「정보시스템연구」 제28권 제4호
한국정보시스템학회
2019년 12월, pp. 105~129

http://dx.doi.org/10.5859/KAIS.2019.28.4.105

SCO Framework을 적용한 조직과 조직원의 정보보안 준수 관계 연구*

황 인 호** · 김 상 현***

〈목 차〉

Ⅰ. 서 론

조직은 최신의 정보시스템 및 스마트 기기 활용을 통하여 정보 공유, 노하우 전수, 다양한 커뮤니케이션 채널 등의 제공함으로써, 생산성 증대를 꾀하고 나아가 구성원들의 인적 역량을 강화하길 원한다(Carr, 2003; Warkentin and Willison, 2009). 반면, 조직 구성원들의 정보시스템 및 조직의 핵심 정보에 대한 접근성이 좋아짐에 따라, 정보보안 사고 위협 또한 높아지고 있다(Bang et al., 2012). 즉, 스마트기기 등과 같은 휴대성이 높은 하드웨어의 보급은 조직원들이 어디서든 공유 및 생산성 향상관점에서 정보를 활용할 수 있도록 지원하지만, 정보보안 우려 또한 높아지고 있는 것이 사실이다. 기업의 정보보안 사고는 단순히 기업의 금전적 피해뿐 아니라, 노출된 정보와 관련된 이해관계자(소비자, 협력 기업 등)까지 2차 피해를 발생시키기 때문에 정보보안 사고 예방을 위한 기업의 노력이 중요해지고 있다(유인진, 박도형,

* 이논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임. (NRF-2018R1D1A1B07050305)
** 한국산업기술대학교, inho1998@kpu.ac.kr(주저자)
*** 경북대학교 경영학부, ksh@knu.ac.kr(교신저자)

2018; Hwang et al., 2017).

정보보안 위협 요인은 여러 측면에서 나타날 수 있다. Loch et al.(1992)은 정보보안 위협 요인을 인간-비인간, 내부-외부의 관점으로 구분하여 분류하였으며, 외부에 의한 시스템 접근 및 정보 해킹, 자연재해 등으로 인한 물리적 시스템 파괴, 그리고 내부 조직원에 의한 정보 노출 등이 발생할 수 있다고 보았다. Verizon (2016)에 따르면, 매년 정보보안 사고의 60~70%가 외부 침입에서 발생하고 있으며, 15~20%는 내부자들의 정보 노출에 기인한다고 보았다. 외부 악의적 세력의 정보 탈취는 보안 시스템 개선 노력으로 해결할 수 있으나, 조직원이 정보 노출에 대한 마음만 먹는다면, 조직차원에서의 통제가 사실상 불가능하다(Whitman, 2004). 즉, 내부 구성원들의 잠재적 보안 위협 감소를 위해서는 조직원의 정보보안 준수에 대한 관심 및 의지를 높임으로써, 조직에서 요구하는 행동을 자발적으로 할 수 있도록 제시하는 것이 중요하다(Hwang and Cha, 2018; Vance et al., 2013).

조직원의 정보보안 준수 행동에 대한 선행연구를 살펴보면, 대부분 정보보안 위협 및 사고 억제 및 예방을 위한 조직원 관점의 동기적 접근과 관련되어 있다. 조직원의 잠재적 이탈 행위와 처벌(sanction)간의 관계를 기반으로 정보보안 위반 억제를 설명한 억제 이론(deterrence theory)을 기반한 연구 (D'Arcy et al., 2009; Herath and Rao, 2009), 조직원의 태도 변화를 유발하는 요인인 공포 소구(fear appeal)를 기반으로 정보보안 사전 예방 원인과 방법을 설명한 보호동기이론(protection motivation theory)을 기반으로 한 연구 (Boss et al., 2015; Vance et al., 2012) 개인의 정보보안 선택에 있어 비용, 혜택에 기반을 둔 선택을 한다는 합리적 선택이론(rational choice theory) 기반의 연구(Bulgurcu et al., 2010) 등이 대표적이다. 선행 연구들은 개개인의 정보보안 준수를 위한 방안을 제시한 측면에서 큰 의미를 가진다.

하지만, 조직에서 조직원은 조직의 행동에 대한 조건을 기반으로 합리적 행동을 하는 경향을 가진다(Molm, 1990), 즉, 개인은 주변 환경의 조건으로부터 최선 또는 차선의 선택을 하려는 경향을 가지는데, 선행연구들은 조직과 개인 간의 관계에서 정보보안 준수를 설명하는데 한계점을 가진다.

조직은 개인이라는 조직원들의 모임이지만, 조직 자체로서 특성을 가지기 때문에, 조직과 조직원이 의사결정을 할 때는 상대방의 특성과 요구사항을 고려하여 합리적 의사결정을 한다(Emerson, 1976). 이와 관련된 이론이 사회적교환이론(social exchange theory)이다. 사회적교환이론은 상호간의 합리적 관계를 기반으로 경제적 또는 비경제적 자원을 교환함으로써 이익(profit)과 비용(cost)을 기반으로 사회관계를 유지한다는 이론이며(Eisenberger et al., 1990), 조직과 조직원간의 정보보안 활동과 관련된 관계에 대한 설명이 가능할 것으로 판단된다.

본 연구는 사회적교환이론이 조직의 정보보안 활동과 조직원 준수와의 관계를 설명할 수 있는지를 찾음으로써, 정보보안을 위한 조직의 행동과 조직원의 준수 의도가 교환적 관점에서 설명이 가능함을 제시하고자 한다.

이를 위하여, 사회적교환이론의 단계별 적용 모델인 구조(structure), 행동(conduct), 그리고 결과(outcome)로 구조화된 SCO프레임워크를

활용하되, SCO프레임워크 각 구조에 적정 정보보안 요인을 제시하고 조직 정보보안 구조, 행동, 결과 요인간의 관계를 증명하고자 한다.

세부적으로 정보보안 구조를 현재 구축한 조직의 정보보안 시스템과 정책으로 구성하였으며, 정보보안 행동은 조직 차원의 정보보안 위협 최소화를 위한 전략적 행동 요인으로 구성하였다. 그리고 정보보안 결과는 구성원들의 자발적인 정보보안 준수와 관련된 요인으로 구성하였다.

이를 통하여 조직에서 조직원에게 제시하는 전략적 행동에 대하여 구성원들이 보안 준수와 관련하여 어떻게 받아들이는지를 제시하고, 정보보안 구조화 노력이 조직의 정보보안 전략적 행동에 미치는 영향을 파악함으로써, 정보보안 환경 구축의 중요성을 제기하고자 한다.

Ⅱ. 이론적 배경

2.1 사회적교환이론과 정보보안

사회적교환이론(social exchange theory)은 Thibaut and Kelley(1959)와 Emerson(1962, 1972)에 의해 이론이 확립되었으며, Cook et al.(1983)과 Molm(1990) 등의 연구자들에 의해 관련 이론이 확장 및 체계화되어, 현재는 사회적 관계에 관한 영향력 있는 사회심리학 이론으로 평가되고 있다.

사회적교환이론은 인간이 타인 또는 조직과 자원 교환 관계에 있을 경우, 자신이 받을 자원에 대한 가치를 고려하여 행동으로 전환한다는 것을 가정한다(Emerson, 1972). 행동 전환의 대상이 되는 가치는 돈, 상품과 같은 보상 등의 유형적 상태의 가치와 행동, 자존심과 같은 심리적 상태의 가치 등이 있다(Molm, 1990). 교환대상인 보유하고 있는 자원에 대하여 거래당사자간 가치가 있다고 판단할 경우 관계를 유지하지만, 상호간의 호혜의 규칙이 깨질 경우 관계는 단절된다(Hendricks, 1995).

조직과 개인의 관계에서도 교환관계는 가치에 기반을 두어 평가되는데, 개인은 조직의 환경, 문화 등에 대하여 주관적인 평가를 하고, 평가 결과에 따라 조직에 대한 우호적 또는 적재적 지각을 인지하고 행동한다(Eisenberger et al., 1990). 즉, 개인과 조직사이의 관계 또한 가치에 기반한 교환관계를 기반으로 움직이기 때문에, 상호간에 교환되는 가치를 높이는 것이 중요하다(Armeli et al., 1998).

정보보안 측면에서, 조직과 조직원들 간에는 교환 관계가 성립된다. 조직은 정보보안 정책, 시스템 등을 구축하고 조직원들의 준수행동을 요구하며(Bulgurcu et al., 2010; D'Arcy et al., 2009; Hwang and Cha, 2018), 조직원들은 조직의 보안 목표에 맞는 행동을 할 의무를 가진다(Dhillon et al., 2016). 하지만, 조직원은 자신만의 고유의 업무과 성과 목표를 가지고 있으며, 정보보안 준수 상황에 직면할 경우 자신을 둘러싼 환경과 정보를 기반으로 준수에 대한 추가적인 의사결정을 한다(West, 2008). 즉, 조직은 조직원에게 정보보안의 필요성과 가치(보상, 제재 등)를 제시하고, 조직원은 조직으로부터 주어진 가치에 대한 주관적 평가를 통하여 수용여부를 결정하기 때문에, 사회적 교환 관점이 성립된다.

최근, 사회적교환이론에 대하여 보다 구조적 관점에서 원리를 설명하고, 분야에 활용하기 위

하여 여러 학자들이 SCO(structure-conduct-outcome) 프레임워크를 적용하고 있다(Devaraj et al., 2006; Geyskens et al., 1999; Molm, 1990). SCO 프레임워크는 조직 단위와 개인 단위의 상호관계를 제시하고, 상호 이익을 얻기 위한 노력을 하기 위한 단계적 절차를 제시하고 있어, 조직원 통제 및 관리가 필수적인 정보보안 분야에 구조적 의미를 줄 수 있다.

