Information Systems Review
Vol. 18, No. 3 September 2016 http://dx.doi.org/10.14329/isr.2016.18.3.137

경영진의 정보보안 지능이 조직원의 보안대책 인식에 미치는 영향

The Effect of Managerial Information Security Intelligence on the Employee's Information Security Countermeasure Awareness

한 진 영 (Jin Young Han) 중앙대학교 창의ICT공과대학
유 현 선 (Hyun-Sun Ryu) 성균관대학교 소프트웨어 대학, 교신저자

요 약

조직의 비즈니스 환경이 스마트워크와 같이 모바일이나 네트워크에 의존하는 비중이 높아지면서, 기업들은 정보보안에 더 높은 관심을 가지게 되었다. 특히, 내부자의 의한 정보유출은 기업입장에서 상당히 부정적인 영향을 미치게 된다. 따라서 기업뿐 아니라 정보보안 관련 연구자들은 조직원의 정보보안 정책 준수에 초점을 두어 연구를 해왔다. 그 중에서 정보보안 대책(Information security countermeasure)은 조직원의 정보보안 정책 준수 의도의 선행요인으로 알려져 왔다. 하지만 조직원이 정보보안 대책을 인식하도록 하는 선행요인에 대한 연구는 미흡한 실정이다. 본 연구는 조직원의 보안대책 인식에 대한 선행요인으로 경영진의 정보보안 지능을 제안하고 이들의 관계를 실증적으로 연구하였다. 정보보안 지능은 Kirwan(2008)이 제안한 안전지능을 응용하여 정보보안 관련 문제해결능력, 사회적 역량, 정보보안 지식으로 구성된다. 연구결과 경영진의 정보보안 관련 문제해결 능력과 정보보안 지식은 조직원이 정보보안 정책 및 교육/훈련 프로그램을 인식하는데 긍정적인 영향을 미치는 것으로 나타났다.

키워드 : 정보보안지능, 정보보안대책 인식, 정보보안대책 선행요인, 문제해결능력, 사회적 역량, 정보보안지식

Ⅰ. 서 론

현대 비즈니스 환경은 네트워크에 의존적이며 대부분은 기업들은 정보시스템을 통하여 비즈니스를 운영하고 있다. 급증하는 모발일 환경으로 인해 노트북, 스마트폰, 태블릿 등 자신의 디바이스로 언제 어디서나 회사 업무를 처리할 수 있는 BYOD(Bring Young Own Device)족이 증가하고 있다. 이와 같은 스마트워크 환경으로 기업 내부 정보에 접근할 수 있는 공간적 제약이 사라지면서 다계층, 다각도에서 보안정책을 수립하는 것이 필수적이다. 기업의 정보유출이나 보안 사고는 기업 입장에서 금전적 손실은 물론 기업의 명성이나 이미지에도 큰 손실을 가져올 수 있어 정보보안에 대한 관심은 더욱 높아지고 있다(Ponemon Institute, 2012, 윤일한, 권순동, 2015). 한국인터넷진흥원의 기업부문 실

태조사에 따르면 기업의 정보유출 사고의 원천으로는 외부로부터의 해킹, 내부자에 의한 고의 유출, 기업의 관리실수로 인한 유출, 수탁사에 의한 유출로 순으로 나타났다(임재명 등, 2013). 내부자에 의한 유출의 경우, 조직원의 단순한 실수와 의도적인 유출을 포함한다. 사고의 피해 정도로 따지면 내부자에 의한 사고의 부정적인 영향이 큰 것으로 나타난다. 2014년 발생한 카드 3사의 1억 여건의 개인 카드정보 유출 사례에서 해당 카드사의 직접 또는 간접적인 손실이 보고되었다. 관련 카드사들은 영업정지처분 및 손해배상 등으로 2,000억 원 가량의 비용을 지불한 것으로 추산하였다(안상호, 2014). 또한, 카드사에 대한 신뢰도 측면에서도 상당히 타격이 있었다. 정보유출 당사자인 카드 3사 외에도 카드사 전체의 브랜드 지수(BMSI)가 모두 하락하여 카드사 전체에 부정적인 영향을 미친 것으로 나타났다(리얼미터, 2014).

정보보안 관련 연구 분야에서도 내부 조직원들의 정보보안 준수의도에 영향을 미치는 요인에 대한 연구들이 활발히 진행되어 왔다(Bulgurcu *et al*., 2009, 임명성, 2013). 선행연구들은 조직원의 정보보안정책 준수의도에 영향을 미치는 요인으로 정보보안 정책 및 정보보안 교육/훈련에 대한 조직원의 인지를 연구해 왔고, 정보보안 정책이나 교육/훈련에 대한 인지가 조직원 준수 의도에 긍정적인 영향을 미치는 것으로 나타났다. 하지만 Bulgurcu *et al*.(2010)은 정보보안 정책이나 교육훈련에 대한 인지의 중요성을 강조해 온 반면 이들에 영향을 미치는 선행요인에 대한 연구는 많이 이뤄져 있지 않아 연구의 필요성을 제기하였다. 본 연구의 목적은 정보보안 정책이나 교육/훈련에 대한 조직원의 인지에 영향을 미치는 선행요인을 제시하고 이에 대한 실증연구를 진행하고자 한다. 특히 조직의 정보보안 분위기를 형성하는데 기여하는 것으로 알려진 경영진의 정보보안 관련 지원 또는 참여에 초점을 두어 연구를 하고자 한다(Kankanhalli *et al*., 2003, Knapp *et al*., 2006, Yim, 2012; 황인호 등, 2016). 기존 연구들이 경영진의 정보보안 관련한 참여나 지원을 단순히 하나의 개념으로 다뤄왔으나(Kankanhalli *et al*., 2003, Knapp *et al*., 2006; Yim, 2012; 황인호 등, 2016), 본 연구에서는 경영진의 안전지능 개념을 응용하여 경영진의 정보보안 지능과 이를 구성하고 있는 하위 차원을 제안하여 경영진의 지원이라는 개념을 구체화하고자 한다.

Ⅱ. 정보보안 선행연구

2.1 정보보안 대책 인식

정보보안 대책(information security countermeasure)은 절차적 대책과 기술적 대책으로 구분되며, 절차적 보안대책으로는 정보보안 정책, 정보보안 교육/훈련 프로그램 등이 있고 기술적 보안대책으로는 정보시스템 모니터링이나 안티 바이러스 소프트웨어 등이 있다(Hovav and D'Arcy, 2012). 조직원들이 정보보안 정책을 준수할 수 있도록 하기 위해서는 절차적, 기술적 정보보안 대책이 통합적으로 마련되어야 한다. 두 가지 정보보안 대책 중 조직원의 인적 요인을 고려한 정보보안 교육이나 훈련 프로그램에 대한 조직원들의 인식은 보안준수에 상당한 영향을 미치는 것으로 나타났다(Bulgurcu *et al*., 2009; Hovav and D'Arcy, 2012; 임명성, 2013). 본 연구에서는 절차적 정보보안 대책에 초점을 두며 특히 절차적 정보보안 대책의 선행요인을 탐색하고자 한다.

