조직 구성원들의 정보보안 정책 준수행위 의도에 관한 연구

임명성*

A Path Way to Increase the Intention to Comply with Information Security Policy of Employees

Myung-Seong Yim*

요 약 본 연구는 조직원들의 정보보안 정책준수 의도에 영향을 미치는 요인을 규명하고자 시작되었다. 기본 문헌의 경우 특정한 이론을 기반으로 보안정책 준수를 설명하려 하였으나 본 연구의 경우 총체적인 관점에서 접근하였다. 분석결과 적발가능성과 개인의 조직에 대한 애착심이 보안정책 준수의도를 유발할 수 있는 것으로 나타났다. 여기서 적발가능성은 정보보안 인식 교육에 영향을 받는 것으로 나타났다. 그러나 인지된 준수비용의 경우 보안 정책 준수를 방해 할 수 있는 것으로 나타났다.

주제어 : 정보보안, 정보보안 정책, 예방 동기 이론, 일반 억제 이론, 사회적 결속 이론

Abstract This study is to identify the factors that influence an intention to information security policy compliance of employees. To do this, this study is based on three theoretical backgrounds because of the lack of holistic perspective. Research results show that detection certainty and individual attachment have a positive effect on information security policy compliance intention. Detection certainty is influenced by security awareness education and training. Finally, response cost has a negative effect on information security policy compliance intention.

Key Words : Information Security, Information Security Policy, Protection Motivation Theory, General Deterrence Theory, Social Bond Theory

1. 서론

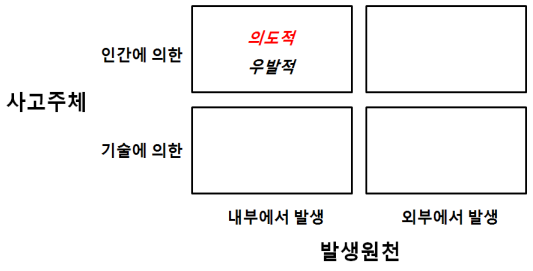
대한민국의 정보기술 기반이 전 세계적으로 가장 우수하다는 것은 자명하다. 정보 기술 인프라의 발달은 고객과의 친밀감 확보의 혁신적 향상과 같은 다양한 부분에서 괄목할 만한 성과를 야기했다. 이에 따라 정보기술에 대한 투자가 지속되어왔는데, 투자와는 반비례하게 정보기술의 확산으로 인해 야기될 수 있는 대표적인 부작용인 정보보안에 대해서는 지금까지 무관심해왔다.

이로 인해 다양한 보안 사고가 발생하고 있는데 보안 사고는 두 가지 기준에 의해 4개의 사분면으로 구분해 볼 수 있다[34]. 첫 번째는 보안 사고의 발생원천에 따라 내부와 외부로 구분해 볼 수 있다. 다음으로는 사고주체로 인간에 의한 것인지 기술에 의한 것인지로 구분해 볼 수 있다<그림 1>. 이 기준에 따라 구분할 경우 해킹과 같은 사고는 발생원천이 외부이며, 사고주체는 인간에 의한 것으로 구분된다.

본 기준에 따라 구분된 네 가지 보안사고 중 가장 큰 주목을 받는 부분은 내부인(발생원천 내부, 사고주체 인간)에 의한 사고이다[17]. 그 이유는 첫째, 내부인의 경우 조직의 신뢰를 얻은 개인이기 때문에 이들의 행위는 특정한 이유 없이 감시되지 않는다[15]. 그렇기 때문에 권한 내에서 내부 시스템에 접속이 자유롭다. 둘째, 내부 시스템의 약점을 알고 있는 내부인에 의해 피하가 발생할

본 논문은 성결대학교 연구지원비에 의해 작성된 논문임
*삼육대학교 경영학과 조교수
논문접수: 2012년 9월 16일, 1차 수정을 거쳐, 심사완료: 2012년 10월 29일

경우 외부의 악의적인 접속으로 인한 피해보다 클 수 있다. 특히 내부 직원이 우연히 아닌 의도적으로 피해를 입히는 경우 쉽게 예방할 수 없다. 예를 들어, 2007년 5월 기아자동차의 전직 직원 5명이, 현직 직원 2명으로부터 USB 메모리를 이용하여 사내 컴퓨터의 자동차 핵심기술을 반출한 후 이메일을 통하여 중국 자동차 회사에 유출하는 사고가 발생하였다. 같은 해 7월 대우조선 기술자료를 관리하는 총 책임자가 지식관리시스템 서버에 접속할 수 있는 권한을 이용해 선박 공정도, 설계완료보고서 등 1,100여 개의 파일을 외장하드에 저장하여 반출하려다 적발되는 사고가 발생하였다. 2008년 3월에는 LG 전자 직원이 처우에 불만을 품고 현직 직원과 공모해 중국업체에 PDP 공장 건축과 생산설비와 관련된 컴퓨터 파일 1,182개를 몰래 외장형 하드디스크에 담아 유출하였다. 이러한 사고는 제조업에만 국한된 것은 아니다. 2011년 9월 삼성카드 내부직원에 의해 81만 7330여건의 고객정보가 유출되는 사고가 발생하였으며, 같은 해 10월에는 하나SK카드 내부직원이 자신의 이메일을 통해 고객정보 5만 1723건을 외부로 유출하고 이 자료를 가지고 하나SK카드사를 직접 협박하기도 하였다. 2012년 9월에는 한국거래소에서 내부직원이 공시정보를 외부로 유출하는 사건이 발생하기도 하였다.



[그림 1] 보안 사고의 구분

이와 같이 내부인에 의해 발생하는 악의적인 보안사고는 내부통제체계도 속수무책인 경우가 많다. 따라서 이를 위한 해결책이 필요한데 기존 연구에서 주목받고 있는 것은 보안 정책 미준수[30]이다. 즉, 내부직원들이 사내에 수립되어 있는 보안 정책을 준수하도록 유도할 수 있다면 어느 정도 내부인에 의한 보안 사고를 미연에 예방할 수 있다는 것이다[30].