2.2 정보보안분야 SCO프레임워크 구성

SCO프레임워크에서 구조(structure)는 "교환 네트워크에서 교환 관계 당사자 간 의존성을 높이도록 제공하는 잠재적 구조적 파워"로 정의된다(Molm, 1990). 정보보안 관점에서, 조직원이 정보보안 행동을 할 수 있도록 조직 차원의 보안 체계를 구조화 해놓은 것을 지칭한다. 본 연구는 정보보안 구조를 물리적 정보보안 시스템 구축과 체계적인 정보보안 정책 정립으로 유형화하였다.

행동(conduct)은 "상호간에 관계를 유지하도록 제공하는 전략 또는 행동 패턴"으로 정의된다(Devaraj et al., 2006). 정보보안관점에서 행동은 조직원의 정보보안 행동을 유도하기 위한 조직 차원의 전략적 행동을 지칭한다. 본 연구는 정보보안의 전략적 행동을 경영층의 정보보안 지원, 정보보안 프로그램 개발 및 교육, 그리고 정보보안 정보 가시성 확보로 유형화하였다.

결과(outcome)는 "상호작용 과정을 통하여 나타나는 상호간에 질적 가치 측면의 행동 교환결과"로 정의된다(Molm, 1990). 정보보안관점에서, 조직원이 조직의 전략적 행동을 통해 정보보안 준수가 제공하는 이익과 비용을 판단하고 행동하는 주체이다. 본 연구는 결과 요인을 조직의 정보보안 대상인 조직원이 받아들이는 정보보안 지식, 정보보안 준수의도로 유형화하였다.

2.2.1 SCO프레임워크 결과

사회적교환이론에서 결과는 상호작용으로 나타나는 행동적 교환의 결과로서, 당사자들은 상대방에서 제시하는 상호교환의 전략적 행동에 기반하여, 대상에 대한 가치를 인식하고 교환을 한다(Molm, 1990). 예를 들어, 기업과 소비자와의 관계에서 결과는 소비자의 기업에 대한 선호도 및 만족도 등으로 제시된다(Devaraj et al., 2006; Geyskens et al., 1999).

정보보안 관점에서 조직은 구조적 파워와 행동을 통해 조직원들의 정보보안 준수를 유도하고, 조직원은 조직이 제공하는 조건과 상호관계에 기반을 두어 정보보안 준수에 대한 의사결정을 한다. 따라서 정보보안을 적용한 SCO프레임워크의 결과요인은 조직원 단위의 정보보안 준수 의사결정을 위한 조직원의 정보보안 지식과 준수의도로 구성된다.

1) 정보보안 준수의도

내부자에 의한 정보보안 위협 우려는 스마트기기의 확산을 통한 생산성 확대를 추구하는 정보시스템 구축 전략의 확대에 따라 더욱 커지고 있다(Hwang et al., 2017). 실제로 조직원의 정보 노출 사고와 같은 위협 요인은 물리적, 시간적 제약에서 벗어나고 있으며, 이에 대한 해결을 위해 조직들은 많은 시간과 비용을 투자하고 있다.

조직원의 정보보안 준수와 관련된 선행 연구

에 따르면, 정보보안 준수는 심리적 요인이기 때문에(West, 2008), 조직으로부터 정보보안을 요구받더라도 자신의 보안 준수에 대한 의지가 형성되지 않으면 미준수행동으로 이어질 가능성이 높다(Chou and Chou, 2017; Pham, 2019). 그러므로, 조직원들의 정보보안 준수는 자발적인 준수의도 형성이 무엇보다 중요하며, 조직차원에서 개개인의 준수의도 형성을 위한 지원이 필요하다고 보고 있다(황인호, 김대진, 2016; Chen et al., 2012).

정보보안 준수의도에 대한 개념을 살펴보면, Bulgurcu et al.(2010)은 “잠재적인 보안 위협으로부터 조직의 정보 및 기술 자원을 보호하기 위한 구성원의 의도”로 정의하고 있으며, Vance et al.(2012)은 “조직의 정보자원을 내부, 외부의 보안 위협에서 보호하고자 하는 조직원의 의지”로 정의하고 있다. 즉, 준수의도는 조직원이 조직의 정보자원을 보호하기 위한 자발적인 의도 수준이기 때문에, 준수의도가 높아질수록 긍정적인 정보보안 행동으로 이어질 가능성이 높다(Safa et al., 2019).

2) 정보보안 지식

개인과 조직사이의 관계에서, 지식은 조직이 요구하는 특정한 규범, 태도, 의사결정 방법 등을 개인이 행동할 수 있도록 영향을 주는 요인이다(Nelson and Cooprider, 1996). 지식은 “명시적 또는 암묵적으로 의사소통이 가능한 정보로서, 개인의 경험과 가치에서 비롯된 개인적이고 직관적인 통찰력과 노하우”로 정의된다(Desouza, 2003). 조직에서 구성원이 업무 등 관련된 지식을 명확하게 보유하지 못할 경우, 개인의 두려움(fear), 압력(pressure), 불확실성(uncertainty), 그리고 걱정(anxiety)과 같은 스트레스 요인이 높아지게 된다(최경선, 안현철, 2019; Cegarra-Navarro et al., 2011).

그러므로 조직원은 조직의 정보보안 정책에 대하여 명확하게 이해하는 것뿐 아니라 자신만의 지식으로 확보하고 있는 것이 필요하다.

개인에게 형성된 지식은 관련된 행동 수준을 높이는 선행 요인이다. Jiang et al.(2008)은 온라인 보안관점에서 지식과 태도간의 관계를 증명하고자 하였는데, 온라인 보안에 대한 지식형성은 온라인 구매 시 판매자에 대한 긍정적 태도를 미치는 것을 확인하였다. Neal et al.(2000)은 조직의 지식문화 형성을 위한 분위기(climate) 구축이 개인의 지식형성에 도움을 주고 형성된 지식은 관련 행동의도 및 조직 참여를 높이기 때문에, 지식 구축을 위한 조직관점의 노력이 중요하다고 보았다.

특히, 정보보안 관점에서도 개인의 정보보안 지식형성은 보안 준수에 영향을 준다. Wang (2010)은 정보보안과 관련한 개인에게 형성된 지식은 수용의도를 높일 수 있다고 하였으며, 보안관련 개인 인지 및 경험 수준을 높이는 것이 중요한 선행 조건이라고 하였다. 개인의 지식형성이 정보보안 준수의도를 높인다는 선행연구를 기반으로 다음과 같은 가설을 제시한다.

H1. 정보보안 지식은 정보보안 준수의도에 긍정적인 영향을 줄 것이다.

2.2.2 SCO프레임워크 행동

사회적교환이론에서 행동은 상호 관계를 유지하도록 하는 전략적 행동으로서(Devaraj et al., 2006), 조직과 개인의 관계에서는 개인의 행동을 유도하기 위한 조직의 전략적 행동을

지칭한다(Emerson, 1976). 즉, 행동은 조직원이 조직의 정보보안 정책을 이해하고 준수할 수 있도록 지원하는 조직 차원의 노력으로서, 선행연구를 분석한 결과, 경영층의 지원, 정보보안 교육, 그리고 정보보안 가시성이 있다.

1) 최고경영층 지원

조직에서 경영층 지원은 조직원의 행동에 긍정적/부정적 영향을 주는 중요 요인이다(Said et al., 2014). 특히, 경영층이 조직차원의 목표를 명확하게 제시하고 성과 달성을 위한 직·간접적인 지원을 할 경우, 구성원들은 조직 내 활동에 대한 긍정적인 태도를 보유하게 된다(Nesheim and Gressgård, 2014).

정보보안 분야에서, 최고경영층의 지원은 조직의 정보보안 문화 형성 및 조직원의 준수 태도 및 행동에 긍정적인 영향을 미치는 요인이다(Said et al., 2014). Kankanhalli et al.(2003)은 정보보안 분야에서 최고경영층의 지원에 대한 개념을 “경영층의 정보보안에 대한 참여 및 조직 내 보안 문화 형성을 위한 지원 수준”으로 정의하였으며, 최고경영층의 지원이 정보보안 사고 방지를 위한 중요한 선행 요인이라고 하였다. 또한, 최고경영층이 정보보안 문화 형성 및 관련 시스템 구축에 관심을 가짐으로써, 조직원들에게 독려할 경우, 조직 내 정보보안 분위기를 빠르게 형성시켜 조직원들의 정보보안 준수 의지를 높인다(Kankanhalli et al., 2003; Mary MacNeil, 2004). 또한, Said et al.(2014)은 조직 차원의 지식 관리를 위해서는 최고경영층의 지원이 중요한 선행요인이며, 최고경영층의 지원 수준이 높을수록 조직의 지식관리 이행과 전술적/전략적 지식 관리 프로세스를 효과를 높일 수 있다고 하였다. Steinbart et al.(2018)은 최고경영층의 정보보안에 대한 지원이 선행될 경우 내부 구성원들의 정보보안 관련 상호 지원 활동에 영향을 주고, 정보보안 효과를 높인다고 하였다. 선행연구를 기반으로 다음과 같은 가설을 제시한다.

H2. 최고경영층의 관심은 조직원의 정보보안 지식에 긍정적인 영향을 줄 것이다.

