한국경호경비학회 – 제56호(2018): 145–163

투고일 2018. 7. 23 심사일 2018. 8. 20 게재확정일 2018. 8. 22

조직구성원들의 정보보안행동에 미치는 영향: 보호동기이론(PMT)과 계획된 행동이론(TPB) 통합을 중심으로

정 혜 인 · 김 성 준

조직구성원들의 정보보안행동에 미치는 영향: 보호동기이론(PMT)과 계획된 행동이론(TPB) 통합을 중심으로*

정 혜 인** · 김 성 준***

〈요 약〉

최근 조직 구성원의 보안행동은 기업 차원의 정보보안에 중요한 부분으로 인식되고 있다. 정보유출 및 정보보안에 대한 연구는 보안 위협에 대한 개인행동이나 보안 기술을 사용하는 조직 구성원을 대상으로 연구가 활발히 진행되고 있다.

본 연구의 목적은 조직구성원들이 정보보안 활동을 촉진할 수 있는 효과적이고 효율적인 발전방안을 제시하고자 한다. 이를 위해 계획된 행동이론과 보호동기이론의 통합을 중심으로 주요 변수들을 적용한 연구모형을 제시하였다. 본 연구모형을 실증적으로 검증하기 위해 기업에서 보안 경험이 있는 조직원들을 대상으로 설문조사를 실시하였다. 이를 통해 조직구성원들이 정보보안 행동에 대해 긍정적인 구전을 유도하는 것이 중요하다.

이를 통해 기업에서는 조직구성원들이 정보보안 사고에 대해서 내 외부에서 발생 가능한 보안위험을 예방 및 대응하고 관리하기 위해 다양한 보안 솔루션 도입해야하며, 정보시스템에 대한 취약점 점검과 보인 패치 등의 보안 사항을 만족시키기 위한 행동을 실시해야 할 것이다.

주제어 : 조직, 정보 보안 행위 조직

* 이 논문은 2017년도 남서울대학교 학술연구비 지원에 의해 연구되었음
Funding for this paper was provided by Namseoul University year
** 한국IT서비스산업협회 선임연구원 (제1저자)
*** 남서울대학교대학원 빅데이터산업보안학과 교수(교신저자)

목 차

Ⅰ. 서 론

1. 연구의 필요성 및 목적

최근 IT비즈니스 환경의 급격한 성장과 정보보안에 관한 이슈가 대두되고 있다. 특히, 오늘날의 보안 위협은 특정 대상을 목표로 오랜 기간을 통해 이루어지고 있다. 또한, 많은 보안 분야 연구들은 보안에 대한 인식을 높여야 할 필요성을 밝히고 있으나 높아진 인식만큼 실제 보안행동을 수행한다고 볼 수 없는 실정이다(김종기, 2018) 많은 회원을 관리하는 기업의 데이터베이스(database)에 대한 악의적인 공격과 정보유출에 관한 사고에 대응하기 위해 기업에서는 정보보호 제품과 서비스를 이용하고 있으며 이를 위해 정보관리자들의 인식 교육과 더불어 관리 점검, 취약점 점검, 보안패치적용, 백업 상황이 적절하게 이루어 지고 있는지에 대한 검토가 불분명한 상태이다(이광규, 2018) 지식정보화 사회가 도래하면서 많은 국내기업이 보안기술 및 보안지식을 확보를 위해 기술개발에 많은 투자를 하고 있다. 하지만 적극적인 기술개발 투자에 비해 기업이 보유한 기술을 보호하기 위한 보안투자가 미흡한 결과 다수의 기업 및 연구소에서 기술유출 사건이 급격하게 증가하고 있다. 이러한 기술유출의 증가는 단순히 기업에 피해뿐만 아니라 국가 경제에도 직·간접적인악영향을 미치고 있는 실정이며 주로 전·현직 직원에 의해 이뤄지고 있지만, 이를 중점적으로 비교

분석한연구는 많지 않다(양현정, 2017) 이는 기업 이미지 훼손 및 금전적 손실 등의 심각한 결과를 초래할 가능성이 있다. 이는 각종 보안위험에 대한 예방 및 대응을 위하여 정보는 금융, 통신, 의료 등 각 분야에 다양한 정보보안 규제 강화를 하고 있다(조성배, 2014).

