Journal of the Korea Convergence Society
Vol. 9. No. 9, pp. 69-81, 2018

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2018.9.9.069

보안정책 준수 비용과 정보보안 중요성 인식 수준에 미치는 요인에 관한 연구: 중소기업을 중심으로

임명성
삼육대학교 경영학과, 부교수

An Exploratory Research on Factors Influence Perceived Compliance Cost and Information Security Awareness in Small and Medium Enterprise

Myung-Seong Yim
Associate Professor, Department of Business Administration, Sahmyook University

요 약 본 연구의 목적은 정보보안 정책 준수 의도의 선행변수인 정보보안에 대한 인지된 중요성에 유의한 영향을 미치는 요인을 규명하는 것이다. 이를 위해 구조방정식 모형을 기반으로 제안 모형을 분석했다. 분석결과, 첫째, 정보보안 교육의 효과성은 정책 준수에 따른 인지된 비용에 통계적으로 유의한 영향을 미치지 못하는 것으로 나타났다. 둘째, 정보보안 정책의 효과성은 정책 준수에 따른 인지된 비용에 유의한 영향을 미치는 것으로 나타났다. 셋째, 인지된 취약성은 정책 준수에 따른 인지된 비용에 유의한 영향을 미치는 것으로 나타났다. 넷째, 정책 준수에 따른 인지된 비용은 정보보안에 대한 인지된 중요성에 유의한 영향을 미치는 것으로 나타났다. 다섯째, 정보보안 침묵에 대한 경영진의 태도는 구성원들의 보안 침묵 행위에 유의한 영향을 미치는 것으로 나타났다. 여섯째, 정보보안에 대한 의사소통 기회는 구성원들의 보안 침묵 행위에 유의한 영향을 미치는 것으로 나타났다. 마지막으로 구성원들의 보안 침묵 행위는 정보보안에 대한 인지된 중요성에 유의한 영향을 미치는 것으로 나타났다.

주제어 : 정보보안, 조직침묵, 위험보상이론, 보안정책, 교육훈련

Abstract The ultimate intention of this research is to identify the factors that have a significant effect on the perceived importance of information security as the antecedent of intention to information security policy compliance. We found that the effectiveness of information security training program did not have statistically significant effect on the perceived cost of policy compliance. Second, the effectiveness of information security policy has significant influence on the perceived cost of policy compliance. Third, perceived vulnerability has a significant effect on the perceived cost of policy compliance. Fourth, perceived cost of policy compliance has a significant effect on perceived importance of information security. Fifth, supervisor's attitude toward information security silence has a significant effect on employee silent behavior towards information security. Sixth, communication opportunities towards information security has a significant influence on employee silent behavior towards information security. Finally, it was shown that employee silent behavior towards information security had a significant influence on the perceived importance of information security.

Key Words : information security, organizational silence, risk compensation theory, security policy, education and training

*This paper was supported by the Fund of the Korea Sanhak Foundation in 2017
*Corresponding Author : Myung-Seong Yim (msyim@syu.ac.kr)
Received July 12, 2018 Revised August 14, 2018
Accepted September 20, 2018 Published September 28, 2018

1. 서론

지난 수십 년 동안 대부분의 조직들은 내부 운영을 효과적으로 관리하기 위해 ICT(Information and Communication Technologies)를 적극적으로 도입해 왔다[1]. 이러한 노력으로 인해 이제는 모든 기기들이 거대한 네트워크를 통해 연결되는 초연결사회(hyper-connectivity)로 진입하게 되었다. 하지만 ICT는 양날의 칼이다[2]. 선의의 목적으로 사용될 경우 개인과 조직의 성과를 향상시킬 수 있는 거대한 잠재력을 가지고 있다[2]. 악의적으로 사용할 경우 개인, 조직, 더 나아가 사회에 거대한 위협이 될 수 있다[2]. 실제로 정보보안 사고(Information Security Breaches)는 조직에 추가적인 사고 처리 비용을 발생시키며, 기업의 명성에도 치명적 영향을 미친다[3]. Bulgurcu et al.(2010)은 정보보안 위험이 조직 안에서 발생할 경우 기업의 부채, 신뢰성 손상, 주가 하락과 같은 금전적 위험들이 복합적으로 발생한다고 주장했다[4]. 따라서 기업이 보유한 정보자산에 대한 위협을 예방하거나 감소시키기 위해 필요한 기술적, 행동적, 관리적, 철학적, 조직적 접근법이 필요하다[5].

기술적 대안의 경우 도입 즉시 효과가 발생한다는 점에서는 매우 효과적인 정보보안 수단이다. 하지만 첫째, 중소기업 입장에서 기술적 대안의 도입 및 유지 보수에 있어서 비용 부담이 된다는 점에서 적극적인 도입을 주저하게 만든다. 심지어 최근의 경제 악화로 중소기업들이 보안 예산을 축소하고 있다. 둘째, 사내에 정보보안 전문가가 존재하지 않을 경우 관리 자체가 어려워질 수도 있다. 셋째, 비용절감을 위해 도입되는 상용 보안 소프트웨어 및 하드웨어는 기업의 정보시스템의 환경적 특성을 반영하고 있지 않기 때문에 정보보안 시스템과 기존 시스템 간의 충돌도 예상된다. 넷째, 보안 기술에 대한 구성원들이 사용횟수가 증가함으로 인해 해당 정보보안 기술이 가지고 있는 약점을 알게 될 경우 처음에 예상했던 결과에서 벗어나는 더 큰 문제를 야기할 수 있다.

감시 및 통제도 내부 구성원들을 감시하는 중요한 수단이 될 수 있다. 하지만 자신이 감시받고 있고 통제되고 있다는 자체가 심리적 압박감과 중압감을 느끼게 만들 수 있기 때문에 강요된 준수에서 더 많은 부담을 구성원들에게 안겨줄 수 있다. 또한 이러한 심리적 압박은 이직과 직무 불만족, 업무 생산성 하락 등의 결과로 연결될 수 있다는 점에서 효과적이라고 보기는 어렵다.

처벌도 역시 중요한 정보보안 사고 예방 수단이 될 수 있다. 하지만 지란지교소프트(2016)[1]가 중소기업을 대상으로 조사한 정보보안 실태 조사 자료에 따르면 응답기업의 38.9%는 징계절차는 있으나 조치는 거의 이루어지지 않는다고 응답하였고, 25.9%는 징계절차가 없다고 응답했다. 따라서 처벌이 구성원들의 정보보안을 위한 확실한 예방책이라고 보기는 어렵다.

따라서 중소기업의 입장에서 가장 확실히 내부인에 의한 정보보안 사고를 예방할 수 있는 수단은 정보보안 정책의 준수와 정보보안 교육 및 훈련이다[6]. 또한 정보보안 정책(Information Security Policy)은 어떻게 조직의 정보시스템 자원을 활용해야 하는지 알려주는 수단이자 구성원들의 보안 행동을 유도하고 영향을 미치는 가장 저렴하고 유용한 메커니즘이다[7]. 따라서 정보보안과 관련된 많은 선행연구들은 어떻게 하면 구성원들이 정보보안 정책을 준수하게 만들 수 있는지에 대해 연구해왔다. 또한 내부 구성원들의 정보보안 인식수준을 제고하기 위해 정보보안 교육 훈련의 중요성에 대해서도 꾸준히 연구해 왔다.

하지만, 선행연구들은 다음의 한계가 있다. 정보보안 정책의 중요성을 인식하고 이를 준수할 수 있는 방법에 대한 연구가 많이 진행되었지만, 정보보안 정책 자체에 대한 평가는 이루어지지 않았다. 즉 준수해야 할 정책자체가 효과적인지에 대한 논의가 많이 부족하다[8]. 따라서 정보보안 정책의 효과성을 측정하는 도구가 필요하다.

또한 정보보안 인식교육에 대한 선행연구를 살펴보면 현재 조직에서 정보보안 인식교육이 운영되고 있는지 여부만을 살펴보고, 존재할 경우 정책 준수에 어떠한 영향을 미치는지 실증적으로 검증해 왔다. 하지만 정보보안 교육을 통해 구성원들의 보안 인식수준을 높이고 보안 정책과 기술에 대한 지식을 전달하기 위해서 교육은 효과적이어야 한다. 즉 교육의 내용, 전달 방법, 전달 횟수 등이 피교육자의 환경에 맞게 이루어져야 한다. 이는 교육의 수행여부만으로 판단할 수 없다. 중소기업에서 민감한 자료를 다루는 임직원을 대상으로 정보보안 교육을 수행하는 비율은 50%가 넘는 것으로 나타났다. 그럼에도 불구하고 내부인에 의한 정보보안 사고가 끊이지 않는 것은 내부인의 정보보안 인식 수준이 낮기 때문이다. 이는 기업에서 운영하고 있는 정보보안 교육 훈련 프로그

1) 지란지교소프트, 2016년 중소기업 정보보안 현황조사, 지란지교소프트.