따라서 본 연구는 내부조직원들이 보안정책을 준수하도록 유도할 수 있는 방안에 대해 연구해보고자 한다. 특히 기존연구와는 다르게 통합적 관점에서 접근하고자 한다. D'Arcy et al.(2008), Herath and Rao(2009a)의 경우 일반 제재 이론(General Deterrence Theory), Johnston and Warkentin(2010), Lee and Larsen(2009)은 예방 동기 이론(Protection Motivation Theory) 등 특정이론을 중심으로 연구를 수행하였는데 여러 연구에서 제시하고 있는 바와 같이 정보보안은 특정한 이론보다는 종합적 관점에서 접근할 필요가 있다[1][15][20][21][33]. 따라서 본 연구는 기존 이론에 대한 검토와 함께 왜 종합적인 관점이 필요한지 살펴보고, 종합적인 관점에서 연구모형을 수립하고 실증적으로 분석하였다.

본 연구는 다음의 차이점이 있다. 기존 연구의 경우 보안의 4가지 요소 중 억제, 예방 등 특정한 하나의 관점에서 접근하였다. 그러나 정보보안은 억제와 예방을 동시에 고려한 접근이 필요하며, 본 연구는 이러한 필요성에 인식하고 억제, 예방을 모두 고려한 종합적 접근을 시도하였다.

2. 문헌연구

정보 시스템의 보안관련 위험을 줄이기 위한 조직전략은 4가지로 구분된다: 억제(deterrence), 예방(prevention), 발견(detection), 복구(recovery)[31]. 효과적인 보안은 시스템의 오용을 억제하고 예방을 극대화함으로 가능하다[8]. 따라서 많은 연구에서는 억제와 예방을 위한 이론에 주목해 왔다. 억제 행위를 위한 기저 이론으로 주목받은 것은 일반 제재 이론(General Deterrence Theory)이며, 예방을 위해 주목받은 이론은 예방동기이론(Protection Motivation Theory)이다. 문헌연구에서는 이 두 이론을 살펴보고자 한다.

2.1 일반 제재 이론

일반 제재 이론은 범죄학 분야에서 수립된 이론으로 범죄 행위 그리고 반사회적 행위에 관한 연구에서 널리 사용되어 왔다[1]. 일반 제재 이론의 주된 가설은 잠재적 이탈 행위는 처벌(Sanctions)에 대한 두려움으로 억제된다는 것이다[20].

본 이론은 정보시스템 환경에서 조직 내에서 수립된 정보보안을 위한 방안들이 어떻게 수행되어야 하는지를 설명하기 위해 사용되어왔다[21]. 즉, 정보보안을 위한 방

안들이 정보시스템을 오용하였을 경우 발생할 수 있는 처벌에 대한 확실성을 증가시켜, 사고 발생행위를 감소시킬 수 있다는 것이다[8].

하지만 본 이론은 내부인들이 처벌(Sanctions)대해 완전한 이해하고 있음을 가정하고 있다[10]. 즉, 자신의 행위가 어떠한 처벌을 유발하는지 개인들은 충분히 인지를 하고 있음을 가정하고 있다. 따라서 개인들이 처벌에 대해 완벽하게 인지하고 있지 못할 경우, 억제 행위가 유발되지 않을 가능성이 충분히 존재한다. 따라서 종합적 억제 모형이 제시되어야 한다[22].

2.2 예방 동기 이론

예방 행위를 유발하기 위해 주목받아온 이론은 예방동기이론이다. Rosers(1975)에 의해 제시된 예방동기이론은 공포전달(Fear Appeal)에 의한 영향에 대한 이론적 기반을 제공한다. 본 이론은 태도 변화를 유발하는 요인을 규명하기 위해 개발되었으며, 공포는 위협의 심각성, 사건(위협)의 발생 가능성, 사건에 대한 대응을 위한 효용 등 세 가지 인지적 평가 과정을 통해 전달된다[27]. 본 평가과정을 통한 결과물은 예방 동기유발이다.

예방동기이론이 태도 및 행위의 변화를 유발하는 것으로 규명되었다 할지라도, 다양한 형태의 공포 위협 메시지와 이에 대한 인간의 수용행위간의 관계는 여전히 명확하지 않다[2]. 뿐만 아니라, 본 이론을 기반으로 수행한 연구를 살펴보면 인간의 의도가 행위를 유발한다는 전제가 적용되지 않는 경우가 많았다. 따라서 의도와 행위간의 관계가 형성되기 위해서는 추가적인 매개체가 필요하다[9].

3. 연구모형 및 가설

기존 선행연구에서 사용된 이론의 문제점은 종합적 접근의 부족이다. 따라서 본 연구에서는 선행연구를 종합적인 관점에서 접근하고자 한다. 이를 위해 일반제재이론, 예방동기이론, 사회결속이론을 중심으로 가설 및 연구모형을 수립하였다.

3.1 정보보안 인식 교육

D'Arcy and Hovav(2007)에 따르면 장기적인 정보보안을 위한 효과적인 방법은 정보보안 인식교육이라고 제시하였다. 그들에 따르면, 직원들의 컴퓨터 감시나 보안 문제 예방을 위한 소프트웨어가 효과적이기는 하나 이는 단기적 효과에 그칠 뿐이고, 기업이 장기적인 보안 효과를 누리기 위해서는 지속적인 정보보안 교육을 수행해야 한다고 주장하였다[8]. 그러나 많은 기업들은 빠른 시간 안에 효과를 달성하기 위해서 기술적 해결책에 의존하는 경향이 있다. 하지만 정보보안에 대한 장기적인 효과는 개인의 인식 전환으로부터 시작되기 때문에 감시만이 능사는 아니다. 따라서 장기적인 정보보안 효과를 위해 정보보안 인식 교육에 투자하고 교육 프로그램을 지속적으로 유지할 경우 정보보안에 대한 많은 지식을 조직원들에게 전달할 수 있으며, 이탈행위에 대한 인지된 비용을 증가시킬 수 있기 때문에 정보보안 인식 교육이 추구하고자 하는 성과를 달성할 수 있다[20].

