사회과학연구 제29권 4호(2018) 충남대학교 사회과학연구소 pp. 3-17
http://dx.doi.org/10.16881/jss.2018.10.29.4.3

성실성과 정보보안 풍토가 조직 구성원의 정보보안 행동에 미치는 효과: 산업 안전행동 개념적 접근*

박 세 웅, 민 윤 기†

충남대학교 심리학과

본 연구는 조직에서의 정보보안 행동을 일반적인 산업 안전행동 개념 측면에서 접근하였다. 산업 안전 연구문헌에서 개인의 안전행동에 영향을 미치는 중요 요인이 개인 차원의 성실성과 조직 차원의 안전풍토라는 점에 착안하여, 이 두 변인을 통해 개인의 정보보안 행동을 조직에서의 일반적인 안전행동 프레임으로 접근할 수 있는지 검증하였다. 구체적으로, 일반적인 안전행동과 같이 개인의 성실성 수준이 높고, 조직의 정보보안 풍토에 대한 지각 수준이 높을수록 정보보안 행동을 더 많이 할 것이라고 기대하였다. 나아가 개인의 성실성과 정보보안 행동과의 정적인 관계는 조직의 정보보안 풍토 지각 수준이 조절할 것이라고 가설을 설정하였다. 이러한 가설들을 검증하기 위하여 직장인 206명을 대상으로 실증 분석을 실시하였다. 그 결과, 기대한 바와 같이 성실성이 높을수록 개인의 정보보안 행동 수준이 높았으며, 조직의 정보보안 풍토를 높게 지각할수록 개인의 정보보안 행동 수준이 높았다. 또한 성실성과 정보보안 행동과의 정적 관계는 조직의 정보보안 풍토 지각 수준이 조절하였는데, 개인이 조직의 정보보안 풍토를 높게 지각하는 경우에서만 둘 간의 관계가 유의한 것으로 나타났다. 본 연구에서는 조직에서의 개인 정보보안 행동을 일반적인 산업 안전행동의 개념으로 접근할 수 있을 것이라고 제안하였으며, 이를 통해 기존 산업 안전 분야 연구에서 축적되어온 결과들을 조직에서의 정보보안 행동에 적용해볼 수 있을 것으로 기대한다.

주요어: 정보보안 행동, 조직 정보보안 풍토, 성실성, 안전행동

* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2018-2016-0-00304).

† 교신저자(Corresponding Author) : 민윤기, 충남대학교 사회과학대학 심리학과 교수, 대전시 유성구 대학로 99, E-mail : ykmin@cnu.ac.kr

■ 최초투고일 : 2018년 2월 12일 ■ 심사마감일 : 2018년 3월 25일 ■ 게재확정일 : 2018년 4월 2일

1. 서 론

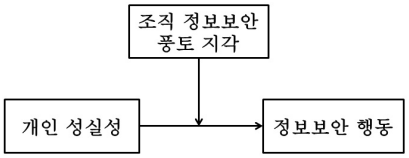
컴퓨터와 인터넷 사용이 보편화되면서 정보 시스템은 조직의 직무수행에 필수적인 부분이 되었다. 이렇듯 정보 시스템의 사용이 증가함에 따라 정보보안 관련 피해도 증가하고 있는데, 이러한 피해는 개인의 사생활 침해뿐만 아니라 조직의 기밀 정보 유출 등과 같은 조직 차원의 큰 손실을 발생시키기도 한다(안흥기, 2007). 따라서 조직에서는 정보 시스템의 보안 기능을 강화시켜 나가는 동시에 다양한 정책을 통해 조직 구성원의 정보보안 행동을 증가시키기 위해 노력하고 있다(박종원, 우현종, 김현규, 2017).

구성원의 실수 혹은 고의적인 보안 위반 행동으로 발생하는 정보보안 사고를 물리적인 정보 시스템 측면에서 완벽하게 방어할 수 있다면 더할 나위 없이 좋겠지만, 정보 시스템의 발전과 함께 해킹과 바이러스 등의 공격기법 역시 진화해가기 때문에(박대우, 2015) 시스템 차원에서의 한계는 늘 존재할 수밖에 없다. 더욱이 정보 시스템이 완벽하다고 하더라도 구성원들이 보안규범과 절차를 준수하지 않는다면 해당 조직에서의 정보보안은 기대하기 어려울 것이다(김상훈, 박선영, 2011). 결국, 조직에서는 정보 시스템의 보안을 강화해 나가야 할 뿐 아니라 주어진 시스템 환경 내에서 구성원의 정보보안 행동을 최대화할 수 있는 방안을 고민해야만 한다(전수현, 아낫 호바브, 이해원, 2015; 하상원, 김형중, 2013). 이를 위해서는 조직에서의 개인 정보보안 행동에 대해 보다 포괄적으로 이해할 필요가 있으며, 특히 개인행동에 영향을 주는 심리 메커니즘에 대한 체계적 접근이 필요하다.

최근 들어, 개인의 정보보안 행동에 대한 다양한 학제 융합적 접근이 시도되고 있다(김상훈, 박선영, 2011; 박종원 외, 2017). 그렇지만 아직까지 조직 구성원의 정보보안 행동을 이해하는데 있어서 통합적인 심리 모형을 체계적으로 제안한 연구는 많지 않다. 조직에서 정보보안의 필요성이 빠르게 증가하고 있고, 이러한 정보보안의 성공 여부에는 정보 시스템 뿐 아니라 구성원들의 정보보안 행동이 결정적 역할을 할 수 있다는 점을 감안하면, 정보보안 행동에 대한 개인의 심리적 메커니즘을 산업 및 조직 심리학 등에서 축적되어 온 개인행동 예측모형을 통해 검증하는 것이 효율적일 수 있다.

