Journal of Korea Society of Industrial Information Systems Vol.29 No.5, Oct. 2024 :69-94
http://dx.doi.org/10.9723/jksiis.2024.29.5.069 ISSN:1229-3741

조직구성원의 보안정책 수용성 향상에 관한 연구: 건강신념모델을 바탕으로+

(A Study on Improving the Acceptability of Security Policies among Organizational Members: Based on the Health Belief Model)

김 보 영[1], 서 우 종[2]*
(Boyoung Kim and Woojong Suh)

요 약 조직의 보안정책 준수성과를 향상시키기 위해서는 조직구성원들이 보안정책을 적극적으로 수용하려는 의도가 중요하다. 이에 따라, 본 연구에서는 조직구성원들의 보안정책 수용성을 향상시킬 수 있는 방안들을 모색하기 위해 건강심리 분야의 주요 이론인 건강신념모델을 기반으로 연구모형을 개발하였다. 본 연구에서는 설문을 통해 데이터를 수집하였으며, 통계적 기법을 사용하여 데이터를 분석하였다. 그 결과, 본 연구는 조직구성원이 지각하는 보안 위협과 보안정책 준수에 대한 조직의 지원이 보안정책 준수를 통해 얻을 수 있는 이점에 대한 인식(지각된 이익)의 매개역할을 통해 보안정책 수용성에 유의적인 영향을 미친다는 점을 규명할 수 있었다. 또한, 본 연구는 보안정책 준수과정에서 겪게 될 노력 및 업무 지장에 대한 부담감(지각된 장애)이 보안정책 수용성에 유의적으로 부정적인 영향을 미친다는 점도 입증할 수 있었다. 본 연구는 의료보건에 뿌리를 두고 있는 건강신념모델을 적용하여 조직구성원들의 보안정책 수용성에 영향을 미치는 인지적 메커니즘을 효과적으로 분석할 수 있는 모형을 제시했다는 점에서 학술적 의의가 있다. 본 연구에서 논의된 분석 결과와 다양한 시사점들은 향후 조직구성원들의 보안정책 수용성을 높이기 위한 전략을 수립하는 데 유용한 정보와 통찰을 제공할 수 있을 것으로 기대된다.

핵심주제어: 보안정책, 보안정책 수용성, 건강신념모델

Abstract In order to improve the security policy compliance performance of an organization, it is crucial for organizational members to have a strong intention to actively accept these policies. Accordingly, this study proposes a research model based on the Health Belief Model, a key theory in the field of health psychology, with the aim of seeking ways to enhance the acceptability of security policies among organizational members. Data were collected through surveys and analyzed

* Corresponding Author: wjsuh@inha.ac.kr
+ 이 논문은 2022년 대한민국 교육부와 한국연구재단의 지원에 의해 연구되었음(NRF-2022S1A5C2A03093690).
+ 이 논문은 인하대학교의 지원에 의하여 연구되었음.

Manuscript received September 02, 2024 / revised September 29, 2024 / accepted September 30, 2024
1) 인하대학교 대학원 산업보안거버넌스전공, 제1저자
2) 인하대학교 경영학과, 교신저자

using statistical methods. The results of the study revealed that the perceived security threats and the perception of support for security policy compliance at the organizational level significantly influence the acceptance of security policies through the mediating role of perceived benefits from security policy compliance. Additionally, the study demonstrated that the perceived burden of effort and work disruption associated with complying with security policies, i.e., perceived barriers, has a significant negative impact on the acceptance of security policies. This study holds academic significance as it presents a model that effectively analyzes the cognitive mechanisms influencing the acceptance of security policies by applying the Health Belief Model, originally rooted in healthcare. The analysis results and various implications discussed in this study are expected to provide useful information and insights for developing strategies to enhance the acceptance of security policies among organizational members in the future.

Keywords: Security Policy, Security Policy Acceptability, Health Belief Model

1. 서 론

보안에 대한 기업의 투자가 증가하고 있음에도 불구하고, 기업에서 첨단 산업기술이 유출되는 보안사고는 꾸준히 발생하고 있으며, 기업들은 이로 인해 경제적으로 막대한 손실을 입고 있는 것으로 보도되고 있다(Hwang and Hu, 2021; Etnews, 2023; Hankyung, 2023). 이러한 보안사고의 주요 원인으로는 조직 내부자의 무지, 부주의, 악의적 의도가 중요한 원인으로 분석되고 있으며(GTT Korea, 2024), 특히 악의적 의도를 가진 산업 스파이는 91%가 조직 내부자인 것으로 보고된 바 있다(Boannews, 2023). 게다가 오늘날 기업 간 경쟁이 더욱 치열해지는 상황 속에서 직원들의 이직과 연계된 기존 근무지의 핵심기술 유출 사고도 증가하는 추세를 보이고 있다(Kim et al., 2017).