2) 정보보안 교육

내부원에 의한 정보보안 사고는 언제 어디서나 발생할 가능성이 존재한다. 따라서 조직원의 정보보안 인식(awareness)를 높이기 위한 예방활동이 중요하다(Whitman et al., 2001). 정보보안 교육은 보안 사고에 대한 사전 예방을 위한 정보보안 관련 정보 및 이행 방법을 조직원들에게 제공하는 대표적 활동이다(Tomson and van Niekerk, 2012).

D’Arcy et al.(2009)은 정보보안 교육을 “조직에 구축된 보안 정책, 규정, 그리고 정보보안 적용 환경에 대하여 조직원의 인식을 위하여 제공하는 프로그램”으로 정의하였다. 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 오용(misuse)를 감소시킴으로써 생산성 향상을 유도한다(D’Arcy et al., 2009; Lee and Lee, 2002).

또한 정보보안 교육 프로그램은 개인의 정보보안 지식 형성 및 조직 내 지식 공유 활동을 높일 수 있는 선행요인이다. Nesheim and Gressgård(2014)는 조직의 요구수준에 맞는 개

인의 지식 형성 및 공유를 위해서는 교육, 훈련 프로그램의 효과적인 운영을 통해서 가능하다고 하였다. Griffin and Neal(2000)은 조직차원에서의 교육 프로그램과 훈련 방법을 제공하는 것이 개인의 지식수준을 높이는 요인이라고 하였다. 선행연구를 기반으로 다음과 같은 가설을 제시한다.

H3. 정보보안 교육은 조직원의 정보보안 지식에 긍정적인 영향을 줄 것이다.

3) 정보보안 가시성

조직에서 새로운 기술 및 정책을 확산시키기 위해서는 새로운 정보 및 규칙 등을 적용 시 발생할 수 있는 불안감 및 불확실성 등을 줄이는 것이 중요하다(Cegarra-Navarro et al., 2011). 가시성은 “조직 내 시스템을 활용하여 대상을 볼 수 있는 수준”으로서(Venkatesh et al., 2003), 새로운 정책 및 기술 적용 시, 조직원들에게 발생가능한 불확실성을 감소시키는 중요한 요인이다(Moore and Benbasat, 1991).

정보보안 관점에서 가시성은 보안 관련 행동에 긍정적인 영향을 준다. Siponen et al.(2010)은 정보보안에 대한 가시성이 높을수록 조직원의 정보보안 준수의도가 높아진다고 하였으며, 조직에서 정보보안 가시성을 확보하는 방법은 보안 관련 캠페인, 포스터, 커피 머그잔 홍보 등 일상적인 부분에서의 정보보안에 대한 정보를 제공하는 것에 있다고 하였다. 즉, 정보보안 중요성과 방법에 대하여 조직원이 보다 편안하게 이해하고 실천할 수 있도록 캠페인을 실행함으로써 보안 가시성을 향상시키는 것이 조직원의 정보보안 준수의도를 높이는 요인이라고 하였다(Siponen et al., 2010)

더불어, 정보보안 가시성은 조직원의 보안 지식에 긍정적인 영향을 미친다. Vroom and von Solms(2004)는 조직구성원이 자발적으로 지킬 수 있는 보안 문화가 장기적인 관점에서 내부자의 보안 위협을 감소시킨다고 하였으며, 조직 차원의 보안에 대한 가시적 활동이 개인의 보안 지식을 형성하고 조직구성원들의 보안 문화를 형성한다고 보았다. 또한, Griffin and Neal(2000)은 조직차원에서의 지속적인 홍보 등의 커뮤니케이션 노력을 수행할 경우, 개인의 지식 형성에 도움을 준다고 하였다. 선행연구를 기반으로 다음과 같은 가설을 제시한다.

H4. 정보보안 가시성은 조직원의 정보보안 지식에 긍정적인 영향을 줄 것이다.

2.2.2 SCO프레임워크 구조

사회적교환이론에서 구조는 교환대상간의 상호의존성을 높이기 위한 구조적 파워로서(Molm, 1990), 정보보안에서는 조직원이 정보보안을 지키도록 규제하는 조직의 구조로 설명할 수 있다. 본 연구는 선행연구를 기반으로 정보보안 정책과 정보보안 시스템 구축을 제시한다.

1) 정보보안 정책

정보보안 정책은 “조직의 정보보안 관련 자원의 적절한 사용에 대한 규칙과 가이드라인”으로 정의된다(Whitman et al., 2001). 정보보안정책은 조직의 정보보안 목표, 조직의 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, 정보보안 정책은 조직에서 수행하고자 하는 정보보안 임무, 구성원

역할, 운영 방식 등을 포괄하며, 구성원들에게 전사적 보안 목표 달성을 위해 행동을 요구하는 규칙이다.

조직의 현실에 맞게 잘 정의되고 검증된 보안 정책은 조직원으로부터 신뢰성을 확보할 수 있다(von Solm, 1999). 따라서 조직의 외부 영향 요인(기술적 변화, 산업 표준, 법적 and 규범적 요구사항, 외부 위협 요인)과 내부영향요인(비즈니스 목표, 조직 문화, 기술 아키텍쳐, 그리고 내부 위협 요인)를 함께 고려하여 보안 정책을 구성하는 것이 필요하다(Knapp et al., 2009).

조직 특성 및 환경을 고려한 보안 정책은 조직원의 보안 행동 실수를 억제 및 예방할 수 있는 선행 요인이다(D'Arcy et al. 2009). 특히, 조직의 규범은 조직원 행동 제재(sanction)를 부여하여, 그들의 불법적 행동을 최소화할 수 있어, 억제 관점에서 활용되는 대표적인 요인이다(Lee et al., 2004).

또한, 정보보안 정책은 조직 차원의 보안 활동을 할 수 있도록 돕는다. Lowry et al.(2015)은 조직에 적합한 정보보안 정책은 조직의 보안 활동에 대한 저항을 감소시키고 조직 신뢰를 형성시켜 조직원들의 보안 행동에 긍정적인 영향을 준다고 하였으며, Da Veiga and Martins(2017)은 조직의 보안 전략 및 관리 비전에 기반하여 구축된 정보보안 정책은 조직원들의 개인 보안 행동과 조직 차원의 보안 문화에 긍정적인 영향을 주기 때문에, 정보보안 정책 구축이 선행되어야 한다고 보았다. Griffin and Neal(2000)은 조직의 안전 규정 및 정책 정보 제공이 안전 관련 분위기를 형성한다고 하였다. 즉, 조직에 맞는 정보보안 정책 수립은 조직의 정보보안 행동(conduct)에 영향을 줄 것으로 판단된다. 선행연구를 기반으로 다음과 같은 가설을 제시한다.

H5. 정보보안 정책은 조직의 정보보안 행동에 긍정적인 영향을 줄 것이다.

H5a. 정보보안 정책은 최고경영층의 지원에 긍정적 영향을 줄 것이다.

H5b. 정보보안 정책은 정보보안 교육에 긍정적 영향을 줄 것이다.

H5c. 정보보안 정책은 정보보안 가시성에 긍정적 영향을 줄 것이다.

2) 정보보안 시스템

조직 수준에서 구조적으로 내부자들의 정보보안 사고를 최소화하고 정보보안을 유지하는 방법은 정보보안 시스템을 구축하는 것이다(Lee et al., 2004). 정보보안 시스템은 "조직원의 정보자원 접근 통제 및 억제를 위한 시스템 구축 및 투자 수준"으로 정의된다(Kwok and Longley, 1999). Kwok and Longley(1999)는 조직원의 핵심 정보자원 접근 통제 및 억제를 위한 정보보안 시스템(물리적 출입 통제, 데이터 센터 및 컴퓨터실의 보안, 케이블 보안, 조직 내 장비 보안 및 적정 폐기 등)의 물리적 구축이 사전적으로 구축되는 것이 필요하다고 하였다. 즉, 조직 내에 구조적 보안 시스템 구축이 사전적으로 구축되어야 보안 위협을 최소화할 수 있다(D'Arcy et al,. 2009).

조직 내 특정한 시스템을 구축하는 것은 조직원의 목표를 제어하기 위한 조직의 행동에 영향을 준다. 특히, 시스템의 구축은 조직 내 관련 구조, 프로세스, 목표 등을 표준화하는 것이기 때문에, 시스템 구축 수준이 높을수록 조직에서 수행하는 활동(교육, 캠페인 등) 수준을

높이고, 나아가 조직원의 목표 성과에 영향을 준다(Da Veiga and Eloff, 2007). Da Veiga and Eloff(2010)는 조직의 정보보안 문화 프레임워크 제시하면서, 정보보안 관련 기술, 정책, 관리 표준 등 구조 요인이 조직과 그룹 수준의 행동에 영향을 주고, 개인 보안 행동으로 이어진다고 하였다. 그들은 조직과 그룹 수준의 행동을 교육/훈련, 자산관리, 시스템 관리 등 관리적 행동으로 제시하였는데, 조직에 구축된 보안 요인들을 개인이 실행에 옮길 수 있도록 지원하는 체계를 조직과 그룹 수준의 행동으로 판단하였다. 특히, 그들은 조직원들이 수용가능한 조직 차원의 행동이 수반되어야 하며, 물리적 기반을 사전 구축하는 것이 조직 보안 문화 향상에 도움을 준다고 하였다. Jacobs and Washington (2003)은 환경적 요인인 직무 시스템에 대한 구축 수준이 조직원에 대한 교육 프로그램 및 프로세스에 영향을 주며, 개인의 교육성과에 영향을 미친다고 하였다.