이러한 맥락에서, 본 연구에서는 조직에서의 정보보안 행동을 일종의 사고를 예방하기 위한 안전행동이라고 가정하고, 산업 및 조직 심리 분야의 포괄적인 “안전행동” 개념으로 접근하였다. 이를 통해 산업 안전 분야의 연구가 정보보안 행동을 이해하는 데 유용한 이론적 틀을 제공할 수 있는지 살펴보고자 하였다. 구체적으로, 조직 풍토를 활용한 산업 안전행동의 예측 모형(Griffin & Neal, 2000)이 정보보안 행동에서도 동일하게 적용될 수 있는지 검증하고자 하였다. 특히, 최근의 산업 안전 분야의 문헌에서 개인 특성 차원의 성실성과 조직 특성 차원의 안전풍토가 개인의 안전행동 수준에 영향을 주는 중요한 요인이라는데 의견이 일치하고 있다는 점에 착안하여(Christian, Bradley, Wallace & Burke, 2009), 산업 안전 행동의 개념에서 중요하게 작용하는 예측 변인들의 효과가 정보보안 행동에 있어서도 동일하게 나타날 수 있는지를 확인하고자 하였다. 종합적으로, 본 연구에서는 개인의 성실성이 높을수록 정보보안 행동을 더 많이 할 것이며, 나아가 조직의 정보보안 풍토 수준을 높게 지각할수록 개인의 성실성과 정보보안 행동과의 정적인 관계가 더욱 강해질 것으로 가정하고 이를 검증하였다. 이를 통해 조직에서의 개인 정보보안 행동이 산업 및 조직 심리학 등에서 제안하는 산업 안전행동의 포괄적 프레임에서 이해될 수 있는지 살펴보고자

하였다. 이와 같은 연구모형을 <그림 1>에 도식화하여 제시하였다.



<그림 1> 연구 모형

2. 이론적 배경 및 연구 가설

1) 산업 안전행동으로서의 정보보안 행동

산업 안전 분야의 문헌에서 안전행동은 직무수행의 한 영역으로서, "자신, 고객, 공익 및 주변의 건강과 안전을 향상시키기 위해 개인이 행하는 행동이나 활동"(Burke, Sarpy, Tesluk & Kristian, 2002, p. 432)으로 정의될 수 있다. 한편, 정보보안은 연구자들에 따라 다양하게 정의되고 있지만, "정보의 가치나 속성이 상실되거나 방해받지 않도록 위협으로부터 보호하고, 오용과 남용을 방지하기 위한 수단과 방책을 강구하는 행위"(강성민, 송은수, 2008, 4쪽)로 볼 수 있다. 이러한 정의적 측면에서 볼 때, 정보보안 행동은 신체적 건강의 피해는 아닐지라도 개인과 조직의 정보 및 정보 관련 물리적 피해와 사고를 예방하기 위해 필요하다는 점에서 일종의 안전행동으로 간주될 수 있을 것이다. 만약, 이와 같이 정보보안 행동을 산업 안전 분야의 포괄적인 안전행동 개념으로 이해할 수 있다면, 산업 안전 분야의 많은 연구결과들을 정보보안 행동에 접목시키는 것이 유용할 것으로 생각해볼 수 있다.

산업 안전 분야에서는 안전행동과 관련한 여러 이론들과 그에 대한 실증 연구들이 오래전부터 연구되어 왔는데(Greenwood & Woods, 1919), 연구결과들을 종합한 최근의 여러 메타 연구에서는 구성원의 안전행동에 영향을 주는 중요한 변인을 크게 개인의 성격 차원(성실성)과 조직의 풍토 차원(안전풍토)의 요인으로 인정하는데 동의한다(Beus, Dhanani & McCord, 2015; Christian et al., 2009; Clarke, 2006). 그런데 이러한 변인들은 정보보안에 있어서도 동일하게 중요한 역할을 할 것으로 기대된다. 예를 들어, 조직에서의 안전행동은 부정적인 상황(안전규범을 무시하여 사고가 발생한 경우)에서 주로 높은 관심을 받게 되는데, 반대로 말하면 문제적 상황이 발생하기 전까지는 조직에서 구성원의 안전행동에 대해 상대적으로 관심을 적게 기울이게 된다. 따라서 안전행동은 상당 부분 조직 구성원의 성격적 특성에 의존하게 된다(Wallace & Vodanovich, 2003). 이와 마찬가지로 정보보안 행동도 개인 PC내에서의 행동으로서 타인의 관찰이 어렵고 개인이 스스로 수행해야 하는 특성 상 개인의 성향에 따라 상당한 개인차가 존재할 것으로 예상된다(김상훈, 박선영, 2011). 또, 정보보안 행동은 추가적인 자원과 노력을 소모하게 만들어 조직의 효율성 측면과 대치될 수 있다. 복잡하고 바쁜 상황에서 정해진 절차와 프로그램들을 사용해야 하는 것은 업무의 신속성을 저하시킬 수 있기 때문인데, 이러한 속성 역시 일반적인 산업 안전행동과 크게 다르지 않다. 즉, 조직이 효율성을 강조하는 경우 안전에 대한 전반적인 인식이 저하되어 안전보다는 즉각적인 생산성을 선호하게 되기 때문이다. 조직의 안전풍토는 조직마다 다르게 나타날 수 있고, 구성원의 안전행동에 영향을 미치게 된다(Clarke, 2006). 마찬가지로, 조직에서의 정보보안 풍토 역시 조직의 효율성을 강조하는 분위기 등에 따라 다르게 형성될 수 있을 것으로 예상할 수 있다. 따라서 조직의 정보보안 풍토 수준은 개인의

정보보안 행동에 있어서도 중요한 역할을 할 것으로 기대된다(Chan, Woon & Kankanhalli, 2005).

이와 같은 맥락에서, 본 연구에서는 정보보안 행동을 “조직 구성원이 컴퓨터나 인터넷 등의 정보 시스템을 사용하는 데 있어서의 해킹 및 바이러스 등에 대한 안전행동”으로 정의하고 산업 안전 분야의 포괄적인 “안전행동” 개념에서 이를 예측해보고자 하였다. 즉, 정보보안 행동을 이해하는데 있어서 산업 안전 분야의 문헌에서 개인의 안전행동에 영향을 주는 중요한 요인으로 인정되고 있는, 개인의 성실성과 조직의 안전풍토를 활용하여 조직에서의 정보보안 행동이 일반적인 산업 안전행동의 범주로 인식될 수 있는지 검증하고자 하였다.