2. 연구의 차별화 및 목적

본 연구의 차별점은 이상의 논의를 바탕으로 크게 3가지로 구분한다. 첫째, 조직구성원 측면에서 정보보안행동에 영향을 미치는 주요 요인들을 고찰하고자 한다. 또한 조직구성원들이 보안 위험에 대한 예방 및 대응을 위해서 관련 보안규정 및 지침을 수립하고 정보보안 솔루션 도입을 지원해야 하는 것은 물론 조직구성원들의 정보보안 인식을 향상시키기 위한 전략적 대안을 제언하고자 한다. 둘째, 조직구성원들이 보안에 관련한 업무를 수행함에 있어서 명확하게 보안위험을 인지하고 있는지 알아보고자 한다. 셋째, 조직구성원들이 정보보안행동에 관련한 연구에서 계획된 행동이론과 보호동기이론의 통합을 이용하여 조직구성원의 보안성을 측정하는 연구가 거의 없는 실정이기 때문에 통합된 모델의 측정은 매우 중요하다.

이를 통해 본 연구의 목적은 계획된 행동이론과 보호동기이론의 통합을 중심으로 이론의 주요 변수들의 지각된 취약성, 지각된 심각성, 지각된 효율성, 지각된 장애, 태도에 대한 행동, 주관적 규범, 지각된 행동 통제, 의도를 통하여 정보보안 행동에 어떠한 영향을 미치는 요인들에 대해 실증연구 하고자 한다. 이를 통해 조직구성원들이 정보보안활동을 촉진할 수 있는 효과적이고 효율적인 발전방안을 제시하고자 한다.

3. 연구의 범위 및 방법

본 연구방법은 수집된 자료를 분석하기 위해 PLS를 이용하였다. 첫째, PLS를 이용하여 모형 적합도보다는 구성개념의 설명력을 측정하였다. 둘째, PLS 구조방정식은 이론의 검증보다는 인과관계의 예측, 인지 및 행동특성 분석 등에 사용되는 것이 더 유용하다. 셋째, PLS 구조방정식은 다중회귀에서의 모든 가정을 공유하며, 요인들의 수가 많거나 매우 높은 다중 공선성을 가질 때 예측모델을 만드는 방법이다.

넷째, 분포에 대한 가정이 거의 만족되지 않는 경우뿐만 아니라 AMOS의 적용 시 발생하는 부적절한 결과와 요인의 불확정성을 피하기 위한 대안적 방법으로 활용 가능하다.

조직 정보보안행동에서 중요한 2가지 이론인 보호동기이론과 계획된 행동이론의 중요한 변수들을 통해 구전의도의 모든 요인을 포함한 측정모델을 개발하였다. 측정모델의 개발은 PLS Graph version 3.0을 이용한 확인적 요인분석을 실시하였다. 이 측정 모델의 개발을 통해 요인들의 집중타당도(convergent validity)와 판별타당도(discriminant validity)를 검증하였다. 마지막으로 연구 모형의 가설을 검증하기 위해 PLS Graph version 3.0을 사용하였다. PLS는 기존의 LISREL, AMOS 등의 구조방정식 모델이 공통요인(common factor)을 기반으로 하는 것과는 달리 총 분산인 주성분(principal component)을 기반으로 한 구조방정식 모델이다.

이를 위한 본 연구범위로 조직 정보보안에서 현재 기업을 다니고 있으면서 정보보안행동을 하고 있을 가능성이 큰 기업 조직구성원들을 대상으로 설문조사를 실시하였다. 직접 방문하거나 또는 온라인 설문조사를 이용해 설문을 배포, 회수하였다. 설문조사는 2015년 10월 12일부터 26일까지 15일간 실시되었다. 이 기간에 총 209의 설문이 회수되었으며, 자료 분석에 사용되었다. 설문지가 자료 분석에 사용되었다. 설문응답의 단순화를 위해 모든 측정항목에 단일 균형 리커트 6점 척도를 사용하였고 설문은 익명으로 실시되었다.

본 연구는 총 5장으로 구성되어 있으며, 각 장의 내용 및 구성은 다음과 같다. 제1장 서론에서는 연구배경 및 목적, 그리고 연구범위 및 방법에 대하여 기술하였다. 제2장은 이론적 배경 부분으로서 국내 외 조직구성원들이 정보보안 행동 현황과 계획된 행동이론, 보호동기 모델을 정리하고 기존 정보보안행동 관련 개념과 특성 그리고 선행 연구에 대해 기술하고 우리의 연구인 보호동기이론모델과 계획된 행동이론의 통합의 모델을 도출하였다. 제3장에서는 연구모형, 변수의 조자적 정의와 측정도구, 연구 설계에 관한 내용을 기술하였다. 제4장에서는 사전 설계된 분석방법에 따라 표본의 특성을 분석하고 측정항목의 타당성 및 신뢰도 분석과 함께 구조모형의 연구가설 검정 결과를 기술하였다. 제5장에서는 연구의 요약 및 시사점, 연구의 한계점 및 향후 연구방향을 제시하였다.