램이 효과적이지 못하다는 것을 반증하고 있다. 따라서 이제는 정보보안 교육 훈련 프로그램의 존재 여부에서 한 발 더 나아가 효과적인 교육 훈련 프로그램을 운영하기 위한 방법에 대해 생각해 보아야 한다. 이에 본 연구는 다음의 연구문제(Research Question)를 제안하고 이에 대한 답을 찾고자 한다.

RQ1. 중소기업 상황에서 내부인의 정보보안의 중요성 인식 제고에 영향을 미치는 요인은 무엇인가?
RQ2. 정보보안의 조직적 대책인 정책 및 보안 교육의 효과성은 정보보안 준수 비용에 어떠한 영향을 미치는가?
RQ3. 정보보안에 대한 구성원들의 침묵은 정보보안 행위에 어떠한 영향을 미치는가?

정리하면, 중소기업은 비용 부담으로 인해 고가의 보안 기술을 도입하기 어렵다. 또한 감시 및 통제하는 수단도 결국 기술이 필요하기 때문에 동일한 비용부담을 안게 됨과 동시에 감시 및 통제로 인해 직원에게 위화감을 조성할 수 있어서 이 방법도 중소기업의 정보보안을 위한 적절한 수단이 될 수 없다. 처벌도 관련 규정은 있으나 실제로 이를 적용하기는 어렵다. 그 이유로 내부자에 의한 사고는 실제 발견되기 전까지 미리 알 수가 없기 때문이다. 또한 사고 규모가 크지 않은 이상 이를 공식적으로 처벌하게 되면 자사 내부의 보안 사고를 외부에 알리는 발화점이 되어 브랜드 이미지에 악영향을 줄 수 있기 때문에 암묵적으로 용인해 주는 경우도 많다.

따라서 중소기업 입장에서 가장 저렴하지만 효과적인 정보보안 강화 수단은 정보보안 정책의 준수와 정보보안 교육 훈련이다. 본 연구는 이 두 수단의 효과성을 측정하고 해당 효과성이 정보보안의 중요성 인식에 미치는 영향을 살펴봄으로써 중소기업 입장에서 어떻게 정보보안을 강화할 수 있는지, 특히 내부 구성원들의 정보보안의 인식 수준을 높일 수 있는 방안을 제시하고자 한다.

2. 이론적 배경

2.1 구성원들의 침묵

조직 안에서 구성원들의 침묵 행위는 일반적이다[9]. 그러나 구성원 침묵(employee silence)에 대한 학문적 연구는 상대적으로 부족하다[9]. Pinder and Harlos(2001)는 침묵 행위를 조직 안에서 쉽게 목격할 수 있음에도 불구하고 연구자들에 의해 주목받지 못했다고 주장했다[10]. 이러한 학문적 무관심은 2가지 이유가 있다. 첫째, 많은 경우 침묵을 무언(the absence of speech)이자 비행위(a non-behaviour)로 보았다[9]. 이 관점에서 발언(speech)이 발생하지 않으면 행위가 발생하지 않은 것으로 볼 수 있다[9]. 둘째, 행위의 부재는 가시적이며 명시적인 연구를 어렵게 만든다고 보았다[9]. 그러나 구성원의 침묵은 개인과 조직의 성과에 함의를 제공하는 중요한 조직적 행위이다[9]. 행위적으로 보면 침묵과 발언은 양극단을 이룬다[9]. 의사소통 문헌에서는 침묵을 사회적 상호작용을 위한 핵심 요소라고 보았다[9]. 효과적인 의사소통을 위한 두 가지 이분법적 요소는 침묵과 발언이다[9]. 침묵과 발언이 없다면 누군가 듣는 사람이 없다는 것이기 때문에 효과적인 대화가 불가능하다[9].

Morrison and Milliken(2000)은 조직 침묵을 체념적 침묵(acquiescent silence)과 회피적 침묵(quiescent silence)으로 구분하였는데, 체념적 침묵은 단념(resignation)에 기반을 둔 체념적 행위(disengaged behaviour)이며, 회피적 침묵은 두려움에 기반을 둔 자기보호행위이다[11]. Van Dyne et al.(2003)은 여기에 더하여 친사회적 동기에 의한 구성원들의 침묵(employee silence)을 추가하였는데[9], 이는 이타주의와 협력에 기반을 둔 친사회적 그리고 타인지향적 행위이다.

체념적 침묵: 사람들은 침묵하는 사람을 볼 때 능동적 대화를 하지 않는 사람으로 치부한다[9]. 하지만 체념적 침묵은 구성원들이 관련 아이디어, 정보, 의견을 가지고 있음에도 불구하고 아이디어를 표현하지 않는 상황을 기반으로 한다[9]. 따라서 체념적 침묵은 단념에 의해 관련 아이디어, 정보, 의견 등을 삼가는 행위를 말한다[9]. 체념적으로 침묵하는 사람들은 현재 상황에 대해 기대를 버린 나머지 무엇인가를 말하고자 하는 노력, 몰입하는 노력 혹은 상황을 변화시키고자 하는 시도를 하지 않는다[9]. 이들은 의도적으로 수동적으로 행동하며, 비참여적 행위를 보일 가능성이 높다[9]. 또한 자신의 행동이 변화를 유발할 수 없다고 생각할 경우 그들은 능동적으로 아이디어 혹은 제안을 제시하는 것을 포기한다[9].

방어적 침묵(defensive silence): Pinder and Harlos (2001)는 자신의 발언이 유발할 수 있는 결과에 대한 개인적 두려움으로 인해 의도적 누락을 실행하는 것을 회

피적 침묵(quiescence silence)이라고 정의했다. Morrison and Milliken(2000)은 두려움이라는 개인적 감정이 조직 침묵의 가장 핵심적인 동기라고 주장했다[11]. 이와 같은 관점에서 업무 현장에서 구성원들의 발언을 위한 핵심적인 전제조건은 심리적 안정과 발언 기회 등이다[9]. 방어적 침묵은 자아보호를 위한 하나의 유형으로 두려움 때문에 관련 아이디어, 정보, 의견 등을 삼가는 것을 말한다[9]. 따라서 방어적 침묵은 외부의 위협으로부터 자신을 보호하기 위해 의도적으로 수행되는 능동적 행위이다[9]. 즉, 자아 보호의 한 형태로 개인적 실수를 의도적으로 숨기는 것이다[9].

친사회적 침묵(prosocial silence): 친사회적 침묵은 Van Dyne et al.(2003)에 의해 소개된 개념으로 이타주의나 협력적 동기로 인해 동료들 혹은 조직에 이익이 되고자 업무관련 아이디어, 정보, 의견 등을 삼가는 것을 말한다[9]. 친사회적 침묵은 조직 시민 행동과 마찬가지로 의도적이고 능동적 행동이며 주된 초점은 타인이다[9]. 친사회적 침묵은 방어적 침묵과는 다르게 발언으로 인해 발생하는 부정적 결과보다는 타인의 관심으로 인해 발생한다[9]. 또한 조직시민 행동과 마찬가지로 친사회적 침묵은 자유재량에 의한 행위이며 조직에 의해 강제적으로 수행되지 않는다[9].