즉, 정보보안 시스템의 구축은 조직 차원의 보안 관련 행동에 영향을 주는 기반요인이다. 이에 본 연구는 구조적 요인인 정보보안 시스템의 구축은 조직 차원의 행동요인으로 제시한 최고경영층의 지원, 교육, 가시성에 긍정적인 영향을 줄 것으로 판단하고, 다음과 같은 가설을 제시한다.

H6. 정보보안 시스템은 조직의 정보보안 행동에 긍정적인 영향을 줄 것이다.

H6a. 정보보안 시스템은 최고경영층의 지원에 긍정적 영향을 줄 것이다.

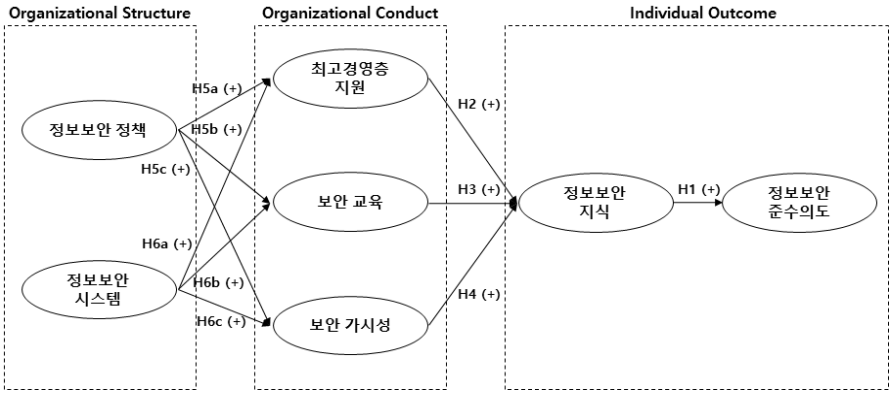
H6b. 정보보안 시스템은 정보보안 교육에 긍정적 영향을 줄 것이다.

H6c. 정보보안 시스템은 정보보안 가시성에 긍정적 영향을 줄 것이다.

Ⅲ. 연구 방법

3.1 연구 모델

본 연구는 사회적교환이론인 SCO 프레임워크를 정보보안 분야에 적용함으로써, 조직과 조직원의 교환관계에서 내부자의 정보보안 준수를 높이기 위한 방안을 제시하는 것을 목적으로 한다. 연구 목적에 기반을 둔 연구 모델은 다음 <그림 1>과 같다.



<그림 1> 연구 모델

3.2 설문지 개발

연구 모델에 대한 실증분석은 설문 대상에 대한 설문지 기법을 적용하여 구조방정식모델링을 기반으로 실시한다. 더불어, 연구 모델 구성 요인들을 설문항목으로 측정하기 위하여 측정 도구 개발을 실시하였다. 우선 정보보안 및 사회적교환이론 분야의 선행연구들을 통해 대상 분야에 활용되었던 구성 요인별 설문항목을 도출하였으며, 정보보안 분야에 적합하도록 수정하였다. 이후, 정보보안 분야 설문 타당성 확보를 위하여, 정보보안 정책을 보유한 기업에 다니는 대학원생 10명에게 설문지에 대한 논리적 타당성 검증을 받았으며, 추가적인 수정을 실시하였다.

정보보안 분야에 적용된 SCO 프레임워크 구

<표 1> 연구 변수 구성 항목

변수	구성 항목	관련문헌
정보보안 정책	우리 조직은 전자메일 사용 방법을 설명하는 상세 지침이 있다. 우리 조직은 컴퓨터 자원(예. pc, 서버 등)을 사용하기 위한 행동 규칙을 보유하고 있다. 우리 조직은 사전 인가를 받지 않은 컴퓨터 시스템 접근을 금지하는 공식적인 정책을 가지고 있다. 우리 조직은 컴퓨터 패스워드 사용 방법을 설명하는 상세 지침을 가지고 있다.	D'Arcy et al. (2009)
정보보안 시스템	우리 조직의 정보보안 시스템은 효율적으로 구축되어 있다. 우리 조직은 정보보안 시스템 구축을 위한 투자를 적절히 한다. 우리 조직은 정보보안 시스템에 대한 예산을 충분히 배정한다.	Lee et al.(2004)
최고경영층 지원	우리 조직의 경영진은 정보보안 회의에 참석한다. 우리 조직의 경영진은 정보보안 의사 결정에 참여한다. 우리 조직의 경영진은 정보보안 활동에 참여한다. 우리 조직의 경영진은 정보보안 시스템 활성화를 위한 기능적 지원을 한다.	Kankahalli et al. (2003)
정보보안 교육	우리 조직은 사내 네트워크 접속 계정을 부여하기 전에 컴퓨터 사용자를 대상으로 적절한 보안 교육을 실시하고 있다. 우리 조직에서는 직원들에게 컴퓨터 보안책임에 관한 교육을 하고 있다. 우리 조직은 직원들의 컴퓨터 및 정보보안 이슈에 대한 인식 수준을 높이기 위해 교육/훈련을 제공하고 있다. 우리 조직의 직원들은 정보기술에 대한 적절한 활용법을 교육받고 있다.	D'Arcy et al. (2009)
정보보안 가시성	우리 조직에서 정보보안 활동은 널리 보급되어 있다. 정보보안 정책은 조직 내에서 자주 볼 수 있다. 적절하지 못한 정보보안 사례를 조직 내 공동장소에서 자주 볼 수 있다(역)(Drop)	Siponen et al. (2010)
정보보안 지식	나는 정보보안 정책을 준수하며 업무를 수행하는 방법을 알고 있다. 나는 정보보안 장비 및 절차를 업무에 적용하는 방법을 알고 있다. 나는 정보보안 안전 수준을 유지하거나 향상시키는 방법을 알고 있다. 나는 정보보안 관련 사건/사고를 줄이기 위한 방법을 알고 있다.	Neal et al. (2000)
정보보안 준수의도	나는 우리 조직의 정보보안 정책을 지속적으로 따를 것이다 나는 우리 조직의 정보시스템을 보호하기 위해 조직의 정보시스템 보안 정책을 지속적으로 준수할 가능성이 높다. 나는 우리 회사의 정보 시스템을 접속할 때마다 정보보안 정책을 준수할 것이다. 나는 업무를 수행할 때마다 정보보안 절차를 준수할 것이다. 나는 조직의 정보 보안 정책을 준수하겠다는 나의 태도에 대해 확신을 느낀다.	Herath & Rao(2009) 박철주, 임명성 (2012)

성 요인을 살펴보면, 구조는 정보보안 정책과 정보보안 시스템으로 구성된다. 정보보안 정책은 D'Arcy et al.(2009) 연구를 통해 4개의 설문항목을 도출하였으며, 정보보안 시스템은 Lee et al.(2004)의 연구를 통해 3개의 설문항목을 도출하였다.

행동은 최고경영층 지원, 정보보안 교육, 그리고 정보보안 가시성으로 구성된다. 최고경영층 지원은 Kankahalli et al.(2003)의 연구를 통해 4개의 설문항목을 도출하였으며, 정보보안 교육은 D'Arcy et al.(2009)의 연구를 통해 4개의 설문항목을 도출하였다. 그리고 정보보안 가시성은 Siponen et al.(2010)의 연구를 통해 3개의 설문항목을 도출하였다.

마지막으로 결과는 정보보안 지식과 정보보안 준수의도 구성된다. 정보보안 지식은 Neal et al. (2000)의 연구를 통해 4개의 설문항목을 도출하였으며, 정보보안 준수의도는 Hearth and Rao(2009), 박철주와 임명성(2012)의 연구를 통해 5개의 설문항목을 도출하였다.

본 연구에서 적용한 변수들의 구성항목은 <표 1>과 같다.

3.3 자료 수집

설문 대상은 국내 정보보안 정책을 구축한 기업에서 근무하는 직장인이다. 다만, 정보보안 정책은 있으나, 직무가 정보보안 팀과 관련된 직장인은 설문대상에서 제외하였다. 그 이유는 정보보안 팀의 목표는 조직 구성원의 정보보안 준수에 있기 때문에, 조직과 교환관계에서 다른 부서의 직장인과 상이한 가치로 인식할 것으로 판단하였기 때문이다.

설문은 대학의 사회교육원에 다니는 직장인들에게 오프라인으로 실시하였다. 설문 실시전에 설문에 대한 충분한 설명을 하였으며, 설문에 응답하기로 한 직장인 및 정보보안 부서에서 근무하지 않는 직장인들만 대상으로 설문을 실시하였다. 총 480부를 배포하였으며, 설문 응답에 문제가 있는 42부를 제외한 438개의 응답을 표본으로 활용하였다.

Ⅳ. 가설 검증

4.1 설문응답자의 표본특성

설문 대상자의 인구통계학적 특성을 살펴보았다. 성별, 연령, 업종, 업력, 직급 기반의 인구통계적 특성 분석 결과, 표본이 전체적으로 고르게 분포되어 있어 표본 군 설정이 적절한 것으로 판단된다<표 2>.

<표 2> 인구통계학적 특성

구분		빈도	비율(%)
합계		438	100%
성별	남성	220	50.12%
	여성	218	49.88%
연령	< 30	120	27.47%
	31~40	165	37.59%
	41~50	121	27.71%
	> 50	32	7.23%
업종	제조업	123	28.19%
	서비스업	315	71.81%
업력	< 5년	144	32.77%
	6~10년	88	20.00%
	11~15년	75	17.11%
	16~20년	43	9.88%
	> 21년	89	20.24%
직급	사원	86	19.63%
	대리	76	17.35%
	과장	109	24.89%
	차/부장	99	22.60%
	임원	68	15.53%

4.2 신뢰도 및 타당성 분석

SCO 프레임워크에 대한 전체적인 구조 모형 영향 관계를 파악하기 위하여 AMOS 22.0을 활용하여 구조방정식모델링을 실시한다. 구조방정식을 통한 연구가설 검증을 위해, 우선 신뢰성 및 타당성 검증을 실시하였다.