이처럼 보안사고의 주체는 전·현직 직원이 대다수이기 때문에, 보안사고를 예방하기 위해서는 내부 조직구성원들의 보안정책에 대한 수용성과 실천 의도를 높이기 위한 노력이 중요하다. 가트너(Gartner)의 사이버보안 전망 보고서에 따르면, 업무 중 자신의 행동이 보안 리스크를 증가시킬 수 있음을 인지했음에도 그 행동을 멈추지 않은 직원이 90% 이상인 것으로 조사되었다(ITBizNews, 2023). 또한, 이 보고서는 이러한 현상을 방지하기 위해서는 강력한 보안 솔루션의 도입과 보안정책 수립도 중요하지만, 이러한 조치들이 조직구성원들에게 효과적으로 수용될 수 있는 방안을 마련하는 것도 중요하게 고려해야 한다는 점을 지적하고 있다(ITBizNews, 2023). 조직구성원이 조직의 보안정책을 수용하고 이를 준수하는 것은 장기적 관점에서 조직의 보안 수준을 향상시키는 데 필수적으로 요구되는 사항이다. 그런데 보안정책 수립자와 수용자 간에는 정책을 바라보는 시각이나 이해에 차이가 있을 수 있다(Yim, 2013). 따라서 성공적인 보안정책 수립과 운용을 위해서는 정책 사용자 관점에 충실한 접근이 필요하다.

본 연구에서는 이러한 정책 사용자 관점을 수용성(acceptability)의 개념으로 대변하고자 한다. 수용성이란 어떤 대상의 내적, 외적 가치를 마음속으로 받아들이는 태도나 인식의 정도라 할 수 있다(Lee et al., 2014). 보안정책 수용성은 자신이 속한 조직의 보안정책 내용에 동의하고 이를 따르려는 의도라 할 수 있다. 즉, 보안정책 수용성은 조직구성원이 정책에 따라 행동하기 이전에 정책에 대해 얼마나 긍정적으로 평가하는지 그리고 이를 실천하려는 의도가 얼마나 있는지를 복합적으로 설명해주는 심리적 요인이라 할 수 있다. 조직에서 보안정책의 구현은 조직구성원의 보안정책에 대한 수용으로부터 시작된다. 따라서 조직이 보안정책을 효과적으로 구현하기 위해서는 조직구성원들의 보안정책

수용성을 향상시키기 위한 노력이 중요하다.

이러한 맥락에서, 본 연구에서는 조직구성원들의 보안정책 수용성을 높일 수 있는 방안을 모색해보고자 한다. 이를 위해 본 연구에서는 우선, 보안정책 수용성에 영향을 미치는 요인들을 식별하고 이 요인들이 보안정책 수용성에 영향을 미치는 메커니즘을 규명해보고자 한다. 이러한 요인들을 식별하기 위해 본 연구에서는 의료보건 분야에서 사용되어 온 건강신념모델(Health Belief Model)을 이론적 기반으로 활용하고자 한다. 건강신념모델은 사람들의 질병예방 행위에 영향을 미치는 심리적 요인들을 통해 사람들의 질병예방 행위에 대한 수용 및 거부 심리를 이해할 수 있도록 해줌으로써 질병예방 방안을 효과적으로 모색하는 데 유용하게 활용되어 온 모델이다(Jo and Han, 2020). 이 모델은 질병이라는 부정적 결과를 대상으로 이를 예방하기 위한 목적으로 활용된다는 점에서, 보안사고라는 부정적 결과를 대상으로 이를 예방하기 위한 목적을 가지는 본 연구의 관점과 논리적으로 잘 부합한다.