3. 가설 수립 및 연구모형

3.1 정보보안 효과성

3.1.1 정보보안 교육의 효과성

구성원들이 정보보안 인식을 형성하는 것이 가장 효과적인 정보보안 대책이다[12]. 정보보안 정책의 인식은 구성원들이 유해한 공격과 다른 취약성들로부터 정보자산을 안전하게 지켜야 하는 이유를 인식하게 해준다[12]. 인식(awareness)은 훈련과 교육에 의해 달성된다[13]. 따라서 정보보안 훈련은 정보보안 정책을 구성원들이 효과적으로 준수할 수 있도록 도와준다[12]. 정보보안 훈련 및 교육을 통해 구성원들을 설득하고 동시에 구성원들의 사고 과정을 활성화시켜서 정보보안 정책을 준수하는 것이 왜 중요한지 그 이유를 깨닫고 이를 내면의 가치로 받아들이게 만들 수 있다[14]. 또한 구성원들을 대상으로 제공되는 보안 훈련 및 교육은 구성원들이 정보시스템의 최종 사용자이기 때문에 그리고 조직을 보호하는데 있어서 약한 고리를 형성하고 있기 때문에 핵심적이다[13]. 따라서 구성원들에게 정보보안 인식 교육을 시키는 것과 정책 준수를 위한 동기를 부여하는 것은 정보보안 정책 준수에 긍정적 영향을 미침과 동시에 보안 정책 위배 행위를 억제할 수 있다[12].

성숙한 정보보안 교육 프로그램은 어떻게 그리고 왜 해당 프로그램이 효과가 있는지에 대한 이론적 설명을 제공할 수 있어야 한다[14]. 반면에 현장에서 효과적이지 못한 훈련 프로그램은 제한적 가치만 제공한다[14]. 따라서 효과적인 보안 교육 및 훈련 프로그램을 제공하는 것은 조직이 목표로 하는 지속적인 보안 강화에 기여할 수 있다고 판단된다.

H1. 정보보안 훈련 프로그램의 효과성은 인지된 정책 준수 비용에 뷰-)의 영향을 미칠 것이다.

3.1.2 정보보안 정책의 효과성

정보보안 정책(information security polity)이란 조직의 정보와 기술 자원을 구성원들이 보호하기 위한 책임과 역할을 기술해 놓은 문서를 말한다[4]. 정보보안 정책은 조직의 정보와 기술을 보호하기 위해 무엇을 해야 하며, 언제 상호작용해야 하는지에 대한 방향성을 제시해 준다[4]. 따라서 효과적인 정보시스템 보안을 위해 명료한 정책의 개발은 중요하다[15].

구성원들의 정보보안 정책의 미준수는 정보보안 연구 분야의 핵심으로 자리잡아왔다[14]. 만약 구성원들이 사내의 정보보안 정책을 준수하지 않는다면, 보안 정책은 자체의 실효성을 잃어버리게 된다[12,14]. 기업 내 데이터 유출의 주된 원인들은 주로 구성원들의 보안 인식 부족, 정보보안 정책 준수 결여, 정책 위반, 훈련 부족, 동기 결여 등이다[12].

정보보안 정책은 최고경영진들에 의해 수립되었기 때문에 실제 이를 준수해야 하는 많은 구성원들의 관점에서 정보보안 정책이 수립되었고 자신이 이를 알고 있다는 것에 대한 인식보다는 해당 정책이 얼마나 현실적이고, 자신의 정보보안 행위를 수행하는데 있어서 효과가 있는지에 대한 평가가 필요하다. 따라서 다음의 가설을 제시할 수 있다.

H2. 정보보안정책의 효과성은 인지된 정책 준수 비용에 뷰(-)의 영향을 미칠 것이다.

3.1.3 인지된 취약성

조직내 대부분의 보안 프로그램은 위험에 대한 방어, 위험 관리, 위험 감소와 같은 높은 수준의 목표를 가지고 있다[16]. 그러나 정보보안 분야에 근무하는 많은 사람들은 조직 안에 새로운 보안 대책이 마련됨에도 불구하고 보안 사고가 줄어들지 않는다는 것을 알고 좌절하게 된다. 이러한 현상을 설명해 주는 이론이 위험보상이론(risk compensation theory)이다[16].

위험보상이론에 따르면 새로운 보안 대책이 기업에 도입된 이후 새로운 보안 수준은 조직 안에서 쉽게 수용되어 보안 수준이 상승하는 것이 아니라 실제로 동일한 수준에 머물러 있게 된다[16]. 즉 위험 수준은 사라지는 것이 아니라 재배열된다는 것이다[16]. 예를 들어 영국에서는 안전벨트 규정이 시행된 이후 자동차관련 사망자가 오히려 증가했다[16]. 이는 안전벨트 규정으로 인해 많은 운전자와 동승자들이 안전벨트를 착용함으로 인해 위험이 일정부분 감소되었다고 느낌에 따라 다소 무모하게 운전하는 사례가 많아지다 보니 보행자 사고가 증가한 것이다[16].

Zhang et al.(2009)은 자신이 무엇으로부터 안전하게 보호받고 있다고 느낄 경우 자신의 행동에 대한 주의가 감소한다고 주장했다[17]. 즉 보호 장치가 안전을 향상시키는 반면에 사람들을 더 위험한 행동에 몰입하도록 유도하는 경향도 있다[17]. 따라서 정보보안 측면에서 시스템의 취약성은 보안 정책을 준수하는데 발생하는 비용에 부정적 영향을 미칠 수 있다.

H3. 인지된 시스템 취약성은 인지된 정책 준수 비용에 정(+)의 영향을 미칠 것이다.

3.1.4 정책 준수에 따른 인지된 비용

정보보안 정책이 개인에게 미치는 영향에 대해서 아직 일관된 결과를 도출하지 못하고 있다. Gopal and Sanders(1997)는 정책의 사용이 해적판 소프트웨어 사용을 억제하고 법적 결과에 대한 경고를 알리는데 기여한다고 주장했다[18]. 반면에 Wiant(2003)는 조직의 보안 정책의 사용이 보안 사고의 심각성이나 보안 사고의 발생과 관련되지 않는다고 보고했다[19]. Foltz(2000)도 컴퓨터 사용정책이 정보시스템 오남용 의도와 행위에 아무런 영향도 미치지 않는다고 주장했다[20]. Harrington (1996)은 윤리적 행동 방침이 컴퓨터 남용에 대한 판단과 의도에 아무런 영향도 미치지 않는다는 결과를 제시했다[21]. Lee et al.(2004)도 보안 정책이 컴퓨터 남용 행위에 아무런 영향을 미치지 않는다는 결과를 제시했다[22]. 이러한 불일치된 결과의 이면에는 보안 정책이 가지고 있는 부정적 측면에 대한 고려가 없었다. 정보보안 정책들은 조직의 모든 수준에서 비효과적이고, 불필요하며, 강제성이 없다고 비판받기도 한다[8]. 심지어 구성원들은 보안 정책이 업무 생산성의 방해물이 된다고 생각하기도 한다[8]. 구성원들은 정보보안 정책이 경영진이 자신들을 모니터링하고 통제하기 위한 도구라고 생각하기도 한다[8]. 그렇기 때문에 정책을 준수하는데 있어서 인지적 비용이 발생하는 것이다.

H4. 인지된 정책 준수 비용은 인지된 정보보안의 중요성에 부(-)의 영향을 미칠 것이다.

3.2 침묵 분위기

3.2.1 정보보안 침묵에 대한 경영진의 태도

최고 경영진은 보안 효과성에 긍정적 영향을 미친다[12,23]. 또한 그들은 직접적으로 정보보안 효과성에 영향을 미치기도 하고 다양한 보안 프로그램과 정책을 통해 정보보안의 효과성에 영향을 미칠 수도 있다[23]. 최고경영진의 모범(practices)은 개별 구성원들에 의해 관찰되는 경영진의 습관적 행위를 말한다[24]. 경영진의 정보보안에 대한 관심은 문서화된 정보보안 정책뿐만 아니라 정보보안 인식 훈련 프로그램을 통해 드러난다[24]. 직속상관의 모범은 개별 구성원들에게 관찰되는 직속상관의 반복적 행위를 말한다[24]. 조직의 공식적 대리인으로서 직속상관은 직속 부하직원과 가장 빈번하게 상호작용한다[24]. 그들은 구성원들에게 조직의 목표에 대해 공유하고 강조할 수 있는 가장 이상적인 대리인이다[24].

경영진의 지원은 정보시스템의 구축과 IT 프로젝트의 핵심성공요인으로 널리 연구되어 왔다[23]. Soomro et al.(2016)은 최고경영진의 지원의 결여는 정보보안의 효과성의 핵심 장벽이라고 주장했다[12]. 경영진은 이러한 장벽을 표명할 수 있는 책임이 있는 사람들이다[12]. 선행연구에 따르면 직속상관의 참여가 구성원들의 안전 분위기에 대한 인식 수준의 향상과 높은 수준의 안전을 유도한다는 것을 발견했다[24].