2) 정보보안 행동의 예측변인

Christian et al.(2009)에 따르면, 개인 성격 중 안전행동을 예측하는 가장 대표적인 변인은 성실성이다. 조직에서 성실성이 높은 직원은 책임감 있고, 체계적이며 신뢰할 수 있고, 효율적이며 성공적 업무수행을 추구하는 성향을 보인다. 나아가, 성실성이 높은 경우는 주의가 깊고 충동적이지 않으며, 조직의 규율을 잘 따르는 특성 등을 나타낸다(McCrae & Costa, 1987). 산업 및 조직 심리 분야의 선행 연구들에서는 성실성의 정의적 속성과 같이 성실성이 높을수록 직무를 보다 효율적으로 수행하며(Barrick & Mount, 1991), 안전행동이 증가하고(Christian et al., 2009), 조직의 안전 규범을 더 잘 따른다고 설명하고 있다(최정열, 2014).

정보보안에 대한 연구문헌에서는 개인이 피싱과 같은 인터넷 범죄에 취약한 이유, 즉 정보 시스템 사용 시 정보보안 행동이 감소하게 되는 이유를 개인의 인지와 노력 관점에서 접근하고 있다(이원영, 2006; Aytes & Connolly, 2004; Wang, Herath, Chen, Vishwanath & Rao, 2012). 다시 말하면, 개인이 인터넷 사용 시에 피해를 입는 것은 잘못된 정보를 탐색하지 못하도록 다른 자극이나 관심에 주의가 분산되기 때문이며, 관련 지식이 높고 이를 탐색하고자 노력할 경우는 피해가 줄어들 것이라고 주장한다. 이러한 정보보안 행동에 대한 실증적 결과 역시 앞서 설명한 성실성 관점에서 이해될 수 있다. 왜냐하면, 성실성이 높은 경우는 인터넷 등의 사용 시에 다른 자극의 간섭이 있더라도 충동을 조절하고 절제하여 주의력을 유지할 가능성이 높을 것이며, 최초 사용 목적을 달성하는데 보다 초점을 두어 잘못된 정보를 더욱 체계적으로 탐색할 것이라고 예상할 수 있기 때문이다. 또한 책임감이 높고 조직의 규율을 준수하고자 하는 등 성실성의 능동적인 성향 역시 정보보안 행동과의 정적인 관련성을 설명해 줄 수 있다. 이러한 맥락에서, 구성원의 성실성이 높을수록 정보 시스템 사용 시 관련 규범 및 절차를 보다 준수하는 등 개인의 정보보안 행동 수준이 높을 것으로 기대해볼 수 있다.

그런데, 조직의 관리자 관점에서는 정보보안 행동을 구성원 개인의 성향에만 의존할 수 없다. 즉, 정보보안은 그 중요성만큼 조직의 적극적인 개입이 요구된다. 따라서 본 연구에서는 조직의 정보보안 풍토를 조직에서 적극적으로 개입할 수 있는 수단으로 생각하고, 개인의 성격과 정보보안 행동과의 관계를 조절할 수 있는 조절변인으로서 연구하고자 하였다.

조직 풍토는 조직의 정책, 실행, 보상 등에 대한 구성원들의 공유된 지각으로 정의되는데, 조직 내에는 영역별로 세부적인 다양한 풍토들(안전풍토, 혁신풍토)이 존재하게 된다(Griffin & Neal, 2000). 이러한 맥락에서 정보보안 풍토를 정의하자면, “조직의 정보보안 정책과 실행 등에 대한 구성원들의

공유된 지각"이라고 할 수 있다. 그런데, 조직 풍토는 조직의 정책 등에 대한 구성원 개개인의 심리적 지각을 바탕으로 형성된다는 점에 주목할 필요가 있다(Schneider, 1990). 즉, 조직의 전반적인 분위기를 개인이 어떻게 지각하느냐 하는 것이 조직에서의 개인행동을 유발하는 중요한 조건이 될 수 있는 것이다. 산업 안전 분야의 문헌에서도 조직의 안전풍토에 대한 지각이 개인의 안전행동 수준에 정적인 영향을 미친다고 설명하고 있다(Griffin & Neal, 2000). 따라서 개인이 조직의 정보보안 풍토 수준을 높다고 지각할수록, 즉 조직이 정보보안에 대한 정책 등을 강하게 추진하고 있다고 느낄수록 개인은 정보보안에 대한 조직의 요구를 느끼고, 조직의 기대에 부응하기 위해 정보보안 행동을 더 많이 수행할 것으로 예상할 수 있다.

개인 성향과 환경과의 상호작용은 오래 전부터 심리학 분야의 중요한 연구 주제 중 하나로 자리 잡아 왔다(Schneider, 1983). 산업 안전 분야 문헌에서, 안전행동에 대한 개인 성향과 조직 안전풍토의 상호작용을 연구한 선행 연구자들은 조직의 안전풍토 수준이 높을수록 개인 성향과 안전행동과의 관계가 더욱 강해진다는 것을 밝혀온 바 있다(Hofmann, Morgeson & Gerras, 2003; Probst, 2004). 예를 들어, Hofmann et al.(2003)의 연구에서는 조직의 안전 풍토가 높은 경우에서만 상사와의 관계가 좋을수록 개인이 다른 사람의 안전행동을 더 도와주는 것으로 나타났다. 정보보안 행동에 있어서도, 극단적으로 자신의 조직이 정보보안에 대해 전혀 신경을 쓰지 않는다고 지각한다면, 아무리 성실한 사람이라도 정보보안 행동을 지속적으로 수행할 것으로 예상하기는 어려울 것이다. 따라서 안전행동에서와 같이 정보보안 행동에 있어서도 개인이 조직의 정보보안 풍토 수준을 높게 지각할수록 개인의 성실성과 정보보안 행동과의 정적 관계가 강하게 나타날 것으로 기대해볼 수 있다. 즉, 성실성이 높은 개인이 조직의 정보보안 풍토를 높게 지각하는 경우라면, 본래의 성격적 특성 외에도 조직의 정책 등을 따라야 한다는 압박이 더해지면서 정보보안 행동이 보다 증가하게 될 것으로 예상할 수 있다. 결과적으로, 산업 안전 분야의 연구에서 제안하는 안전행동에 대한 개인의 성실성과 조직 풍토 지각의 상호작용 효과는 정보보안 행동에 있어서도 동일하게 적용될 것으로 기대해 볼 수 있다.

