는 선행요인이라고 하였으며, Van Niekerk and von Solms(2003)은 보안 교육 프로그램의 지원 정도가 조직이 원하는 보안 문화 수준을 결정할 수 있는 선행 요인이라고 하였다. 또한, D'Arcy and Greene(2014)은 보안 훈련과 교육을 통한 조직원의 보안 인식 수준을 높이는 것이 보안 커뮤니케이션을 향상시키고, 보안 문화 수준을 결정한다고 하였다. 선행연구를 기반으로, 본 연구에서는 조직의 정보보안 교육 및 훈련과 정보보안 문화와의 관계에 대하여 다음과 같은 가설을 제시한다.

H7: 정보보안 교육 및 훈련은 조직의 정보보안 문화 형성에 긍정적인(+) 영향을 미칠 것이다.

Ⅲ. 연구 모델 및 방법

3.1 연구 모델

선행 연구를 기반으로 본 연구는 조직의 정보보안 문화 형성이 조직원의 정보보안 지식 형성, 준수의도에 미치는 영향을 분석한다. 더불어, 조직의 정보보안 문화를 형성하기 위한 조직의 행동 요인을 제시하고 관계를 증명하고자 한다. 이에 따른 연구 모델은 다음 <그림 1>과 같다.



〈그림 1〉 연구 모델

3.2 변수의 조작적 정의

연구 모델에서 제시한 변수들의 조작적 정의는 다음 <표 1>과 같다. 각 변수는 정보보안 관련 선행 연구를 기반으로 작성하였으며, 국내 실정에 맞도록 수정 보완하였다.

〈표 1〉 조작적 정의

변수	조작적 정의	선행 연구
경영층 지원	• 정보보안을 위한 경영층 지원 및 노력 정도 • 설문 항목: 경영진의 정보보안 회의 참석/보안 의사결정 참여/보안 활동 참여/보안 시스템 활성화를 위한 기능적 지원	Kankahalli *et al.* (2003)
보안 규정	• 정보시스템 보안 침해 및 사고를 최소화하기 위한 조직의 보안 규정 및 권장하는 절차 • 설문 항목: 시스템 활용 행동 규칙 보유/사전 비인가 컴퓨터 시스템 접근 정책 보유/패스워드 활용 상세 지침 보유/컴퓨터 수행 상세 지침 보유	D'Arcy *et al.* (2009)
보안 가시성	• 조직 내 정보보안 활동이 조직원에게 보이는 정도 • 설문 항목: 정보보안 활동이 조직 내에서 잘 알려져 있음/정보보안 정책은 조직 내에서 자주 볼 수 있음/정보보안 준수 사례를 주위에서 볼 수 있음	Siponen *et al.* (2010)
교육 및 훈련	• 정보보안 정책 및 방향에 대한 교육 및 훈련 정도 • 설문 항목: 조직은 시스템 접속 권한 부여 전에 적절한 교육 및 훈련 수행/인터넷 사용과 관련된 위험에 대한 사전 교육 및 훈련 수행/정보보안 의식 향상을 위한 커뮤니케이션 방법 제공/정보 관련 기술 사용을 위한 사전 교육 및 훈련 수행	D'Arcy *et al.* (2009)
조직 정보보안 문화	• 조직원의 활동과 의식에 조직이 요구하는 보안 수준이 내재하여 올바르게 이루어지는 정도 • 설문 항목: 보안이 조직의 중요한 가치로 인식/보안 활동은 업무 수행에 인정/조직의 전반적 환경이 보안을 고려하도록 설계/조직의 정보보안은 공유되는 핵심 규범	Knapp *et al.* (2006)
조직원 보안지식	• 조직의 정보보안 요구 수준에 대하여 정확하게 알고 있는 정도 • 설문 항목: 정보보안 정책 준수 및 업무 수행 방법 알고 있음/보안 장비 및 절차의 업무 적용 방법을 알고 있음/정보보안 수준 유지 방법을 알고 있음/보안 사고 감소 방법을 알고 있음	Neal *et al.* (2000)
정보보안 준수의도	• 정보보안을 지속적으로 준수할 것인지에 대한 정도 • 설문 항목: 정보보안 정책을 지속적으로 따를 것/정보보호를 위한 준수 가능성이 높음/시스템 접속 시 마다 정보보안 정책 준수/업무 수행 시 정보보안 절차 준수/보안 준수에 대한 나의 태도에 확신	Herath and Rao (2009)

3.3 데이터 측정 방법 및 수집

각 측정 변수들은 7점 리커트 척도를 사용하였으며, "매우 그렇지 않다 (1점)"에서 "매우 그렇다 (7점)"로 설문 문항을 구성하였다. 또한 설문 참여자들은 정보보안 정책을 보유하고 있는 기업에 다니는 조직원을 대상으로 하였다. 한국의 정보보안 상황에 적합한 설문 개발을 위하여, 개발한 설문 문항을 실제 정보보안 정책이 있는 기업에 다니는 10명의 사람들에게 사전 인터뷰를 하였고, 정보보안 관련 10명의 대학원생들에게 설문 항목의 이해도를 질문하였으며, 요구사항에 맞도록 수정하였다.

연구 모델과 가설을 검증하기 위하여 구조방정식 모델을 적용하였으며, 이를 위한 설문을 실시하였다. 설문 수집은 2014년 5월 한 달 동안 연구진이 직접 당사자들을 방문 또는 이메일을 기반으로 실시하였다. 총 535개의 설문이 수집되었으며, 공백으로 제출한 설문 등 오류가 있는 응답 9개를 제외하고 총 526개의 응답지를 분석에 활용하였다.

Ⅳ. 가설 검증

4.1 설문응답자의 표본 특성

설문응답의 인구통계학적 특성은 다음 <표 2>와 같다. 총 526명의 응답 중 남성 271개, 여성 255개가 수집되었으며, 연령은 직업을 보유하고 있는 응답자의 특성을 고려하여 30대 미만에서 50대 미만까지 고르게 표본을 회수했으며, 50대 이상은 37개를 회수하였다. 업종은 서비스업의 비중이 71.9%로 나타났으며, 직급은 사원부터 임원까지 고르게 응답하였다.