H5. 정보보안 침묵에 대한 경영진의 태도는 정보보안에 대한 구성원들의 침묵행위에 정(+)의 영향을 미칠 것이다.

3.2.2 정보보안에 대한 의사소통 기회

인간의 신념을 변화시킬 수 있는 두 가지 방법은 적극적 참여와 설득 의사소통이다[25]. 의사소통 기회는 의사소통, 정보공유에 있어서 개방성과 신뢰와 관련되며, 타인의 이야기를 받아들인다는 느낌, 그리고 이를 진심으로 받아들인다는 느낌을 반영하고 있다[26]. 선행연구에 따르면 경영진과 상사들의 개방적 의사소통은 구성원들의 조직의 일체성과 업무 생산성 등에 직접적으로 영향을 미친다[26]. 따라서 다음의 가설을 수립할 수 있다.

H6. 정보보안에 대한 의사소통 기회는 정보보안에 대한 구성원들의 침묵행위에 (+)의 영향을 미칠 것이다.

3.2.3 구성원들의 보안 침묵 행위

구성원들의 역할이 모든 기업의 성공에 핵심이기는 하나 여전히 정보보안 측면에서는 약한 고리를 형성하고 있다[27]. 조직의 내부인에 의한 보안사고는 외부인에 의한 보안 사고의 발생비율보다 더 높은 것이 현실이고, 그렇기 때문에 실질적으로 구성원들이 보안 사고의 가장 큰 위협으로 인식되고 있다[27]. 보안 행위에 더 많은 시간을 보내는 것은 높은 수준의 인지된 보안 효과성과 밀접하게 관련된다[28].

H7. 정보보안에 대한 구성원들의 침묵행위는 인지된 정보보안의 중요성에 (+)의 영향을 미칠 것이다.

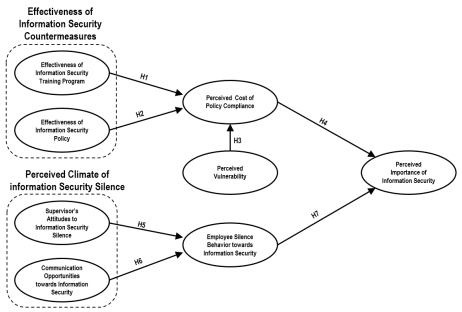

Fig. 1. Research Model

4. 데이터 수집

4.1 측정항목과 데이터 수집 방법

본 연구에서는 제안 모형을 검정하기 위해 설문 기법을 사용했다. 설문 항목은 Churchill(1979)이 제안한 체계적 절차에 근거하여 개발했다. 본 절차는 1) 잠재변수의 영역 설정, 2) 포함되어야 할 항목과 제거되어야 할 항목에 대한 결정, 3) 선행연구를 기반으로 대상 항목 결정, 4) 데이터 수집을 통해 측정항목의 반복적 정제화, 5) 신뢰성 및 타당성 평가의 단계로 구성된다[30]. 수립된 설문은 관련 영역 전문가 2인(현직 교수이자, 실증분석을 수행한 경험이 있는 전문가)을 대상으로 검토 절차를 요청했으며, 어색한 문장, 의미 전달에 있어서 문제가 있는 문장 등 전반적인 내용에 대해 검토를 수행했다[31].

정보보안 교육의 효과성이란 조직이 제공하는 정보보안 절차를 준수하는데 있어서 정보보안 교육이 도움이 되는 정도를 말하며, Knapp et al.(2007), Knapp and Ferrante(2012)의 연구에서 9개의 항목을 차용했다. 정보보안 정책의 효과성은 정보보안 정책의 명확성, 포괄성 수준을 말하며, Goel and Chengalur-Smith(2010)의 연구에서 8개의 항목을 차용했다. 인지된 취약성은 사내 정보시스템의 보안사고 발생 가능성 정도를 말하며, Workman et al.(2008)의 연구에서 6개의 항목을 차용했다. 정책 준수에 따른 인지된 비용은 정보보안 정책의 준수에 뒤따르는 인지적 불편함과 생산성 저하 정도를 말하며, Bulgurcu et al.(2010)의 연구에서 6개의 항목을 차용했다. 정보보안 침묵에 대한 경영진의 태도는 구성원들이 사내 정보보안에 대해 자유롭게 의견을 교환할수록 만드는 경영진의 노력 정도를 말하며, Vakola and Bouradas(2005)의 연구에서 5개의 항목을 차용했다. 정보보안에 대한 의사소통 기회는 구성원이 사내 정보보안에 대해 관리자와 의견을 나누는 정도를 말하며, Vakola and Bouradas(2005)의 연구에서 3개의 항목을 차용했다. 구성원들의 보안 침묵 행위는 구성원들이 사내 구성원들과 사내 정보보안의 강화 및 취약점에 대해 용이하게 의견을 나눌 수 있는 정도를 말하며 Vakola and Bouradas(2005)의 연구에서 3개의 항목을 차용했다. 인지된 정보보안 중요성이란 정보보안 이슈에 대한 인지된 중요성의 수준을 말한다[29]. Knapp and Ferrante(2012)의 연구에서 8개의 항목을 차용했다.

각 항목에 대한 응답은 Likert type 7점 척도법(7 point Likert Scale)을 사용했다. 1점은 “전혀 그렇지 않다”, 7점은 “전적으로 그렇다”를 의미한다. 모든 항목은 반영적 개념(reflective construct)으로 측정했다.

응답대상자는 1) 현재 중소기업에 재직 중인 사람, 2) 현재 재직 중인 기업에서 정보보안 교육을 1회 이상 받은

사람, 3) 현재 재직 중인 기업의 정보보안 정책을 1회 이상 읽어(perusal)본 사람을 전제조건으로 선정되었다. 위의 3가지 조건 중 하나라도 충족하지 않은 대상은 응답자에서 제외했다.

2018년 2월 19일부터 4월 2일까지 총 300부의 최종 설문을 배포했다. 배포는 응답자의 편의와 상황에 맞도록 이메일, 우편을 복합적으로 사용했다. 이 중 19부는 이메일로 수거되었으며, 248부는 우편으로 수거되었다. 따라서 총 267부(response rate: 89%)를 수거했다. 응답률이 높은 이유는 사전에 각 조직의 핵심 구성원에게 본 설문의 목적을 설명하고 참여 의사를 문의하였기 때문이라고 판단된다. 또한 총 1개월간의 충분한 시간을 두고 설문을 수집했기 때문에 응답을 위한 시간적 여유도 하나의 이유라고 생각된다. 뿐만 아니라 선정 대상은 응답대상 조건에 맞는 사람들이기 때문에 어렵지 않게 응답할 수 있기 때문이라고 생각된다.

회수된 설문 중에 무성의한 설문(5개 이상의 연속된 항목에 동일한 번호로 응답, 혹은 하나의 잠재변수의 절반 이상의 항목을 응답하지 않은 경우), 혹은 한 페이지 이상을 실수로 응답하지 않은 응답은 분석에서 제외했다. 또한 각각의 잠재변수에는 하나 이상의 역코딩 응답(reverse coding)을 포함시켜 응답자의 성실성을 확인했다. 이 또한 제거 대상의 기준으로 활용했다. 이와 같은 절차를 거쳐 총 231개의 응답을 최종 분석에 사용했다. 분석에는 설문코딩을 위해 Microsoft Excel 2016을 사용했으며, 기초통계분석 및 요인분석을 위해 IBM SPSS Statistics v23을 사용하였고, 구조모형 분석을 위해 SmartPLS v2.0 M3을 사용했다. 응답자에 대한 인구통계학적 특성을 정리하면 Table 1과 같다.

4.2 측정모형의 신뢰성 분석

PLS 분석을 통해 제공되는 교차요인 분석(crossloading analysis)에서 각각의 적재값이 연구자가 의도한 잠재변수에 높은 수준(0.707이상)으로 적재될 경우 항목 신뢰성(individual item reliability)이 존재한다고 판단한다[33,34]. 항목 신뢰성은 각각의 항목과 해당 잠재변수간의 공유 분산이 오차 분산(error variance)보다 크다는 것을 의미한다[33,35]. 물론 이 기준은 인과모형을 활용한 새로운 측정지표 혹은 표준화된 지표에 대해서까지 엄격하게 적용되는 것은 아니다[33]. 본 연구에서는 최소값이 0.7253(sc13)으로 본 기준을 만족하고 있다.