또한, 본 연구에서는 보안정책 수용성과 이것에 영향을 미치는 요인들 사이에 존재하는 메커니즘을 보다 깊이 있게 분석하기 위해, 건강신념모델에서는 단순히 상호 독립적인 관계로 다루어졌던 영향 요인들 간의 관계에 대해 인과관계의 가능성 고찰하고 검증하기 위한 시도를 해보고자 한다. 이와 더불어, 본 연구에서는, 건강신념모델에서 제시하고 있는 영향 요인들 외에도, 보안정책 준수에 대한 조직의 지원이 보안정책 수용성에 미치는 영향도 추가적으로 규명해보고자 한다. 이는 조직차원의 지원이라는 긍정적 측면의 요인을 건강신념모델에서 가져온 부정적 측면의 요인과 함께 다룸으로써, 보안정책 수용성을 높일 수 있는 방안을 긍정과 부정적 측면으로 보다 다양하게 모색하기 위함이다. 본 연구의 분석결과와 이를 바탕으로 논의되는 시사점들은 향후 조직구성원들의 보안정책 수용성을 높이기 위한 전략을 수립하는 데 유용한 정보와 통찰을 제공할 수 있을 것으로 기대된다.

2. 이론적 배경

2.1 건강신념모델과 보안연구

건강신념모델(Health Belief Model)은 1950년대 미국에서 사람들이 질병예방이나 무증상 질병의 조기 발견을 위한 검진을 받아들이지 않는 현상을 이해하기 위한 연구를 통해 개발되었는데(Janz and Becker, 1984), 이 모델은 개인이 질병을 예방하기 위한 행동을 하게 되는 이유가 바로 자신이 질병에 걸릴 가능성이 있으며 질병에 걸리는 경우 자신의 삶이 부정적인 영향을 받게 될 것이라는 인식 때문이라는 점을 강조하고 있다(Rosenstock, 1974). 즉, 사람들이 질병예방 행위를 적극적으로 하도록 만들기 위해서는 질병에 걸릴 가능성과 질병으로 인한 부정적인 영향을 인식하도록 만드는 것이 중요하다는 지침을 주는 이론이라 할 수 있다.

건강신념모델은 Fig. 1에서 볼 수 있듯이, 질병예방 행위에 영향을 미치는 요인들은 크게 지각된 위협(perceived threat)과 행위 평가(behavioral evaluation)로 구분된다(Janz and Becker, 1984; Lee et al., 2008; Jo and Han, 2020). 지각된 위협은 자신이 질병에 걸릴 가능성에 대해 가지는 두려운 감정을 의미하며, 구체적으로 지각된 심각성(perceived severity)과 지각된 민감성(perceived susceptibility)으로 구성된다. 지각된 심각성은 특정 질병으로부터 직접적으로 입을 수 있는 피해의 심각성을 의미한다(Lee et al., 2008; Ng et al., 2009). 이러한 심각성에는 의학적 결과뿐만 아니라 사회적 관계에 대한 피해까지도 고려될 필요가 있다(Jo and Han, 2020). 지각된 민감성은 특정 질병에 대하여 자신이 얼마나 노출되어 있으며 나아가 그 질병에 걸릴 가능성이 얼마나 있는지에 대한 개인의 인식을 의미한다(Rosenstock, 2005; Lee et al., 2008).

한편, 행위 평가는 질병예방 행위로 인해 초래될 수 있는 결과에 대한 평가를 의미하며(Lee et al., 2008; Ng et al., 2009), 구체적으로 지각된 장애(perceived barriers)와 지각된 이익(perceived benefits)으로 구성된다(Jo and Han, 2020). 지

각된 장애는 질병예방 행위를 수행함으로써 초래될 수 있는 고통이나 불편함 또는 비용이 발생할 수 있다는 인식을 의미한다(Rosenstock, 2005). 지각된 이익은 질병예방 행위를 수행함으로써 심각성과 민감성 같은 위협 요인을 감소시킬 수 있을 것이라는 기대를 의미한다(Ng et al., 2009; Jo and Han, 2020).