한편, Griffin & Neal(2000)의 산업 안전행동에 대한 예측 모형에서는 안전에 대한 지식 수준이 조직 안전풍토와 개인의 안전행동 간의 관계에서 중요한 매개 역할을 할 것이라고 제안하고 있다. 조직에서 안전행동과 정보보안 행동이 모두 직무수행의 한 영역으로 간주될 수 있다는 점에서 직무수행에 필요한 관련 지식의 보유 는 성공적인 수행의 필수 요소가 될 것으로 생각해볼 수 있다(Campbell, McCloy, Oppler & Sager, 1993). 그런데, 안전행동과 정보보안 행동에 있어서 직무지식이 축적되는 경로는 다를 수 있을 것으로 추측된다. 왜냐하면, 안전행동의 경우 조직에서 실제 업무를 수행하지 않고는 관련 행동에 대해 알 수 없기 때문에 조직이 제공하는 교육이나 실무를 통한 경험 등 조직의 안전 풍토가 안전 관련 지식을 형성하는 데 직접적인 역할을 하게 될 것이다(Griffin & Neal, 2000). 반면, 컴퓨터와 인터넷 같은 정보 시스템의 사용이 일상에까지 보편화되어 있다는 점을 감안하면, 정보보안 관련 지식은 조직의 정보보안 풍토를 통해서가 아니라 다양한 경로(학교, 가정, 게임)를 통해서 이미 형성되었을 수도 있기 때문이다. 따라서 정보보안 행동에 있어서도 일반적인 직무수행과 마찬가지로 개인의 정보보안 관련 지식이 중요한 역할을 할 것으로 기대는 되지만, 개인의 지식 수준이 형

성되는 메커니즘 등이 안전행동 분야와 동일하게 발생할 것으로 가정하기에는 다소 무리가 따른다. 이에 본 연구에서는 정보보안 행동에 있어서 개인의 정보보안 관련 지식 수준에 대해서는 별도의 가설을 설정하지 않고, 성실성과 조직 정보보안 풍토에 대한 지각이 개인의 정보보안 행동을 예측하는데 있어서 개인의 정보보안 관련 지식 수준을 중요한 통제변인으로 사용하고자 하였다.

이와 같은 맥락에서 본 연구에서는 산업 안전 분야의 안전행동 연구결과와 마찬가지로, 개인의 성실성이 높을수록 정보보안 행동이 높을 것으로 기대하였으며, 개인의 성실성과 정보보안 행동과의 정적인 관계는 조직의 정보보안 풍토에 대한 개인의 지각이 높을수록 강화될 것이라고 기대하였다. 따라서 아래와 같이 가설을 설정하고 이를 검증하고자 하였다.

- 가설 1. 개인의 성실성이 높을수록 정보보안 행동 수준이 높을 것이다.
- 가설 2. 개인이 조직의 정보보안 풍토를 높게 지각할수록 정보보안 행동 수준이 높을 것이다.
- 가설 3. 개인의 성실성과 정보보안 행동의 정적 관계는 조직의 정보보안 풍토 지각 수준이 조절할 것이다. 즉, 조직의 정보보안 풍토를 높게 지각하는 경우가 낮게 지각하는 경우에 비해, 개인의 성실성과 정보보안 행동과의 정적 관계가 더 강하게 나타날 것이다.

3. 연구 방법

1) 참여자

본 연구에서는 연구업무를 주로 수행하고 있는 조직으로서, 정보보안에 대한 관심이 높은 국내 한 연구기관의 직원들을 대상으로 설문조사를 실시하였다. 이를 위해 연구자가 해당 기관의 담당자에게 연구 승인을 득한 후 직원들에게 연구에 대한 참여를 요청하는 안내문과 함께 설문지를 무선적으로 배포하였으며, 참여를 희망하는 직원에 한해 응답한 자료를 회수하였다.

설문에 응답한 직원은 총 206명이었으며, 참여자들은 대부분 남성이었다(179명, 87%). 평균 연령은 38.4세(SD=7.41), 평균 근속기간은 9.9년(SD=6.67)이었으며, 하루 평균 인터넷을 사용하는 시간은 약 2.6시간(SD=2.22)이었다.

2) 측정 도구

정보보안 행동. 박준경, 김범수, 조성우(2011)가 사용한 조직 구성원의 정보보안 관련 태도 문항 중 4문항을 본 연구 맥락에 맞게 수정하여 사용하였다(문항의 예: “나는 회사 컴퓨터의 보안 프로그램이 최신 상태인지 수시로 점검한다”). 응답자에게는 5점 리커트식 척도(1=전혀 그렇지 않다 ~ 5=매우 그렇다) 중 하나를 선택하도록 하였으며, 척도의 내적 일관성 신뢰도(Cronbach′s alpha)는 .79이었다.

성실성. Gosling, Rentfrow, Swann(2003)이 개발한 성실성 문항을 번안하여 사용하였다. 본 문항은 성격 특성을 설명하는 두 개의 단어들을 하나의 문항으로 묶어 2문항으로 측정하는 방식이나, 2개의 단어에 대한 의미를 다르게 해석할 수 있을 것으로 생각되어, 각 단어들을 하나의 문항으로 하는 총 4개의 문항을 사용하였다(문항의 예: “신뢰할 수 있는”, “부주의한”). 응답은 5점 리커트식 척도(1=전혀 그렇지 않다 ~ 5=매우 그렇다) 중 하나를 선택하도록 하였다. 척도의 내적 일관성 신뢰도는 .61이었다.

조직의 정보보안 풍토 지각. Griffin과 Neal(2000)

이 개발한 조직 안전풍토 척도 중 Lee와 Dalal (2014)의 연구에서 사용한 10개 문항을 정보보안 풍토 맥락에 맞게 수정하여 사용하였다. 문항의 예로는 “우리 회사는 인터넷 사용 시 정보보안을 매우 강조한다.” 등이며, 5점 리커트식 척도(1=전혀 그렇지 않다 ~ 5=매우 그렇다)를 사용 하였다. 척도의 내적 일관성 신뢰도는 .85이었다.

정보보안 지식 수준. 개인의 정보보안 관련 지식 수준은 Aytes와 Connolly(2004)의 컴퓨터 보안 지식 관련 문항을 토대로 3개 문항을 자체 제작하여 측정하였다. 문항의 예로는 “나는 컴퓨터와 인터넷 사용에 대한 지식이 높다.” 등이며, 5점 리커트식 척도(1=전혀 그렇지 않다 ~ 5=매우 그렇다)를 사용 하였다. 척도의 내적 일관성 신뢰도는 .76이었다.