신뢰성이란 복수의 관측변수 간의 일관성 정도를 나타낸다[36]. 신뢰성을 평가하는 가장 일반적인 지표는 통합 지표(summated scale) 내에 존재하는 변수들의 일관성을 평가하는 내적 일관성이다[36]. 내적 일관성(internal consistency)이란 측정항목의 동질성 수준을 말하며[37], 내적 일관성을 평가하기 위한 두 가지 지표인 Cronbach'a alpha와 CR(Composite Reliability)이 0.7이상일 경우 적정한 내적 일관성을 가지고 있다고 판단한다[38,39]. Fornell and Larcker(1981)에 따르면 그들이 제시한 CR이 Cronbach's alpha값보다 우수한데, 그 이유는 인과모형 안에서 추정된 항목 적재값이 CR을 계산하는

Table 1. Demographic Informations of Respondents

Category		Freq.	Ratio	Category		Freq.	Ratio
Gender	Male	195	84.42	Age: 40.912 years (Mean)			
	Female	33	14.29	the # of Years of Service		10.87 years (Mean)	
	No Response	3	1.30	Employment Types	Permanent	222	96.10
Position Level	Employee	18	7.79		Contract	7	3.03
	Deputy	45	19.48		Dispatched	1	0.43
	Section Head	46	19.91		No Response	1	0.43
	Deputy Head of Department	45	19.48	Industry Type	IT/SI	82	35.50
	Head of Department	49	21.21		Manufacturing	57	24.68
	Director	22	9.52		Fiance	26	11.26
	Executive Director	2	0.87		Medical Service	0	0.00
	No Response	4	1.73		Government	0	0.00
Education Level	High School	10	4.33		Transportation	4	1.73
	2 Years College	11	4.76		Education	1	0.43
	College Degree Program	1	0.43		Construction	46	19.91
	4 Years University	175	75.76		Other Services	5	2.16
	Master Degree	33	14.29		ETC	7	3.03
	No Response	1	0.43		No Response	3	1.30

Table 2. PLS Crossloading Analysis

	Manager Att	Training Effect	Comm Opprt	Importance	Policy Effect	Perc Cost	Vulnerability	Silence Beh
ed1	0.6091	**0.9066**	0.4790	0.5741	0.7293	-0.2331	-0.2312	0.4483
ed2	0.5724	**0.9214**	0.4950	0.5764	0.7287	-0.1986	-0.2138	0.4107
ed3	0.5871	**0.8885**	0.4781	0.5661	0.7327	-0.1940	-0.1892	0.3658
ed4	0.5807	**0.9305**	0.4686	0.6116	0.7704	-0.2093	-0.2004	0.4527
ed5	0.5682	**0.8966**	0.4375	0.5808	0.7454	-0.1841	-0.1512	0.4297
ed6	0.5362	**0.8883**	0.4015	0.5826	0.7168	-0.1294	-0.2075	0.4304
ed7	0.4313	**0.7985**	0.3914	0.4618	0.6396	-0.1153	-0.1295	0.4881
ed8	0.4582	**0.8524**	0.3994	0.4964	0.6749	-0.1493	-0.1493	0.4023
ed9	0.5128	**0.8375**	0.4353	0.5354	0.6965	-0.1293	-0.1228	0.4431
sp1	0.5916	0.7361	0.4848	0.5680	**0.8747**	-0.2807	-0.2065	0.4674
sp2	0.5704	0.7224	0.4487	0.5770	**0.8752**	-0.2569	-0.1450	0.4374
sp3	0.5769	0.7383	0.4785	0.5605	**0.8846**	-0.2222	-0.1391	0.4432
sp4	0.5681	0.7325	0.4803	0.5670	**0.8931**	-0.2834	-0.1431	0.4309
sp5	0.6006	0.7006	0.4786	0.5233	**0.8800**	-0.2405	-0.1285	0.4226
sp6	0.6770	0.6154	0.5220	0.6066	**0.7798**	-0.2259	-0.2264	0.3433
sp7	0.5872	0.6110	0.4356	0.5555	**0.8120**	-0.2113	-0.1375	0.4152
sp8	0.5714	0.6698	0.4282	0.5685	**0.8142**	-0.2258	-0.1150	0.3953
ss1	**0.8794**	0.5281	0.5720	0.5636	0.5879	-0.2356	-0.2105	0.4256
ss2	**0.8849**	0.6110	0.5446	0.5649	0.6569	-0.1913	-0.2247	0.4361
ss3	**0.8976**	0.5527	0.6172	0.5391	0.6225	-0.2465	-0.2067	0.4572
ss4	**0.9095**	0.5166	0.5956	0.5425	0.6083	-0.2751	-0.2292	0.3995
ss5	**0.8855**	0.5528	0.5259	0.5904	0.6099	-0.2918	-0.1822	0.4518
so1	0.4675	0.4556	0.4549	0.3835	0.4762	-0.0934	-0.0568	**0.9738**
so2	0.4805	0.4683	0.4481	0.3790	0.4835	-0.0925	-0.0340	**0.9844**
so3	0.4856	0.4918	0.4744	0.4023	0.4889	-0.0916	-0.0544	**0.9793**
so4	0.6130	0.5293	**0.9592**	0.4640	0.5365	-0.2286	-0.2736	0.4863
so5	0.6074	0.4986	**0.9695**	0.4757	0.5447	-0.2539	-0.2482	0.4635
so6	0.5407	0.3328	**0.8094**	0.4216	0.4157	-0.2652	-0.2716	0.3096
sc6	-0.2570	-0.1546	-0.2322	-0.3835	-0.2348	**0.8834**	0.3885	-0.0463
sc7	-0.2606	-0.1990	-0.2516	-0.3717	-0.2815	**0.9042**	0.3218	-0.0630
sc8	-0.1993	-0.1320	-0.1790	-0.3466	-0.2087	**0.8772**	0.3332	-0.1135
sc9	-0.1825	-0.1229	-0.2026	-0.3110	-0.1769	**0.8789**	0.2951	-0.0931
sc10	-0.2879	-0.2340	-0.2767	-0.4768	-0.3016	**0.9073**	0.3871	-0.1041
sc11	-0.2807	-0.2210	-0.2689	-0.4321	-0.3113	**0.9175**	0.3926	-0.0887
sc13	-0.0764	-0.1075	-0.1116	-0.0343	-0.0823	0.1782	**0.7253**	0.0272
sc14	-0.1146	-0.1894	-0.1869	-0.2011	-0.1452	0.3042	**0.8117**	-0.0698
sc15	-0.2065	-0.1266	-0.2176	-0.2269	-0.1184	0.3591	**0.7824**	-0.0993
sc16	-0.2385	-0.1407	-0.3073	-0.3046	-0.1798	0.3609	**0.8169**	-0.0404
sc18	-0.1237	-0.1123	-0.1694	-0.1259	-0.0501	0.2609	**0.7313**	0.1098
sc19	-0.2811	-0.2714	-0.2854	-0.3252	-0.2388	0.3497	**0.8472**	-0.0952
aw1	0.4678	0.4389	0.3551	**0.7284**	0.4445	-0.2320	-0.3192	0.1684
aw2	0.5293	0.5235	0.4324	**0.8043**	0.5108	-0.2836	-0.3285	0.2344
aw3	0.5021	0.6001	0.4098	**0.8641**	0.6320	-0.3380	-0.1792	0.4699
aw4	0.5278	0.5767	0.3974	**0.8741**	0.5922	-0.3442	-0.2282	0.4062
aw5	0.5789	0.5185	0.4687	**0.8622**	0.5841	-0.4942	-0.2500	0.2888
aw6	0.5453	0.5738	0.4024	**0.8667**	0.6111	-0.4146	-0.1351	0.4010
aw7	0.5959	0.5251	0.4430	**0.8992**	0.5504	-0.4265	-0.2580	0.3261
aw8	0.4807	0.4682	0.4230	**0.8151**	0.4788	-0.3439	-0.3028	0.2679

데 사용되기 때문이다[38]. 반면에 Cronbach's alpha는 전체 인과모형이 아닌 하나의 잠재개념 내 각각의 측정항목이 동일하게 잠재개념에 기여한다는 전제조건을 가지고 있다[33]. 또한 Cronbach's alpha는 관측변수의 수가 10개에 근접하거나 10개가 넘을 경우 자연적으로 값이 높아지는 경향이 있다[36]. 따라서 두 지표를 종합적으로 살펴보고 신뢰성을 평가하는 것이 적절하다. 본 연구에서 가장 낮은 Cronbach's alpha값이 0.8786이며, CR은 0.9069로 모두 0.7이상의 값을 갖는 것으로 나타났다.