Ⅱ. 이론적 배경

1. 조직 정보보안

Halibozek and Kovacich(2005)은 조직 정보보안 행동이란 “최소 공개의 원칙, 보안 인증의 지침 등의 절차 등을 준수하여 조직구성원으로부터 보안 문제가 야기되는 것을 방지하기 위한 활동”을 말한다. 또한 Siponen & Vance(2000)의 연구에서는 정보보안 행동은 조직에서 정보시스템 사용자와 관련된 실수를 최소화 하고 사용자 관점의 보안 기술 및 절차의 효율성을 최대화 하는 것이다.

Chen et al(2008)의 연구에서는 기술적 보안 솔루션뿐만 아니라 인간이 정보자산 보호의 중요 요소라고 주장하며 보안행동의 주체를 인간이라고 말했다. 실제로 보안 위협은 사용자의 지식과 행동의 부주의와 결핍에 그 직접적인 원인이기도 하며, 조직 내의 보안사고가 발생할 경우 손실을 최소화하기 위해 불확실한 문제를 규명 및 측정하고 관리하기 위한 행동이다(Caelli et al, 1989).

2. 보호동기이론

보호동기이론은 기대가치이론(Expectancy-Value Theory)과 인지적 정보처리 이론(Cognitive Processing Theory)을 기반으로 공포소구(Fear Appeal)에 의한 태도 및 행동의 변화과정을 설명한다(Ifinedo, 2012). 최초의 보호동기이론은 건강에 한 태도 및 행동 에서 공포소구의 효과를 설명하기 위해 개발되었다(Rogers, 1975).

보호동기이론에 따르면, 위험으로부터 스스로를 보호하고자 하는 보호동기는 심리적 요인에 의하여 형성되어 행동을 변화시킨다. 또한 심리학, 보건학, 교육학 등의 다양한 분야에서 개인의 보호행동을 설명하기 위해 주로 연구되어 왔다

3. 계획된 행동이론

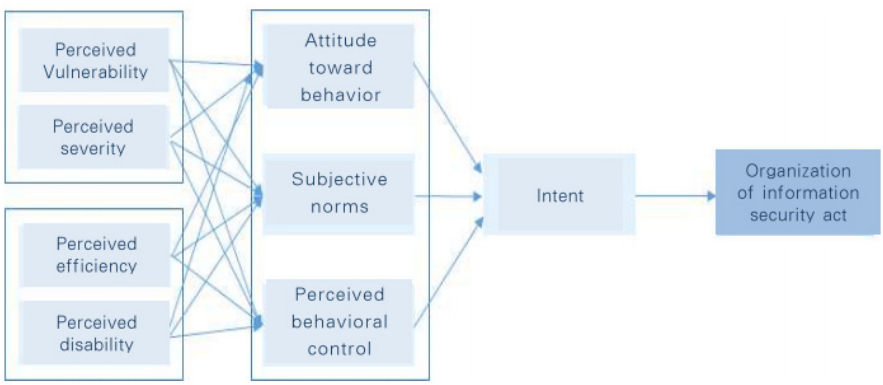
계획된 행동이론(Theory of Planned Behavior) 은 합리적 행위 이론(Theory of Reasoned Action)에서 발전된 이론이다(Ajzen, 1991). 합리적 행위 이론은 태도(attitude)와 주관적 규범(subjective norms)의 두 변인이 행동의도(behavior intention)에 유의미한

영향을 미치고, 이러한 행동의도는 최종적으로 인간의 행동(behavior)과 관계가 있는 이론이다(이현지, 2015)

Ⅲ. 연구방법

1. 연구모형의 설정

본 연구는 조직구성원들이 정보보안 행동에 영향을 미치는 영향요인들에 대해 파악하고 이들 요인들이 정보보안행동에 어떠한 영향을 미치는지 분석하고자 한다. 본 연구모형은 보호동기 이론과 계획된 행동이론을 기반으로 조직구성원들이 정보보안 행동에 영향을 미칠 것으로 예상되고 정보보안 분야에서 보안행동에 영향을 미치는 요인을 살펴보기 위해 공통적으로 사용하는 보호동기이론의 주요 변수를 추가하였다. 구체적으로 조직구성원들이 정보보안 행동 영향요인인 지각된 취약성, 지각된 심각성, 지각된 효율성, 지각된 장애가 계획된 행동이론의 주요 변수인 지각된 태도에 대한 행동, 주관적 규범, 지각된 행동통제와 종속변수인 조직 정보보안 행동에 어떠한 영향을 미치는지 알아보고자 하였다.