통제 변인. 조직 맥락의 연구라는 점을 감안하여 조직에 대한 태도에 영향을 줄 수 있다고 생각되는 근속년수와 성별을 통제변수로 설정하였고, 정보보안 사고는 인터넷 등의 정보보안 시스템 사용 시간이 증가할수록 높아질 것으로 예상할 수 있으므로 인터넷 사용 시간을 통제변인으로 추가하였다.

3) 분석 방법

가설 검증을 위해 SPSS 21버전을 사용하였으며, 상호작용 효과 및 단순 기울기 검증(Aiken & West, 1991) 시에는 PROCESS 메크로를 활용하였다(Hayes, 2017). 분석 방법으로는 정보보안 행동을 종속변수로 하는 위계적 회귀분석을 실시하였다. 이를 위해 1단계에서는 정보보안 행동을 예측하는 독립변수로서 인구통계학적 변인과 인터넷 사용 시간을 기본 통제변인으로 투입하였고, 2단계에서는 정보보안 지식 수준을 투입하였으며, 3단계에서는 성실성과 조직 정보보안 풍토 지각을, 4단계에서는 성실성과 조직 정보보안 풍토 지각의 상호작용항을 각각 투입하여 분석하였다. 분석 시에는 변인의 의미 해석을 명확하게 하기 위해 변인들을 평균 중심화 변환하여 사용하였다.

4. 결 과

분석모형에 포함된 변인들의 기술 통계치 및 상관관계는 <표 1>에 제시하였다. 상관분석 결과, 정보보안 행동은 개인의 정보보안 지식과 정적 관계로 나타났으며(r=.419, p<.001), 성실성(r=.261, p<.001) 및 조직의 정보보안 풍토 지각과도 정적 상관을 보였다(r=.472, p<.001). 이는 가설에 가정한 관계의 방향을 일차적으로 지지해주는 결과이다. 본격적인 가설 검증을 위한 위계적 회귀분석 실시 결과는 <표 2>와 같이 나타났다. 분석 결과, 기본적인 통제변인만을 포함한 1단계 모형은 유의하지 않았다(F=.238, ns). 정보보안 지식을 포함한 2단계 모형(F=10.999, p<.001)과 성실성 및 정보보안 풍토 지각을 포함한 3단계 모형(F=15.142, p<.001) 그리고 성실성과 정보보안 풍토 지각의 상호작용항까지 포함한 4단계 모형(F=15.057, p<.001)은 모두 유의하였다. 구체적인 결과를 살펴보면, 개인의 정보보안 관련 지식 수준이 높을수록 정보보안 행동이 높은 것으로 나타났으며(B=.383, t=6.567, p<.001), 개인의 정보보안 지식은 정보보안 행동 변량의 약 17.7%를 설명하였다. 또한, 가설에서 기대한 바와 같이 개인의 성실성이 높을수록 정보보안 행동 수준이 높은 것으로 나타났으며(B=.227, t=3.095, p<.01), 조직의 정보보안 풍토를 높게 지각할수록 개인의 정보보안 행동 수준이 높은 것으로 분석되었다(B=.417, t=5.229, p<.05). 따라서 가설 1과 가설 2가 지지되었다. 개인의 성실성과 조직의 정보보

<표 1> 변인들 간의 상관 및 기술통계치

(N=206)

변인명	1	2	3	4	5	6	7
정보보안 행동	(.79)						
성실성	.268 ***	(.61)					
정보보안 풍토 지각	.472 ***	.119	(.85)				
정보보안 지식	.425 ***	.189 **	.483 ***	(.76)			
성별	-.009	.115	.033	.096	-		
근속년수	.034	.141 *	-.015	.027	.188 **	-	
하루 인터넷 사용시간(hour)	.041	-.091	-.102	-.012	-.169 *	-.038	-
평균	4.107	3.660	3.761	3.435	.869	9.913	2.609
표준편차	.689	.572	.584	.763	.338	6.676	2.225

주1. 성별(남=1, 여=0), 대각선 ( )안의 숫자는 Cronbach's α 신뢰도 계수임
주2. *p<.05, **p<.01, ***p<.001

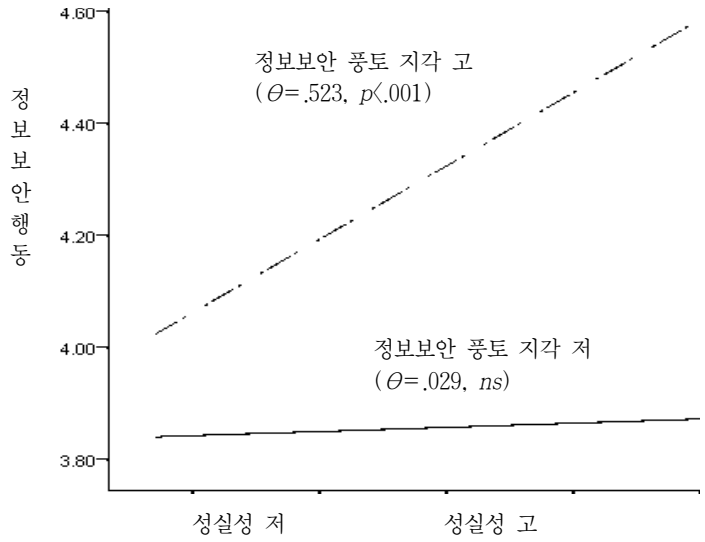
<표 2> 정보보안 행동에 대한 위계적 회귀분석 결과

(N=206)

변인명	1단계		2단계		3단계		4단계	
	비표준화 계수	t값	비표준화 계수	t값	비표준화 계수	t값	비표준화 계수	t값
(상수)	3.964 ***	24.681	4.013 ***	27.419	4.051 ***	29.939	3.998 ***	30.034
성별	0.076	0.582	0.034	0.283	-0.012	-0.106	-0.002	-0.019
근속년수	0.003	0.396	0.002	0.259	0.001	0.085	0.002	0.326
하루 인터넷 사용 시간(hour)	0.016	0.727	0.016	0.809	0.030	1.628	0.036 *	1.994
정보보안 지식			0.378 ***	6.530	0.196 **	3.190	0.197 **	3.281
성실성					0.227 **	3.095	0.274 ***	3.755
정보보안 풍토 지각					0.417 *	5.229	0.394 ***	5.044
성실성*정보보안풍토 지각							0.439 **	3.277
F값	0.317		10.945***		14.907***		14.940***	
R^2값	0.005		0.182		0.309		0.343	
R^2 변화량	-		0.177		0.132		0.034	