H1a. 정보보안 인식교육은 적발가능성에 정의 영향을 미칠 것이다.

H1b. 정보보안 인식교육은 기술적 규범에 정의 영향을 미칠 것이다.

H1c. 정보보안 인식교육은 인지된 준수비용에 음의 영향을 미칠 것이다.

3.2 적발가능성

일반 제재 이론에 따르면 처벌의 확실성, 그리고 처벌 강도는 원치 않는 행위를 줄여주는 역할을 한다. 일반 제재 이론의 기본 가정은 개인은 자신의 이익의 최대화와 비용을 최소화할 수 있는 범위에서 합리적인 의사결정을 한다는 것이다[20]. 즉, 범죄 행위를 하는 사람은 처벌에 대한 비용이 범죄 행위로 인한 기대 이익보다 크지 않다. 따라서 본 이론은 범죄로 인한 인지된 비용을 증가시키기 위해 설계된 보안 정책, 보안 시스템, 보안 인지 프로그램과 같은 메커니즘에 초점을 맞추고 있다[20]. 하지만 이러한 메커니즘이 범죄 의도나 행위를 줄이는데 실패하는 경우가 많다. 그 이유는 조직 내에 존재하는 정보보안 정책이 강제성이 없는 경우가 많기 때문이다. Peace et al.(2003)에 따르면 규율에 대한 강제성 없이 단지 규율의 문서화만으로는 조직원들의 행동변화를 유발하지 못한다고 주장하였다. 또한 이탈 행위에 대한 가벼운 처벌도 그 원인이다[20]. 뿐만 아니라, 특권층에 대한 차별적 대우도 원인이 된다[20]. 따라서 자신의 이탈 행위가 조직에 의해 적발이 가능하고, 직급에 상관없이 무거운 처벌

이 내려진다면 조직원들이 이탈 행위가 줄어들 수 있다.

H2a. 적발가능성은 기술적 규범에 정의 영향을 미칠 것이다.

H2b. 적발가능성은 보안정책 준수의도에 정의 영향을 미칠 것이다.

3.3 인지된 준수비용

예방동기이론에서 제시된 인지된 준수 비용(response costs)은 얼마나 많은 비용이 제안된 행위를 수행하는데 발생하는가를 나타내며, 예방 동기에 음의 영향을 미친다[15]. Herath and Rao(2009b)는 조직원이 보안정책을 준수하는데 있어서 불편함이 있기 때문에 정보보안 정책을 제대로 준수하지 않는다고 주장하였다. Chan et al.(2005)은 정보보안 정책의 준수가 업무 생산성과 일부 상충관계에 있기 때문에 보안 정책을 준수하도록 유도하는데 어려움이 있음을 제시하였다. 즉, 개인이 업무를 수행함에 있어서 여러 가지 인지된 준수 비용이 존재할 경우 조직원들이 보안정책을 준수하도록 유도하는데 장애가 될 수 있다.

H3a. 인지된 준수비용은 기술적 규범에 음의 영향을 미칠 것이다.

H3b. 인지된 준수비용은 보안정책 준수의도에 음의 영향을 미칠 것이다.

3.4 기술적 규범

기술적 규범(descriptive norms)이란 어떠한 개인이 타인이 요구된 행위(desired behavior)를 수행할 것이라고 믿는 정도를 말한다[15]. 기술적 규범은 개인이 타인의 행위를 복제, 즉 따라하는 경향에 초점을 맞추고 있다[15]. 사회 학습 이론(Social Learning Theory)에 따르면, 개인은 주변인의 이탈행위를 학습 후 범죄에 몰입하는 경향이 있다[20]. 정보보안 측면에서 주변인이 조직의 보안 정책을 준수하는 것을 관찰하거나 학습하게 되면, 해당 행위를 학습한 개인은 조직의 정보보안 정책을 준수할 가능성이 높아진다.

H4. 기술적 규범은 보안정책 준수의도에 정의 영향을 미칠 것이다.

3.5 조직에 대한 애착심

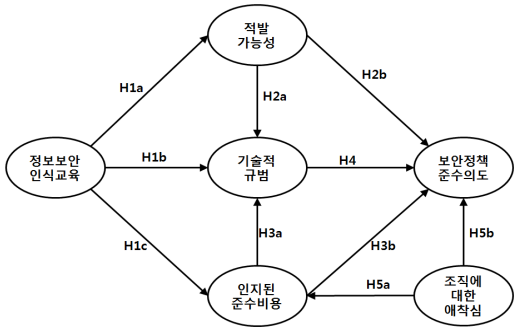
범죄학에서 자주 인용되는 이론 중 하나인 사회 결속 이론(Social Bond Theory)은 개인의 사회적 결속력이 약하거나 부재할 경우 범죄에 몰입하게 된다고 가정하고 있다[20]. 즉, 모든 인간은 사회적 결속이라는 강력한 통제 메커니즘이 존재하지 않을 경우 자연적으로 범죄행위에 몰입하게 된다고 주장한다[20]. 사회적 결속은 네 가지로 구분되는데, 애착심(attachment), 몰입(commitment), 참여(involvement), 믿음(belief) 등이 있다.