〈그림 1〉 연구 모델

2. 연구변수의 개념적 정의

본 연구의 선행연구들을 기반으로 도출된 조직구성원들이 정보보안행동의 영향요인에 관한 개념적 정의를 내리고 선행연구자들의 측정항목을 수정하여 연구문항을 구성하였다. 연구 변수에 대한 개념적 정의 및 측정항목을 정리한 것이다. 독립변수인 보호동기이론으로 지각된 취약성, 지각된 심각성, 지각된 효율성, 지각된 장애로 정의하였다. 매개변수는 계획된 행동이론의 주요 변수인 태도에 대한 행동, 주관적 규범, 지각된 행동통제, 의도이며 종속변수는 조직 정보보안 행동이다.

〈표 1〉 변수와 측정의 개념적 정의

variable	Conceptualdefinition	Previous research
지각된 취약성 (PV)	정보보안 행동에 의해 제기된 위험 수준에 대한 개인이 평가에 대해 정의한다.	Rogers, 1983; Woon, et al., 2005; Ifinedo, 2012; Rogers, 1975
지각된 심각성 (PS)	정보보안행동에 관련 위협적인 사건에 대한 심각성 정도를 정의한다.	Rogers, 1983; Woon, et al., 2005; Ifinedo, 2012; Rogers, 1975
지각된 효율성 (PE)	위협으로부터 발생하는 잠재적인 손실을 방지하고 대처하는 능력에 대한 정보보안 행동에 대한 개인의 평가정도를 정의한다.	Rogers, 1983; Woon, et al.,2005; Ifinedo, 2012; Rogers, 1975; Rogers, 1983;Woon, et al., 2005; Ifinedo, 2012
지각된 장애 (PF)	정보보안행동에 대해서 대체로 이용자들이 어렵다는 인식을 느끼는 정도라고 정의한다.	Rogers, 1983; Woon, et al.,2005; Ifinedo, 2012; Rogers, 1975; Rogers, 1983;Woon, et al., 2005; Ifinedo, 2012
태도에 대한 행동 (BA)	정보보안 행동을 하는 것에 대한 결과가 긍정적 또는 부정적 결과를 가져올 것이라는 개인적 '평가'와 그 행동으로 나타날 결과가 얼마나 '가능성'이 있는지에 따라 결정됨	율금정, (2012), Ryu et al.(2010), Ajzen et al.(1980)
주관적 규범 (SN)	개인 주변의 주요 지인들이 그 개인에 대해 특정 행동을 수행하기 원하는 정도에 관한 자신의 믿음을 뜻함(자신의 결정을 넘어선 다른사람들이 가지고 있는 평가)	율금정, (2012), Ryu et al.(2010), Ajzen et al.(1980)
지각된 행동 통제 (PBC)	정보보안 행동을 하는 이용자의 자발적인 통제의 범위를 벗어나 매우 어렵거나 쉽게 느끼는 행동에 대한 이용자의 지각된 믿음	고대영(2012), 이현명 (2012), Ajzen et al.(1986), Sheppard et al. (1988)
의도 (BI)	정보보안 행동을 지속적으로 할 것이라는 자기 예측 또는 기대정도라고 정의한다.	율금정, (2012), Ryu et al.(2010), Ajzen et al.(1980)

variable	Conceptualdefinition	Previous research
정보보안 행동 (IS)	정보보안 문제점으로부터 발생가능한 보안위험을 예방 대응 및 관리하고 보안 정책, 전략, 인적자원 등을 이용하고 수행하는 정도라는 것을 정의한다.	지범석 외(2011), 이병관 외(2008), Rosen stock(1974), Rosen stock et al.(1994)

3. 표본선정 및 자료수집 방법

본 연구는 제시된 가설을 검증하기 위해 정보보안행동 경험이 있는 조직원들을 대상으로 설문을 실시하였다. 연구 표본으로 조직원들을 선정한 이유는 현재 기업을 다니고 있으면서 정보보안행동을 하고 있을 가능성이 크기 때문에 연구 목적에 맞는 표본을 수집할 수 있기 때문이다.

설문조사는 정보보안행동 경험이 있는 조직구성원 들을 대상으로 실시하였으며, 직접 방문하거나 또는 이메일을 이용해 설문을 배포, 회수하였다. 2015년 10월 12일부터 10월 26일까지 15일간 실시되었다. 이 기간에 총 209부의 설문을 회수되었으며 자료 분석에 모든 설문지가 사용되었다. 설문응답의 단순화를 위해 모든 측정항목에 단일 균형 리커트 6점 척도를 사용하였고 설문은 익명으로 실시되었다.