조직은 정책을 수립함으로써 조직 구성원에게 어떤 행위가 조직에서 수용되는지를 명시적으로 제시하고 구성원들의 의사결정이나 행위에 영향을 미친다(Thomson, 2006). 정보보안 정책에 대한 조직원들의 인식은 정보보안 준수의도나 행위에 대체로 긍정적인 영향을 미치는 것으로 나타났다(Bulgurcu *et al*., 2009; Yim, 2012; 임명성, 2013; 한진영, 김유정, 2015). 정보보안 정책에 대한 인식이 업무생산성 저해나 경영진의 감시 수단으로 인식되는 경우, 정보보안 준수의도에 부정적인 영향을 미치기도 한다(Goel and Chengalur-Smith,

2010).

정보보안 교육/훈련은 조직의 정보자원에 대한 적절한 사용에 대한 교육과 훈련을 의미하며, 조직 구성원들의 정보보안에 대한 인식전환을 통해 장기적인 정보보안 효과를 가져 온다(D'Arcy *et al*., 2009). 또한 정보보안 교육/훈련 프로그램은 조직의 정보자원에 대한 오·남용에 대한 억제수단 중의 하나로 사용되어 왔다. 일반억제이론에 의하면, 조직은 보안교육과 훈련 프로그램을 통해 보안인식을 높일 수 있고, 이를 통해서 내부 직원들의 정보보안 사고를 감소시킬 수 있다(D'Arcy *et al*., 2009). <표 1>에서 보는 바와 같이 최근의 정보보안정책이나 교육/훈련 프로그램 인식은 정보보안 준수의도의 선행요인으로 연구가 진행되어 왔다. Haeussinger and Kranz(2013)는 정보보안 정책의 제공을 선행요인으로, 정보보안 인식을 매개로 하여 정보보안 준수의도를 연구하였고, Bulgurcu *et al*.(2010)은 정보보안 준수태도를 매개로 하여 정보보안 정책에 대한 인식이 정보보안 준수의도에 긍정적인 영향을 미친다는 결과를 보여주었다.

이와 같이 정보보안 정책이나 교육/훈련 프로그램과 같은 정보보안 대책이 정보보안 준수의도나 행동에 미치는 영향에 대한 연구는 진행되어 온 반면 정보보안 대책에 대한 조직원의 인식을 향상시키기 위한 선행요인에 대한 연구는 미흡한 실정이다. 정보보안 관련 정책이 수립되더라도 이를 조직원이 인식하지 못한다면 이는 이빨 없는 종이호랑이에 불과하다(Knapp *et al*., 2009). 따라서 정보보안 대책에 대한 조직원의 인식에 영향을 미치는 요인에 대한 연구가 필요하다.

2.2 관리자의 정보보안 지능

2.2.1 경영진의 지원

회사정책이나 교육에 대해 단순한 공지 정도로는 조직원에게 효과적으로 전달되지 않는다. 적절한 보상이나 제재, 커뮤니케이션을 통한 설득 등 다각적이고 조직적인 지원이 뒷받침되어야 한다. 일반적으로 사람들은 명령이나 규정이 정의된 것만으로 그에 대한 인식이나 준수의지가 높아지지 않는다(Goel and Chengalur-Smith, 2010). 오히려 충분한 설명이 없이 강요되는 경우 불만을 가지게 된다(Goel and Chengalur-Smith, 2010). 실제로 경영

〈표 1〉 정보보안 대책 관련 선행연구

연구자	선행요인	조절/매개요인	분석방법론	연구결과
Bulgurcu *et al*. (2009)	정보보안정책 인식	정보보안 준수태도 절차공정성	조직원 464명 설문	정보보안정책 인식 → 절차적 공정성(+) 정보보안정책인식 → 정보보안 준수태도(+)
Bulgurcu *et al*. (2010)	정보보안정책 인식	결과에 대한 믿음 정보보안 준수태도	조직원 464명 설문	정보보안정책 태도 → 정보보안준수(+)
임명성(2013)	보안정책 효과성 보안 인식 프로그램	인지된 준수비용	금융권 조직원 118명 설문	보안정책 효과성 → 정보보안준수의도(+)
Haeussinger *et al*. (2013)	보안정책 제공 보안 인식 교육/훈련 제공	정보보안 인식	조직원 475명 설문	정보보안 인식 → 정보보안준수의도(+)
이성규 등(2014)	보안교육	조직공정성 (분배, 절차, 상호작용)	조직원 437명 설문	보안교육 → 산업보안정책 준수의도 (유의하지 않음)
한진영, 김유정 (2015)	보안정책 보안 인식 교육프로그램	조직시민행동	조직원 324명 설문	보안정책, 보안인식 교육프로그램 → 정보보안준수의도(+)

진이 정보보안에 대해 충분히 이해하고 관심을 가질 때, 정보보안 정책이나 관련 교육/훈련 프로그램이 원활하게 수립된다고 할 수 있다(Chan *et al*., 2005; Hong *et al*., 2003). 또한, 정보보안에 대한 조직의 분위기 형성에 경영진의 참여가 긍정적으로 기여한다. 정보보안에 대한 경영진의 지원은 조직원의 보안정책 준수의도에 긍정적인 영향을 미치는 것으로 나타났다(Kankanhalli *et al*., 2003; Knapp *et al*., 2006; Yim, 2012, 황인호 등, 2016). 그러나 경영진의 정보보안 관련 참여에 대한 연구는 여전히 부족하며(Knapp *et al*., 2006), 정보보안 관련 경영진의 지원은 “top management support” 또는 “top management attention” 등 제한된 개념과 변수로 연구되어 왔다.

본 연구에서는 정보보안 관련 경영진의 지원이나 참여에 대한 개념을 명확히 하고 세분화하고자 한다. 또한 조직원들의 정보보안 대책에 대한 인식을 향상시키기 위한 요인으로 경영진의 정보보안에 대한 참여를 연구한다. 특히 Kirwin (2008)이 제시한 경영진의 안전지능 개념을 적용하여 경영진의 정보보안 지능을 제안하고 이를 기반으로 조직원의 정보보안 대책 인식의 선행요인으로 연구모델을 수립한다.

2.2.2 경영진의 정보보안 지능

경영진의 안전지능(safety intelligence) 개념은 Kirwan(2008)이 제안하였고, Fruhen *et al*.(2014)은 관련 개념을 발전시켜 하위차원을 정의하고 측정변수를 제안하였다. 안전관련 정책을 수립하여 이행하고, 조직 구성원들의 안전에 대한 인식을 격려하는데 경영진의 안전에 대한 개인성향이 영향을 미치는 것으로 나타났다. 따라서 Fruhen과 연구자들은 경영진의 안전과 관련된 개인속성, 스킬, 지식으로 구분하여 경영진의 안전지능을 제시하였다. 개인성향에는 성격(personality)과 동기부여(motivation)를 포함시켰고, 스킬에는 사회적 역량과 문제해결력(problem-solving)을, 지식에는 안전에 대한 지식(safety knowledge)을 두어 경영진의 안전지능을 구성하였다(Fruhen *et al*., 2014).