우선, 신뢰성 검증은 내적 일관성(Internal consistency) 분석을 통해 적정성 검증을 하였다. 내적 일관성은 설문지 기법처럼 특정 요인에 대하여 다양한 항목을 통해 구성하였을 때, 항목들의 요인에 대한 일치성을 살펴보는 것으로서, 탐색적 요인분석과 Cronbach's Alpha 계수를 통해 적합성을 확인한다(Nunnally, 1978). 신뢰성 검증은 SPSS 21.0을 활용하였으며, 탐색적 요인분석과 Cronbach's Alpha 값을 도출하였다. 연구 모델은 7개 요인(총 27개 항목)으로 구성되어 있으나, 신뢰성 분석 결과 정보보안 가시성(Visi 3) 한 개 항목을 제외한 26개 항목을 적용하였으며, 신뢰성 요구치인 0.7이상을 확보하였다<표 4>.

<표 3> 확인적 요인분석에 대한 적합도 결과

변수	χ2/df	GFI	AGFI
분석 결과	2.645	0.922	0.857
권고 사항	< 3	> 0.9	> 0.8
변수	CFI	NFI	RMSEA
분석 결과	0.945	0.950	0.052
권고 사항	> 0.9	> 0.9	< 0.1

<표 4> 측정 모형의 신뢰성 및 타당성 검증

변수	측정 항목 명	평균	표준편차	표준 적재치	Cronbach's Alpha	개념 신뢰도	분산추출 지수
정보보안 정책	Pol1 Pol2 Pol3 Pol4	5.73	0.87	0.712 0.742 0.744 0.760	0.915	0.828	0.548
정보보안 시스템	Sys1 Sys2 Sys3	5.22	0.65	0.762 0.716 0.703	0.907	0.771	0.529
최고경영층지원	Top1 Top2 Top3 Top4	5.83	1.01	0.826 0.854 0.814 0.789	0.899	0.892	0.674
정보보안 교육	Edu1 Eud2 Eud3 Eud4	5.39	1.17	0.703 0.794 0.718 0.700	0.910	0.820	0.533
정보보안 가시성	Visi1 Visi2	5.60	0.95	0.806 0.778	0.861	0.771	0.627
정보보안 지식	Know1 Know2 Know3 Know4	5.91	1.05	0.727 0.753 0.809 0.709	0.908	0.837	0.563
정보보안 준수의도	Int1 Int2 Int3 Int4 Int5	6.18	1.33	0.830 0.829 0.834 0.819 0.799	0.939	0.913	0.676

다음으로, 집중타당성과 판별타당성 검증을 통해 타당성 분석을 하였다. 집중타당성은 개념신뢰도(Construct reliability)와 평균분산추출(Average variance extracted) 분석을 통해 파악하였다. 집중타당성 분석을 위하여 AMOS 22.0을 활용하여 확인적 요인분석을 실시하였으며, 확인적 요인분석에서 적용한 모델의 적합도 평가를 우선적으로 실시하였다. <표 3>은 확인적 요인분석의 적합도 평가 결과로서, 전체적으로 요구수준을 달성하여 확인적 요인분석에 문제가 없는 것으로 나타났다. 선행연구들은 개념신뢰도를 0.7이상의 값을, 평균분산추출을 0.5이상의 값을 요구한다(Wixom and Watson, 2001). 분석 결과 요인들의 개념신뢰도와 평균분산추출의 값들이 요구수준을 상회한 것으로 나타나 집중타당성이 존재하는 것으로 판단된다<표 4>.

더불어, 판별 타당성 검증을 위하여 평균분산추출 값과 피어슨 상관관계 분석 비교 방법을 사용하였다(Fornell and Lacker, 1981). 선행연구의 요구사항에 따르면, 판별타당성이 존재하기 위해서는 평균분산추출의 제곱근값이 각 요인들의 상관관계를 통해 도출된 값보다 커야 한다. 판별타당성을 분석한 결과 문제가 없는 것으로 나타나, 연구 모델에 활용한 요인들의 신뢰성과 타당성이 확보된 것으로 판단되어<표 5>, 구조 모형 분석을 실시한다.

<표 5> 확인적 요인분석에서 구성 개념간 상관관계

변수	1	2	3	4	5	6	7
정보보안 정책	***0.740***						
정보보안 시스템	0.423	***0.727***					
최고경영층지원	0.360	0.410	***0.821***				
정보보안 교육	0.238	0.387	0.266	***0.730***			
정보보안 가시성	0.368	0.417	0.283	0.294	***0.792***		
정보보안 지식	0.283	0.287	0.362	0.389	0.261	***0.750***	
정보보안 준수의도	0.266	0.206*	0.418	0.264	0.350	0.581	***0.822***

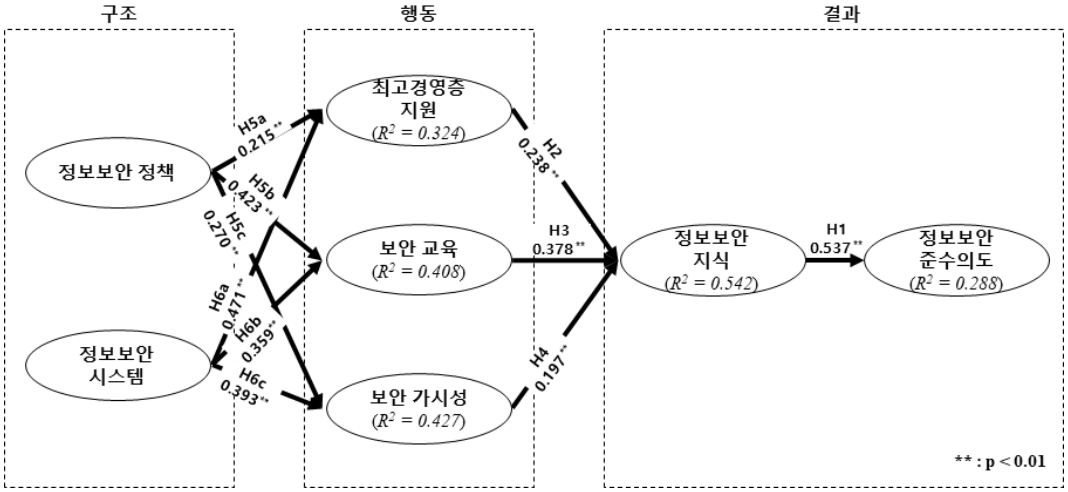
주) * = p<0.05 / 대각선의 볼드체 값은 분산추출지수의 제곱근

4.3 구조 모형 분석

구조모형분석은 모델의 적합도 검정, 경로계수(β) 분석, 그리고 결정계수(R^2) 분석을 실시함으로써, 전체적인 영향관계를 파악한다. 우선 구조모형에 대한 모델의 적합도 검정을 실시하였다. 모델의 적합도 검정은 χ^2/df, GFI, AGFI, CFI, NFI, RMSEA값에 대하여 종합적으로 확인하였다. 분석 결과는 적합도 요구수준을 상회하는 것으로 나타나, 구조모형을 통한 연구가설 검증을 실시하는 것에 문제가 없는 것으로 나타났다<표 6>.

<표 6> 연구 모형에 대한 적합도 결과

변수	χ^2/df	GFI	AGFI
분석 결과	2.011	0.924	0.897
권고 사항	< 3	> 0.9	> 0.8
변수	CFI	NFI	RMSEA
분석 결과	0.965	0.961	0.038
권고 사항	> 0.9	> 0.9	< 0.1



<그림 2> 가설 검정 결과

<표 7> 가설검정 결과

가설		경로	경로 계수	t-value	결과
H1		정보보안 지식→정보보안 준수의도	0.537**	13.257	채택
H2		최고경영층지원→정보보안 지식	0.283**	6.953	채택
H3		보안교육→정보보안 지식	0.378**	5.930	채택
H4		보안가시성→정보보안 지식	0.197**	4.125	채택
H5	H5a	정보보안 정책→최고경영층지원	0.215**	3.624	채택
	H5b	정보보안 정책→보안교육	0.423**	8.652	채택
	H5c	정보보안 정책→보안가시성	0.270**	4.106	채택
H6	H5d	정보보안 시스템→최고경영층지원	0.471**	9.841	채택
	H6a	정보보안 시스템→보안교육	0.359**	5.552	채택
	H6b	정보보안 시스템→보안가시성	0.393**	5.823	채택

연구 가설 검증은 변수들간의 경로 분석을 실시함으로써 변수들의 영향관계 수준을 파악한다. 경로계수(β) 분석결과는 <그림 2>, <표 7>과 같다. 첫째, 조직원의 정보보안 지식형성과 정보보안 준수의도간의 경로 분석을 실시한 결과(H1), 정보보안 지식이 정보보안 준수의도에 긍정적 영향을 미치는 것으로 나타났다(β=0.537, p<0.01). 이러한 결과는 개인에게 형성된 지식이 준수의도를 증가시킨다는 선행연구(Wang, 2010)와 동일한 결과이다. 즉, 개인의 정보보안 준수의도는 정보보안 규정, 절차, 대응 방법 등에 대한 조직원의 보안 지식이 형성되었을 때 높아지는 것을 의미한다.