〈표 2〉 인구통계학적 특성

구 분		빈도	백분율
총 합계		526	100.0%
성별	남성	271	51.5%
	여성	255	48.5%
연령	30세 미만	137	26.0%
	31~40세	204	38.8%
	41~50세	148	28.1%
	50세 이상	37	7.0%
업종	제조업	148	28.1%
	서비스업	378	71.9%
직급	사원	188	35.7%
	대리	104	19.8%
	과장	104	19.8%
	차부장	112	21.3%
	임원	18	3.4%

인구통계학적 특성 분석 결과, 조직의 정보보안 특성을 분석하기에 적합한 표본으로 수집된 것을 확인하였으며, 수집된 표본을 기반으로 가설 검증을 실시하였다.

4.2 신뢰도 및 타당성 분석

연구 모델 가설 검증 이전에 신뢰성 및 타당도 분석을 실시하였다. 분석 툴은 SPSS 18.0과 SmartPLS 2.0을 활용하였다.

단일 차원 구조로 변환한 측정모형의 평가를 위해 측정 변수들의 신뢰성과 타당성을 평가하였다. 타당성은 측정변수와 요인간의 상관관계 정도를 나타내는 집중 타당성(convergent validity)과 개념들 간의 차이를 나타내는 판별 타당성(discriminant validity)으로 나누어서 평가하였다. 신뢰성 평가는 잠재변수들의 크론바흐 알파값(Cronbach's α)과 합성 신뢰도값(composite reliability)이 0.7 이상이고, 평균분산추출값(Average Variance Extracted: AVE)이 0.5 이상이면 신뢰성이 있는 것으로 보는데, <표 3>을 보면 측정변수 모두 기준 값을 만족하므로 신뢰성이 있는 것으로 평가할 수 있다(Nunnally *et al*., 1994).

집중 타당성 평가는 PLS의 부트스트랩(bootstrap) 방식을 이용해 구성개념에 적재된 측정문항의 요인 적재량과 t-값을 분석하였다. 측정문항들의 요인적재량(factor loading)이 0.5 이상이면 집중 타당성이 있는 것으로 보는데, <표 3>을 보면 측정문항들 모두 기준값을 만족하고, 각 요인의 t-값이 2.576 이상으로 나타나 유의수준 1%에서 모두 유의하므로 집중 타당성이 있는 것으로 평가할 수 있다.

또한, 판별 타당성은 각 구성요소의 평균분산추출값의 제곱근은 종과 횡의 구성개념간 상관계수값보다 커야 판별 타당성이 존재한다고 할 수 있다(Fornell and Larcker, 1981; Noh *et al*., 2013). 분석결과, <표 4>와 같이, 각 구성요소의 평균분산추출값의 제곱근은 종과 횡의 구성개념간 상관계수값보다 커서 판별 타당성이 존재한다고 할 수 있다.

다음으로 독립변수들에 대한 다중공선성의 가능성을 알아보고자 한다. 독립변수의 다중공선성은 공차한계와 분산팽창요인(Variance Inflation Factor: VIF)으로 분석하였다. 일반적으로 VIF가 4 이상, 공차한계가 0.1 이하일 때 다중공선성이 존재한다고 판단한다(Walpole *et al*., 1993).

측정결과 공차한계값은 경영층 지원, 보안 규정, 보안 가시성, 교육 및 훈련 등 측정변수들의 공차한계가 모두 0.1 이상으로 나타났다. VIF 값

〈표 3〉 측정모형의 확인적 요인분석

구성 변수	측정 항목수	요인 적재량	t-값	Cronbach's α	Composite Reliability	AVE
경영층 지원	4	0.946	40.935	0.966	0.908	0.908
		0.959	52.555			
		0.956	49.734			
		0.950	53.493			
보안규정	4	0.915	42.113	0.953	0.877	0.877
		0.957	56.036			
		0.928	49.397			
		0.946	54.267			
보안 가시성	3	0.883	18.757	0.816	0.733	0.733
		0.906	19.355			
		0.774	12.241			
교육 및 훈련	4	0.937	44.072	0.957	0.885	0.885
		0.945	49.726			
		0.952	49.806			
		0.930	55.103			
조직 정보보안 문화	4	0.943	53.575	0.937	0.842	0.842
		0.854	37.327			
		0.938	47.885			
		0.932	52.054			
조직원 보안지식	4	0.952	64.657	0.962	0.897	0.897
		0.962	64.974			
		0.923	49.172			
		0.951	62.820			
정보보안 준수의도	5	0.934	48.280	0.970	0.893	0.893
		0.958	60.776			
		0.962	69.796			
		0.950	65.854			
		0.920	49.953			

〈표 4〉 확인적 요인분석에서 판별 타당성 분석

구성 변수	평균	표준편차	1	2	3	4	5	6	7
경영층 지원	5.96	1.41	**0.953**						
보안 규정	5.83	1.52	0.648**	**0.937**					
보안 가시성	5.31	1.36	0.297**	0.384**	**0.856**				
교육 및 훈련	5.63	1.60	0.678**	0.794**	0.406**	**0.941**			
조직 정보보안 문화	5.69	1.43	0.637**	0.781**	0.454**	0.736**	**0.918**		
조직원 보안 지식	5.80	1.29	0.597**	0.696**	0.444**	0.679**	0.676**	**0.947**	
정보보안 준수의도	6.17	1.16	0.571**	0.667**	0.365**	0.626**	0.666**	0.750**	**0.945**

**p < 0.01/주 대각선의 볼드체 값은 평균분산추출값(AVE)의 제곱근.

〈표 5〉 다중공선성 검증

종속 변수	독립변수	B	β	t	p	공차	VIF
보안 문화	(상수)	0.521					
	경영층 지원	0.170	0.169	4.890	.000	0.508	1.968
	보안 규정	0.423	0.451	10.685	.000	0.342	2.925
	보안 가시성	0.107	0.109	3.992	.000	0.810	1.234
	교육 및 훈련	0.205	0.229	5.1997	.000	0.314	3.184

또한 측정변수들 모두 4 이하로 나타나 다중공선성 문제는 없는 것으로 나타났으며, 타당성이 있다고 평가할 수 있다(<표 5> 참조).