안전(safety)이 우발적 피해를 예방하고 감소시키며 적절히 대처하는 정도라면 보안(security)은 악의적인 피해를 예방하고 감소시키기 위해 적절히 대응하는 정도라고 할 수 있다(변상호, 김태윤, 2014). 안전과 보안을 구별하여 사용하기도 하지만 본 연구에서는 조직의 분위기를 형성하는 측면에서 경영진이 관련 주제에 대해 이해하고 정책을 수립하고 조직원을 격려하는 역량에 초점을 두었다. 따라서 안전과 보안의 차별적인 정의나 속성보다는 해당 주제에 대해 경영진 이해정도, 조직원 설득역량, 해당주제에 대한 문제해결력을 중심으로 연구한다.

본 연구에서는 Fruthen *et al*.(2014)이 제시한 안전지능의 구성요소인 개인속성, 스킬, 지식 중 개인속성을 제외하고 정보보안 지능을 구성한다. 안전지능 속성 중에서 개인속성에 해당하는 동기성향, 성격, 리더십 스킬을 제외하였으며, 이들은 안전지능에 미치는 정도가 상대적으로 낮은 속성들이다(Fruthen *et al*., 2014). 따라서 경영진의 정보보안 지능은 정보보안 관련 문제를 이해하고 도출된 아이디어를 실행하는 문제해결능력, 조직원들을 이해하고 조직원을 설득하는 사회적 역량, 정보보안에 대한 지식 세 가지로 구성한다.

문제해결 능력은 경영진의 주요 업무능력 중 하나이며 전반적인 조직의 안전에 영향을 미치는 것으로 알려져 왔다(Zohar and Luria, 2005). 경영진은 정보보안 관련 문제를 이해하고 다양한 원천을 통해 정보를 습득한다. 경영진의 문제해결 능력은 전반적인 조직의 구조나 업무환경의 변화를 가져올 수 있다. 관련 문제에 대해 연구하고 아이디어를 제시하고 실행계획을 수립하는 경영진의 능력은 관련 정책을 효과적으로 수립하는데 영향을 미치게 된다(Fruhen *et al*., 2014). 이와 같이 경영진의 정보보안 관련 문제해결 능력은 조직원들의 정보보안관련 인식에 긍정적인 영향을 미칠 수 있다. 이상의 논의를 토대로 본 연구는 다음과 같은 가설을 설정한다.

H1a: 경영진의 정보보안관련 문제해결력은 직원의 정보보안 정책에 대한 인식에 긍정적인 영향을 미친다.
H2a: 경영진의 정보보안관련 문제해결력은 직원의 정보보안 교육프로그램에 대한 인식에 긍정적인 영향을 미친다.

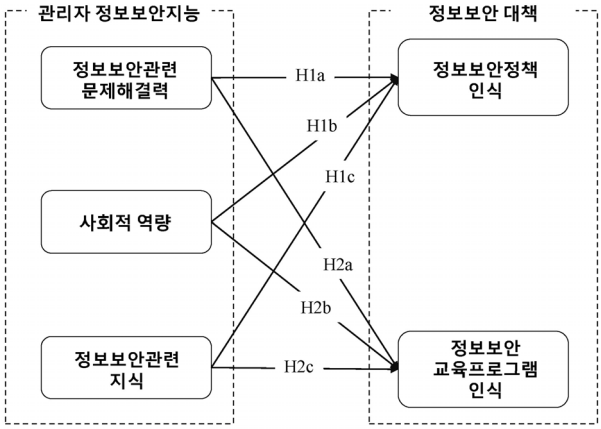
경영진이 조직원들과 커뮤니케이션 하는 주제나 횟수는 경영진의 메시지를 조직원들에게 전달하고 이와 관련된 주제를 강조하는 효과를 가질 수 있다(Harper *et al*., 1996; Hopkins, 2011). 최근 Furhen *et al*.(2013)의 연구는 경영진이 안전과 관련된 주제를 가지고 직원들과 커뮤니케이션 하는 것이 조직의 안전 문화를 형성하는데 긍정적인 영향을 미친다는 것을 보여주었다. 이와 같은 경영진의 사회적 역량은 조직원들과의 정보보안 관련 주제를 가지고 상호작용하는 것은 물론, 조직원이 정보보안 정책이나 관련 훈련 프로그램을 인식하는데 긍정적인 영향을 미칠 것이다. 따라서, 이와 같은 선행연구들을 바탕으로 본 연구는 다음과 같이 가설을 설정한다.

H1b: 경영진의 사회적 역량은 직원의 정보보안 정책에 대한 인식에 긍정적인 영향을 미친다.
H2b: 경영진의 사회적 역량은 직원의 정보보안 교육프로그램에 대한 인식에 긍정적인 영향을 미친다.

업무 전문지식 및 경영관련 지식은 경영진의 리더십이나 경영능력의 한 속성이라 할 수 있다(Finkelstein, 1992). 경영진의 안전관련 지식은 조직 내의 안전성과를 향상시키는 결과를 가져왔다(Griffin and Neal, 2000). 정보보안 관련 지식은 경영진이 정보보안 관련 이슈를 이해하고 관련한 정책을 효과적으로 수립하도록 할 것이다. 정보보안 관련 주제, 사건, 정보에 대한 이해를 기반으로 수립된 정책이나 훈련 프로그램은 조직원들의 인식에 긍정적인 영향을 미칠 것이다. 따라서, 이상의 논의를 토대로 본 연구는 다음과 같은 가설을 설정한다.

H1c: 경영진의 정보보안관련 지식은 직원의 정보보안 정책에 대한 인식에 긍정적인 영향을 미친다.
H2c: 경영진의 정보보안관련 지식은 직원의 정보보안 교육프로그램에 대한 인식에 긍정적인 영향을 미친다.

<그림 1>은 본 연구의 모형을 나타낸 것이다.



〈그림 1〉 연구모형

Ⅲ. 실증분석

3.1 연구대상 및 측정방법

본 연구의 가설검증을 위해서 100명 이상 조직원을 보유하고 있는 기업의 직원을 대상으로 설문조사를 실시하였다. 본 연구 모형에서 제안하는 잠재변수들의 측정을 위한 항목들은 기존의 연구를 바탕으로 추출하여 1차적으로 연구의 목적과 내용에 맞게 수정 및 보완하였다. 관측변수의 내용타당성(content validity) 검증을 위해서 경영관리 및 경영정보시스템 연구자들의 검토를 거쳤다. <표 2>는 연구모형에서 제안하는 각 변수의 조작적 정의, 측정항목, 관련연구를 보여주고 있다. 연구모형의 잠재변수를 측정하기 위한 설문항목은 7점 리커트 척도(Likert scale)로 측정하였다.