Table 3. Correlation Analysis among Constructs along with Reliability

	Manager Att	Training Effect	Comm Opprt	Importance	Policy Effect	Perc Cost	Vulnerability	Silence Beh
ManagerAtt	**(0.8915)**							
TrainingEffect	0.6205	**(0.8810)**						
CommOpprt	0.6405	0.5071	**(0.9156)**					
Importance	0.6288	0.6318	0.4944	**(0.8408)**				
PolicyEffect	0.6928	**0.8127**	0.5504	0.6623	**(0.8526)**			
PercCost	-0.2783	-0.2032	-0.2666	-0.4392	-0.2880	**(0.8949)**		
Vulerability	-0.2358	-0.2066	-0.2848	-0.2816	-0.1826	0.3988	**(0.7871)**	
SilenceBeh	0.4881	0.4822	0.4691	0.3967	0.4932	-0.0944	-0.0495	**(0.9792)**
AVE	**0.7947**	**0.7761**	**0.8384**	**0.7069**	**0.7270**	**0.8008**	**0.6195**	**0.9588**
Cronbach's α	**0.9354**	**0.9642**	**0.9032**	**0.9413**	**0.9461**	**0.9505**	**0.8786**	**0.9785**
Composite Reliability	**0.9509**	**0.9689**	**0.9393**	**0.9506**	**0.9551**	**0.9602**	**0.9069**	**0.9859**

4.3 측정모형의 타당성 분석

측정모형은 잠재변수와 해당 변수를 측정하는데 사용된 관측변수 간의 관계로 구성된다[24]. 측정모형에 대한 평가는 관측변수의 집중타당성 및 판별타당성에 대한 평가로 구성된다[24]. 집중타당성(convergent validity)이란 둘 이상의 관측변수들이 동일한 잠재변수를 측정하고 있는 수준을 말한다[40]. 집중타당성을 측정하기 위해서 AVE(Average Variance Extracted)이 0.5이상 되어야 한다[36]. AVE란 측정오차(measurement error)에 의한 분산의 양 대비 잠재변수에 의해 설명되는 측정항목 내 분산의 양을 말한다[38,41]. Table 3을 보면 가장 작은 AVE 값이 0.6195로 본 기준을 만족하고 있다. 판별타당성(discriminant validity)은 특정 개념을 측정하는 잠재변수들 간에 차이가 존재하는 정도를 말한다[40]. 각각의 잠재개념으로부터 추출된 AVE의 제곱근 값이 모든 잠재개념의 상관관계 계수를 초과해야 문제가 없다고 판단한다[34,42]. Table 3을 보면 취약성이 0.7871로 보안정책의 효과성과 보안 교육의 효과성 간의 상관관계 계수인 0.8127보다 낮게 나타났으나, 이외의 모든 값들은 상관관계 계수보다 높게 나타나 판별타당성에 큰 문제는 없다고 판단된다. 판별타당성을 평가하는 또 다른 방법은 PLS에 의해 산출된 성분구조 행렬(component structure matrix) 상에서 각각의 항목들이 의도된 잠재개념에 다른 잠재개념에 적재된 값보다 높은 적재값을 가지는 것으로 평가한다[33]. Table 2를 살펴보면 모든 적재값이 의도된 요인에 높게 적재되어 판별타당성에 문제가 없다고 판단된다.

5. 구조모형 검정

본 연구에서는 PLS-SEM(Partial Least Square Structural Equation Modeling) 기법을 활용하여 제안한 연구가설을 검정했다. 본 기법을 활용한 이유는 전통적인 통계 기법인 다중회귀분석과 분산분석보다 나은 장점이 있기 때문이다. 본 기법은 다른 SEM기법과 마찬가지로 측정모형과 구조모형을 동시에 추정이 가능하다. 즉, PLS는 잠재변수의 관측변수에 대한 주성분 분석(PCA)의 반복적 조합과 잠재변수의 구조에 대한 경로분석이 가능하다[33]. 측정모형과 경로분석으로 표현되는 모수에 대한 추정은 OLS(Ordinary Least Squares)를 활용하여 달성된다[33]. 또한 PLS는 모수의 통계적 유의수준을 검정하는데 있어서 다변량 동질성과 데이터에 대한 정규성 기준에서도 자유롭다[28,33,43,44].

본 연구에서는 구조모형 내 각각의 경로 추정치의 유의수준에 대한 t값을 산출하기 위해 bootstrapping 기법(resample=500)을 활용했다. 각 경로에 대응되는 가설들에 대한 판단은 각 경로의 통계적 유의수준과 방향(sign, positive or negative)에 의해 결정된다. 탐색적 연구에서 고려하는 수용할 만한 통계적 수준은 최소 0.5(t-value of 1.960, two-tailed)이다. 분석결과는 Fig. 2와 Table 4와 같다.

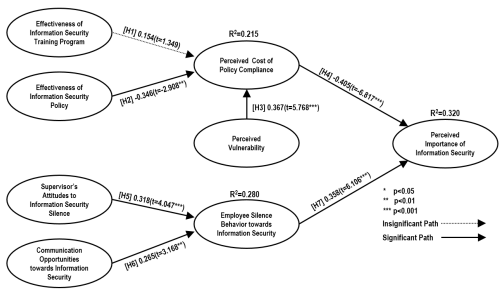

Fig. 2. Results of PLS-SEM Analysis

Table 4. Results of Hypotheses Tests

Hypotheses	Mean	Standard Deviation	Path Coefficient	Standard Error	t Statistics	p value	Results
H1.TrainingEffect → PercCost	0.1539	0.1356	0.1141	0.1141	1.3486	0.1788	Reject
H2.PolicyEffect → PercCost	-0.3460	-0.3352	0.1190	0.1190	2.9077	0.0040	**
H3.Vulnerability → PercCost	0.3674	0.3730	0.0637	0.0637	5.7679	0.0000	***
H4.PercCost → Importance	-0.4054	-0.4094	0.0595	0.0595	6.8170	0.0000	***
H5.ManagerAtt → SilenceBeh	0.3182	0.3191	0.0786	0.0786	4.0469	0.0001	***
H6.CommOpprt → SilenceBeh	0.2653	0.2663	0.0838	0.0838	3.1677	0.0017	**
H7.SilenceBeh → Importance	0.3584	0.3619	0.0587	0.0587	6.1062	0.0000	***
TrainingEffect → Importance	-0.0624	-0.0548	0.0471	0.0471	1.3232	0.1871	-
PolicyEffect → Importance	0.1402	0.1382	0.0548	0.0548	2.5570	0.0112	*
Vulnerability → Importance	-0.1489	-0.1519	0.0305	0.0305	4.8773	0.0000	***
CommOpprt → Importance	0.0951	0.0966	0.0348	0.0348	2.7305	0.0068	**
ManagerAtt → Importance	0.1141	0.1167	0.0381	0.0381	2.9935	0.0031	**

Note. * p<0.05, ** p<0.01, *** p<0.001
ManagerAtt: Supervisor's Attitudes to Information Security Silence, TrainingEffect: Effectiveness of Information Security Training Program, CommOpprt: Communication Opportunities towards Information Security, Importance: Perceived Importance of Information Security, PolicyEffect: Effectiveness of Information Security Policy, PercCost: Perceived Cost of Policy Compliance, Vulnerability: Perceived Vulnerability, SilenceBeh: Employee Silence Behavior towards Information Security

분석결과를 정리하면 다음과 같다. 첫째, 정보보안 교육의 효과성은 정책 준수에 따른 인지된 비용에 통계적으로 유의한 영향을 미치지 못하는 것으로 나타났다(β=0.154, t=1.349). 따라서 가설 1은 기각되었다. 둘째, 정보보안 정책의 효과성은 정책 준수에 따른 인지된 비용에 유의한 영향을 미치는 것으로 나타났다(β=-0.346, t=-2.908, p<0.01). 따라서 가설 2는 지지되었다. 셋째, 인지된 취약성은 정책 준수에 따른 인지된 비용에 유의한 영향을 미치는 것으로 나타났다(β=0.367, t=5.768, p<0.001). 따라서 가설 3은 지지되었다. 넷째, 정책 준수에 따른 인지된 비용은 정보보안에 대한 인지된 중요성에 유의한 영향을 미치는 것으로 나타났다(β=-0.405, t=-6.817, p<0.001). 따라서 가설 4는 지지되었다. 다섯째, 정보보안 침묵에 대한 경영진의 태도는 구성원들의 보안 침묵 행위에 유의한 영향을 미치는 것으로 나타났다(β=0.318, t=4.047, p<0.001). 따라서 가설 5는 지지되었다. 여섯째, 정보보안에 대한 의사소통 기회는 구성원들의 보안 침묵 행위에 유의한 영향을 미치는 것으로 나타났다(β=0.265, t=3.168, p<0.01). 따라서 가설 6은 지지되었다. 마지막으로 구성원들의 보안 침묵 행위는 정보보안에 대한 인지된 중요성에 유의한 영향을 미치는 것으로 나타났다(β=0.358, t=6.106, p<0.001). 따라서 가설 7은 지지되었다.