4.3 동일방법편의 검증

본 연구에서 사용된 데이터가 동일시점에 동

〈표 6〉 동일 방법 편의 분석

구성변수	측정변수	실제요인 적재량(R1)	$R1^2$	방법요인 적재량(R2)	$R2^2$
경영층 지원	MS_1	0.746**	0.556	-0.005	0.000
	MS_2	0.732**	0.536	-0.067**	0.004
	MS_3	0.761**	0.579	0.018	0.000
	MS_4	0.768**	0.590	0.052*	0.003
보안규정	SR_1	0.808**	0.653	-0.047	0.002
	SR_2	0.860**	0.740	0.059	0.004
	SR_3	0.832**	0.692	0.064	0.004
	SR_4	0.823**	0.677	-0.069*	0.005
보안 가시성	SV_1	0.452**	0.205	-0.025	0.001
	SV_2	0.488**	0.238	0.027	0.001
	SV_3	0.357**	0.127	0.094	0.009
교육 및 훈련	ET_1	0.833**	0.694	0.064	0.004
	ET_2	0.799**	0.638	-0.117**	0.014
	ET_3	0.843**	0.710	0.058	0.003
	ET_4	0.810**	0.656	-0.005	0.000
조직정보 보안문화	ISC_1	0.837**	0.701	0.015	0.000
	ISC_2	0.698**	0.487	-0.259**	0.067
	ISC_3	0.825**	0.681	0.033	0.001
	ISC_4	0.832**	0.693	0.076*	0.006
조직원 보안지식	SK_1	0.828**	0.686	0.051	0.003
	SK_2	0.824**	0.679	0.000	0.000
	SK_3	0.769**	0.592	-0.117*	0.014
	SK_4	0.837**	0.701	0.077**	0.006
정보보안 준수의도	CI_1	0.786**	0.618	-0.010	0.000
	CI_2	0.821**	0.674	0.047	0.002
	CI_3	0.807**	0.652	-0.013	0.000
	CI_4	0.803**	0.645	0.009	0.000
	CI_5	0.769**	0.591	-0.032	0.001
평균		0.762	0.596	-0.001	0.005

*p < 0.05, **p < 0.01.

일한 측정대상으로부터 자기보고 방법을 통해 측정되었다는 점에서 동일방법편의(common methods bias)가 발생했을 가능성이 있다(Malhotra *et al*., 2006). 이에, 본 연구에서는 동일방법편의를 진단하기 위해 두 가지 검증을 실시하였다.

첫째, 일반적인 방법으로 구성요인들에 대한 상관관계 분석을 실시하여 값이 0.9 이상이면 동일방법편의가 존재한다고 판단할 수 있다(Pavlou *et al*., 2007). <표 4>에서 상관관계 분석을 통해 0.9 이상의 값은 확인되지 않았으므로, 동일방법편의 관련 문제는 없는 것으로 확인되었다.

둘째, 보다 엄격하게 동일방법편의를 진단하기 위해 Podsakoff *et al*.(2003)이 제안한 '비측정 단일 동일방법요인'을 Liang *et al*.(2007)이 PLS에 적용한 방법으로 분석하였다. Podsakoff *et al*.(2003)과 Williams *et al*.(2003)은 PLS 모델로 동일방법편의를 분석하기 위해서 방법변수에 모든 주요 구성변수의 측정변수들을 포함하고, 주요 구성변수와 방법변수에 의해 설명되는 분산을 계산해야 한다(<표 6> 참조).

분석결과 측정변수들의 설명된 평균 분산은 0.596이며, 방법기반 평균 분산은 0.005이다. 실제요인 평균 분산과 방법요인 평균 분산의 비율은 약 109:1이다. 또한 대부분의 방법요인 적재량도 유의하지 않고, 방법요인 분산의 규모가 작고 무의미하므로, 본 연구에서는 동일방법편의에 따른 문제는 심각하지 않다고 볼 수 있다.

4.4 가설 검정

4.4.1 모형 타당성 검증

구조모형에 대한 적합도는 구조모형의 통계추정량을 나타내는 Redundancy 값이 양수일 때 적합도가 있는 것으로 평가하며(Chin, 1998), 내생변수의 R^2 값이 0.26 이상이면 적합도가 '상', 0.13~0.26 미만이면 '중', 0.02~0.13 미만이면 '하'로 평가한다(Cohen, 1988). 그리고 전체 적합도(goodness of fit)은 R^2 값의 평균값과 공통성(communality)의 평균값의 곱을 제곱근한 값으로 평가하는데, 0.36 이상이면 '상', 0.25~0.36 미만이면 '중', 0.1~0.25 미만이면 '하'로 평가한다(Tenenhaus, *et al*., 2005).

<표 7>의 분석 결과를 보면 Redundancy값, R^2 값 그리고 전체 적합도값이 기준 값을 모두 초과하므로 구조모형의 적합도는 높은 것으로 평가할 수 있다. 구조모형의 경로 간 유의성을 검증하기 위한 방법으로 반복적으로 표본을 추출하여 t-값을 제시하는 부트스트랩핑(bootstrapping)을 실시하였으며, 반복샘플(resamples) 수는 1,500회를 실시하였다(Chin, 1998).

〈표 7〉 구조모형의 적합도 분석

변수	R^2	Redundancy	Communality
경영층 지원			0.908
보안 규정			0.877
보안 가시성			0.733
교육 및 훈련			0.885
조직 정보보안 문화	0.677	0.146	0.842
조직원 보안 지식	0.457	0.410	0.897
정보보안 준수의도	0.609	0.272	0.893
평균값	**0.581**		**0.862**
모형적합도	$\sqrt{0.581 \times 0.862} = 0.708$		

본 연구에서는 Redundancy 값의 경우 모두 양의 값을 가지는 것으로 나타났으며, 따라서 구조모형의 적합성이 존재하는 것으로 나타났다.