데이터 수집은 설문을 웹 페이지로 제작하여 온라인으로 응답할 수 있도록 하였다. 설문 조사 기간은 사전조사는 2014년 11월 1주간 실시하였고, 본 조사는 2014년 12월 1주간 실시하였다. 설문은 357부가 회수되었으며 이 중 미완성 설문 등 유효하지 않은 설문을 제거하고 연구에서는 324부를 사용하였다. 본 연구의 자료 분석에 사용된 설문응답자의 인구통계 특성 및 산업군은 <표 3>과 <표 4>와 같다.

〈표 3〉 표본의 특성

구 분		빈도	비율(%)
성별	남성	160	49.4
	여성	164	50.6
나이	20~29	85	26.2
	30~39	87	26.9
	40~49	87	26.9
	50~59	65	20.1
합계		324	100

〈표 4〉 응답자 조직의 특성

산업군	빈도	비율(%)
제조	114	35.2
전기, 가스 및 수도사업	3	0.9
건설	21	6.5
도소매	19	5.9
통신	13	4.0
금융 및 보험	31	9.6
사업서비스	37	11.4
공공행정, 국방 및 사회보장행정	17	5.2
교육 서비스	34	10.5
보건 및 사회복지사업	14	4.3
오락, 문화 및 운동관련 서비스	6	1.9
기타	15	4.6
합계	324	100

〈표 2〉 변수 정의

변수		조작적 정의	선행 연구
관리자 정보보안지능	정보보안 관련 문제해결력 (Problem-Solving)	정보보안과 관련 문제를 이해하고, 문제해결을 위한 아이디어를 제시 및 실행계획을 수립하는 능력	Fruhen *et al.*(2014)
	사회적 역량 (Social Competence)	타인의 감정을 이해하고 설득할 수 있는 능력	Fruhen *et al.*(2014)
	정보보안관련 지식 (Security Knowledge)	정보보안관련 이슈나 정보에 대해서 이론적으로, 실무적으로 이해하는 정도	Fruhen *et al.*(2014)
정보보안 대책	정보보안 정책 인식 (Information Security Policy Awareness)	정보보안 관련해서 조직에서 정의한 규정 및 권장하는 절차에 대해 조직원이 인식하는 정도	D'Arcy *et al.*(2009)
	정보보안 교육/훈련 프로그램 인식 (Information Security Education Training Awareness Program)	정보보안 정책 및 방향에 대한 교육 및 훈련 프로그램에 대해 조직원이 인식하는 정도	D'Arcy *et al.*(2009)

3.2 요인분석

탐색적 요인분석은 관측변수들 집합 내에서 공변을 설명해주는 잠재변수를 식별하는데 목적이 있다. 본 연구에서는 탐색적 요인분석 기법으로 주성분분석(Principal component analysis)를 사용하였다. 탐색적 요인분석의 기준으로 KMO (Kaiser-Meyer-Olkin)의 표본 적절성 평가와 Bartlett의 구형성 검정이 있다. 수집된 데이터가 요인분석에 적합한 상관관계 행렬을 도출할 수 있는지를 평가하는 기법이다. KMO값은 0.7 이상이 되어야 하며 Bartlett의 구형성은 통계적으로 유의해야 한다. <표 5>와 같이 본 연구에서는 KMO는 0.957이며 Bartlett의 구형성은 유의하게 나타났다.

〈표 5〉 KMO와 Bartlett 검정

표본 적절성 척도		값
KMO(Kaiser-Meyer-Olkin) 척도		.957
Bartlett 구형성 검정	근사카이제곱	8454.077
	자유도	325
	Sig.	.000

탐색적 요인분석은 Varimax 회전을 통한 Kasier 정규화를 실행하였다. 분석결과, 고유값이 1 이상

〈표 6〉 탐색적 요인분석 결과

변수		요인					공통성
잠재변수	측정항목	1	2	3	4	5	
문제해결력	PS1	.337	.378	.281	.208	.651	.802
	PS2	.342	.409	.290	.166	.648	.815
	PS3	.327	.421	.289	.137	.696	.871
	PS4	.359	.452	.270	.156	.648	.851
사회적 역량	SC3	.848	.159	.174	.072	.234	.835
	SC4	.765	.131	.134	.121	.339	.749
	SC5	.847	.219	.153	.061	.265	.862
	SC6	.832	.280	.153	.054	.074	.803
	SC7	.824	.324	.126	.089	.176	.838
	SC8	.861	.314	.170	.017	.103	.880
	SC9	.825	.329	.118	.022	.033	.804
정보보안관련 지식	SK2	.351	.615	.187	.278	.344	.732
	SK7	.353	.705	.227	.191	.352	.834
	SK8	.432	.701	.237	.109	.284	.826
	SK9	.367	.757	.205	.179	.308	.878
	SK10	.400	.717	.243	.136	.271	.825
	SK11	.316	.763	.198	.172	.094	.760
정보보안 정책 인식	ISP2	.162	.291	.471	.571	.019	.660
	ISP3	-.050	.076	.187	.860	.130	.801
	ISP4	.073	.161	.208	.824	.145	.774
	ISP5	.131	.162	.358	.722	.068	.698
정보보안 교육/훈련 프로그램 인식	SETA1	.080	.256	.718	.183	.198	.659
	SETA2	.230	.074	.784	.179	.157	.729
	SETA3	.166	.147	.808	.145	.049	.726
	SETA4	.160	.176	.732	.297	.256	.745
	SETA5	.137	.217	.758	.302	.171	.760
고유값(Eigenvalue)		6.292	4.522	4.077	2.899	2.740	
% 분산		24.200	17.391	15.679	11.110	10.539	
누적 %		24.200	41.591	57.270	68.380	78.919	

이며 요인 적재값(factor loading)의 기준인 0.5를 상회하는 요인 5개를 도출하였다. 각각 측정항목들의 공통성(communality)은 최소 0.66 이상으로 나타났다. 또한 분산 설명력은 일반적 기준인 60% 상회하는 78.9%로 추출된 요인에 대한 충분한 분산설명력이 있는 것으로 나타났다(<표 6> 참조).

공통방법오류(Common method bias)를 검증하기 위하여 Harman single-factor 검증을 수행하였다 (Podsakoff *et al*., 2003). Varimax 회전을 활용한 주성분분석 결과 모든 요인들은 각 각의 해당요인에 높은 적재값을 갖는 것으로 나타났다. 각 요인의 설명력은 전체 분산의 78.9%를 차지하는 것으로 나타났으며 각각의 요인은 최소 10.5%에서 최대 24.2%의 설명력을 가지는 것으로 나타나 공통방법오류 문제가 본 연구에 심각한 영향을 미치지 않는다고 볼 수 있다.