정보보안 분야에서 조직원들의 정보보안정책 준수를 위해 필요한 요인으로 주목받는 것이 조직에 대한 내부인들의 애착심이다[15]. 조직에 대한 애착심이란 개인의 정체성, 그리고 조직에 대한 소속감을 말하며, 조직원과 조직 간의 관계를 설명해준다[21][33]. 사회 결속 이론에 따르면, 조직에 대한 애착심과 같은 강력한 결속은 개인이 부정적 행위에 몰입하는 것을 예방하는 중요한 요인이 된다[15]. 따라서 다음의 가설을 제시할 수 있다.

H5a. 조직에 대한 애착심은 인지된 준수비용에 음의 영향을 미칠 것이다.

H5b. 조직에 대한 애착심은 보안정책준수의도에 정의 영향을 미칠 것이다.

지금까지 제시한 가설을 중심으로 연구모형을 제시하면 <그림 2>와 같다.



[그림 2] 연구모형

4. 분석

4.1 자료 수집

본 연구는 자료의 수집을 위해 국내 대표적 IT기업 5

개사(모두 SI(System Integration)기업 임)를 선정하여 핵심 관계자(상위 관리자)와의 사전 동의를 통해 연구목적에 대해 설명하고 설문을 배포하였다. 설문배포에 대한 전체적인 관리는 해당 관계자를 통해 이루어졌다. IT 기업을 설문 대상으로 선정한 이유는 정보보안 관련 프로젝트를 수행한 경험이 있기 때문에 다양한 정보보안 방안을 마련하고 있기 때문에 국내 기업들의 정보보안 관련 상황을 대표적으로 보여주는데 충분할 것으로 판단되기 때문이다. 2011년 5월부터 9월까지 5개월간 총 300부를 배포하였고 이중 189부(응답률: 63%)가 회수되었다. 이중 불성실한 응답이나 무응답이 포함된 46부를 제외하고 143부를 최종분석에 사용하였다.

〈표 1〉 응답자의 인구통계학적 분석

항목	구분	빈도	비율
성별	남성	100	70
	여성	41	29
	무응답	3	1
연령	18-24	2	1
	25-34	69	48
	35-44	59	41
	45-54	13	9
학력	고졸	1	1
	2년제 졸	11	8
	4년제 졸	96	67
	석사	26	18
	박사	4	3
	기타	1	1
	무응답	4	3
직위	기술직	43	30
	사무직	45	31
	중간관리자	37	26
	전문직	15	10
	기타	3	2
현 직장 근무기간		평균: 5.91년	
하루 컴퓨터 활용시간		평균: 8.88시간	
컴퓨터 활용능력		5.26(1-7)	
합계		143	100

배포된 설문은 Likert type 7점 척도법을 사용하였으며, 측정항목의 신뢰성을 위해 기존 문헌에서 신뢰성과 타당성이 존재한다고 규명된 지표들을 사용하였다.

측정도구로 인구통계학적 분석은 대표적 사회과학도구인 IBM SPSS Statistics v19를 사용하였다. 연구모형에 대한 검증은 컴포넌트 기반(component based approach) 추정방법을 활용하여 구조모형을 분석하는 기법인 PLS(Partial Least Squares) 기법을 활용하는 SmartPLS v2.0 M3을 사용하였다.

PLS는 1세대 다변량 기법과 마찬가지로 회귀분석과 공분산기반 구조모형분석과 유사한 접근법을 활용한다[16]. 또한 이론적 잠재 변수들의 관측변수에 대한 신뢰성과 타당성뿐만 아니라(측정모형, measurement model) 잠재변수간의 관계를 동시에 평가(simultaneous assessment)할 수 있다(구조모형, structural model)[16]. 반면에 공분산 기반 접근법(covariance based approaches)과 다르게 PLS는 측정지표의 수와 표본 수, 분포가정에 대해 엄격하지 않다[4].

응답자에 대한 특성을 정리하면 <표 1>과 같다.

4.2 탐색적 요인 분석

요인타당성(factorial validity)을 평가하기 위해 탐색적 요인분석(exploratory factor analysis)을 수행하였다. 탐색적 요인 분석은 주성분분석을 통해 검증하였는데, 주성분분석과 공통요인분석은 비교할 필요가 있다. 일반적으로 언급되는 탐색적 요인 분석은 공통요인 분석을 말하는데, 만약 측정변수의 공통성(communality)이 기준 이상일 경우 공통요인분석 대신 주성분분석을 통해 탐색적 요인 분석을 수행하는 것이 가능하다. 일반적 기준에 따르면 공통성이 0.5이상이 되면 해당 측정변수의 설명력이 50%라는 것을 나타내며 적정수준이라고 판단한다[13]. <표 2>에 나타나 있듯이 최소 공통성이 0.550이기 때문에 본 연구에서는 주성분분석을 수행하였다.

요인 추출은 적재값(factor loading)이 0.5이상이고 고유값(eigenvalue)이 1.0이상인 값이 선택된다. 또한 0.4이상의 교차요인(cross-loading)이 존재하지 않아야 한다. 본 연구에서는 본 기준에 따라 주성분 분석을 수행하였고 6개의 요인이 추출되었다. 결과는 <표 2>와 같다.

다음으로 Harman의 1요인 검증기법을 통해 공통방법오류(common method bias)를 검증하였다[26]. 본 기법은 주성분분석과정에서 요인회전 전(unrotated factor analysis)에 나타난 결과에서 요인 하나의 설명력이 총 분산 설명력의 어느 정도를 차지하는지를 통해 평가하는데, 절대적 권고 기준은 존재하지 않는다는 단점이 존재한다. 본 연구의 총 분산 설명력이 77.992이고, 가장 많은 설명력을 차지하는 요인이 29.917의 설명력을 나타내고 있는 것으로 나타났다. 이는 절대적인 기준이 없기 때문에 단언할 수는 없으나 하나의 요인이 전체 분산 설명력의 절반이하를 설명하고 있기 때문에 공통방법오류의 위험이 크지 않다고 판단할 수 있다[16].