4.4.2 가설 검증

본 연구에서 제안한 인과모형에 대한 경로 관계는 조직원의 정보보안 의도와 관련된 조직원 보안지식과 정보보안 준수의도가 있으며, 조직 차원의 정보보안 문화 형성과 관련된 경영층 지원, 보안 규정, 보안 가시성, 보안 교육 및 훈련으로 구성된다. 경로간의 인과관계는 다음 <그림 2>, <표 8>의 분석결과에 경로계수 값과 t-값을

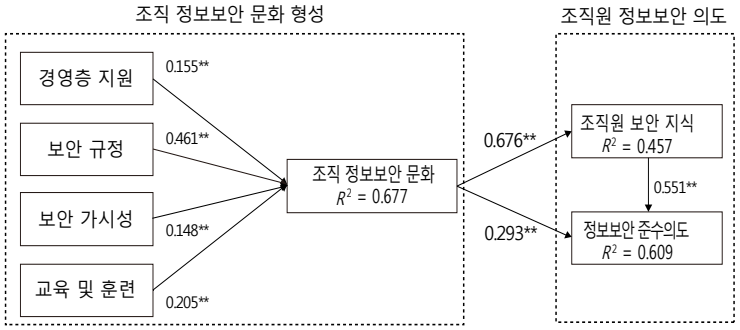
제시함으로써 경로 간 유의성을 평가하였다.

구조방정식 모형 분석 후 다음과 같은 결과가 도출되었다.

첫째, 조직원의 보안지식 형성이 조직원 정보보안 준수의도에 긍정적인 영향을 미친다는 가설은 채택되었다(β = 0.551, p < 0.01). 이러한 결과는 조직의 규정에 맞는 조직원의 행동을 요구하기 위해서는 조직원의 사전 지식 형성을 지원하는 것이 필요하다는 Neal *et al.*(2000)의 연구 결과와 일치한다. 따라서 조직의 정보보안 수준에 맞게 조직원들이 보안 준수를 하도록 하기 위해서는 보안 절차 및 행동 방법 등을 조직원에게 체계적으로 전달함으로써, 정보보안 지식 형성을 할 수 있도록 지원하는 것이 필요하다.

둘째, 조직의 정보보안 문화 형성이 조직원의 정보보안 지식 형성에 긍정적인 영향을 미친다는 가설은 채택되었다(β = 0.676, p < 0.01). 이러한 결과는 조직의 특성에 맞는 보안 문화의 형성이 조직원의 자발적인 보안 지식을 형성할 수 있도록 도움을 준다는 Said *et al.*(2013) 연구와 일치한다. 즉, 조직원들 간의 정보보안 지식 형성 및 공유 활동 등이 자발적으로 이루어질 수 있도록 조직 내 문화를 형성 할 수 있도록 지원하는 것이 필요하다.

셋째, 조직의 정보보안 문화 형성이 조직원의 정보보안 준수의도에 긍정적인 영향을 미친다는 가설은 채택되었다(β = 0.293, p < 0.01). 이러한 결과는 D'Arcy and Green(2014), van Niekerk and von Solms(2010)의 연구 결과와 일치한다. 따라서 문화를 구성할 수 있도록 가시적인 구조, 프로세스, 보안 믿음 및 느낌 등 공유된 정보보안 행동 방식을 조직



**p < 0.01.

〈그림 2〉 경로분석 결과

〈표 8〉 가설검정 결과

가설	경로	경로 계수	표준 오차	t-value	결과
H1	조직원 보안 지식→정보보안 준수의도	0.551	0.053	10.475**	채택
H2	조직 정보보안 문화→조직원 보안 지식	0.676	0.035	19.265**	채택
H3	조직 정보보안 문화→정보보안 준수의도	0.293	0.053	5.564**	채택
H4	경영층 지원→조직 정보보안 문화	0.155	0.050	3.122**	채택
H5	보안 규정→조직 정보보안 문화	0.461	0.068	6.785**	채택
H6	보안 가시성→조직 정보보안 문화	0.148	0.031	4.823**	채택
H7	교육 및 훈련→조직 정보보안 문화	0.205	0.064	3.202**	채택

**p < 0.01.

원들에게 제공하는 것이 필요하다.

넷째, 경영층의 지원이 조직의 정보보안 문화 형성에 긍정적인 영향을 미친다는 가설은 채택되었다(β = 0.155, p < 0.01). 이러한 결과는 D'Arcy and Green(2014), 김영춘, 정민숙(2012)의 연구 결과와 일치한다. 조직의 정보보안은 단순히 보안 시스템 도입만으로 해결되는 문제가 아닌 조직 구성원들의 참여와 행동을 유도해야 하므로, 경영층의 자발적인 참여와 보안 목표 제시, 그리고 참여 유도를 위한 캠페인 등을 실시함으로써, 보안 문화를 형성할 수 있도록 돕는 것이 필요하다.

다섯째, 보안 규정이 조직의 정보보안 문화 형성에 긍정적인 영향을 미친다는 가설은 채택되었다(β = 0.461, p < 0.01). 이러한 결과는 조직 차원의 규정 정립과 프랙티스 제공이 조직의 분위기를 형성한다고 한 Griffin and Neal(2000)의 연구 결과와 일치한다. 즉, 조직의 임무, 정보시스템 활용, 보안 행동 방식 등의 조직 보안 목표와 특성에 맞는 규정을 체계적으로 정립하여 조직원에게 배포하는 것이 필요하다.

여섯째, 정보보안 가시성이 조직의 정보보안 문화 형성에 긍정적인 영향을 미친다는 가설은 채택되었다(β = 0.148, p < 0.01). 이러한 결과는 Faly and Flechais(2010)의 연구 결과와 일치한다. 결국 다양한 상황별 보안 행동 방식에 대하여 쉽게 이해할 수 있는 가시적인 동영상 및 사진 등의 자료들을 조직원들이 볼 수 있는 공간에 제시함으로써 보안에 대한 이해도를 높일 수 있는 지원이 필요하다.

마지막으로, 정보보안 교육 및 훈련이 조직의 정보보안 문화 형성에 긍정적인 영향을 미친다는 가설은 채택되었다(β = 0.205, p < 0.01). 이러한 결과는 van Niekerk and von Solms(2010)의 연구 결과와 일치한다. 조직원의 보안 이슈에 대한 인식 및 오용 방지를 위하여 체계적인 교육 및 훈련을 지속적으로 조직원에게 제공함으로써, 보안 문화를 정립하는 것이 필요하다.