6. 결론

본 연구는 여전히 사내 보안 사고가 내부인에 의해 발생하고 있는 이유를 조직에서 제공하는 다양한 보안 대책이 사내 정보자원에 대한 중요성을 인식시키지 못했기 때문이라고 판단하고 정보보안에 대한 중요성 인지에 영향을 미치는 요인을 규명하고자 수행되었다.

분석결과 정책 준수에 따른 인지된 비용에 정보보안 교육의 효과성은 유의한 영향을 미치지 않은 반면에 정보보안 정책의 효과성은 통계적으로 부(-)의 영향을 미치는 것으로 나타났다. 이는 여러 가지 해석이 가능한데 첫째, 정보보안 교육이 효과가 없는 것은 조직에서 제공하는 다양한 정보보안 교육이 구성원들의 눈높이에 맞지 않거나, 보안 교육을 업무시간 이외에 받을 수 있는 이러닝 형태가 가장 많았기 때문이라고 생각된다. 설문 조사에서 이러닝으로 보안 교육을 받는다는 사례는 101건으로 가장 많았다. 따라서 퇴근 후 이러닝으로 충실히 교육을 받았을 것으로 보기는 어렵다고 판단된다. 또한 보안 교육이 자주 제공되지 않는 것도 하나의 이유일 수 있다. 설문 결과에 따르면 한 달에 한 번 보안 교육을 받는다는 응답이 75명이었다. 다음으로 1년에 한 번 교육을 받는다는 응답은 63명이었다. 따라서 보안 교육이 정책 준수 비용에 미치는 영향이 없을 것으로 판단된다. 다음으로 정보보안 정책의 효과성은 정책 준수 비용에 통계적으로 유의하게 나타났다. 이 결과는 정보보안 정책은 모든 구성원들이 읽어야 하며 지켜야 하는 정보보안 가이드라인이다. 정책이 효과적이면 사내의 정보 자원이 왜 중요한지를 인식할 수 있기 때문에 정책 준수 비용에 부(-)의 영향을 미치는 결과가 나타났을 것으로 해석된다. 다음으로 인지된 취약성은 정책 준수 비용에 유의한 영향을

미치는 것으로 나타났다. 이는 위험보상이론에서 제시된 바와 같이 사내 시스템이 취약하다고 판단될 경우 구성원들이 보안 정책을 준수하고자 하는 노력은 높아질 것이다. 이 경우 절차 준수로 인해 발생할 수 있는 불편함과 생산성 저하 문제를 더 심각하게 느낄 수 있을 것이다. 반면에 사내 시스템이 취약하지 않다고 느낄 경우 더 위험한 행위 혹은 이탈행위에 몰입하고자 하는 경향이 강해져 정책 준수에 따른 불편함이나 인지적 비용이 감소할 것을 설명해준다. 다음으로 정책 준수 비용은 정보보안에 대한 인지된 중요성에 부(-)의 영향을 미치는 것으로 나타났다. 이러한 결과는 정책을 준수 하는데 있어서 발생하는 절차의 복잡성, 불편함, 비효율성, 생산성 저하는 결국 구성원들이 정보보안에 대해 느끼는 중요성을 감소시킬 수 있다는 것을 의미한다. 정보보안 침묵에 대한 경영진의 태도는 구성원들의 보안 침묵 행위에 긍정적 영향을 미치는 것으로 나타났다. 이는 구성원들이 사내 정보보안에 대해 적극적으로 이야기를 나눌 수 있는 분위기를 조성하고 경영진이 적극적으로 정보보안에 대해 이야기를 나눌려는 솔선수범을 보인다면 구성원들은 정보보안에 대해 이야기를 나누는 것이 용이하고 편하게 정보보안에 대해 언급할 수 있다고 느낀다는 것을 의미한다. 정보보안에 대한 의사소통 기회는 구성원들의 보안 침묵 행위에 긍정적 영향을 미치는 것으로 나타났다. 이 결과는 정보보안에 대해 관리자와 이야기를 나누는 빈도가 높을 경우 구성원들은 정보보안에 대해 관리자나 동료들과 이야기를 나누는 것이 어렵지 않다고 느낄 수 있으며, 편안한 마음으로 정보보안을 언급할 수 있다고 생각한다는 것을 의미한다. 마지막으로 구성원들의 보안 침묵 행위는 정보보안에 대한 인지된 중요성에 정(+)의 영향을 미치는 것으로 나타났다. 이는 구성원들이 사내 관리자나 동료들과 사내 정보보안의 강점이나 취약점에 대해 이야기 하는 것이 용이하고 자유롭게 이야기를 나눌 수 있는 여건이 조성될 경우 사내 정보보안에 대한 중요성을 인식할 가능성이 높아진다는 것을 의미한다.

6.1 시사점

본 연구의 실무적 의의를 제시하면, 구성원들의 사내 정보자원과 사내 정보보안을 중요하다고 느끼게 만들기 위해서는 그들이 정보보안 정책을 준수하는데 발생하는 인지적 비용(절차적 불편함, 복잡성, 생산성과의 충돌)을 감소시키는 노력이 필요하다. 정보보안이 기업을 위해서 필요하다는 점을 강조하는데서 한 발 더 나아가 정보보안 정책을 준수하는데 발생하는 다양한 인지적 비용을 감소시켜야 구성원들이 정보보안의 중요성을 느끼게 만들 수 있을 것이다. 또한 경영진은 정보보안에 대한 중요성을 높이기 위해 정보보안에 대해 구성원들이 동료들과 더 쉽게 이야기를 나눌 수 있는 분위기와 환경을 조성해야 한다. 정보보안에 대해 언급할 수 있는 기회조차 주어지지 않거나 무관심한 환경이 조성된다면 그리고 정보보안 사고에 대해 비밀스럽게 함구하는 것도 결국 정보보안에 대한 중요성을 인식시키는데 장애가 될 수 있다.

본 연구는 이론적으로 다음과 같은 함의가 있다. 본 연구는 정보보안 대책(보안정책, 보안교육)의 효과성을 평가했다는 것이다. 이 전 연구의 경우 조직에서 제공하는 보안 대책의 존재여부만 고려하였을 뿐 조직에서 제공하는 보안 대책이 과연 효과적인가에 대해서는 고려하지 않았다. 단지 조직에서 대책을 수립해서 제공만 한 것이다. 하지만 중요한 것은 조직이 제공하는 다양한 대책이 구성원들이 생각한 것만큼 효과적인가에 대한 것이다. 효과적이지 못한 대책은 불필요한 비용만 발생시킬 뿐 의도된 목표를 달성하는 것은 어렵다. 또한 그동안 이론적 주장만 존재했던 위험보상이론에 근거한 시스템 취약성을 적용했다. 시스템이 취약할 경우 더 위험한 행동을 취할 수 있다는 위험보상이론의 가정을 적용하여 그 주장이 실증적으로 정보보안 관점에서도 적용이 가능하다는 것을 규명했다. 마지막으로 정보보안 측면에서 조직 침묵 이론을 적용했고, 실증적 분석에서 정보보안에 대한 구성원들의 침묵행위가 결국 정보보안에 유의한 영향을 미칠 수 있다는 것을 규명했다.