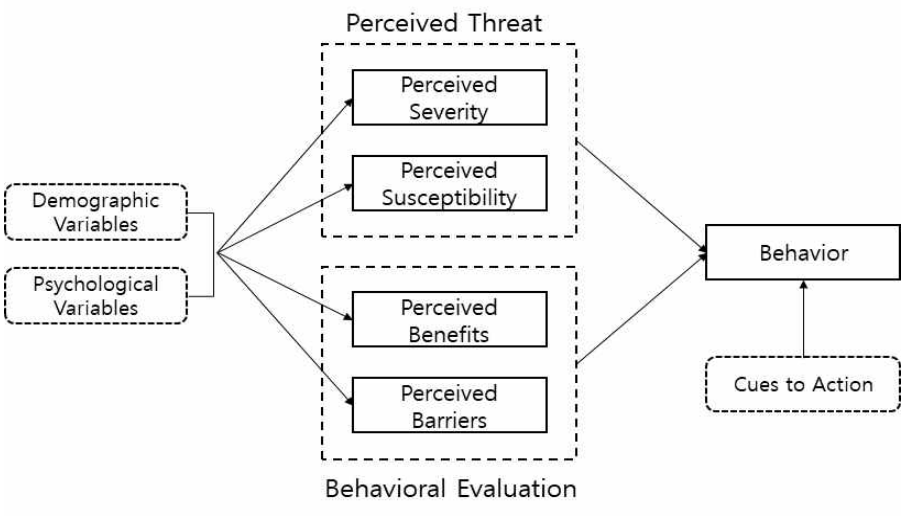


Fig. 1 Health Belief Model

건강신념모델은 사람들이 위협을 인지하게 될 때 그 위협에서 벗어날 수 있는 방법을 찾고, 찾은 방법이 자신을 보호할 수 있다고 판단이 되면, 그 방법을 행위로 옮기는 일련의 과정을 설명해준다(Jee et al., 2011). 이러한 과정은 일반적으로 사람들이 위협을 지각했을 때 본인을 보호하려고 하는 인간의 기본 심리에 기반하고 있다(Ng et al., 2009; Jee et al., 2011). 이러한 이유로 건강신념모델은 의료보건 분야 외에도 커뮤니케이션, 심리학, 경영학 등 인간의 심리에 관심을 가지는 다양한 분야들에서 활용되어 왔다(Jo and Han, 2020).

특히, 건강신념모델은 보안 분야에서도 사용되어 왔는데, 이는 질병 관련 상황이 보안 관련 상황과 일맥상통한다는 점이 많기 때문이다. 예를 들어, Ng et al.(2009)에서는 질병의 발생이 신체의 정상적인 기능을 방해하는 것과 보안사고의 발생이 정보시스템, 조직, 개인의 기능을 방해하는 것이 유사하다고 주장한 바 있다. 또한 Cho et al.(2014)은 개인이 질병을 인지하고 이를 예방하기 위한 행위를 하는 것은 기업이 보안 위험을 인지하고 이를 예방하기 위해 정보보안 행위를 하는 것에 대응된다고 주장한 바 있다. 이러한 맥락에서, 집에서 사용하는 컴퓨터의 보안(Johnson, 2012), 소셜 게임 이용자에 대한 보안관리 행동(Ahn et al., 2016), 보안준수의도(Jung et al., 2016) 등과 같은 보안 주제의 연구들이 건강신념모델을 활용한 바 있다.

이러한 배경에서, 본 연구도 건강신념모델을 기반 이론으로 연구모델을 개발하고 분석하였다. 본 연구에서는 보안정책 수용성과 이것에 영향을 미치는 심리적 요인들에 초점을 두고 있다. 이에 따라, 건강신념모델에 포함된 변인들 중 성별, 연령 등을 나타내는 인구통계적 변인(demographic variables)과 개인의 성격 등을 나타내는 심리학적 변인(psychological variables) 그리고 질병예방 행위에 직접 영향을 미치는 외부의 자극을 나타내는 행위단서(cues to action) 변인은 본 연구의 범위 밖이라 판단되어 적용하지 않았다.

2.2 보안정책 수용성

보안정책이란 조직의 정보, 기술, 영업비밀이 유출되지 않도록 보호하기 위한 조직구성원의 역할과 책임을 문서로 명시한 것으로서, 조직 내

정보보안 임무를 수행하는 데 필수적으로 요구되는 요소이다(Kim and Kang, 2008; Bulgurcu et al., 2010; Soh and Kim, 2017). 보안정책은 기업 내부의 보안규정과 규칙 그리고 보안기준에 대한 전반적인 사항들이 명시되어 있어야 하고, 조직구성원들 전체에게 전달되어야 한다(Kang and Chang, 2014). 이러한 보안정책의 조직에 대한 기여도를 극대화하기 위해서는 보안정책에 조직의 목표와 특성 그리고 조직의 비즈니스 및 환경적 특성들이 잘 반영될 수 있도록 노력할 필요가 있다(Kim and Jeon, 2006; Kang and Chang, 2014; Cho et al., 2014).