추가적으로, 구조모형 분석 추가 결과인 내생변수(endogenous variable)에 대한 결정계수(R^2)를 도출하였다. 결정계수는 연구모형의 총 변동 중 외생변수(설명변수, 독립변수)들에 의해 설명되는 비율을 의미한다. 연구모형에서 제안한 경영층 지원, 보안 규정, 보안가시성 그리고 교육 및 훈련은 조직의 정보보안 문화 형성 분산의 67.7%를 설명하고 있다. 정보보안 문화는 조직원의 보안 지식 분산의 45.7%를 설명하고 있으며, 조직의 보안문화와 조직원의 보안지식은 정보보안 준수의도 분산의 60.9%를 설명하고 있는 것으로 나타났다.

Ⅴ. 결론 및 향후 연구과제

5.1 연구의 요약

본 연구는 조직원에 의한 정보보안 위협 요인이 많아지고 있는 현 시점에서, 조직원들의 정보보안 준수의도를 높이기 위하여 조직차원의 노력과 조직원의 이해와의 관계를 찾고자 하였다. 정보보안 준수와 관련된 선행연구는 조직원의 관점에서 준수 행동 선행 요인을 주로 도출하고 증명하였으나, 본 연구는 조직과 조직원간의 정보보안 관련 노력 요인과 준수 요인간의 연관성을 제시함으로써, 조직 차원의 정보보안 준수 노력 방법을 제시하고자 하였다.

조직원의 보안 준수 행동 요인으로 보안 지식 형성과 준수의도를 제시하였으며, 조직의 보안 준수 행동 요인으로 보안 문화, 그리고 보안 문화를 형성하는 선행 요인(경영층 지원, 보안 규정 확립, 보안 가시성 확립, 보안 교육 및 훈련)을 제시하였다.

선행 연구를 기반으로 연구 가설 및 연구 모델을 제시하였으며, 구조방정식 모델링을 통하여 연구 가설을 검증하였다. 실증 분석 결과는 조직원의 정보보안 지식이 정보보안 준수의도에 긍정적 영향을 미치는 것을 찾아냈으며, 조직 차원의 정보보안 문화 형성이 조직원의 정보보안 지식 형성

과 준수의도를 높이는 것을 찾아내었다. 더불어, 정보보안 문화를 형성하기 위해서는 경영층의 지원, 보안 규정 정립, 보안 가시성 확립, 보안 교육 및 훈련 제공의 필요성을 증명하였다.

본 연구의 결과는 정보보안의 필요성을 견지하고 있는 많은 조직들에게 조직 구성원의 자발적인 준수의도를 높이기 위한 조직차원의 노력 방향성을 제시할 것으로 판단된다.

5.2 연구의 시사점 및 한계점

본 연구는 다음과 같은 이론적, 실무적 시사점을 가진다. 첫째, 조직원의 정보보안 지식 형성과 준수의도와의 관계를 증명하였다. 조직에서 지식관리는 업무와 관련된 부분에 중점적으로 연구되었으나, 본 연구는 정보보안 지식 형성의 중요성을 제시하였다. 이론적으로, 정보보안 지식 및 지식 공유와 같은 보안 지식 관리 체계 연구를 위한 요인 관계를 제시하였으며, 실무적으로, 조직원의 정보보안 지식 형성을 위한 지원 체계의 필요성을 제시하였다.

둘째, 조직의 정보보안 문화 형성과 조직원의 정보보안 지식 및 준수의도와의 관계를 증명하였다. 보안 문화는 최근까지 조직 전체 측면에서 거버넌스 관점에서 접근되었으나, 본 연구는 조직원과의 관계 측면에서 관련성을 찾고자 하였다. 이론적으로 정보보안 문화 형성이 조직원의 보안 이해 및 행동 수준에 긍정적인 영향을 미치는 것을 증명하였기 때문에, 향후 조직의 문화적 관점에서 보안을 설명하기 위한 선행연구로서의 의미를 가진다. 실무적으로 조직 차원의 보안 문화 형성을 위한 사전 전략적인 접근의 필요성을 제시하였다.

셋째, 정보보안 문화 형성을 위한 조직차원의 노력 요인을 제시하였다. 정보보안은 보안 부서만의 노력으로 이루어지는 것이 아닌 조직 구성원 전체의 문화 형성이 중요한 것이며, 경영층 지원, 보안 규정, 보안 가시성, 보안 교육 및 훈련이 보안문화를 형성하는 선행 요인임을 증명하였다. 이론적으로 향후 보안 문화와 관련한 상세 연구 시 선행 요인으로 활용할 수 있는 기반을 마련하였다. 실무적으로 보안 문화 형성을 위하여 조직이 수행해야 할 방향성을 제시하였기 때문에, 전략적 관점에서 보안 예방을 위한 우선적 고려 요인으로 활용할 수 있을 것으로 판단된다.

본 연구는 향후 연구 측면에서 다음과 같은 한계점을 가진다. 첫째, 본 연구는 정보보안 정책을 보유한 조직에 근무하는 일반인을 대상으로 관련 생각에 대한 설문을 실시하였기 때문에, 보안 관련 실제 행동의 직접적인 요인으로 활용하기에는 어려움이 있다. 따라서 향후 연구 시 외부 환경을 통제하여 정보보안 준수 행동의 원인에 대한 연구를 실시함으로써, 실제 조직과 조직원간의 보안 행동 관계를 찾는 것이 필요할 것으로 판단된다.

둘째, 본 연구는 정보보안 문화 형성을 위한 선행 변수를 제시하여, 보안 문화 형성을 위한 조직의 노력 방향을 제시하였다. 향후 연구 시 문화 형성을 위한 다각적 선행 요인을 제시함으로써, 조직이 수행해야 할 상세한 접근 방향을 제시하는 것이 필요할 것으로 판단된다.