주1. 성별(남=1, 여=0), 정보보안 지식・성실성・정보보안 풍토지각은 평균 중심화 변환하여 사용함
주2. *p<.05, **p<.01, ***p<.001

안 풍토 지각은 개인의 정보보안 지식 수준 등을 통제하고도 정보보안 행동 변량의 약 13.2%를 설명하는 것으로 나타났다. 끝으로, 성실성과 정보보안 풍토 지각의 상호작용 역시 유의하였으며(B=.439, t=3.277, p<.01), 개인 정보보안 행동 변량의 약 3.4%를 추가 설명하는 것으로 나타났다. 이러한 상호작용의 패턴을 알아보기 위해(Aiken & West, 1991), 정보보안 풍토 지각 평균의 ±1 표준편차 값에서 개인의 성실성과 정보보안 행동과의 관계를 그래프로 살펴보았다(<그림 2> 참조). 그 결과, 개인의 성실성과 정보보안 행동의 정적 관계는 개인이 조직의 정보보안 풍토를 높게 지각하는 경우가 낮게 지각하는 경우에 비하여 강한 것으로 나타났다. 또한 상호작용 패턴에 대한 단순 기울기 검증을 실시한 결과, 정보보안 풍토를 높게 지각하는 경우는 성실성과 정보보안 행동과의 정



<그림 2> 정보보안 행동에 대한 성실성과 정보보안 풍토 지각과의 상호작용 패턴

적 관계가 유의하였으나(Θ=.523, t=4.41, p<.001), 정보보안 풍토를 낮게 지각하는 경우는 성실성과 정보보안 행동과의 관계가 유의하지 않았다(Θ=.029, t=.309, ns). 즉, 개인이 조직의 정보보안 풍토를 높게 지각하는 경우는 개인의 성실성 수준이 높을수록 정보보안 행동 수준도 높아지지만 조직의 정보보안 풍토를 낮게 지각하는 경우는 개인의 성실성과 정보보안 행동 간의 관계가 유의하지 않은 것으로 분석되었다.

추가 분석으로, 조직에서의 안전행동에 대해 Griffin & Neal(2000)이 제안한 안전행동 예측 모형을 적용하여, 정보보안 지식을 매개변수로 하는 정보보안 행동 예측 모형을 분석하였다. 비록, 정보보안 지식의 형성 과정에는 조직의 정보보안 풍토 외에도 다른 외부적 요인의 영향이 중요할 것으로 예상되는 등, 정보보안 지식과 정보보안 풍토 간의 인과관계 방향을 명확히 제시할 수는 없으나, 안전행동에 대한 연구모형이 정보보안 행동에도 적용될 수 있는지를 탐색적으로 살펴보고자 하였다. 이를 위해, 개인의 성실성과 조직의 정보보안 풍토에 대한 지각이 개인의 정보보안 지식 수준에 정적인 영향을 미치고, 이렇게 형성된 정보보안 지식 수준에 따라 개인 정보보안 행동에 차이가 발생하는 모형을 설정하고 이를 검증하였다. 그 결과, 안전행동 모형에서와 같이 정보보안 지식 수준은 조직 정보보안 풍토 지각 및 개인의 성실성 수준과 정보보안 행동과의 정적 관계를 유의하게 매개하는 것으로 나타났다(간접효과(정보보안 풍토 지각)=.115, 95% CI [.043, .207]; 간접효과(성실성)=.034, 95% CI [.004, .081]).

5. 논 의

본 연구에서는 정보보안 행동을 산업 안전 분야의 포괄적인 안전행동의 개념으로 접근하는 것이 타당한지 살펴보고자 하였다. 이를 위해 안전행동에 대한 메타연구들을 바탕으로(Beus et al., 2015; Christian et al., 2009; Clarke, 2006), 안전행동을 예측하는 중요 요인으로 인정되고 있는 성실

성과 조직 풍토를 이용하여 동일한 프레임이 정보보안 행동에도 적용되는지 검증하였다. 연구결과, 가설에서 기대한 바와 같이 개인의 성실성이 높을수록 정보보안 행동 수준이 높은 것으로 나타났으며, 조직의 정보보안 풍토를 높게 지각하는 개인일수록 정보보안 행동을 더 많이 하는 것으로 분석되었다. 이러한 결과는 조직 구성원의 정보보안 행동에 있어서 개인의 성실성과 조직의 풍토가 매우 중요함을 보여줄 뿐 아니라 정보보안 행동을 산업 안전 행동의 개념으로 접근할 수 있다는 가능성을 제시한다. 또 본 연구에서는 개인의 정보보안 행동과 개인의 성실성의 정적 관계가 조직의 정보보안 풍토 수준을 지각하는 정도에 의해 조절된다는 것을 보여주었다. 특히 이러한 상호작용 효과에 대한 단순 기울기 검증 결과, 개인이 조직의 정보보안 풍토를 높게 지각하는 경우에서만 개인의 성실성과 정보보안 행동과의 관계가 정적으로 유의하다는 것을 보여주었다. 이는 개인이 조직의 정보보안 풍토를 낮게 지각하는 경우, 아무리 성실한 직원이라 하더라도 정보보안 행동에 적극적으로 참여하지 않을 수 있는 반면, 성실성이 다소 낮은 직원이라도 조직의 정보보안 풍토가 강하다고 인식할 경우, 정보보안 행동에 참여할 가능성이 증가할 것이라는 것을 의미한다. 이러한 연구결과의 이론적, 실무적 함의를 구체적으로 살펴보면 다음과 같다.