보안정책의 성공여부는 궁극적으로 정책 사용자인 조직구성원들이 보안정책을 실질적으로 실천하는지에 달려있다(Yim, 2013). 조직구성원들의 보안정책에 따른 행위는 보안정책에 대한 수용으로부터 시작된다(Kim and Jeon, 2006; Kang and Chang, 2014). 그러나, 일반적으로 보안정책 수립자와 수용자가 정책에 대해 서로 다른 시각을 가지고 있으며 보안정책 수립 과정에서 정책 수용자들의 의견이 반영되는 절차가 확립되어 있지 않아, 보안정책은 수용자의 입장과 상황을 충분히 이해하지 못한 상태에서 작성되는 경향이 있다(Yim, 2013). 또한, 조직구성원들 간의 보안에 대한 인식 차이로 인해, 어떤 특정 보안정책 사항에 대해서 서로 다르게 해석을 하는 일이 발생하기도 한다(Yim, 2013). 이러한 점들로 인해 조직구성원의 보안정책 수용성은 조직의 기대에 못 미칠 수 있으며, 또한 조직구성원들 간에 상당한 격차가 존재할 수도 있다.

이러한 상황을 고려할 때, 조직이 보안정책의 효과를 증진시키기 위해서는 조직구성원들이 보안정책에 대해 가지는 수용성에 관심을 가질 필요가 있다. 수용성(acceptability)이란 어떤 대상의 내적, 외적 가치를 마음속으로 받아들이는 태도나 인식의 정도로 정의할 수 있다(Lee et al., 2014). 여기서 마음으로 받아들인다는 것은 단순히 대상에 대한 평가를 넘어서 정책을 준수할 의도까지 내포한 인식으로 볼 수 있다. 개인은 특정 정책이 자신의 신념과 일치할 때 그 정책을 지지하고 수용하고자 하는 태도를 가지게 되지만, 그 반대의 경우에는 정책에 저항하는 태도를 보인다(Jang and Sung, 2022). 여기에서 '태도'라는 표현에는 정책에 대한 판단뿐만 아니라 정책에 대한 지지나 준수 의도도 내포된 것으로 해석할 수 있다. 일반적으로 태도는 대상에 대한 긍정적 또는 부정적 평가나 판단을 의미하고(Douglass, 1977), 의도는 태도가 행동으로 옮겨질 가능성 또는 해당 대상을 사용하고자 하는 의지를 의미한다(Kim and Lee, 2017).

이러한 점을 고려할 때 수용성의 개념은 개인이 특정 정책에 대해 긍정적으로 평가하고(태도), 이를 실제 행위로 옮기려는 의도가 복합된 개념으로 볼 수 있다. 공공기관 구성원들의 제도 변화 수용성에 대해 연구한 Lee and Kwon (2011)에서도 수용성의 개념을 대상 집단이 주어진 제도의 변화를 얼마나 긍정적으로 평가하고 얼마나 행동으로 따르려는 의도를 보이는가의 문제로 정의하였다. 또한 공무원의 정책수용 요인을 연구한 Sung(2013)에서도 정책수용을 정책 대상자가 지속적인 준수의도를 가지고 정책에 대한 긍정적인 평가와 적극적 지지를 보이는 내적 심리상태라고 정의하였다. 이와 같은 연구들에 볼 수 있듯이, 수용성의 개념은 태도와 의도가 결합된 개념으로서, 정책 관련 연구 분야에서 주요한 연구 변인으로 활용되어 왔음을 알 수 있다.

이러한 맥락에서, 본 연구에서는 보안정책 수용성의 개념을 '자신이 속한 조직의 보안정책 내용에 대한 태도 및 이를 따르려는 의도'로 정의하고자 한다. 조직구성원들은 일반적으로 조직에서 제시한 보안정책의 내용에 대한 평가를 통해 긍정적 또는 부정적 인식을 가지게 되는데, 이는 태도의 개념과 대응될 수 있다. 또한 이와 동시에 조직구성원들은 태도를 바탕으로 조직의 보안정책을 실질적으로 준수하려는 의지도 가지게 되는데, 이는 의도의 개념과 대응될 수 있다. 이러한 의도는 태도가 밀접하게 반영된 심리적 상태로서 결국 보안준수 행위의 실행 여부를 결정짓는 데 있어 직접적인 역할을 한다는 점에서, 본 연구에서는 보안정책 준수행위라는 최종 변인에 대해 태도와 의도가 복합한 수용성이라는 하나의 변인으로 접근하고자 한다.