마지막으로, 본 연구는 특정 시간의 설문 응답자 생각을 기반으로 설문을 실시하였기 때문에, 변화하는 조직 구성원들의 생각을 담지 못하였다. 따라서 종단적 연구를 통하여 조직의 정보보안 노력에 따른 조직원의 변화까지 파악한다면, 조직의 정보보안 위협 요인을 체계적으로 판단하여 조직의 보안 정책을 효과적으로 설계할 수 있을 것이다.

참 고 문 헌

[1] 김영춘, 정민숙, “리더십, 조직 문화와 조직 몰입과의 관계”, *한국콘텐츠학회논문지*, 제12권, 제12호, 2012, pp. 201-211.

[2] 김혜정, 안중호, “정보보호 거버넌스 효율성 제고를 위한 조직원의 정보보호 행위에 관한 실증 연구”, *한국전자거래학회지*, 제18권, 제

1호, 2013, pp. 147-164.

[3] 최성욱, "한국행정조직의 문화적 프로필에 관한 연구", *한국행정학보*, 제39권, 제2호, 2005, pp. 41-62.

[4] Adler, N. J. and M. Jelinek, "Is "organization culture" culture bound?", *Human Resource Management*, Vol.25, No.1, 1986, pp. 73-90.

[5] Bang, Y., D. J. Lee, Y. S. Bae, and J. H. Ahn, "Improving information security management: An analysis of id-password usage and a new login vulnerability measure", *International Journal of Information Management*, Vol.32, No.5, 2012, pp. 409-418.

[6] Bulgurcu, B., H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol.34, No.3, 2010, pp. 523-548.

[7] Cameron, K. S. and R. E. Quinn, *Diagnosing and Changing Organizational Culture: Based on The Competing Values Framework*, Addison-Wesley, Readings, MA, 1999.

[8] Cameron, K. S. and S. J. Freeman, "Cultural congruence, strength, and type: Relationships to effectiveness", *Research in Organizational Change and Development*, Vol.5, 1991. pp. 23-58.

[9] Campbell, J. L. and A. S. Göritz, "Culture corrupts! A qualitative study of organizational culture in corrupt organizations", *Journal of Business Ethics*, Vol.120, No.3, 2014, pp. 291-311.

[10] Carr, N. G., "IT doesn't matter", *Educause Review*, Vol.38, No.6, 2003, pp. 24-38.

[11] Cegarra-Navarro, J. G., G. Cepeda-Carrion, and S. Eldridge, "Balancing technology and physician-patient knowledge through an unlearning context", *International Journal of Information Management*, Vol.31, No.5, 2011, pp. 420-427.

[12] Chan, M., I. Woon, and A. Kankanhalli, "Perceptions of information security in the workplace: Linking information security climate to compliant behavior", *Journal of Information Privacy and Security*, Vol.1, No.3, 2005, pp. 18-41.

[13] Chang, J. J. and C. C. Lai, "Is the efficiency wage efficient? The social norm and organizational corruption", *The Scandinavian Journal of Economics*, Vol.104, No.1, 2002, pp. 27-47.

[14] Chang, S. E. and C. S. Lin, "Exploring organizational culture for information security management", *Industrial Management & Data Systems*, Vol.107, No.3, 2007, pp. 438-458.

[15] Chen, Y., K. Ramamurthy, K. and K. W. Wen, "Organizations' information security policy compliance: Stick or carrot approach?", *Journal of Management Information Systems*, Vol.29, No.3, 2012, pp. 157-188.

[16] Chin, W. W., "Issues and opinion on structural equation modeling", *MIS Quarterly*, Vol.22, No.1, 1998, pp. 52-104.

[17] Cohen, J., *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.), Lawrence Erlbaum Associates, Hillsdale, NJ, 1988.

[18] Crossan, M., D. Vera, and L. Nanjad, "Transcendent leadership: Strategic leadership in dynamic environments", *The Leadership Quarterly*, Vol.19, No.5, 2008, pp. 569-581.

[19] D'Arcy, J. and G. Greene, "Security culture and the employment relationship as drivers of employees' security compliance", *Information Management & Computer Security*, Vol.22, No.5, 2014, pp. 474-489.

[20] D'Arcy, J., A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach", *Information Systems Research*, Vol.20, No.1, 2009, pp. 79-98.

[21] Desouza, K. C., "Facilitating tacit knowledge ex-

change", *Communications of the ACM*, Vol.46, No.6, 2003, pp. 85-88.

[22] Dhillon, G., "Managing and controlling computer misuse", *Information Management & Computer Security*, Vol.7, No.4, 1999, pp. 171-175.

[23] Dhillon, G. and J. Backhouse, "Technical opinion: Information system security management in the new millennium", *Communications of the ACM*, Vol.43, No.7, 2000, pp. 125-128.

[24] Dugo, T., *The Insider Threat to Organizational Information Security: A Structural Model and Empirical Test* (Doctoral dissertation), Auburn University, Auburn, AL., 2007.

[25] Emerson, R. M., "Social exchange theory", *Annual Review of Sociology*, Vol.2, 1976, pp. 335-362.

[26] Faily, S. and I. Fléchais, "Designing and aligning e-science security culture with design", *Information Management & Computer Security*, Vol.18, No.5, 2010, pp. 339-349.

[27] 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.

[28] Goodhue, D. L. and D. W. Straub, "Security concerns of system users: a study of perceptions of the adequacy of security", *Information & Management*, Vol.20, No.1, 1991, pp. 13-27.

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

[30] Griffin, M. A. and A. Neal, "Perceptions of safety at work: A framework for linking safety climate to safety performance, knowledge, and motivation", *Journal of Occupational Health Psychology*, Vol.5, No.3, 2000, pp. 347-358.

[31] Guo, K. H., Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding nonmalicious security violations in the workplace: A composite behavior model", *Journal of Management Information Systems*, Vol.28, No.2, 2011, pp. 203-236.

[32] Harnesk, D. and J. Lindström, "Shaping security behaviour through discipline and agility: Implications for information security management", *Information Management & Computer Security*, Vol.19, No.4, 2011, pp. 262-276.

[33] Herath, T. and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol.47, No.2, 2009, pp. 154-165.