6.2 한계점

본 연구는 다음과 같은 한계점이 존재한다. 첫째, 수집된 데이터에 대한 공통방법편의 검정을 수행하긴 하였으나, 응답자로 하여금 선행변수와 결과변수를 특정한 시점에 동시에 응답하도록 하였기 때문에 공통방법편의로부터 완전히 자유롭다고 보기 어렵다. 둘째, Soomro et al.(2016)에 따르면 산업 유형, 조직의 규모, 조직의 구조와 같은 조직적 요인이 정보보안 구현에 강력한 영향을 미친다. 즉 조직의 일반적 특성에 따른 차이가 존재할 수 있으나 본 연구에서는 이를 고려하지 않았다. 따라서 이러한 요인에 대한 고려가 향후 연구에서 이루어져야 한다. 셋째, Goel and Chengalur-Smith(2010)의 연구에서

는 정보보안 정책의 효과성이 4개로 구분되었다. 하지만 본 연구에서는 하나의 요인으로 수렴되었다. 그 이유에 대한 논의가 필요함에도 불구하고 본 연구에서는 하나로 수렴된 것이 연구의 궁극적 목적이 아니기 때문에 이를 논의하거나 규명하지는 않았다. 추후 연구에서는 정보보안 정책이 수렴되는 경우 그리고 구분되는 경우를 구분하여 그 이유를 규명하는 것도 의미가 있다고 판단된다.

REFERENCES

[1] Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005), Analysis of End User Security Behaviors, *Computers & Security*, 24(2), 124-133.

[2] Liang, H., & Xue, Y. (2010), Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective, *Journal of the Association for Information Systems*, 11(7), 394-413.

[3] Safa, N. S., Von Solms, R., & Furnell, S. (2016), Information Security Policy Compliance Model in Organizations, *Computers & Security*, 56, 1-13.

[4] Bulgurcu, B., Cavusoglu, H., & Banbasat, I. (2010), Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, 34(3), 523-548.

[5] Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013), Future Directions for Behavioral Information Security Research, *Computers & Security*, 32, 90-101.

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

[7] Ifinedo, P. (2012), Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory, *Computers & Security*, 31, 83-95.

[8] Goel, S., & Chengalur-Smith, I., (2010), Metrics for Characterizing the Form of Security Policies, *Journal of Strategic Information Systems*, 19(4), 281-295.

[9] Van Dyne, L., Ang, S., & Botero, I. C. (2003), Conceptualizing Employee Silence and Employee Voice as Multidimensional Constructs, *Journal of Management Studies*, 40(6), 1359-1392.

[10] Pinder, C. C., & Harlos, K. P. 2001, Employee Silence: Quiescence and Acquiescence as Responses to Perceived Injustice. In Rowland, K. M., & Rerris, G. R. (eds), *Research in Personnel and Human Resources Management*, 20, New York: JAI Press, 331-369.

[11] Morrison, E. W., & Milliken, F. J. (2000), Organizational Silence: A Barrier to Change and Development in a Pluralistic World, *Academy of Management Review*, 25, 706-725.

[12] Soomro, Z. A., Shah, M. H., & Ahmed, J. 2016, Information Security Management Needs More Holistic Approach: A Literature Review, International Journal of Information Management, Vol. 36, pp. 215-225.

[13] Knapp, K. J., & Ferrante, C. J. (2012), Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations, *Journal of Management Policy and Practice*, 13(5), 66-80.

[14] Puhakainen, P., & Siponen, M. (2010), Improving Employees' Compliance through Information Systems Security Training: An Action Research Study, *MIS Quarterly*, 34(4), 757-778.

[15] Mishra, S., & Chasalow, L. (2011), Information Security Effectiveness: A Research Framework, *Issues in Information Systems*, 12(1), 246-255.

[16] Stewart, A. (2004), On Risk: Perception and Direction, *Computers & Security*, 23, 362-370.

[17] Zhang, J., Reithel, B. J., & Li, H. (2009), Impact of Perceived Technical Protection on Security Behaviors, *Information Management & Computer Security*, 17(4), 330-340.

[18] Gopal, R. D., & Sanders, G. L. (1997), Preventative and Deterrent Controls for Software Piracy, *Journal of Management Information Systems*, 13(4), 29-47.

[19] Wiant, T. L. (2003), *Policy and its Impact on Medical Record Security*, Unpublished Doctoral Dissertation, University of Kentucky, Lexington.

[20] Foltz, C. B. (2000), *The Impact of Deterrent Countermeasures upon Individual Intent to Commit Misuse: A Behavioral Approach*, Unpublished Doctoral Dissertation, University of Arkansas, Fayetteville.

[21] Harrington, S. J. (1996), The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions, *MIS Quarterly*, 20(3), 257-278.

[22] Lee, S. M., Lee, S. -G., & Yoo, S. (2004), An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories, *Information and Management*, 41(6), 707-718.

[23] Knapp, K. J., Marshall, T. E., Rainer, Jr., R. K., & Ford, F. N. (2007), Information Security Effectiveness: Conceptualization and Validation of a Theory,

International Journal of Information Security and Privacy, 1(2), 37-60.

[24] 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).

[25] Siponen, M. T. (2000), A Conceptual Foundation for Organizational Information Security Awareness, *Information Management & Computer Security*, 8(1), 31-41.

[26] Vakola, M., & Bouradas, D., (2005), Antecedents and Consequences of Organisational Silence: An Empirical Investigation, *Employee Relations*, 27(5), 441-458.

[27] Vroom, C., & von Solms, R. (2004), Towards Information Security Behavioural Compliance, *Computer & Security*, 23, 191-198.

[28] Kankanhalli, H., 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.

[29] Leonard, L. N. K., Cronan, T. P., & Kreie, J. (2004), What Influences IT Ethical Behavior Intentions-Planned Behavior, Reasoned Action, Perceived Importance, or Individual Characteristics?, *Information & Management*, 42, 143-158.

[30] Churchill, G. A. (1979), A Paradigm for Developing Better Measures of Marketing Constructs, *Journal of Marketing*, 9(4), 168-178.

[31] Moore, G. C., & Benbasat, I. (1991), Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation, *Information Systems Research*, 2(3), 192-222.

[32] Workman, M., Bommer, W. H., & Straub, D. (2008), Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test, *Computers in Human Behavior*, 24(6), 2799-2816.

[33] Barclay, D., Higgins, C., & Thompson, R. (1995), The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration, *Technology Studies*, 2(2), 285-309.

[34] Gefen, D., & Straub, D. (2005), A Practical Guide to Factorial Validity Using PLS-graph: Tutorial and Annotated Example, *Communications of the AIS*, 16(5), 91-109.

[35] Chin, W. W., & Sambamurthy, V. (1994), The Effects of Group Attitudes toward Alternative GDSS Designs on the Decision-Making Performance of Computer-Supported Groups, *Decision Sciences*, 25(2), 215-241.

[36] Hair, J. F., Black, B., Babin, B., & Anderson, R. E. (2010), *Multivariate Data Analysis*, 7th eds., Upper Saddle River, NJ, PrenticeHall.

[37 Cronbach, L. J. (1951), Coefficient Alpha and the Internal Structure of Tests, *Psychometrika*, 16, 297-334.

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

[39] Nunnally, J. C. 1978, Psychometric Theory, New York, NY: McGraw-Hill.

[40] Cook, T. D., & Campbell, D. T. (1979), *Quasi-Experimentation: Design and Analysis Issues for Field Setting*, Boston, MA: Houghton Mifflin.

[41] Grant, R. A. (1989), Building and Testing a Causal Model of an Information Technology's Impact, *Proceedings of the Ten International Conference on Information Systems*, December 4-6, Boston, MA, 173-184.

[42] Fornell, C. (1982), *A Second Generation of Multivariate Analysis: Methods*, 1, New York, NY: Praeger.

[43] Chin, W. W. (1998), Issues and Opinion on Structural Equation Modeling, *MIS Quarterly*, 22(1), vii-xvi.

[44] Gefen, D., Straub, D. W., & Boudreau, M. C. (2000), Structural Equation Modeling and Regression: Guidelines for Research Practice, *Communications of the AIS*, 4, 1-77.

임 명 성(Yim, Myung-Seong) [정회원]

- 2002년 2월 : 삼육대학교 경영정보학과(경영학사)
- 2004년 2월 : 한국외국어대학교 경영정보 대학원(MS)
- 2011년 8월 : 서강대학교 경영전문대학원(Ph.D)
- 2011년 8월 ~ 2012년 2월 : 서강대학교 경영대학 대우교수
- 2012년 3월 ~ 현재 : 삼육대학교 경영학과 부교수
- 관심분야 : 정보보안, 서비스 시스템, 테크노 스트레스
- E-Mail : msyim@syu.ac.kr