둘째, 최고경영층의 지원과 정보보안 지식간의 경로 분석을 실시한 결과(H2), 최고경영층의 지원이 개인의 정보보안 지식에 긍정적 영향을 미치는 것으로 나타났다(β=0.283, p<0.01). 이러한 결과는 최고경영층의 지원이 대상에 대한 지식을 형성하는데 도움을 준다는 선행연구(Neal et al., 2000)와 같은 결과이다. 따라서, 최고경영층 차원에서 정보보안에 대한 관심을 가지고 자발적 보안 행동을 하고, 조직

원이 정보보안 활동을 능동적으로 할 수 있도록 지속적인 지원을 하는 것이 필요하다.

셋째, 정보보안 교육과 정보보안 지식간의 경로 분석을 실시한 결과(H3), 정보보안 교육이 개인의 정보보안 지식에 긍정적 영향을 미치는 것으로 나타났다(β=0.378, p<0.01). 이러한 결과는 정보보안 교육 프로그램이 활성화될수록 개인의 정보보안 지식 형성을 높인다는 선행연구(Nesheim and Gressgård, 2014)와 같은 결과이다. 따라서, 조직은 개인의 보안 지식 형성을 높이기 위한 교육 프로그램을 개발 및 보급, 그리고 지속적인 피드백을 통하여, 조직원이 요구하는 보안에 대한 관점을 이해하고 지원하는 것이 필요하다.

넷째, 정보보안 가시성과 정보보안 지식간의 경로 분석을 실시한 결과(H4), 정보보안 가시성이 개인의 정보보안 지식에 긍정적 영향을 미치는 것으로 나타났다(β=0.197, p<0.01). 이러한 결과는 조직에서 보안 가시성을 높이기 위한 다양한 활동이 개인의 정보보안 지식 형성에 도움을 준다는 선행연구와 같은 결과이다 (Hwang et al. 2017). 따라서, 조직은 일회성 정보보안 교육 프로그램만 제공하는 것이 아니라, 조직원에게 지속적으로 정보보안의 중요성을 노출시킬 수 있는 캠페인, 홍보 동영상 제공 등의 활동을 함으로써, 조직원이 정보보안에 대한 지식을 자연스럽게 확보할 수 있도록 지원하는 것이 필요하다.

다섯째, 정보보안 정책과 조직의 정보보안 행동(최고경영층의 지원, 정보보안 교육, 정보보안 가시성)의 경로 분석을 실시한 결과(H5), 정보보안 정책 수립이 조직의 정보보안 행동 요인들에게 모두 긍정적 영향을 미치는 것으로 나타났다 (H5a : β=0.215, p<0.01; H5b : β=0.423, p<0.01; H5c : β=0.270, p<0.01). 이러한 결과는 정보보안 정책이 명확하게 규정되어 있을수록 조직의 정보보안 활동 수준과 조직원의 준수 의도를 높인다는 선행연구와 같은 결과이다(D'Arcy et al. 2009; Hwang et al., 2017). 조직 내 구조화된 정보보안 정책 수준은 조직 차원의 전략적 행동(conduct) 기반 요소가 된다. 특히, 구조적인 정책 수립은 최고경영층의 정보보안에 대한 관심을 높이고, 정보보안 교육 프로그램을 활성화하는데 도움을 주고, 정보보안 캠페인 등을 통한 정보보안가시성 확보를 하는데 도움을 준다. 따라서, 교환 관계에서 조직이 조직원에게 정보보안 준수를 요구하기 위해서는 우선적으로 조직의 보안 정책을 명확하게 구조화하는 것이 필요하다.

마지막으로, 정보보안 시스템과 조직의 정보보안 행동(최고경영층의 지원, 정보보안 교육, 정보보안 가시성)의 경로 분석을 실시한 결과 (H6), 정보보안 시스템 구축이 조직의 정보보안 행동 요인들에게 모두 긍정적 영향을 미치는 것으로 나타났다 (H6a : β=0.471, p<0.01; H6b : β=0.359, p<0.01; H6c : β=0.393, p<0.01). 이러한 결과는 정보보안 시스템이 물리적으로 명확하게 구축되어 있을수록 조직의 정보보안 활동 수준과 조직원의 준수 의도를 선행연구와 같은 결과이다(D'Arcy et al., 2009). 구조화된 물리적 정보시스템은 조직이 조직원에게 보안 준수 행동을 요구할 수 있는 파워를 가지게 하며, 조직 차원에서 보안 행동을 할 수 있는 기반 요인이 된다. 따라서, 물리적 보안시스템을 조직의 특성에 맞게 도입하는 것이 필요하다.

마지막으로, 선행 요인들에 의한 설명력을 파악하기 위하여, 결정계수 분석을 하였다. 준수의도는 선행 요인인 정보보안 지식의 28.8%의 설명력을 가지고 있는 것으로 나타났으며, 정보보안 지식은 선행 요인인 최고경영층의 지원, 정보보안 교육, 정보보안 가시성에 의해 54.2%의 설명력을 가지고 있는 것으로 나타났다. 최고경영층의 지원은 정보보안 정책과 정보보안 시스템으로부터 32.4%의 설명력을 가지는 것으로 나타났으며, 정보보안 교육은 정보보안 정책과 정보보안 시스템으로부터 40.8%의 설명력을 가지는 것으로 나타났다. 정보보안 가시성은 정보보안 정책과 시스템으로부터 42.7%의 설명력을 가지는 것으로 나타났다.

Ⅴ. 결 론

최근 몇 년 사이 정보보안 정책이 엄격하게 구축된 국내 은행들에서조차 정보보안 사고가 지속적으로 발생하고 있다(KBresearch, 2015). 특히, 내부자의 정보복제를 통한 유출사고는 정보보안 기술로만 해결할 수 없는 요인으로, 조직원 개인의 준수의지 확보가 무엇보다 중요하다. 정보보안은 심리적 요인이기 때문에, 조직 내 개인들의 보안 준수를 위해서는 조직의 환경이 구축되고, 조직 차원의 보안 준수를 위한 행동이 개인들이게 보여지는 것이 중요하다(West, 2008). 이에, 본 연구는 사회적교환이론의 SCO프레임워크를 정보보안 분야에 적용함으로써, 조직원의 정보보안 준수가 조직에서 구축 및 제공하는 전략적 행동 요인과의 상호 교환관계에 있음을 제시하고, 조직원의 정보보안 준수에 대한 조직의 전략에 대한 방향성을 제시한다.

선행 연구를 통하여 사회적교환이론이 정보보안을 위한 조직과 조직원간의 행동 관계를 설명할 수 있음을 파악하였으며, 조직과 조직원의 정보보안 관계를 보다 명확하게 설명하기 위하여 SCO 단계별 프레임워크에 정보보안 요인들을 접목하였다. 정보보안 관련 조직 구조의 세부 요인은 정보보안 정책과 정보보안 시스템을 제시하였으며, 정보보안 관련 조직 행동의 세부 요인은 최고경영층의 지원, 정보보안 교육, 정보보안 가시성을 제시하였다. 정보보안 관련 조직원 차원의 결과의 세부 요인은 정보보안 지식과 정보보안 준수의도를 제시하였다.

정보보안 분야가 적용된 SCO프레임워크 요인들의 관계 증명은 종합적 관점에서 관련성을 파악하기 위하여 구조방정식 모델링을 통해 실시하였다. 연구의 결과는 조직원의 보안 준수를 위해서, 조직이 실행하는 전략적 행동인 최고경영층의 지원, 정보보안 교육, 정보보안 가시성이 중요한 선행요인임을 제시하였으며, 조직의 전략적 행동은 조직에서 구조화된 보안 체계인 정책과 시스템의 구축이 선행되어야 하는 것을 증명하였다.

5.1 연구의 시사점

본 연구는 조직과 조직원의 정보보안이 상호 교환관계에 있다는 사회적교환이론의 단계별 접근 프레임워크를 적용하여, 조직원의 정보보안 준수를 위한 조직차원의 구조화 및 행동 요인이 무엇인지를 제시하였다. 실증 분석결과는 정보보안 관련 이론적 측면과 실무적 측면에서

시사점을 제시한다.

첫째, 본 연구는 정보보안 분야에 사회적교환이론을 적용하였다. 조직원은 보안 준수 상황에서 조직에서 제시한 보안 관련 가치를 기반으로 준수 행동을 결정할 것으로 보고 사회적 교환이론을 적용하였다. 즉, 보호동기이론, 억제 이론 등과 같은 정보보안 준수 관련 선행이론들은 개인의 준수동기에 초점을 맞추고 준수 행동 향상 부분을 중점적으로 연구하였으나, 본 연구는 조직과 개인사이의 교환관계에 따른 합리적 의사결정이 중요하다고 보았다. 특히, 개인의 합리적 선택을 위한 제공되는 조직의 여러 환경 및 행동적 요인이 중요하다고 보았으며, 사회적교환이론을 적용하였다.

사회적교환이론에 따르면, 조직과 조직원의 관계에서 조직이 요구하는 수준으로 조직원이 행동하도록 하기 위해서는 가치를 조직원에게 제공해야 하며, 가치는 경제적 관점 및 사회/정서적 욕구까지 포함된다. 따라서, 사회적교환이론은 단순히 성과와 목표로서 조직원의 정보보안 준수를 요구하는 것이 아닌 조직원의 자발적 참여를 위한 정서적 접근이 필요함을 제시한다. 이러한 교환관계가 정보보안 분야에 적용되는 것을 확인하기 위하여, 조직의 노력요인과 조직원의 행동요인간의 관계성을 사회적교환이론의 단계별 프레임워크인 SCO모델을 통해 적용하였다. 즉, 이론적 측면에서 기존 개인의 동기기반의 접근을 시도하고 있던 정보보안 분야 선행 연구들과 달리, 본 연구는 조직과 조직원간의 교환관계적 특성을 정보보안 분야에 적용하였다. 즉, 조직-조직원 사이의 구조적 관계의 중요성을 정보보안 분야에 제시한 측면에서 시사점을 가진다.