3.3 측정모형 검증

측정모형 검증은 구조방정식 접근방법인 부분최소자승(Partial least Square: PLS) 방식을 사용하였으며, 주요 분석 도구로는 SmartPLS 2.0 M3을 사용하였다. PLS의 경우 컴포넌트를 기반으로 한 접근방식에 의해 추정하기 때문에 표본의 크기와 잔차분포에 대해 다른 구조방정식 접근방법보다 엄격하지 않아 표본수가 적은 경우 유용하다고 할 수 있다. 또한 PLS는 추정모형에 대한 평가와 구조모형에 대한 평가를 동시에 할 수 있는 기법으로, 본 연구에서 측정항목과 구조모형 검증을 실시하기 위해 PLS를 분석도구로 채택하였다(Chin *et al*., 2003). 측정모형의 수렴타당성(Convergent validity), 구성신뢰성(Composite Reliability), 판별타당성(Discriminant validity)을 검증하였다. 수렴타당성은 구성신뢰도와 평균분산추출(Average Variance Extracted: AVE)에 의해 평가하며 <표 7>에서 보는 바와 같이 모든 잠재변수의 AVE의 값이 임계치인 0.5를 충족한다(Fornell and Larcker, 1981). 구성신뢰성 역시 임계치인 0.7보다 큰 것으로 나타나 측정변수들이 수렴 타당성을 가지고 있음을 보여준다(Fornell and Larcker, 1981). 내적일관성을 평가하는 지표로 Cronbach's α는 0.7 이상으로 기준을 충족하는 것으로 나타났다(Fornell and Larcker, 1981).

마지막으로 판별타당성은 AVE의 제곱근 값과 잠재변수들 간의 상관관계 분석 방법을 통해 판단하였다(Fornell and Larcker, 1981). 연구모형에 포함된 각 잠재변수의 AVE 제곱근 값이 해당 잠재변수와 다른 잠재변수 간의 종과 횡의 상관계수 값보다 높게 나타나면 판별타당성이 존재하는 것으로 판단하다. <표 8>에서 보는 바와 같이 모든 잠재변수에 대한 AVE의 제곱근 값이 인접하고 있는 종과 횡의 변수들 간의 상관관계보다 높게 나타났다. 또한, 모든 잠재변수를 측정하는 측

〈표 7〉 변수 타당성 및 신뢰성 분석결과

잠재변수	관측변수 개수 (누락개수)	평균	표준 편차	평균분산추출 (AVE)	복합신뢰성 (CR)	CA
문제해결능력(PS)	4(0)	5.00	1.25	0.85	0.96	0.94
사회적 역량(SC)	9(2)	4.00	1.45	0.78	0.97	0.96
정보보안관련 지식(SK)	11(5)	5.00	1.35	0.79	0.98	0.97
정보보안 정책 인식(ISP)	5(1)	5.00	1.28	0.64	0.90	0.86
정보보안 교육/훈련 프로그램 인식(SETA)	5(0)	5.00	1.32	0.71	0.93	0.90

* AVE: Average Variance Extracted CR: Composite Reliability, CA: Cronbach's Alpha.
( ) 안은 변수의 약어를 나타냄.

정항목의 요인 값이 타 변수의 측정항목 요인 값보다 크다는 것을 알 수 있어 판별타당성을 확보하였다.

〈표 8〉 변수 판별타당성 분석결과

잠재변수	PS	SC	SK	SP	SETA
PS	0.921				
SC	0.709	0.884			
SK	0.857	0. 767	0.889		
SP	0.541	0.367	0.541	0.797	
SETA	0.621	0.458	0.586	0.676	0845

* 진하게 음영으로 표시된 값은 AVE의 제곱근 값을 나타냄.

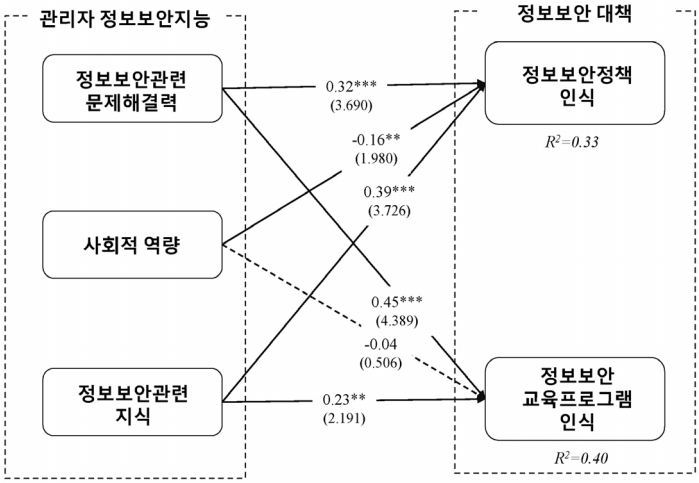
3.4 구조모형 검증

본 연구에서 제안한 6개 가설에 대한 검증은 각 개념 간의 회귀(경로)계수를 부분최소제곱(partial least squares: PLS)에 의해 구하고, PLS의 부트스트랩 리샘플링 방법에 의해 각 회귀(경로)계수의 t-값을 구해 각 가설에 대한 통계적 지지여부를 검증하였다(Chin, 1998). 부트스트랩 샘플 수는 표본 수보다 큰 수인 1,500으로 설정하였다. 본 연구에서 제안한 가설에 대한 검증은 각 변수 간의 회귀(경로)계수를 PLS에 의해 구하고, PLS의 부스트랩 리샘플링 방법에 의해 각 회귀(경로)계수의 t-값을 구해 각 가설에 대한 통계적 지지여부를 검증하였다. PLS 모형의 적합성에 대한 평가는 R^2를 통해 예측타당성을 검토할 수 있으며, 정보보안정책 인식과 정보보안교육프로그램 인식의 R^2는 각 각 0.33, 0.40으로 예측타당성이 확보되었다고 할 수 있다 (<그림 2> 참조).

PLS 경로모형의 구조모형에 대한 평균적인 적합도 평가는 우선 각 내생변수 별 경로모형에 대한 평가로서 해당 내생 (종속)변수의 R^2 값의 효과정도는 상(0.26 이상), 중(0.13~0.26), 하(0.02~0.13)으로 구분하고 있다. 또한 PLS 모형에서 글로벌 적합지수로 GoF(Goodness-of-Fit)의 사용을 제안하였다(Tenenhaus *et al*., 2005). GoF값은 내생변수에 대해 평균 공통성(Communality)과 평균 R^2의 기하평균에 의해 구할 수 있다(Wetzels *et al*., 2009).

$$GoF = \sqrt{\text{평균 Communality} \times \text{평균 } R^2}$$
$$= \sqrt{0.754 \times 0.361} = 0.522$$

구조모형의 적합도(GoF)는 0.1 이하는 낮은 수



( ) 안은 t-값, ***p <0.01, **p < 0.05.

〈그림 2〉 구조모형 경로 분석 결과

준, 0.25 이하는 중간수준, 0.36 이상은 높은 수준으로 평가할 수 있다(Wetzels *et al*., 2009). 본 연구의 분석결과 GoF값은 0.522로, 상위 기준(0.36)을 상회하여 본 연구의 구조모형이 적합하다고 판단할 수 있다.