〈표 3〉 PLS 요인 분석: 집중타당성 및 신뢰성 분석

	Certainty	Commitment	Compliance	DesNorm	ResCost	Training
Training1	0.2358	0.2435	0.3695	-0.1994	-0.1155	**0.8148**
Training2	0.3227	0.1589	0.3199	-0.181	-0.1434	**0.8249**
Training3	0.3415	0.2254	0.3613	-0.3039	-0.064	**0.9105**
Training4	0.3139	0.2297	0.2584	-0.2936	-0.0987	**0.8659**
Training5	0.2522	0.1197	0.3573	-0.2577	-0.0661	**0.8887**
Training6	0.3155	0.1583	0.3329	-0.2382	0.0034	**0.9041**
Training7	0.4048	0.1402	0.3685	-0.2496	-0.0062	**0.8487**
Certainty1	**0.8439**	0.1479	0.2537	-0.4284	-0.1063	0.3693
Certainty2	**0.7487**	-0.1121	0.289	-0.3728	-0.1781	0.2552
Severity1	**0.8586**	-0.0178	0.2583	-0.2957	-0.0051	0.2931
Severity2	**0.8623**	0.022	0.2636	-0.254	0.0418	0.2814
DesNorm1	-0.4487	-0.0776	-0.1932	**0.9612**	0.0965	-0.3147
DesNorm2	-0.2975	0.0705	-0.0856	**0.8961**	0.0098	-0.197
Commitment1	0.0239	**0.7984**	0.2644	0.0463	0.0229	0.2166
Commitment2	-0.0116	**0.851**	0.3893	-0.0207	0.0212	0.1209
Commitment4	0.0312	**0.7403**	0.2258	0.03	-0.0608	0.2198
Commitment6	0.0014	**0.8541**	0.2913	-0.0315	-0.0997	0.1668
Commitment7	0.0422	**0.7944**	0.3225	-0.0885	-0.0396	0.1625
ResCost2	-0.0947	0.0009	-0.1822	0.0903	**0.9104**	-0.0775
ResCost3	-0.0708	-0.0377	-0.1014	0.068	**0.9001**	-0.0546
ResCost4	-0.0639	-0.0514	-0.1876	0.0585	**0.959**	-0.0572
ResCost5	-0.0758	-0.0433	-0.2049	0.0374	**0.9349**	-0.0915
Compliance1	0.3364	0.3451	**0.9346**	-0.1226	-0.1977	0.3603
Compliance2	0.3347	0.3408	**0.9477**	-0.1793	-0.1692	0.3513
Compliance3	0.2951	0.3971	**0.9403**	-0.1383	-0.1864	0.3268
Compliance4	0.2308	0.3099	**0.9032**	-0.1563	-0.165	0.3864
Compliance6	0.2531	0.3272	**0.822**	-0.146	-0.1424	0.3576
Cronba's α	**0.8486**	**0.8683**	**0.9480**	**0.8498**	**0.9455**	**0.9443**
AVE	**0.6883**	**0.6540**	**0.8295**	**0.8634**	**0.8582**	**0.7501**
CR	**0.8980**	**0.9041**	**0.9604**	**0.9266**	**0.9603**	**0.9545**

AVE: Average Variance Extracted(평균분산추출)

CR: Composite Reliability(복합신뢰성)

Values in bold show high loading of items on respective construct indicating high convergent validity.

4.3 측정모형 검증

교차요인분석 <표 3>에서 요인 적재값은 최소 0.6, 이상적으로는 0.7이상이 되어야한다[5][29]. 이 경우 측정항목이 해당 잠재변수의 분산의 50%이상을 설명하고 있다고 말할 수 있다[5]. 잠재변수에 대한 신뢰성과 타당성은 내적 일관성(internal reliability), 집중타당성(convergent validity), 판별타당성(discriminant validity) 검증을 통해 제시될 수 있다[16]. 내적 일관성을 평가하는 방법은 Cronbach's alpha와 복합신뢰성이 있다. 두 지표의 차이는 Cronbach's alpha의 경우 선택된 항목간의 상관관계 계수를 나타내지만, 복합신뢰성의 경우 전체 항목이 주어진 상황에서 내적 일관성을 평가하기 때문에 더 정확하다[25]. 참고로 일반적으로 복합신뢰성이 Cronbach's alpha보다 크게 나타나는 경향이 있다. 집중타당성과 판별타당성은 개념 타당성(construct validity)을 구성하는 핵심 요소들이기 때문에 타당성 검증에서 반드시 수행되어야 한다[12]. 일반적으로 사회과학에서는 복합신뢰성이 0.7이상이 되어야 한다[4]. 어떤 학자는 0.8이상을 주장하기도 한다[11]. 본 연구에서는 복합신뢰성의 최소값이 0.8980으로 나타나 높은 수준의 신뢰성을 확보하고 있다고 볼 수 있다. Nunnally(1978)는 신뢰성(내적 일관성)이 0.7이상이 될 경우 집중타당성이 있는 것으로 볼 수 있다고 하였다. 하지만 본 연구에서는 집중타당성을 위해 추가적인 검증절차를 수행하였다. 집중타당성은 평균분산추출(Average Variance Extracted)을 통해 평가할 수 있다[25]. 만약 평균분산추출이 0.5이상일 경우 집중타당성이 존재한다고 평가한다[11]. <표 3>에 제시된 바와 같이 평균분산추출의 최소값이 0.6540으로 나타났기 때문에 집중타당성이 존재한다고 볼 수 있다. 판별타당성은 잠재변수간의 상관관계 계수와 평균분산추출의 제곱근 값(표 4의 대각선 값)을 비교함으로 평가할 수 있다[4][12]. 만약 각각의 평균분산추출의 제곱근 값이 잠재변