또한, 실무적 측면에서 내부자에 의한 정보보안 위협 요인 최소화는 결국 조직과 조직원의 교환관계에서 제공되는 가치에 근거함을 제시하였기 때문에, 조직원의 정보보안 준수 향상을 위해서 조직이 수행해야할 전략적 행동 체계에 대한 시사점을 제시한다.

둘째, 사회적교환이론 단계별 프레임워크인 SCO 모델에 정보보안 요인을 적용하였으며, 상호관계를 증명하였다. 구조는 조직에 대한 조직원의 의존성을 높이기 위한 정보보안 차원의 잠재적 구조를 의미한다. 본 연구에서는 구조의 세부요인으로 정보보안 정책과 정보보안 시스템을 제시하였으며, 각 요인들을 효과적으로 구축할 경우 조직에 대한 의존성이 높아진다. 행동은 조직원과의 관계를 유지하기 위한 조직차원의 전략적 행동이다. 본 연구에서는 조직 행동의 세부요인으로 최고경영층 지원, 정보보안 교육, 보안 가시성을 제시하였다. 각 전략적 행동 세부 요인들을 체계적으로 조직원에게 제시할 경우 결과가 좋을 수 있다. 결과는 조직원의 정보보안관련 행동으로서, 본 연구에서는 조직원의 정보보안 지식과 정보보안 준수의도를 제시하였다. 즉, 조직 차원의 정보보안 구조화와 정보보안 관련 전략적 행동이, 조직원의 정보보안 행동 결과로 이어지는 관계를 증명하였다.

세부적으로, 조직원의 결과 행동(정보보안 지식, 정보보안 준수의도) 수준을 높이기 위해서는 조직의 정보보안 관련 전략적 행동(최고경영층의 지원, 정보보안 교육, 정보보안 가시성)을 높여야 하는 것을 증명하였다. 즉, 최고경영층의 정보보안 활동에 대한 관심 및 참여는 개인의 정보보안 수준을 높이는데 도움을 준다. 예를 들어, 경영층의 정보보안 독려 프로그램

참여 및 이메일 활동 등은 조직원의 정보보안 지식 확보에 도움을 주고, 나아가 정보보안 준수의지 확보에 도움을 줄 수 있다. 또한, 보안 관련 세부적인 교육 프로그램과 참여 독려와, 보안관련 가시성 향상을 위한 다양한 캠페인은 조직원에게 정보보안 지식형성에 도움을 준다. 예를 들어, 사내 카페에 24시간 정보보안 필요성, 절차 등을 제시하는 동영상을 제공하고 포스터를 붙이는 활동이 정보보안 가시성을 높여줄 수 있다.

이론적 측면에서 정보보안 분야에 조직원의 행동 결과요인과 조직의 전략적 행동 요인을 제시하고 영향 관계를 확인하였기 때문에, 조직원의 정보보안 준수 관련 연구에 선행연구로서의 시사점을 가진다. 특히, 정보보안 준수의지가 개인의 관련 지식 형성을 통해서 이어지는 것을 증명하였으며, 지식 형성을 위한 조직차원의 보안 행동간의 연관관계를 증명하였다는 측면에서 시사점을 가진다. 또한, 실무적 측면에서 정보보안 준수의도 향상은 개인의 정보보안 지식 형성을 통해 이루어짐을 증명하였고, 정보보안 준수의도 향상을 위한 조직의 행동 요인과의 관계를 증명하였기 때문에, 조직의 정보보안 행동 전략 수립에 대한 시사점을 가진다.

더불어, 정보보안 관련 조직의 전략적 행동은 구조화된 정보보안 체계 구축에 기반을 둔다고 보았다. 본 연구에서는 정보보안 구조의 세부 요인으로 정보보안 정책 수립 및 보안 시스템 구축으로 제시하였다. 조직의 특성에 맞는 구조화된 정보보안 정책과 시스템 구축이 선행되는 것의 중요성을 제시하였다. 이론적 측면에서, 조직차원의 보안 행동 수준을 높이기 위한 구조적 요인을 제시하고 상호간에 긍정적 영향관계가 있음을 증명하였기 때문에, 조직 정보보안 구축과 관련된 연구에 선행연구로서의 시사점을 가진다. 또한, 실무적 측면에서, 조직의 특성을 반영한 구조화된 보안 정책과 시스템 구축이 우선 시 되어야 하는 것을 제시하였기 때문에, 정보보안 확립을 위한 조직의 접근 방안을 제시한 측면에서 시사점을 가진다.

5.2 연구의 한계점

본 연구는 다음과 같은 연구적 한계점을 가진다. 첫째, 본 연구는 사회적교환이론을 정보보안 분야에 적용하고 요인들의 영향관계를 증명하기 위하여, 설문 당시의 개인의 생각을 파악하는 설문조사를 실시하였다. 즉, 사회적교환이론은 조직과 개인의 교환관계를 가정하기 때문에 조직 관점을 파악해야하나 개인이 판단하고 있는 조직의 수준을 설문하는 것으로 조직 관점을 수집하였다. 보다 객관적인 교환관계를 설명하기 위해서는 설문지 방식이 아닌 조직의 상황을 제시하고 판단할 수 있는 실험 방식의 접근이 필요할 것으로 판단된다.

둘째, 본 연구는 SCO프레임워크를 이용하여 정보보안분야에 사회적교환이론을 적용하고자 하였다. 선행연구를 기반으로 SCO프레임워크 각각의 단계에 적합하다고 판단되는 요인들을 적용하였는데, 본 연구에서 적용한 단계별 요인 이외 다른 변수도 존재할 것으로 판단된다. 향후 연구에서는 SCO프레임워크의 적용 확장을 위한 보안 분야 요인들을 추가적으로 적용하는 것이 필요할 것으로 판단된다.

마지막으로, 본 연구는 정보보안 정책을 보유한 기업에서 근무하는 조직원을 대상으로 하

나, 설문의 편의상 대학에 다니는 직장인들에게 조사를 실시하였다. 정보보안은 업종의 특성에 영향을 많이 받을 수 있기 때문에, 향후 연구에서는 업종의 특성을 반영한 연구가 진행되는 것이 필요하다.

참고문헌

박철주, 임명성, "기술스트레스가 정보보안에 미치는 영향에 관한 연구," 디지털융복합연구, 제10권, 제5호, 2012, pp.37-51.

유인진, 박도형 "중소기업 프로파일링 분석을 통한 기술유출 방지 및 보호 모형 연구," 정보시스템연구, 제27권, 제1호, 2018, pp.171-191.

최경선, 안현철, "개인적·사회적 요인을 고려한 가상 공동체에서의 지식 공유 모형," 정보시스템연구, 제28권, 제5호, 2019, pp.41-72.

황인호, 김대진, "조직의 정보보안 환경이 조직 구성원의 보안 준수의도에 미치는 영향," 정보시스템연구, 제25권, 제2호, 2016, pp.51-77.

Armeli, S., Eisenberger, R., Fasolo, P., and Lynch, P., "Perceived Organizational Support and Police Performance: The Moderating Influence of Socioemotional Needs," *Journal of Applied Psychology*, Vol. 83, No. 2, 1998, pp.288-297.

Bang, Y., Lee, D. J., Bae, Y. S., and Ahn, J. H., "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.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., and Polak, P., "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly*, Vol. 39, No. 4, 2015, pp.837-864.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I., "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.

Carr, N. G., "IT doesn't Matter," *Educause Review*, Vol. 38, 2003, pp.24-38.

Cegarra-Navarro, J. G., Cepeda-Carrion, G., and Eldridge, S., "Balancing Technology and Physician–patient Knowledge Through an Unlearning Context," *International Journal of Information Management*, Vol. 31, No. 5, 2011, pp.420-427.

Chen, Y., Ramamurthy, K., and Wen, K. W., "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *Journal of Management Information Systems*, Vol. 29, No. 3, 2012, pp.157-188.

Chou, H. L., and Chou, C., "An Analysis of Multiple Factors Relating to Teachers' Problematic Information Security Behavior," *Computers in Human Behavior*, Vol. 65, 2016, pp.334-345.

Cook, K. S., Emerson, R. M., Gillmore, M. R., and Yamagishi, T., "The Distribution of Power in Exchange Networks: Theory and Experimental Results," *American Journal of Sociology*, Vol. 89, No. 2, 1983, pp.275-305.

D'Arcy, J., Hovav, A., and Galletta, D., "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.

Devaraj, S., Fan, M., and Kohli, R., "Examination of Online Channel Preference: Using the Structure-Conduct-Outcome Framework," *Decision Support Systems*, Vol. 42, No. 2, 2006, pp.1089-1103.

Da Veiga, A., and Eloff, J. H., "An Information Security Governance Framework," *Information Systems Management*, Vol. 24, NO.4, 2007, pp.361-372.

Da Veiga, A., and Eloff, J. H., "A Framework and Assessment Instrument for Information Security Culture," *Computers & Security*, Vol. 29, No. 2, 2010, pp.196-207.

Da Veiga, A., and Martins, N., "Defining and Identifying Dominant Information Security Cultures and Subcultures," *Computers & Security*, Vol. 70, 2017, pp.72-94.