관리자의 정보보안 지능이 조직원의 정보보안 정책 및 정보보안 교육/훈련 프로그램 인식에 미치는 영향을 회귀(경로)계수를 나타내면 <표 9>과 같다.

〈표 9〉 PLS 경로 분석결과

경로	표준화 계수	t-값	p-값	검증결과
PS → SP	0.32	3.690	<0.001	채택
SC → SP	-0.16	1.980	<0.05	기각
SK → SP	0.39	3.726	<0.001	채택
PS → SETA	0.45	4.389	<0.001	채택
SC → SETA	-0.04	0.506	0.31	기각
SK → SETA	0.23	2.191	<0.05	채택

경영진의 정보보안 지능은 조직원의 정보보안 정책에 대한 인식이나 정보보안 교육/훈련 프로그램에 대한 인식에 긍정적인 영향을 미치는 것으로 나타났다. 하지만 정보보안 지능 구성요인 중 경영진의 사회적 역량은 유의미한 영향을 미치지 않는 것으로 나타났다. 따라서 6개의 가설 중 H1b, H2b를 제외한 4개의 가설을 채택할 수 있다.

Ⅳ. 결론 및 시사점

본 연구는 정보보안 대책(정보보안 정책, 정보보안 교육/훈련)에 대한 조직원들의 인식을 향상시키기 위한 선행요인으로 경영진의 정보보안 지능을 제안하였다. 또한, 경영진의 정보보안 지능의 하위 구성요인들이 정보보안 대책 인식에 미치는 영향을 검증하였으며 연구결과는 다음과 같다.

첫째, 경영진이 정보보안 관련 문제해결 능력이 있는 경우, 조직원들의 정보보안 정책이나 정보보안 교육/훈련 프로그램에 대한 인식이 높아진다는 연구결과가 제시되었다. 경영진이 정보보안관련 문제해결능력이 있다는 것은 정보보안관련 문제를 이해하고 충분한 정보를 기반으로 의사결정을 하고 비용지불을 한다는 것을 의미한다. 이러한 상황은 수립된 정보보안 대책이 합리적인 의사결정을 통해 이뤄졌음을 조직원들이 인지하게 되어 정보보안 대책에 대한 인식이 향상되는 것을 의미한다.

둘째, 경영진이 정보보안 관련 지식을 보유하고 있는 경우, 조직원들의 정보보안 대책에 대한 인식이 높아진다는 연구결과가 제시되었다. 이는 경영진이 정보보안의 위험이나 이슈를 이해하고 있고, 관련 규제를 이해하여 조직원들에게

〈표 10〉 가설검증 결과 요약

가설		검증결과
H1a	경영진의 정보보안관련 문제해결력은 직원의 정보보안 정책에 대한 인식에 긍정적인 영향을 미친다.	채택
H1b	경영진의 사회적 역량은 직원의 정보보안 정책에 대한 인식에 긍정적인 영향을 미친다.	기각
H1c	경영진의 정보보안관련 지식은 직원의 정보보안 정책에 대한 인식에 긍정적인 영향을 미친다.	채택
H2a	경영진의 정보보안관련 문제해결력은 직원의 정보보안 교육프로그램에 대한 인식에 긍정적인 영향을 미친다.	채택
H2b	경영진의 사회적 역량은 직원의 정보보안 교육프로그램에 대한 인식에 긍정적인 영향을 미친다.	기각
H2c	경영진의 정보보안관련 지식은 직원의 정보보안 교육프로그램에 대한 인식에 긍정적인 영향을 미친다.	채택

관련 데이터를 요구하기도 한다는 것이다. 이런 기업환경에서 조직원들은 정보보안 정책이나 정보보안 교육/훈련 프로그램을 중요하게 인지한다.

셋째, 경영진의 사회적 역량이 높은 경우, 가설에서 주장한 바와는 다르게 조직원들은 정보보안 정책에 대한 인식을 약화시키고, 정보보안 교육/훈련 프로그램에 대해서는 경영진의 사회적 역량이 유의한 영향을 미치지 않는 것으로 나타났다. 경영진의 사회적 역량은 다양한 직급의 조직원들과 좋은 관계를 유지할 뿐 아니라 그들과 원활한 커뮤니케이션을 한다는 것을 의미한다. 연구결과는 한국의 독특한 문화적 가치가 반영된 결과로 해석이 될 수 있다. 호프스테드가 제시한 국가별 권력격차에서 한국은 상위에 속하며 이는 한국 문화가 상당히 수직적이라는 것을 의미한다(Hofstede and Hofstede, 1984). 한국의 기업이나 조직에서 종종 발견되는 연공서열이 그 예라 할 수 있다. 경영자와 조직원 사이의 개방적이고 잦은 커뮤니케이션은 조직원들로 하여금 정보보안을 강조하는 경영자의 메시지에 대한 인식을 강화하는데 긍정적인 영향을 미치기 보다는 메시지의 중요성이나 강조를 약화시키는 것으로 해석될 수도 있으나 이에 대해서는 추가적인 연구가 필요하다.

연구의 학문적 시사점은 조직원의 정보보안 대책에 대한 인식의 선행요인으로 경영자의 정보보안 지능이 긍정적인 역할을 한다는 이론을 정립한 것이다. 기존의 연구들은 조직원의 정보보안 준수의도를 향상시키기 위해 정보보안 대책에 대한 조직원의 인식이 중요하다는 것을 제시하였다. 하지만 정보보안 대책에 대한 인식을 향상시킬 수 있는 선행요인에 대한 연구들은 매우 미흡했다. 본 연구에서는 정보보안 대책 인식에 대한 선행요인으로 경영진의 정보보안 지능을 제안하였으며 이를 기반으로 연구모델을 수립하고 실증연구를 수행했다. 특히, 본 연구에서 제시된 경영진의 정보보안 지능은 Kirwan(2008)이 제안하고, Furhen *et al.*(2014)이 개발하고 검증한 안전지능의 하위차원 변수를 응용하여 실증 연구를 진행하였다. 경영진이 정보보안을 어떻게 이해하고 정책을 수립하였으며, 관련 문제를 해결하는 능력에 따라 조직원들의 정보보안 대책을 인식하는 정도가 달라진다. 이는 기존의 연구들이 단순히 경영자 지원이나 참여로 제시한 포괄적인 개념을 세분화하여 제시한다.

연구의 실무적 시사점은 기업에서 정보보안 대책을 수립하여 정보보안 관리를 효과적으로 실행하기 위해서 경영진의 정보보안 지능이 중요하다는 것이다. 경영진의 지원이나 참여는 조직 전반적으로 정보보안 관련 분위기를 형성하는데 기여한다고 할 수 있다. 특히 경영진이 정보보안 관련 사안에 대해 충분한 정보를 기반으로 의사결정이 되는 경우, 관련 비용집행을 균형 있게 하는 경우, 정보보안의 이슈나 위험에 대한 경영진의 이해가 깊을수록 조직원들은 정보보안 대책을 더 잘 인식하게 된다는 결과를 제시한 것이다.