[34] Hu, Q., Z. Xu, T. Dinev, and H. Ling, "Does deterrence work in reducing information security policy abuse by employees?", *Communications of the ACM*, Vol.54, No.6, 2011, pp. 54-60.

[35] Ifinedo, P., "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol.31, No.1, 2012, pp. 83-95.

[36] Jiang, J. C., C. A. Chen, and C. C. Wang, "Knowledge and trust in e-Consumers' online shopping behavior", *2008 International Symposium on Electronic Commerce and Security*, August 2008, pp. 652-656.

[37] Kankanhalli, A., H. H. Teo, B. C. 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.

[38] Knapp, K. J., T. E. Marshall, R. K. Rainer, and F. N. Ford, "Information security: Management's effect on culture and policy", *Information Management & Computer Security*, Vol.14, No.1, 2006, pp. 24-36.

[39] Knapp, K. J., R. F. Morris, T. E. Marshall, and T. A. Byrd, "Information security policy: An organizational-level process model", *Computers & Security*, Vol.28, No.7, 2009, pp. 493-508.

[40] Kwok, L. F. and D. Longley, "Information security management and modelling", *Information Management & Computer Security*, Vol.7, No.1, 1999, pp. 30-40.

[41] Lacey, D., "Understanding and transforming organizational security culture", *Information Management & Computer Security*, Vol.18, No.1, 2010, pp. 4-13.

[42] Lee, Y. and K. R. Larsen, "Threat or 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.

[43] Lee, J. and Y. Lee, "A holistic model of computer abuse within organizations", *Information Management & Computer Security*, Vol.10, No.2, 2002, pp. 57-63.

[44] Li, H., J. Zhang, and R. Sarathy, "Understanding compliance with internet use policy from the perspective of rational choice theory", *Decision Support Systems*, Vol.48, No.4, 2010, pp. 635-645.

[45] Liang, H., N. Saraf, Q. Hu, and Y. Xue, "Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top-management", *MIS Quarterly*, Vol.31, No.1, 2007, pp. 59-87.

[46] Loch, K. D., H. H. Carr, and M. E. Warkentin, "Threats to information systems: Today's reality, yesterday's understanding", *MIS Quarterly*, Vol.16, No.2, 1992, pp. 173-186.

[47] MacNeil, C. M., "Exploring the supervisor role as a facilitator of knowledge sharing in teams", *Journal of European Industrial Training*, Vol.28, No.1, 2004, pp. 93-102.

[48] Malhotra, N. K., S. S. Kim, and A. Patil, "Common method variance in is research: A comparison of alternative approaches and a reanalysis of past research", *Management Science*, Vol.52, No.12, 2006, pp. 1865-1883.

[49] Marcoulides, G. A. and R. H. Heck, "Organizational culture and performance: Proposing and testing a model", *Organization Science*, Vol.4, No.2, 1993, pp. 209-225.

[50] Mitchell, V. L., "Knowledge integration and information technology project performance", *MIS Quarterly*, Vol.30, No.4, 2006, pp. 919-939.

[51] Mitnick, K., "Are you the weak link?", *Harvard Business Review*, Vol.81, No.4, 2003, pp. 18-20.

[52] Molm, L. D., "Structure, action, and outcomes: The dynamics of power in social exchange", *American Sociological Review*, Vol.55, No.3, 1990, pp. 427-447.

[53] Moore, G. C. and I. Benbasat, "Development of an instrument to measure the perceptions of adopting an information technology innovation", *Information Systems Research*, Vol.2, No.3, 1991, pp. 192-222.

[54] Neal, A., M. A. Griffin, and P. M. Hart, P. "The impact of organizational climate on safety climate and individual behavior", *Safety Science*, Vol.34, No.1, 2000, pp. 99-109.

[55] Nelson, K. M. and J. G. Cooprider, "The contribution of shared knowledge to is group performance", *MIS Quarterly*, Vol.20, No.4, 1996, pp. 409-432.

[56] Noh, M., K. Lee, S. Kim, and G. Garrison, "Effect of collectivism on actual s-commerce use and the moderating effect of price consciousness", *Journal of Electronic Commerce Research*, Vol.14, No.3, 2013, pp. 244-260.

[57] Nunnally, J. C. and I. H. Bernstein, *Psychometric Theory*(3rd ed.), McGraw-Hill, New York, 1994.

[58] Nunnally, J. C., *Psychometric Theory* (2nd ed.), New York: McGraw-Hill, 1978.

[59] Pavlou, P. A. and M. Fygenson, "Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior", *MIS Quarterly*, Vol.30, No.1, 2006, pp. 115-144.

[60] Podsakoff, P., S. MacKenzie, J. Lee, and N. Podsakoff, "Common method biases in behavioral research: A critical review of the literature and recommended remedies", *Journal of Applied Psychology*, Vol.88, No.5, 2003, pp. 879-903.

[61] Quinn, R. E. and G. M. Spreitzer, "The psychometrics of the competing values culture instrument and an analysis of the impact of organizational culture on quality of life", *Research in Organizational Change and Development*, Vol.5, 1991, pp. 115-142.

[62] Ruighaver, A. B., S. B. Maynard, and S. Chang, "Organizational security culture: Extending the end-user perspective", *Computers & Security*, Vol.26, No.1, 2007, pp. 56-62.

[63] Said, A. R., H. Abdullah, J. Uli, and Z. A. Mohamed, "Relationship between organizational characteristics and information security knowledge management implementation", *Procedia-Social and Behavioral Sciences*, Vol.123, No.20, 2014, pp. 433-443.

[64] Saint-Germain, R., "Information security management best practice based on ISO/IEC 17799", *Information Management Journal*, Vol.39, No.4, 2005, pp. 60-66.

[65] Sims, C. A., "Implications of rational inattention", *Journal of Monetary Economics*, Vol.50, No.3, 2003, pp. 665-690.

[66] Siponen, M., S. Pahnila, and M. A. Mahmood, "Compliance with information security policies: An empirical investigation", *Computer*, Vol.43, No.2, 2010, pp. 64-71.

[67] 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. 441-464.