Desouza, K. C., "Facilitating Tacit Knowledge Exchange," *Communications of the ACM*, Vol. 46, No. 6, 2003, pp.85-88.

Dhillon, G., Oliveira, T., Susarapu, S., and Caldeira, M., "Deciding Between Information Security and Usability: Developing Value Based Objectives," *Computers in Human Behavior*, Vol. 61, 2016, pp.656-666.

Eisenberger, R., Fasolo, P., and Davis-LaMastro, V., "Perceived Organizational Support and Employee Diligence, Commitment, and Innovation," *Journal of Applied Psychology*, Vol. 75, No. 1, 1990, pp.51-59.

Emerson, R. M., "Power-Dependence Relations," *American Sociological Review*, Vol. 27, No. 1, 1962, pp.31-41.

Emerson, R. M., "Exchange Theory, Part I: A Psychological Basis for Social Exchange," *Sociological Theories in Progress*, Vol. 2, 1972, pp.38-57.

Emerson, R. M., "Social Exchange Theory," *Annual Review of Sociology*, Vol. 2, 1976, pp.335-362.

Fornell, C., and Larcker, D. F., "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*,

Vol. 18, No. 1, 1981, pp.39-50.

Geyskens, I., Steenkamp, J. B. E., and Kumar, N., "A Meta-Analysis of Satisfaction in Marketing Channel Relationships," *Journal of Marketing Research*, Vol. 36, No. 2, 1999, pp.223-238.

Griffin, M. A., and Neal, A., "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.

Herath, T., and Rao, H. R., "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems*, Vol. 47, No. 2, 2009, pp.154-165.

Hendricks, J., *Exchange Theory in Aging*. In G. Maddox (Eds.), The Encyclopedia of Aging (2nd eds.). New York: Springer, 1995.

Hwang, I., and Cha, O., "Examining Technostress Creators and Role Stress as Potential Threats to Employees' Information Security Compliance," *Computers in Human Behavior*, Vol. 81, 2018, pp.282-293.

Hwang, I., Kim, D., Kim, T., and Kim, S., "Why Not Comply with Information Security? An Empirical Approach for the Causes of Non-compliance," *Online Information Review*, Vol. 41, No. 1, 2017, pp.2-18.

Jacobs, R., and Washington, C., "Employee Development and Organizational Performance: A Review of Literature and Directions for Future Research," *Human Resource Development International*, Vol. 6, No. 3, 2003, pp.343-354.

Jiang, J. C., Chen, C. A., and Wang, C. C., "Knowledge and Trust in E-consumers' Online Shopping Behavior," In Electronic Commerce and Security, 2008 International Symposium on IEEE, 2008, pp.652-656.

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

KBresearch, KB Knowledge Vitamin: Recent Information Security Trend of Financial Institution and Outlook, 2015.

Knapp, K. J., Morris, R. F., Marshall, T. E., and Byrd, T. A., "Information Security Policy: An Organizational-Level Process Model," *Computers & Security*, Vol. 28, No. 7, 2009, pp.493-508.

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

Lee, S. M., Lee, S. G., and Yoo, S., "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories," *Information & Management*, Vol. 41, No. 6, 2004, pp.707-718.

Lee, J., and Lee, Y., "A Holistic Model of Computer Abuse within Organizations," *Information Management & Computer Security*, Vol. 10, No. 2, 2002, pp.57-63.

Loch, K. D., Carr, H. H., and Warkentin, M. E., "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly*, Vol. 16, No. 2, 1992, pp.173-186.

Lowry, P. B., and Moody, G. D., "Proposing the Control Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organisational Information Security Policies," *Information Systems Journal*, Vol. 25, No. 5, 2015, pp.433-463.

Mary MacNeil, C., "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.

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.

Moore, G. C., and Benbasat, I., "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.

Nunnally, J. C., *Psychometric theory* (2nd ed.). New York: McGraw-Hill, 1978.

Nesheim, T., and Gressgård, L. J., "Knowledge Sharing in a Complex Organization: Antecedents and Safety Effects," *Safety Science*, Vol. 62, 2014, pp.28-36.

Neal, A., Griffin, M. A., and Hart, P. M., "The Impact of Organizational Climate on Safety Climate and Individual Behavior," *Safety Science*, Vol. 34, No. 1, 2000, pp.99-109.

Nelson, K. M., and Cooprider, J. G., "The Contribution of Shared Knowledge to IS Group Performance," *MIS Quarterly*, Vol. 20, No. 4, 1996, pp.409-432.

Pham, H. C., "Information Security Burnout: Identification of Sources and Mitigating Factors from Security Demands and Resources," *Journal of Information Security and Applications*, Vol. 46, 2019, pp.96-107.

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., and Sookhak, M., "Deterrence and Prevention Based Model to Mitigate Information Security Insider Threats in Organisations," *Future Generation Computer Systems*,

Vol. 97, 2019, pp.587-597.

Said, A. R., Abdullah, H., Uli, J., and Mohamed, Z. A., "Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation," *Procedia - Social and Behavioral Sciences*, Vol. 123, 2014, pp.433-443.

Siponen, M., Pahnila, S., and Mahmood, M. A., "Compliance with Information Security Policies: An Empirical Investigation," *Computer*, Vol. 43, No. 2, 2010, pp.64-71.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N., "The Influence of a Good Relationship between the Internal Audit and Information Security Functions on Information Security Outcomes," *Accounting, Organizations and Society*, Vol. 71, 2018, pp.15-29.

Straub, D. W., and Welke, R. J., "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, Vol. 22, No. 4, 1998, pp.441-464.

Thibaut, J. W., and Kelley, H. H., *The Social Psychology of Groups*. New York: Wiley, 1959.

Thomson, K., and van Niekerk, J., "Combating Information Security Apathy by Encouraging Prosocial Organisational Behaviour," *Information Management & Computer Security*, Vol. 20, No. 1, 2012, pp.39-46.

Vance, A., Siponen, M., and Pahnila, S., "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management*, Vol. 49, No. 3, 2012, pp.190-198.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D., "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly*, Vol. 27, No. 3, 2003, pp.425-478.

Verizon, Verizon 2016 Data Breach Investigations Report, 2016.

Von Solms, R., "Information Security Management: Why Standards are Important," *Information Management & Computer Security*, Vol. 7, No. 1, 1999, pp.50-58.

Vroom, C., and Von Solms, R., "Towards Information Security Behavioural Compliance," *Computers & Security*, Vol. 23, No. 3, 2004, pp.191-198.

Wang, P. A., "Information Security Knowledge and Behavior: An Adapted Model of Technology Acceptance," *In Education Technology and Computer (ICETC), 2010 2nd International Conference on* (Vol. 2, pp. V2-364). IEEE, 2010, June.

Warkentin, M., and Willison. R., "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information*

Systems, Vol. 18, 2009, pp.101-105.

West, R., "The Psychology of Security," *Communications of the ACM*, Vol. 51, No. 4, 2008, pp.34-40.

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.

Whitman, M. E., Townsend, A. M., and Aalberts, R. J., "Information Systems Security and the Need for Policy," *In Information Security Management: Global Challenges in the New Millennium*, 2001, pp.9 – 18.

Wixom, B. H., and Watson, H. J., "An Empirical Investigation of the Factors Affecting Data Warehousing Success," MIS Quarterly, Vol. 25, No. 1, 2001, pp.17-41.

황 인 호 (Hwang, In-Ho)

현재 한국산업기술대학교 연구교수로 재직하고 있다. 중앙대학교 경영학 박사학위를 수여하였다. 기업가정신, IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야에 관심을 가지고 연구를 진행 중이다.

김 상 현 (Kim, Sang-Hyun)

미국 Washington State University에서 호텔경영 및 경영학학사와 MBA 학위를 받았으며, University of Mississippi, Oxford에서 경영정보학 전공으로 경영학 박사학위를 취득하였다. 현재 경북대학교 경영학부 교수로 재직 중이며, Information & Management, Information Systems Frontiers, International Journal of Information Management, DATA BASE for Advances in Information Systems, Communications of the ACM 등에 논문을 발표하였다. 주요 관심 분야는 RFID, OSS, 정보보안, 클라우드 컴퓨팅, SNS 비즈니스 등이다.

<Abstract>

Information Security of Organization and Employees in Social Exchange Perspective : Using Structure-Conduct-Outcome Framework

Hwang, In-Ho · Kim, Sanghyun

Purpose

Issues related to information security have been a crucial topic of interest to researchers and practitioners in the IT/IS field. This study develops a research model based on a Structure-Conduct-Outcome (SCO) framework for the social exchange relationship between employees and organizations regarding information security.

Design/methodology/approach

In applying an SCO framework to information security, structure and conduct are activities imposed on employees within an organizational context; outcomes are activities that protect information security from an employee. Data were collected from 438 employees working in manufacturing and service firms currently implementing an information security policy in South Korea. Structural equation modeling (SEM) with AMOS 22.0 is used to test the validation of the measurement model and the proposed casual relationships in the research model.

Findings

The results demonstrate support for the relationships between predicting variables in organization structure (security policy and physical security system) and the outcome variables in organization conduct (top management support, security education program, and security visibility). Results confirm that the three variables in organization conduct had a positive effect on individual outcome (security knowledge and compliance intention).

Keyword: Information Security, Social Exchange Theory, SCO Framework, Compliance Intention, Security Knowledge

* 이 논문은 2019년 8월 25일 접수, 2019년 10월 23일 1차 심사, 2019년 11월 19일 게재 확정되었습니다.