본 연구의 한계점은 경영자의 정보보안 지능과 조직원의 정보보안 대책 인식과의 관계를 탐색적으로 살펴보면서, 경영자의 정보보안 지능으로 제시된 하위차원들 간의 관계를 살펴보지 못한 점이다. 향후 연구에서는 경영진의 정보보안 지능의 다차원적 개념(second-order construct)과 이를 구성하는 하위차원과의 모형의 정합성을 추가 검증할 필요가 있다. 본 연구에서 경영진의 안전지능을 측정하는 도구를 적용하여 경영진의 보안지능을 측정하는 도구로 사용하였는데 안전과 보안이 개념적으로 구별되므로 추가적인 검증이 필요하다. 또한 경영진의 정보보안 지능이 경영진 스스로 응답한 결과가 아니라 조직원들이 경영진에 대해 어떻게 인식하는지를 측정한 것으로 경영진의 정보보안 지능을 직접적으로 측정하는 연구를 향후에 진행하여 연구를 확장할 수도 있다. 마지막으로 경영진의 정보보안 지능, 조직원의 정보보안 대책에 대한 인식의 관계를 조직원의 정보보안 준수까지 확대하여 이들 간의 관계도 연구할 필요가 있다.

참 고 문 헌

[1] 리얼미터, “카드 정보유출 이후 롯데, 국민, 농협카드 브랜드 지수 하락”, *리얼미터*, 2016. 5.27., Available at http://www.realmeter.net/2014/02/page/3/.2014.

[2] 변상호, 김태윤, “재난과 재난관리정책의 재해석에 기반한 ‘재난대응 수행원칙’의 도출과 검증: 재난대응 사례에 대한 분석을 중심으로”, *한국행정학보*, 제48권, 제2호, 2014, pp. 109-136.

[3] 안상호, “사상 초유의 카드사 고객정보 유출사고 발생”, 뉴스메이커, 2016. 5. 27., Available at http://www.newsmaker.or.kr/news/articleView.html?idxno=4960, 2014.

[4] 윤일한, 권순동, “정보보안 컴플라이언스와 위기대응이 정보보안 신뢰에 미치는 영향에 관한 연구”, *Information Systems Review*, 제17권, 제1호, 2015, pp. 141-169.

[5] 이성규, 채명신, “산업보안정책 준수의지에 영향을 미치는 요인분석”, *대한경영학회지*, 제27권, 제6호, 2014, pp. 927-953.

[6] 임명성, “조직 구성원들의 정보보안 정책 준수에 영향을 미치는 요인에 관한 연구: 금융서비스업을 중심으로”, *서비스경영학회지*, 제14권, 제1호, 2013, pp. 143-171.

[7] 임재명, 유지열, 신종환, 배향은, *2013년 정보보호실태조사-기업부문*, 한국인터넷진흥원, 2013.

[8] 한진영, 김유정, “정보보안 준수의도에 대한 사회심리적 요인 분석: 정보보안과 조직시민행동이론 융합”, *디지털융복합연구*, 제13권, 제1호, 2015, pp. 133-44.

[9] 황인호, 김대진, 김태하, 김진수, “조직의 정보보안 문화 형성이 조직 구성원의 보안 지식 및 준수의도에 미치는 영향 연구”, *Information Systems Review*, 제18권, 제1호, 2016, pp. 1-23.

[10] Bulgurcu, B., H. Cavusoglu, and I. Benbasat, “Roles of information security awareness and perceived fairness in information security policy compliance”, *AMCIS 2009 Proceedings*, p. 419, 2009.

[11] 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.

[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] Chin, W., “The partial least squares approach to structural equation modeling”, *Modern Methods for Business Resarch*, Vol.295, No.2, 1998, pp. 295-336.

[14] Chin, W., B. Marcolin, and P. Newsted, “A partial least squares latent variable modeling approach for measuring interaction effects: Results from aMonte carlo simulation study and an electronic-mail emotion/adoption study”, *Information Systems Research*, Vol.14, No.2, 2003, pp. 189-217.

[15] 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.

[16] Finkelstein, S., “Power in top management teams: Dimensions, measurement, and validation”, *Academy of Management Journal*, Vol.35, No.3, 1992, pp. 505-538.

[17] Fornell, C. and D. Larcker, “Evaluating structural equation models with unobservable variables and measurement error”, *Journal of Marketing Research*, Vol.18, No.1, 1981, pp. 39-50.

[18] Fruhen, L., K. Mearns, R. Flin, and B. Kirwan,

"Safety intelligence: An exploration of senior managers' characteristics", *Applied Ergonomics*, Vol.45, No.4, 2014, pp. 967-975.

[19] Fruhen, L., K. J. Mearns, R. H. Flin, and B. Kirwan, "From the surface to the underlying meaning-an analysis of senior managers' safety culture perceptions", *Safety Science*, Vol.57, August 2013, pp. 326-334.

[20] Goel, S. and I. N. Chengalur-Smith, "Metrics for characterizing the form of security policies", *Journal of Strategic Information Systems*, Vol.19, No.4, 2010, pp. 281-295.

[21] 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, p. 347.

[22] Haeussinger, F. and J. Kranz, "Information security Awareness: Its antecedents and mediating effects on security compliant behavior", *Thiry Fourth International Conference on Information Systems*, 2013, pp. 189-217.

[23] Harper, A. C., J. L. Cordery, N. H. de Klerk, P. Sevastos, E. Geelhoed, C. Gunson, L. Robinson, M. Sutherland, D. Osborn, and J. Colquhoun, "Curtin industrial safety trial: Managerial behavior and program effectiveness", *Safety Science*, Vol.24, No.3, 1996, pp. 173-179.

[24] Hofstede, G. and G. Hofstede, *Culture's Consequences: International Differences in Work-Related Values*, Sage Publications, 1984.

[25] Hong, K. S., Y. P. Chi, L. R. Chao, and J. H. Tang, "An Integrated system theory of information security management", *Information Management & Computer Security*, Vol.11, No.5, 2003, pp. 243-248.

[26] Hopkins, A., "Management walk-arounds: Lessons from the Gulf of Mexico oil well blowout", *Safety Science*, Vol.49, No.10, 2011, pp. 1421-1425.

[27] Hovav, A. and J. D'Arcy, "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea", *Information & Management*, Vol.49, No.2, 2012, pp. 99-110.

[28] 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.

[29] Kirwan, B., "From safety culture to safety intelligence", *Probabilty Safety Assessment and Management Conference (PSAM9)*, 2008.

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

[31] 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.

[32] Podsakoff, M. P., B. S. MacKenzie, J. Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: A critical review of the literature and recommended remedies", *Journal Applied Psychology*, Vol.88, No.5, 2003, pp. 879-890.