연구는 앞 절의 구성개념의 조작적 정의에 제시된 것처럼 대부분 선행연구를 통해 그 타당성이 충분히 입증된 항목만을 이용하였다. 또한 설문지 문항에 대한 정보보안 행동 경험이 있는 조직구성원들과 관련 연구자들의 내용 검토, 설문지에 대한 사전조사 등을 실시하여 구성개념의 내용 타당성(Face Validity) 및 가독성(Readability)을 확보하였다.

Ⅳ. 가설검증 및 분석결과

1. 표본의 기술적 특성

<표 2>는 자료 분석에 사용된 총 209개의 표본의 성별 분포, 연령 분포, 학력, 직책, 정보보안행동 횟수, 직급 대한 응답자의 특성을 보여준다. 표본의 성펼 분포는 남자가 112명(53.6%), 여자가 97명(46.4%)이며, 연령 분포는 20대가 69명(42.6%)으로 가장 많았고, 30대가 48명(23%)으로 전체 표본의 65.6%가 2,30대 인 것으로 조사되었

다. 학력은 대학교 졸업이 146명(69.9%)으로 가장 많았고, 전문대 졸업한 응답자도 23명(11%)인 것으로 나타났다. 근무회사로는 사기업 91명(43.5%)인 것으로 가장 많았고, 사무직 58명(27.8%)인 것으로 나타났다. 정보보안 행동 횟수로는 대체로 1-3회 108명(51.7%)인 것으로 나타나 전체 표본의 81.4%가 하루에 적어도 1회 이상 정보보안 행동을 하는 것으로 조사되었다. 마지막으로 자신의 직급은 사원 98명(46.9%)으로 가장 많았고 임원이 31명(14.8%)으로 조사되었다.

〈표 2〉 표본의 인구 통계

division	Item	frequency (N=209)	ratio(%)
gender	male	112	53.6
	female	97	46.4
age	Teenage	1	.5
	twenty	89	42.6
	thirty	48	23.0
	forty	42	20.1
	fifty	28	13.4
	sixty	1	.5
academic back ground	High school	21	10.0
	junior college	23	11.0
	university	146	69.9
	Completed University	6	2.9
	University graduate	13	6.2
Working Company	Security Company	37	17.7
	office job	58	27.8
	public institution	12	5.7
	Private companies	91	43.5
	etc	10	4.8
The number of information security behavior	None	33	15.8
	1-3 times	108	51.7
	3-5 times	34	16.3
	5 or more times	28	13.4
	etc	6	2.9
rank	executive	31	14.8
	conductor	23	11.0
	director	7	3.3
	exaggeration	25	12.0
	deputy	25	12.0
	employee	98	46.9

2. 측정모형(Measurement Model) 검증

가설 검증에 앞서 본 연구에서 사용된 변수들의 측정도구에 대한 신뢰성과 타당성을 검증하였다. 이를 위해 확증적 요인 분석 도구인 PLS Graph version 3.0을 사용하였다. PLS는 연구원 또는 사용자가 부분 최소 제곱 (PLS) 분석을 수행하는 데 도움이 되는 Windows 기반 그래픽 사용자 인터페이스로 구성된 응용 프로그램입니다. PLS는 기존의 LISREL, AMOS 등의 구조방정식 모델이 공통요인(common factor)을 기반으로 하는 것과는 달리 총 분산인 주성분(principal component)을 기반으로 한 구조방정식 모델이다. 이에 대한 특성은 다음과 같다.

첫째, PLS 구조방정식은 이론의 검증보다는 인과관계의 예측, 인지 및 행동특성 분석 등에 사용되는 것이 더 유용하다.

둘째, PLS 구조방정식은 다중회귀에서의 모든 가정을 공유하며, 요인들의 수가 많거나 매우 높은 다중 공선성을 가질 때 예측모델을 만드는 방법이다. 셋째, 분포에 대한 가정이 거의 만족되지 않는 경우뿐만아니라 AMOS의 적용 시 발생하는 부적절한 결과와 요인의 불확정성을 피하기 위한 대안적 방법으로 활용 가능하다. 이에 본 연구에서는 이론적 견고성, 표본의 수, 설문의 자체 개발이라는 연구의 특성들을 고려하여 데이터 분석방법으로 PLS를 채택하였다(김태호 외, 2013; 78-83).

가설 검증 이전에 측정모형의 검증을 통해 각 변수의 신뢰성과 타당성을 먼저 체크하였다. 이를 위해 개별항목 신뢰성(Individual Item Reliability), 내적 일관성(Internal Consistency), 수렴 타당성(Convergent Validity), 그리고 판별 타당성(Discriminant Validity)을 분석하였다. 본 연구에서 사용한 측정항목은 동일 변수내의 다른 측정항목과의 상관관계가 높기 때문에 반영항목(Reflective Indicators)으로 설정하여 분석하였다(Wixom & Watson, 2001: 17-41).