첫째, 본 연구 결과를 통해 정보보안 행동을 일반적인 산업 안전 분야의 안전행동 개념(Griffin & Neal, 2000)으로 접근하는 것이 타당하다는 것을 보여주었다. 즉, 정보보안 행동을 포괄적인 안전행동의 개념에서 접근하여, 개인의 안전행동에서 중요하게 작용하는 심리적 메커니즘이 정보보안 행동에서도 동일하게 발생할 수 있다는 가능성을 보여주었다. 따라서 산업 및 조직 심리학 분야 등에서 비교적 많이 축적되어 있는 안전행동 관련 연구결과들을 최근에 부각되고 있는 정보보안 연구 분야에 적용할 수 있다는 다학제 융합 측면의 확장된 이론적 시각을 제시해 주고 있다. 또한 실무적으로는 정보보안 정책을 실행하고 강화하는 데 있어서 산업 안전 분야에서 사용하고 있는 다양한 정책들을 적용해볼 수 있다는 가능성을 제시함으로써 실무에서의 보다 폭 넓은 응용을 기대할 수 있게 한다. 예를 들어, 조직의 안전풍토 관련 연구 문헌에서는 안전풍토 수준을 높이는 방안으로 경영진의 적극적인 개입과 동료들의 안전 지지적 환경을 구축하는 것 등이 중요하다고 강조하고 있는데(이종한, 이종구, 석동헌, 2011), 이러한 연구결과의 실무적 함의 역시 정보보안에 있어서도 중요한 고려 요소로 작용할 수 있을 것이다.

둘째, 본 연구에서는 조직에서의 개인행동은 개인 특성과 조직 특성의 상호작용적 관점에서 접근해야 한다는 고전적인 심리 이론을 정보보안 연구에서도 재확인시켜 주었다(Schneider, 1983). 이를 통해 조직 분야의 연구자들에게 연구 시 개인의 특성과 환경적 요인을 항상 함께 염두에 두어야 한다는 기본적인 가정을 강조해주고 있다. 또한, 조직의 관리자들에게는 정보보안을 강화하기 위해서는 구성원 개인의 특성을 고려해야할 뿐 아니라 구성원들이 조직의 정보보안 풍토를 강하게 지각하도록 만드는 것이 중요하다는 것을 확인시켜 주었다(Chan et al., 2005). 특히, 정보보안 풍토를 낮게 지각하는 경우는 아무리 성실한 개인이라도 정보보안 행동에 관여할 가능성이 적다는 것을 보여줌으로써 조직에서의 정보보안과 관련된 정책과 실행이 구성원들에게 일관되고 강력하게 지각될 수 있는 방안을 모색하는 것이 정책의 성공에 무엇보다 중요하다는 것을 강조해주고 있다(김상훈, 박선영, 2011).

본 연구는 위와 같은 이론적·실무적 의의를 지니고 있으나, 여느 연구와 마찬가지로 연구 설계상의 여러 한계점을 가지고 있다.

첫째, 모든 변인을 자기보고식의 설문으로 측정하여 공통방법 편의가 발생했을 가능성이 있다(Podsakoff, MacKenzie, Lee & Podsakoff, 2003). 따라서 향후 연구에서는 정보보안 행동을 실제 조직에서의 보안사고 여부 등과 같이 보다 객관적이고 다양한 출처를 통해 측정하는 방법을 고려할 필요가 있을 것이다. 또한, 본 연구에서 사용한 일부 척도들은 비록 산업 안전 분야 등에서 타당도가 검증된 도구라 할지라도 정보보안 맥락으로 수정하는 과정에서 타당화 절차를 거치지 않았다는 한계점을 지닌다. 따라서 향후 산업 안전 연구의 프레임을 정보보안 연구에 적용함에 있어서는 척도의 타당화 작업이 선행될 필요가 있다.

둘째, 본 연구는 횡단적 연구로서 변인 간의 관계를 인과적으로 설명하는 데에 한계를 지닌다. 향후 연구에서는 종단 설계 혹은 실험 설계 등과 같은 보다 엄격한 방법론을 고민할 필요가 있을 것이다.

셋째, 본 연구는 국내 1개 기관의 근무자를 대상으로 한 연구이기 때문에 결과의 일반화에 주의가 필요하다. 이러한 맥락에서, 본 연구가 같은 조직 내에서도 개인의 지각에 따라 정보보안 풍토의 영향이 다르게 나타날 수 있다는 것을 설명해준다는 의의가 있으나 향후 연구에서는 여러 조직에서 충분한 참여자를 모집하여 다수준 분석을 통해 본 연구의 결과를 재확인하고 조직 특성에 따라 어떤 차이가 발생하는지를 연구하는 것도 필요할 것으로 생각한다. 나아가, 다수준 분석을 통해 조직의 풍토 수준과 함께 최근 관심을 받고 있는 풍토 강도, 즉 구성원들이 조직의 풍토를 얼마나 동일하게 인식하는지가 정보보안 행동에 있어서는 어떠한 영향을 미치는지를 살펴보는 것도 이론적 발전을 기대하게 하는 의미 있는 연구가 될 것이다(Lee & Dalal, 2014).

끝으로, 본 연구에서는 정보보안 행동에 있어서 조직의 정보보안 풍토를 주요 환경적 요인으로 고려하였지만 향후 연구에서는 조직 내에 공존하는 다양한 풍토들 간의 상호작용을 함께 연구해보는 것도 필요할 것으로 생각된다. 특히, 향후 정보보안에 대한 조직의 관심이 지속적으로 증가할 것이라는 점을 감안하면 정보보안 풍토가 높을 경우 발생할 수 있는 부정적 결과에 대해서도 연구해볼 필요가 있다. 예를 들어, 정보보안을 강조하는 조직과 그렇지 않은 조직에서는 물리적 안전에 대한 위협이 발생 시(화재), 구성원들의 행동 패턴이 다르게 나타날 것으로 예상해볼 수 있다.

본 연구에서는 최근 많은 관심을 받고 있는 정보통신 분야의 보안행동을 일반적인 산업 안전 분야의 안전행동 개념으로 접근하였다. 본 연구 결과는 조직에서의 개인 정보보안 행동을 일반적 산업 안전행동 프레임으로 접근하는 것이 가능하다는 것을 보여주었다. 이를 통해 산업 안전 분야 연구에서 축적되어온 여러 결과들을 개인의 정보보안 행동 연구에 적용해볼 수 있다고 제안한다. 본 연구가 정보보안 행동을 보다 체계적으로 이해하고 관련 연구와 실무에서의 통찰의 폭을 넓히는데 도움이 되기를 기대한다.

참 고 문 헌

강성민 · 송은수 (2008). 전자상거래 기업 환경에서의 시스템 사용자의 정보보안에 대한 인식 연구. <전자무역연구>, 6, 1-37.

김상훈 · 박선영 (2011). 정보보안 정책 준수 의도에 대한 영향요인. <한국전자거래학회지>, 16(4), 33-51.