[68] Tanriverdi, H., "Information technology relatedness, knowledge management capability, and performance of multibusiness firms", *MIS Quarterly*, Vol.29, No.2, 2005, pp. 311-334.

[69] Tenenhaus, M., V. E. Vinzi, Y.-M. Chatelin, and C. Lauro, "PLS path modeling", *Computational Statistics & Data Analysis*, Vol.48, No.1, 2005, pp. 159-205.

[70] Thomson, K. and J. van Niekerk, "Combating information security apathy by encouraging prosocial organizational behavior", *Information Management & Computer Security*, Vol.20, No.1, 2012, pp. 39-46.

[71] Trice, H. M. and J. M. Beyer, *The Culture of Work Organizations*, Prentice Hall, Upper Saddle River, NJ, 1993.

[72] Van Niekerk, J. F. and R. von Solms, "Information security culture: A management perspective", *Computers & Security*, Vol.29, No.4, 2010, pp. 476-486.

[73] Vance, A., M. Siponen, and S. Pahnila, "Motivating is security compliance: Insights from habit and protection motivation theory", *Information & Management*, Vol.49, No.3, 2012, pp. 190-198.

[74] Venkatesh, V., "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model", *Information Systems Research*, Vol.11, No.4, 2000, pp. 342-365.

[75] Venkatesh, V., M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view", *MIS Quarterly*, Vol.27, No.3, 2003, pp. 425-478.

[76] Verizon, *2013 Data Breach Investigations Report*,

2013, Available at, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

[77] Von Solms, R., "Information security management: why standards are important", *Information Management & Computer Security*, Vol.7, No.1, 1999, pp. 50-58.

[78] Wang, P. A., "Information security knowledge and behavior: An adapted model of technology acceptance", *2010 2nd International Conference on Education Technology and Computer* (ICETC), (Vol.2), IEEE, June 2010, pp. 364-367.

[79] West, R., "The psychology of security", *Communications of the ACM*, Vol.51, No.4, 2008, pp. 34-40.

[80] Walpole, R. E., R. H. Myers, S. L. Myers, and K. Ye, *Probability and Statistics for Engineers and Scientists* (Vol.5). New York: Macmillan, 1993.

[81] Whitman, M. E., "In defense of the realm: understanding the threats to information security", *International Journal of Information Management*, Vol.24, No.1, 2004, pp. 43-57.

[82] Whitman, M. E., A. M. Townsend, and R. J. Aalberts, "Information systems security and the need for policy", in M. Khosrowpour (ed.), *Information Security Management: Global Challenges in the New Millennium*, Idea Group Publishing, Hershey, PA, 2001, pp. 9-18.

[83] Williams, L. J., J. R. Edwards, and R. J. Vandenberg, "Recent advances in causal modeling methods for organizational and management research", *Journal of Management*, Vol.29, No.6, 2003, pp. 903-936.

[84] Wixom, B. H. and H. J. Watson, "An empirical investigation of the factors affecting data warehousing success", *MIS Quarterly*, Vol.25, No.1, 2001, pp. 17-41.

Information Systems Review
Volume 18 Number 1
March 2016

Effect of Security Culture on Security Compliance and Knowledge of Employees

Inho Hwang* · Daejin Kim** · Taeha Kim*** · Jinsoo Kim****

Abstract

This study proposes an alternative to minimize insider-caused security threats that are relatively difficult to control and cause high uncertainty in information security management. Therefore, we investigate the relationship between organizational effort and the security understanding of employees to eventually enhance security compliance intention among employees. We develop a research model and formulate hypotheses on the basis of past findings. Accomplished questionnaires are collected from 526 employees working in organizations where information security policy is being implemented. In addition, we prove the hypotheses using a structural model. After reviewing the structural model, the security knowledge of employees and information security culture are determined to positively influence the security compliance intention of employees. Moreover, top management support, security policy, security visibility, and security education programs are proven to be antecedent factors in establishing a security culture in organizations. The findings of this study could guide organizations in formulating information security strategies to enhance the security compliance intention of employees.

Keywords: Security Compliance, Security Knowledge, Security Culture

* Lecturer, Researcher, Korea Entrepreneurship & Management Institute
** Corresponding Author, College of Business and Economics, Chung-Ang University
*** Professor, College of Business and Economics, Chung-Ang University
**** Professor, College of Business and Economics, Chung-Ang University

◐ 저 자 소 개 ◑

황 인 호 (hwanginho@nate.com)

현재 (사)한국창업경영연구원 정보전략 연구팀장으로 재직하고 있다. 중앙대학교 경영학 박사학위를 수여하였다. IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야에 관심을 가지고 연구를 진행 중이다.

김 대 진 (yauchee@cau.ac.kr)

현재 중앙대학교 경영경제대학 시간강사로 활동하고 있다. 중앙대학교 경영학 박사학위를 수여하였다. IT 수용, 비즈니스 모델, 정보보안 및 프라이버시 분야 등에 관심을 가지고 연구를 진행 중이다.

김 태 하 (tkim@cau.ac.kr)

현재 중앙대학교 경영경제대학 경영학과 교수로 재직하고 있다. 서울대 경영학과 및 MBA를 거쳐, 아리조나 대학에서 경영정보학 박사학위를 수여하였으며, 조지메이슨 대학에서 교수로 재직하였다. 주요 관심분야는 디지털 제품의 유통 및 보호, IT 투자 전략 등이다.

김 진 수 (sunny@cau.ac.kr)

현재 중앙대학교 경영경제대학 경영학과 교수로 재직하고 있다. 연세대 상경대학 응용통계학과, 텍사스 주립대학 MBA를 거쳐, 루이지애나 주립대학(LSU)에서 경영정보학 박사학위를 수여하였다. 한국데이타베이스 학회장을 역임하였으며, 현재 한국창업교육협의회 회장을 맡고 있다. 주요 관심분야는 ICT 융합 및 IT 서비스전략, 비즈니스 모델, 빅데이터, 기업가정신과 혁신, 벤처기술창업 등이다.

논문접수일 : 2015년 07월 14일 **게재확정일 : 2015년 12월 11일**
1차 수정일 : 2015년 09월 03일 **2차 수정일 : 2015년 10월 29일**