〈표 4〉 판별타당성 분석

	Certainty	Commitment	Compliance	DesNorm	ResCost	Training
Certainty	**0.8296**					
Commitment	0.0189	**0.8087**				
Compliance	0.3215	0.3794	**0.9108**			
DesNorm	-0.4174	-0.0222	-0.1623	**0.9292**		
ResCost	-0.0829	-0.0348	-0.1901	0.0675	**0.9264**	
Training	0.3667	0.2101	0.3891	-0.288	-0.0778	**0.8661**

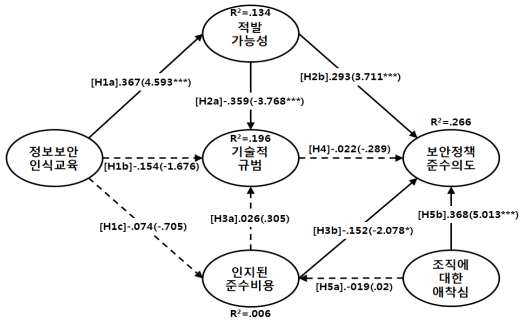
Diagonal elements are the square roots of average variance extracted (AVE).

수간의 상관관계 계수들보다 클 경우 판별타당성이 존재한다고 볼 수 있으며, 집중타당성도 확보되었다고 볼 수 있다. 이때 각각의 상관관계 계수가 0.7이하의 값을 가져야 한다. 만약 잠재변수간의 상관관계 계수가 0.7을 초과할 경우 다중공선성 문제를 의심해 볼 수 있다[25]. 본 연구에서 모든 잠재변수간의 상관관계 계수가 0.7이하로 나타났다. 또한 모든 대각선 값이 잠재변수간의 상관관계 계수보다 크게 나타났기 때문에 판별타당성에 문제가 없다고 볼 수 있다.

4.4 구조모형 검증

일반적으로 재표집 표본으로 200개를 설정할 경우 적정 수준의 표준 오차를 생성한다[6]. 본 연구는 더 견고한 분석을 위해 500개를 재표집을 위한 표본으로 설정하였다.

최종 모형을 분석하기 전에 본 연구에서는 모형의 적합도를 평가하였다. 그동안 모형의 적합도는 20여 가지 이상 개발되었으나 모든 적합도 판별 지표들은 모두 χ^2을 기반으로 하고 있기 때문에 공분산기반 구조모형(covariance-based SEM)에만 국한되어 적용할 수 있다. 그러나 최근 Tenenhaus et al.(2005)은 구조모형에서 산출되는 신뢰성 지표를 기반으로 모형의 적합도를 평가할 수 있는 지표를 개발하였는데, 이 지표는 공분산 기반 구조모형뿐만 아니라 컴포넌트 기반 모형(component-based SEM)에서도 적용할 수 있다[35]. 본 지표는 공통성(communality)과 R^2을 활용하여 계산하는데, PLS분석에서 공통성은 평균분산추출(AVE)과 동일한 값을 갖기 때문에 평균분산추출을 사용하여도 무방하다[35]. 전반적 적합도(Global of Fit, GoF)에 대한 계산식은 다음과 같다: $GoF = \sqrt{\overline{AVE} \times \overline{R^2}}$. 기준 값으로 0.1이하는 낮은 수준, 0.25이하는 중간수준 0.36이상은 높은 수준으로 평가할 수 있다[35]. 본 연구의 경우 0.3415로 나타나 높은 수준의 기준을 상회하지는 못하였으나 0.36에 근사하기 때문에 모형적합도가 적정수준을 보이고 있다고 평가할 수 있다. 이에 따라 최종 모형을 분석하였다.



[그림 3] 구조모형 분석결과

연구결과를 정리하면 다음과 같다. 정보보안 인식교육은 적발가능성에 유의한 영향을 미치는 것으로 나타났다 (β=0.3708, p<0.001). 따라서 조직 내에서 제공되는 보안

〈표 5〉 가설검증결과

		평균	표준편차	경로계수	표준오차	T값	p값
H1a	정보보안 인식교육→적발가능성	0.3708	0.0798	0.3667	0.0798	4.593	0.000***
H1b	정보보안 인식교육→기술적 규범	-0.1561	0.0922	-0.1545	0.0922	-1.676	0.094
H1c	정보보안 인식교육→인지된 준수비용	-0.0761	0.1047	-0.0738	0.1047	-0.7045	0.481
H2a	적발가능성→기술적 규범	-0.3554	0.0952	-0.3586	0.0952	-3.7685	0.000***
H2b	적발가능성→보안정책 준수의도	0.2935	0.0789	0.293	0.0789	3.7108	0.000***
H3a	인지된 준수비용→기술적 규범	0.0251	0.0845	0.0258	0.0845	0.3053	0.760
H3b	인지된 준수비용→보안정책 준수의도	-0.1511	0.0729	-0.1515	0.0729	-2.0784	0.038*
H4	기술적 규범→보안정책 준수의도	-0.0261	0.0747	-0.0216	0.0747	-0.2889	0.773
H5a	애착심→인지된 준수비용	-0.0183	0.0968	-0.0193	0.0968	-0.1998	0.842
H5b	애착심→보안정책 준수의도	0.3783	0.0734	0.3681	0.0734	5.0132	0.000***

* $t_{.05}$=1.960, ** $t_{.01}$=2.576, *** $t_{.001}$=3.291

인식교육을 통해 회사의 보안규정을 인지하게 된 개인은 자신의 이탈행위가 적발될 가능성이 있음을 인지하게 된다고 볼 수 있다.