박대우 (2015). Mobile Smishing 해킹 동향 분석 및 보안대책. <한국정보통신학회논문지>, 19(11), 2615-2622.

박종원 · 우현종 · 김현규 (2017). 정보보안정책지향성과 준수의도의 관계. <기업경영리뷰>, 8(1), 285-315.

박준경 · 김범수 · 조성우 (2011). 기업정보보호 활동을 위한 조직 구성원들의 태도와 주요 영향 요인. <경영학연구>, 40(4), 955-985.

안홍기 (2007). 산업기밀 정보유출방지와 개인정보보호의 현황과 전망. <정보과학회지>, 25(8), 42-47.

이원영 (2006). 안전행동 및 사고에 대한 성실성, 인지실패 및 직무스트레스의 상호작용. <한국심리학회지: 산업 및 조직>, 19(3), 475-497.

이종한 · 이종구 · 석동헌 (2011). 조직 안전풍토의 하위요인 확인 및 안전행동과의 관계. <한국심리학회지: 산업 및 조직>, 24(3), 627-650.

전수현 · 아낫 호바브 · 이해원 (2015). 심리적 임파워먼트, 직급, 감사에 대한 인식이 정보보안정책 준수의도에 미치는 영향. <인터넷전자상거래연구>, 15(6), 39-55.

최정열 (2014). 비행안전에 영향을 미치는 조종사의 심리적 특성에 관한 연구. <한국심리학회지: 산업 및 조직>, 27(1), 1-20.

하상원 · 김형중 (2013). 정보보안의식이 패스워드 보안행동에 미치는 영향에 관한 연구. <한국디지털콘텐츠학회논문지>, 14(2), 179-189.

Aiken, L. S., & West, S. G. (1991). *Multiple regression: Testing and interpreting interactions*. Newbury Park, London: Sage.

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC)*, 16(3), 22-40.

Barrick, M. R., & Mount, M. K. (1991). The Big Five personality dimensions and job performance: A meta-analysis. *Personnel Psychology*, 44, 1-26.

Beus, J. M., Dhanani, L. Y., & McCord, M. A. (2015). A meta-analysis of personality and workplace safety: Addressing unanswered questions. *Journal of Applied Psychology*, 100(2), 481-498.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. *In Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104). ACM.

Burke, M. J., Sarpy, S. A., Tesluk, P. E., & Kristian, S-C. (2002). General safety performance: A test of a grounded theoretical model. *Personnel Psychology*, 55(2), 429-457.

Campbell, J. P., & Wiernik, B. M. (2015). The modeling and assessment of work performance. *Annual Review of Organizational Psychology and Organizational Behavior*, 2(1), 47-74.

Campbell, J. P., McCloy, R. A., Oppler, S. H., & Sager, C. E. (1993). A theory of performance. In N.

Schmitt, W. C. Borman, & Associates (Eds.), *Personnel selection in organizations* (pp. 35-70). SF: Jossey-Bass.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, 1(3), 18-41.

Christian, M. S., Bradley, J. C., Wallace, J. C., & Burke, M. J. (2009). Workplace safety: A meta-analysis of the roles of person and situation factors. *Journal of Applied Psychology*, 94, 1103-1127.

Clarke, S. (2006). The relationship between safety climate and safety performance: A meta-analytic review. *Journal of Occupational Health Psychology*, 11, 315-327.

Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the Big-Five personality domains. *Journal of Research in Personality*, 37(6), 504-528.

Greenwood, M., & Woods, H. M. (1919). *A report on the incidence of industrial accidents with special reference to multiple accidents* (Industrial Fatigue Research Board Report No. 4). London: Her Majesty's Stationery Office.

Griffin, M. A., & Neal, A. (2000). Perceptions of safety at work: A framework for linking safety climate to safety performance, knowledge, and motivation. *Journal of Occupational Health Psychology*, 5, 347-358.

Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. NY: Guilford.

Hofmann, D. A., Morgeson, F. P., & Gerras, S. J. (2003). Climate as a moderator of the relationship between leader-member exchange and content specific citizenship: safety climate as an exemplar. *Journal of Applied Psychology*, 88(1), 170-178.

Lee, S., & Dalal, R. S. (2014). Climate as situational strength: Safety climate strength as a cross-level moderator of the relationship between conscientiousness and safety behaviour. *European Journal of Work and Organizational Psychology*, 25(1), 120-132.

McCrae, R. R., & Costa, P. T., Jr. (1987). Validation of the five-factor model of personality across instruments and observers. *Journal of Personality and Social Psychology*, 52, 81-90.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879-903.

Probst, T. M. (2004). Safety and insecurity: exploring the moderating effect of organizational safety climate. *Journal of Occupational Health Psychology*, 9(1), 3-10.

Schneider, B. (1983). *Interactional psychology and organizational behavior*. In L. L. Cummings & B. M. Staw (Eds), *Research in organizational behavior* (Vol. 5, pp. 1 - 31). Greenwich, CT: JAI.

Schneider, B. (1990). The climate for service: An application of the climate construct. In B. Schneider

(Ed.), *Organizational climate and culture* (pp. 383-412). SF: Jossey-Bass.

Wallace, J. C., & Vodanovich, S. J. (2003). Workplace safety performance: Conscientiousness, cognitive failure, and their interaction. *Journal of Occupational Health Psychology*, 8, 316-327.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, 55(4), 345-362.

The Effects of Personal Consciousness and Organizational Information Security Climate on the Employee's Security Behavior: from the Perspective of Industrial Safety Behavior

Se-Ung Park, Yoon-Ki Min

Chungnam National University

This study approached organizational information security behavior from the perspective of general industrial safety behavior frame. In the literature concerning industrial safety behaviors, personal conscientiousness and the organizational safety climate are the most influential factors of personal safety behaviors. This study verified whether information security behaviors can be considered general safety behaviors. Specifically, we hypothesized that individuals who have higher levels of conscientiousness, and perceived higher levels of organizational information security climate behave the more information security actions. Furthermore, we anticipated that the relation between conscientiousness and individual information security behavior would become stronger when the individual perceived a higher level of organizational information security climate. To test these hypotheses, we conducted a survey of 206 employees in a company. Study results show that all hypotheses were supported, sothe information security behaviors could be seen from the perspective of industrial safety behavior frame. Finally, we discussed the implications and limitations of this study.

Keywords: Information Security Behavior, Organizational Information Security Climate, Consciousness, Safety Behavior