이에 본 연구에서는 이론적 견고성, 표본의 수, 설문의 자체 개발이라는 연구의 특성들을 고려하여 데이터 분석방법으로 PLS를 채택하였다. 모형 적합도 보다는 구성개념의 설명력을 측정하고자 한 최근의 정보기술 관련 연구에서도 PLS를 분석도구로 채택하고 있다.

가설 검증 이전에 측정모형의 검증을 통해 각 변수의 신뢰성과 타당성을 먼저 체크하였다. 이를 위해 개별항목 신뢰성(Individual Item Reliability), 내적 일관성

(Internal Consistency), 수렴 타당성(Convergent Validity), 그리고 판별 타당성(Discriminant Validity)을 분석하였다. 본 연구에서 사용한 측정항목은 동일 변수내의 다른 측정항목과의 상관관계가 높기 때문에 반영항목(Reflective Indicators)으로 설정하여 분석하였다(Wixom & Watson, 2001).

Ⅴ. 결론 및 시사점

본 연구는 조직구성원들이 정보보안 행동에 미치는 영향요인들에 대해 파악하고 이들 요인이 조직 정보보안 행동에 어떠한 영향을 미치는지 분석하고자 하였다. 보호동기이론과 계획된 행동이론을 기반으로 조직구성원들이 정보보안 행동에 영향을 미칠 것으로 예상되는 사람들의 태도 변화과정과 위험 관리 행동을 강조한 보호동기이론과 합리적 행동이론의 불완전한 의지 통제에 대한 한계를 해결을 강조한 계획된 행동이론의 주요 변수들을 적용한 연구모형을 제시하였다. 위 연구모형을 실증적으로 검증하기 위해 기업에 다니고 있는 조직구성원들이 정보보안 행동을 해본 경험이 있는 조직구성원들을 대상으로 설문조사를 실시하였다.

본 연구의 주요 연구결과와 시사점, 조직구성원들의 정보보안 활동을 촉진할 수 있는 효과적이고 효율적인 발전방안에 대한 전략적 대안은 다음과 같다.

첫째, 조직구성원들의 정보보안 행동의 지각된 취약성은 지각된 행동 통제에 영향을 미치는 것으로 나타났다. 정보보안 사고가 일어날 가능성에 대해 정보보안 행동을 자발적으로 하거나 쉽게 할 수 있는 조직구성원들의 믿음이 있다는 것이다.

그러나 조직구성원들의 정보보안 행동의 지각된 취약성은 주관적 규범과 태도에 대한 행동이 영향을 미치지 않는다. 정보보안 사고가 일어날 가능성에 대해 정보보안 행동을 하는 것에 대한 결과가 긍정적 또는 부정적 결과를 가져올 것을 인지해야 하며 기업에서는 보안 지침에 즉시 반영하고 있으며 정보보안을 담당하는 조직을 구성하여 기업 정보보안에 대한 지속적인 관리를 해야할 것이다.

둘째, 조직구성원들의 정보보안 행동의 지각된 심각성은 태도에 대한 행동에 영향을 미치는 것으로 나타났다. 최근 발생하는 정보보안 사고가 정보 유출 또는 악성코드에 의한 보안사고 등으로 점차 증가되면서 이에 조직구성원들은 정보보안 사고에 대해서 심각성을 느끼고 이를 해결하기 위해 정보보안 행동을 수행하는 것을 알 수

있었다.

그러나 조직구성원들의 정보보안 행동의 지각된 심각성은 주관적 규범과 지각된 행동통제에 영향을 미치지 않는다. 최근 발생하는 정보보안 사고가 정보유출 또는 악성코드에 의한 보안사고 등으로 점차 증가되면서 이에 조직구성원들은 정보보안 사고에 대해서 내, 외부에서 발생 가능한 보안위험을 예방 및 대응하고 관리하기 위해 다양한 보안솔루션 도입해야 하며, 정보시스템에 대한 취약점 점검과 보안 패치 등의 보안 사항을 만족시키기 위한 행동을 실시해야 할 것이다.

셋째, 조직구성원들의 정보보안 행동의 지각된 효율성은 태도에 대한 행동, 지각된 행동 통제, 주관적 규범에 영향을 미치는 것으로 나타났다. 자신의 정보보안 행동이 정보보안 사고 예방 및 대응에 도움이 된다고 생각하기 때문에 지속적으로 정보보안 관리에 대해서 주의를 기울이며 다양한 보안 취약점에 대해서도 경각심을 가지고 있다.