둘째, 정보보안 인식교육은 기술적 규범(β=-0.1561)과 인지된 준수비용(β=-0.0761)에는 유의한 영향을 미치지 않는 것으로 나타났다. 이는 정보보안 인식 교육은 개인의 정책 준수를 위한 것이기 때문에 보안 인식교육이 수행된다 하더라도 타인의 준수행위가 개인의 관심사가 되지 않는다는 것을 의미한다. 또한 현실적으로 기업 내에서 이루어지고 있는 정보보안 인식교육은 주로 보안기술, 보안정책, 보안 이슈에 대한 부분을 다루기 때문에 완전한 의식전환은 아직 어려운 것으로 볼 수 있다. 즉, 보안정책 준수로 인해 회사가 절감하게 될 잠재적인 이익보다는 개인의 업무 생산성 감소가 더 큰 관심사라는 것을 알 수 있다[3][15]. 예를 들어, 기업 내에서 이루어지는 보안교육은 다양한 매체를 통해 전달되나 업무시간에 전달되기 때문에 자신의 업무시간 중 일부를 할애하여 교육받게 된다. 따라서 상대적으로 개인의 업무시간이 더 늘어나게 되어 개인은 업무의 과부화를 경험하게 된다.

다음으로 적발가능성은 기술적 규범에는 부의 유의관계를 나타낸 반면(β=-0.3554, p<0.001), 보안정책 준수의도에는 정의 영향을 미치는 것으로 나타났다(β=0.2935, p<3.7108). 적발가능성이라는 것의 전제는 개인의 사생활 침해발생이다. 시스템 사용이 추적될 수 있다는 것이기 때문에 적발가능성이 개인의 준수는 강제적으로 유도할 수 있으나 타인도 준수할 것이라는 것에 대해서는 확신할 수 없다는 것을 알 수 있다.

인지된 준수비용은 기술적 규범에 아무런 영향도 미치지 않는 것으로 나타났다(β=0.0251). 이는 보안준수로 인해 개인의 생산성이 낮아질 수도 있다고 생각할 경우 개인의 보안 정책 준수도 보장할 수 없기 때문에 타인도 보안 정책을 따를 것이라고 생각하지 않을 가능성이 있다는 것을 의미한다. 따라서 인지된 준수비용이 보안정책 준수의도에 부의 영향을 미쳤으며(β=-0.1511, p<0.05), 기술적 규범이보안정책 준수의도에는 아무런 영향을 미치지 않았다(β=-0.0261).

마지막으로 개인의 애착심은 인지된 준수비용에 아무런 영향도 미치지 않는 것으로 나타난 반면(β=-0.0183), 보안정책 준수의도에는 유의한 영향을 미치는 것으로 나타났다(β=0.3783, p<0.001). 즉 조직에 대한 애착심이 있는 개인은 보안정책을 준수할 의도가 있는 반면 보안 정책 준수로 인해 발생하는 인지적 비용까지 감내하도록 유도하기에는 부족함을 알 수 있다.

지금까지 제시된 결과를 정리하면 <표 5>와 같다.

5. 결론

정보보안 사고는 이전부터 지금까지 지속적으로 이어지고 있다. 앞으로도 보안 사고는 끊임없이 나타날 것이라고 조심스레 예단할 수 있다. 문제는 완전한 억제는 불가능하다 하더라도 최대한의 예방을 할 수 있는가를 생각해 보아야 한다는 것이다. 특히 최근의 사건들이 말해주고 있듯이 보안사고가 내부인에 의해 발생할 경우 충분히 예방할 수 있음에도 불구하고 이에 실패하여 큰 피해를 보고 있다는 점은 많은 기업들이 주목해야 한다.

본 연구는 어떻게 하면 내부인들에 의해 발생하는 보안사고를 줄일 수 있는지에 대한 하나의 해결책을 제시하기 위해 시작되었다. 연구결과 적발가능성과 개인의 조직에 대한 애착심이 보안정책 준수의도를 유발할 수 있는 것으로 나타났다. 여기서 적발가능성은 정보보안 인식 교육에 영향을 받는 것으로 나타났다. 즉 정보보안 인식 교육을 통해 사내 보안 기술과 정책, 그리고 절차 등에 대해 학습하게 될 경우 자신의 행위가 적발될 가능성이 있음을 인지할 수 있으며, 이는 결국 정보보안 정책 준수를 유발하는 것으로 볼 수 있다. 그러나 인지된 준수비용의 경우 보안 정책 준수를 방해 할 수 있는 것으로 나타났다. 이는 정보보안 정책 준수가 개인의 생산성 저하를 유발할 경우 역으로 보안 정책 준수가 제대로 이루어지지 않을 수 있음을 나타낸다. 주목할 점은 개인의 업무 생산성이 저하됨을 인지하고 있는 직원은 조직에 대한 애착심이 존재한다 하더라도 준수 비용이 절감되지 않는다는 것이다. 즉 정보보안 측면에서 조직에 대한 자신의 애착과 업무의 생산성과는 별개로 고려되고 있다고 판단된다.

따라서 기업은 정보보안 교육을 통해 사내 정보보안 정책에 대해 충분히 교육시키고 어떠한 행위가 보안 행위이고 어떠한 행위가 보안 침해 행위인지를 구성원들에게 인지시킨다면 보안정책준수를 유발할 수 있다. 즉 보안 교육의 우선 목표가 보안정책에 대한 인식 고양이 되어야 하는 것이다. 또한 조직에 대한 애착심을 증가시켜서 구성원과 회사와의 결속력이 높아질 경우 자연스럽게

보안정책 준수로 유도할 수 있다.

본 연구의 한계로는 첫째, 공통방법오류에 대한 검증 절차에 있다. 믿을 수 있는 과학적 절차일 경우 사전에 공통방법오류를 제거하고 시작해야 하야 본 연구에서는 사후적 방법을 선택하였다. 따라서 이 부분에서 완전히 자유롭다고 할 수는 없다. 둘째로, 표본 추출 대상기업들이 모두 IT기업이었다는 것이다. 정보보안에 대한 인식이 IT기업과 비IT기업의 구성원 간에 차이가 존재할 수 있기 때문에 분석결과가 모든 산업군에 적용되기에는 다소 문제가 될 수 있다.