[33] Ponemon Institute, *Cost of Data Breach Study, Ponemon Institute LLC*, North Traverse City, Michigan, 2012.

[34] 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.

[35] Thomson, K. L., R. von Solms, and L. Louw, "Cultivating an organizational information se-

curity culture", *Computer Fraud & Security*, Vol.2006, No.10, 2006, pp. 7-11.

[36] Wetzels, M., G. Odekerken-Schröder, and C. Van Oppen, "Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration", *MIS Quarterly*, Vol.33, No.1, 2009, pp. 177-195.

[37] Yim, M. S., "A path way to increase the intention to comply with information security policy of employees", *Journal of Digital Convergence*, Vol.10, No.10, 2012, pp. 119-128.

[38] Zohar, D. and G. Luria, "A multilevel model of safety climate: Cross-level relationships between organization and group-level climates", *Journal of Applied Psychology*, Vol.90, No.4, 2005, p. 616.

<부 록> 설문 항목

변수		항목	참고문헌
관리자 정보 보안 지능	정보보안 관련 문제해결력	우리회사 경영층은 _____ 1) 정보보안관리와 그에 소요되는 비용의 균형을 적절하게 유지한다. 2) 전문가의 자문을 받은 후에 정보보안관련 의사결정을 한다. 3) 정보보안 문제를 이해할 준비가 되어있다 4) 정보보안 문제에 대해 충분한 정보를 가지고 의사결정을 내린다.	Fruhen *et al.* (2014)
	사회적 역량	우리회사 경영층은 _____ 1) 조직 내 모든 직급의 사람들과 좋은 관계를 유지한다. 2) 개방적으로 의견을 수렴한다. 3) 경청자이다. 4) 직원들에게 질문을 한다. 5) 경청을 잘 한다. 6) 조직의 모든 사람과 대화를 한다. 7) 커뮤니케이션 스킬이 상당히 좋다. 8) 모든 견해를 수렴한다. 9) 하위 직급의 사람들의 관심을 끈다.	Fruhen *et al.* (2014)
	정보보안 관련 지식	우리회사 경영층은 _____ 1) 정보보안관련 문화가 어떻게 형성되는지 이해하고 있다. 2) 정보보안관련 위험을 이해한다. 3) 정보보안에 대해 알고 있다. 4) 정보보안 관련 교육을 받았다. 5) 정보보안 관련 이슈를 이해하고 있다. 6) 정보보안 관련해서 훈련되어 있다. 7) 우리회사 경영층은 정보보안관리를 이해하고 있다. 8) 우리회사 경영층은 정보보안관리 시스템에 익숙하다. 9) 우리회사 경영층은 보안이슈와 관련하여 자신의 영향력을 이해하고 있다. 10) 우리회사 경영층은 정보보안 규제 이슈에 익숙하다. 11) 우리회사 경영층은 정보보안관련 데이터를 요구한다.	Fruhen *et al.* (2014)
정보 보안 대책	정보보안 정책 인식	우리 회사는 _____ 1) 이메일 적절한 사용방법을 명확하게 기술한 가이드라인이 있다. 2) 컴퓨터자원 사용 시 필요한 규칙이 수립되어 있다. 3) 권한없는 직원이 컴퓨터에 접근하는 것을 방지하는 공식적인 정책이 있다. 4) 컴퓨터 비밀번호를 설정방법을 명기한 가이드라인이 있다. 5) 직원별로 접근가능한 컴퓨터 시스템의 자원을 정의하고 관리한다.	D'Arcy *et al.* (2009)
	정보보안 교육/훈련 프로그램 인식	우리 회사는 _____ 1) 직원들이 컴퓨터시스템 보안관련 이슈에 대한 인식향상 교육프로그램을 제공한다. 2) 소프트웨어 라이선스 정책에 대한 교육을 제공한다. 3) 권한이 없는 데이터를 직원들이 조작할 경우 발생할 수 있는 결과에 대해 설명해 준다. 4) 컴퓨터 보안책임에 대해 직원들을 교육한다. 5) 권한이 없는 컴퓨터시스템에 직원들이 접근할 경우 발생할 수 있는 결과에 대해 설명해 준다.	D'Arcy *et al.* (2009)

Information Systems Review
Volume 18 Number 3
September 2016

The Effect of Managerial Information Security Intelligence on the Employee's Information Security Countermeasure Awareness

Jin Young Han* · Hyun-Sun Ryu**

Abstract

Organizations depend on smart working environments, such as mobile networks. This development motivates companies to focus on information security. Information leakage negatively affects companies. To address this issue, management and information security researchers focus on compliance of employees with information security policies. Countermeasures in information security are known antecedents of intention to comply information security policies. Despite the importance of this topic, research on the antecedents of information security countermeasures is scarce. The present study proposes information security intelligence as an antecedent of information security countermeasures. Information security intelligence adapted the concept of safety intelligence provided by Kirwan (2008). Information security intelligence consists of problem solving skills, social skills, and information security knowledge related to information security. Results show that problem solving skills and information security knowledge have positive effects on the awareness of employees of information security countermeasures.

Keywords: ***Information Security Knowledge, Information System Policy Awareness, Management Information Security Intelligence, Problem Solving, Security Education Training Awareness, Social Competence***

* College of ICT Engineering, Chung-Ang University
** Corresponding author, College of Software, Sungkyunkwan University

◐ 저 자 소 개 ◑

한 진 영 (win1999@naver.com)

현재 중앙대학교 창의ICT공과대학 산학협력중점교수로 재직하고 있다. 고려대학교 경영학과에서 MIS 전공 박사를 취득하였다. 주요 관심분야는 차세대 정보전략, 정보보안, 프로젝트 관리, 지식경영 등이다. International Journal of Project Management, Computers in Human Behavior, Information Systems Review, 인터넷전자상거래연구 등을 포함한 다수의 논문을 국내외 학술지에 발표하였다.

유 현 선 (hamkkai@gmail.com)

한국과학기술원 테크노경영대학원에서 MIS 전공으로 석사학위를, 고려대학교 경영학과에서 MIS 전공으로 박사학위를 취득하였다. 삼성전자에서 SW센터와 산업연구원(KIET)에서 선임연구원으로, 고려대학교 정보통신센터에서 연구위원으로 재직하였으며, 현재 성균관대학교 SW대학에서 초빙교수로 재직하고 있다. 주요 연구관심 분야는 IT 또는 SW를 이용한 서비스 혁신, 기술과 서비스 간 융합/통합, SW 융합 서비스 등이다. IEEE Transactions on Management and Engineering, Service Industries Journal, Information Journal, International Journal of Hybrid Information Technology, Information Systems Review, Asian Pacific Journal of Information Systems, 지식경영연구, 한국IT서비스학회지 등을 포함한 다수의 논문을 국내외 학술지에 발표하였다.

논문접수일 : 2016년 05월 31일 **게재확정일 : 2016년 09월 13일**
1차 수정일 : 2016년 08월 29일