넷째, 조직구성원들의 정보보안 행동의 지각된 장애 태도에 대한 행동에 영향을 미치는 것으로 나타났다. 보안에 대한 인지능력 또는 경감심의 부족, 정보보안에 대한 불편함이 높아질수록 기업에서 보안행동을 수행한다면 조직구성원들은 기업을 위해 가치 있는 행동을 했다고 인지하는 것이다.

그러나 조직구성원들의 정보보안 행동의 지각된 장애는 주관적 규범과 지각된 행동통제에 영향을 미치지 않는다. 보안에 대한 인지능력 또는 경각심의 부족, 정보보안에 대한 불편함이 높아질수록 조직구성원들이 서로 정보보안 행동에 대해 관심을 주어야 하며, 또한 회사내의 정보보안 행동규칙을 만들어 그에 따른 실천을 통해 보안위험을 예방 및 대응해야 한다.

다섯째, 주관적 규범, 지각된 행동통제, 태도에 대한 행동은 의도에 영향을 미치는 것으로 나타났다. 합리적 행동이론과 같이 계획된 행동이론의 주어진 행위를 수행하는 것에 대한 의도이다. 의도는 행위에 영향을 미치는 동기적 요인으로 가정한다. 이는 사람들이 얼마나 특정 행위를 하는 것을 기꺼이 시도할 것인가, 얼마나 행위를 위해 노력할 것인가 등을 의미한다(Ajen, 1991). 따라서 조직구성원들은 정보보안 행동을 인식하고 보안행동에 주어진 행위를 수행하고 있어야 하며 얼마나 사람들이 보안 행동에 대해서 기꺼이 시도할 것인가, 얼마나 행위를 위해 노력할 것인가에 대한 여부를 인식하고 있어야 할 것이다.

마지막으로 의도는 정보보안 행동에 영향을 미치는 것으로 나타났다. 본 연구에서

의도한대로 조직구성원들이 정보보안 행동을 함으로써 행동의 의도가 중요한 요인 중 하나임을 재차 입증해 보이는 연구결과이다. 따라서 조직구성원들이 정보보안 행동을 함으로 조직구성원들은 의도가 있으면 정보보안 행동을 할 것이라는 직접적인 영향을 끼칠 것으로 볼 수 있다.

본 연구는 다음과 같은 학문적, 실무적 시사점을 제시한다. 학문적 시사점으로는 첫째, 학문적 시사점으로는 최근까지 진행된 조직구성원들의 정보보안 행동 연구들은 정보유출 및 정보보안 대한 연구는 보안 위협에 대한 개인행동이나 보안 기술을 사용하는 조직구성원들 대상으로 한 연구가 주를 이루어 왔다. 이에 따라 조직구성원들의 정보보안 행동에 대한 연구를 수행했다는 점에서 학문적 기여도가 크다고 할 수 있다.

둘째, 조직구성원들이 정보보안행동을 하는 이유를 개인의 심리적인 특성, 태도 및 행동 그리고 조직내의 영향 등을 복합적으로 살펴보아야 하기에 본 연구는 이들을 반영한 이론적 모델을 제시하였다. 이러한 모델을 조직구성원들의 정보보안 행동에 대한 좀 더 풍부한 예측 설명을 제시할 수 있는 이론적 기반이 될 것이다. 셋째, 조직구성원들이 정보보안 행동을 함으로써 정보보안 활동을 촉진할 수 있고 효과적이고 효율적인 발전방안이 크다는 연구결과를 제시 이론적 기반이 될 것이다. 실무적시사점으로는 첫째, 조직구성원들이 정보보안 행동에 대해서 보호동기이론, 계획된 행동이론으로 조직 정보보안 행동에 미치는 영향에 대한 연구결과를 제시하였다는 점이다.

둘째, 정보보안행동을 했던 조직구성원들의 특성으로 다양한 보안 활동으로인해 정보보안행동의 참여율을 크게 높일 수 있으며 자신의 개인정보를 보호하며 보안에 대해 개선할 수 있을 것이다.

본 연구의 한계점은 첫째, 연구 표본의 일반화와 측정 도구에 관련된 것이다. 즉 연구의 표본이 일반화가 가능할 정도의 대표성을 지니고 있느냐의 문제이다. 본 연구는 조직에서 일하고 있는 구성원들을 대상으로 정보보안 행동 경험이 있는 20대 조직원으로 표본을 한정하였다. 또한 측정도구에 있어서도 설문지법일 이용하였는데, 이 방법은 설문지의 내용과 응답자의 반응 태도에 따라 조사결과가 좌우된다는 것을 완전히 통제할 수 없다는 한계점이 있다. 따라서 개별 면답이나 관찰법 등의 탐색적 조사를 병행 실시하여 각각의 결과를 비교함으로써 연구결과의 타당성을 항상 시켜야 할 필요성이 있다.