추후 연구에서는 조직원들의 보안 정책 준수를 활성화하기 위해 억제 요인으로 규명된 보안정책 준수비용을 어떻게 절감할 수 있는지에 대해 연구해 볼 필요가 있다. 또한 정보보안 교육 전달 채널에 따른 차이를 규명해 볼 필요가 있다. 이메일, 뉴스레터, 오프라인 교육 등 다양한 수단이 활용되나 더 효과적인 방법을 찾아 규명하여 선택과 집중이 필요할 것으로 보인다.

참 고 문 헌

[1] 정태석 · 임명성 · 이재범 (2012). 기업의 지속적 정보보안 강화를 위한 접근법 개발, 디지털 정책연구, 10(2), 1-10.

[2] Beck, K. H., & Frankel, A. (1981). A conceptualization of Threat Communications and Protective Health Behavior, Social Psychology Quarterly, 44(3), 204-217.

[3] 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 & Security, 1(3), 18-41.

[4] Chin, W. W. (1998). The Partial Least Squares Approach for Structural Equation Modeling, In G. A. Marcoulides (Ed.), Modern Methods for Business Research (295-336), Mahwah, NJ:Erlbaum.

[5] Chin, W. W. (1998). Issues and Opinion on Structural Equation Modeling, MIS Quarterly, vii-xvi.

[6] Chin, W. W. (2001). PLS-Graph User's Guide, version 3.0.

[7] D'Arcy, J., & Hovav, A. (2007). Deterring Internal Information Systems, Communications of the ACM, 50(10), 113-117.

[8] D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research, 20(1), 79-98.

[9] Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory, Journal of Applied Social Psychology, 30(2), 407-429.

[10] Foltz, C. B., Schwager, P. H., & Anderson, J. E. (2008). Why Users (Fail to) Read Computer Usage Policies, Industrial Management & Data Systems, 108(6), 701-712.

[11] Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, Journal of Marketing Research, 18(1), 39-50.

[12] Gefen, D., & Straub, D. (2005). A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example, Communication of the Association forInformation Systems, 16, 91-109.

[13] Hair, Jr., J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). Multivariate Data Analysis, 6th ed., Prentice Hall.

[14] Herath, T., & Rao, H. R. (2009a). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness, Decision Support Systems, 47, 154-165.

[15] Herath, T., & Rao, H. R. (2009b). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations, European Journal of Information Systems, 18, 106-125.

[16] Jeffers, P. I., Muhanna, W. A., & Nault, B. R. (2008). Information Technology and Process Performance: An Empirical Investigation of the Interaction Between IT and Non-IT Resources, Decision Sciences, 39(4), 703-734.

[17] Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study, MIS Quarterly, 34(3), 549-566.

[18] Kankanhalli, A., Teo, H-H., Tan, B. C. Y., & Wei, K-K. (2003). An Integrative Study of Information Systems Security Effectiveness, International Journal of Information Management, 23(2), 139-154.

[19] Lee, Y., & Larsen, K. R. (2009). Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software, European Journal of Information Systems, 18, 177-187.

[20] Lee, J., & Lee, Y. (2002). A Holistic Model of Computer Abuse within Organizations. Information Management & Computer Security, 10(2), 57-63.

[21] Lee, S. M., Lee, S. G., & Yoo, S. (2004). An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories, Information & Management, 41, 707-718.

[22] Nagin, D. S., & Pogarsky, G. (2001). Integrating Celerity, Impulsivity, and Extralegal Sanction threats into a Model of General Deterrrence: Theory and Evidence, Criminology, 39(4), 865-892.

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

[24] Peace, A. G., Galletta, D., & Thong, J. (2003). Software Piracy in the Workplace: A Model and Empirical Test, Journal of Management Information Systems, 20(1), 153-177.

[25] Ping, Jr., R. A. (2004). On Assuring Valid Measures for Theoretical Models Using Survey Data, Journal of Business Research, 57, 125-141.

[26] Podsakoff, P. M., MacKenzie, S. B., Lee, J., & 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.

[27] Rippetoe, P. A., & Rogers, R. W. (1987). Effects of Components of Protection Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat, Journal of Personality and Social Psychology, 52(3), 596-604.

[28] Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change, Journal of Psychology, 91, 93-114.

[29] Segars, A. H. (1997). Assessing the Unidimensionality of Measurement: A Paradigm and Illustration within the Context of Information Systems Research, Omega, 25(1), 107-121.

[30] Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations, MIS Quarterly, 34(3), 487-502.

[31] Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making, MIS Quarterly, 22(4), 441-464.

[32] Tenenhaus, M., Vinzi, V. E., Chatelin, Y-M., & Lauro, C. (2005). PLS Path Modeling, Computational Statistics and Data Analysis, 48(1), 159-205.

[33] Young, R., & Zhang, L. (2007). Illegal Computer Hacking: An Assessment of Factors that Encourage and Deter the Behavior, Journal of Information Privacy & Security, 3(4), 33-52.

[34] Warkentin, M., & Willison. R. (2009). Behavioral and Policy Issues in Information Systems Security: The Insider Threat. European Journal of Information Systems, 18, 101-105.

[35] Wetzels, M., Odekerken-Schröder, G., & van Oppen, C. (2009). Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration, MIS Quarterly, 33(1), 177-195.

임 명 성

· 2002년: 삼육대학교 경영정보학과 경영학사
· 2004년: 한국외국어대학교 경영정보대학원 M.B.A.
· 2011년: 서강대학교 경영전문대학원 Ph.D.
· 2011년: 서강대학교 경영학부 대우교수
· 2012년: 삼육대학교 경영학과 조교수
· 관심분야: 정보보안, 서비스 시스템, 기술 혁신
· E-Mail: msyim@syu.ac.kr