둘째, 본 연구는 보호동기이론과 계획된 행동이론의 통합을 중심으로 연구모형을 제시하였으며 통합된 모델에 대한 선행연구가 부족하여 주로 두 이론이 영향을 미쳤다는 결과의 논문보다 두 이론으로 연구를 진행했던 연구 등을 토대로 가설을 설정하였다. 향후 연구에서는 보호동기이론과 계획된 행동이론의 통합된 연구가 계속해서 진행되어야 할 것으로 생각된다.

따라서 향후 연구에서는 보다 다양한 인구통계학적 대상을 선정 한 후 다양한 계층에 걸친 표본을 확보하고 사용자 특성별로 조직구성원들이 정보보안 행동에 영향을 미치는 요인에 관한 연구와 더불어 정보보안에서 확장된 다양한 보안 행동에 대한 추가적인 요인 발굴에 대한 지속적 연구를 통해 이론적 토대를 강화시켜 나갈 것이다.

참고문헌

Bae, J. K., & Kwon, D. S. (2011). *Self-crystalline factors impact on the degree of acceptance microblogging service research.* Vol. 24, No. 5 (XIV No. 88).

Gang, Y. B., Hwang, H. U., Kim, K. B., Son, G. U., & No, B. N. (2014). Physical memory analysis technology for detecting malware. *Privacy Journal, 24*(1), 39-44.

Gim, G. Y., & Nag, W. S. (2000). According to the indicators quantify information security vulnerability assessment: Information weighted assets law. *The Korea Institute of Information Security Engineering, 10*(1), 51-62.

Kim, H. D., Kim, K. H., & Ha, J. C. (2013). GOOSE protocol development environment Snort-based intrusion detection system in the. *Privacy Journal, 23*(6), 1181-1190.

Kim, H. S., & Jeong, H. C. (2000). Relationship with the organization's information security organization, information security awareness and the level of research. *Journal of Information Technology and Database, 7*(2), 117-134.

Kim, I. H., Lee, G. H., & Park, J. H. (2010). Corporate information security issues and direction. *Information Security Association, 20*(1), 13-18.

Kim, J. G. (2013). *Also impact on privacy in the online environment act. the information policy.* Article 20, No. 3.

Kim, Y. H., Moon, J. W., Hwang, S. H., & Jang, H. B. (2014). Study on the ICT outsourcing security management environment. *Information Security Engineering, 24*(1), 23-31.

Park, C. W. (2014). A Study on the Privacy act on the Internet - Focusing on the protection motivation theory. *Journal of Internet Computing and Services, 15*(2), 59-71.

Park, H. I. (2009). Research Information Security Survey Results Analysis for increased security. *Journal of Integrated Conference*, 1-7.

Park, J. H. (2009). Research on Private Security for the Psychological Stability of a Client. *Journal-German Korean Security Guidelines, 18*, 55-72.

【Abstract】

Influence on Information Security Behavior of Members of Organizations: Based on Integration of Theory of Planned Behavior (TPB) and Theory of Protection Motivation (TPM)

Jeong hye in · Kim seong jun

Recently, security behavior of members of organizations has been recognized as a critical part of information security at the corporate level. Leakage of customers' information brings more attention to information security behavior of organizations and the importance of a task force. Research on information breach and information security is actively conducted of personal behavior toward security threats or members of organizations who use security technology.

This study aims to identify factors of influence on information security behavior of members of organizations and to empirically find out how these factors affect information security behavior through behavior toward attitude, subjective norm and perceived behavior control. On the basis of the research, this study will present effective and efficient ways to foster information security activities of members of organizations. To this end, the study presented a research model that applied significant variables based on integration of Theory of Planned Behavior (TPB) and Theory of Protection Motivation (TPM). To empirically verify this research model, the study conducted a survey of members of organizations who had security-related work experience at companies. So, it is critical for members of organizations to encourage positive word of mouth (WOM) about information security behavior. Results show that based on the integration of TPM and TPB, perceived vulnerability, perceived severity, perceived efficiency and perceived barriers of information security behavior of members of organizations had significant influences on mediating variables such as behavior toward attitude, subjective norm, perceived behavior control and intention. They also had significant influences on organization information security behavior

which is a dependent variable.

This study indicates companies should introduce various security solutions so that members of the organizations can prevent and respond to potential internal and external security risks. In addition, they will have to take actions to inspect vulnerability of information system and to meet security requirements such as security patches.

Keywords: Organization, Organization of information security act