2.3 보안정책 준수행위

보안정책 준수행위란 조직이 주요한 정보 및 기술 자원을 보안사고로부터 보호하기 위해 보안정책을 통해 조직구성원들에게 요구하는 행위를 의미한다(Guo, 2013). 보안정책 준수행위들은 보안사고에 대한 예방 단계와 발생 이후의 단계를 구분해서 고려될 수 있으며(Guo, 2013), 이러한 행위들은 조직의 보안 수준을 결정하는 데 직접적인 영향을 미친다(Kim et al., 2016).

따라서, 조직이 성공적인 보안성과를 거두기 위해서는 실질적으로 보안정책에 따른 구체적인 행위들이 효과적으로 이루어져야 한다(Kim and Song, 2011). 이를 위해서는 보안사고 예방 및 대응을 위한 구체적인 방안들이 보안정책에서 제시되어야 한다(Lim, 2006). 조직이 보안사고를 줄이기 위해 여러 가지 측면에서 나름대로 노력을 해오고 있지만, 서론에서도 논의했듯이, 조직구성원의 보안에 대한 태도와 행위를 성공적으로 통제하고 있다고 평가하기는 어려울 것으로 사료된다. 따라서 조직은 조직구성원들이 보안정책에 대한 필요성을 느끼고 긍정적인 태도를 가지도록 만드는 것은 물론이고, 궁극적으로 보안정책을 행위로 옮기도록 지속적인 관심과 노력을 기울일 필요가 있다(Heo and Ahn, 2020). 이러한 맥락에서 본 연구는 보안정책 준수행위의 성과를 높이기 위한 주요 요인으로 보안정책 수용성에 주목하고 있다. 즉, 본 연구에서는 보안정책 수용성을 높일 수 있는 방안들을 모색하고 이를 통해 궁극적으로 보안정책 준수행위의 성과를 향상시키는 데 기여하고자 한다.

2.4 보안정책 준수지원

조직의 성과는 결국 조직구성원들의 행위를 통해 창출되므로 조직은 조직구성원들의 행위에 대한 노력을 중요하게 인식하고 지원할 필요가 있다. 이러한 맥락에서 조직구성원들은 조직이 자신들의 노력에 얼마나 관심을 가지고 있으며 이를 얼마나 존중해주는지에 대해 높은 관심을 가지고 있다(Lee, 2010). 이는 조직의 지원이 조직구성원들의 동기부여에 유의적인 영향을 미칠 수 있음을 시사한다. 조직지원은 다양한 측면에서 이루어질 수 있는데, 대표적인 예로는 교육훈련의 기회를 제공하거나 조직구성원들의 노력에 대한 보상제도를 운영하는 것을 들 수 있다(Kwon and Shin, 2006).

조직이 조직구성원들의 보안정책 준수를 지원하기 위한 노력으로는 우선, 조직구성원들이 보안정책 준수에 대한 가치를 이해하고 적극적으로 보안정책을 실천하도록 유도하는 환경조성을 들 수 있다(Kruger and Kearney, 2006). 조직구성원들은 자신의 보안 인식을 향상시키기 위해 충분한 시간과 노력을 투자하는 것을 꺼리는 경향이 있다(Kruger and Kearney, 2006). 따라서 조직은 이러한 조직구성원들이 보안정책 준수에 대해, 보다 긍정적인 인식을 가지고 보안정책 준수 활동에 적극적으로 참여할 수 있도록 다양한 조직차원의 지원 방안들을 마련할 필요가 있다.

대표적인 조직지원 방안으로는 보안정책에 대한 교육훈련을 고려할 수 있다. 보안정책에 대한 교육훈련은 보안사고로 인한 조직의 피해를 방지하기 위해서 제공하는 것이기 때문에, 조직구성원들에게 교육훈련 참여 및 지식 획득에 대한 책임을 부여할 필요가 있다(Kim and Kim, 2003). 또한, 일반적으로 교육훈련의 궁극적인 성과를 위해서는 교육훈련을 통해 습득한 지식을 실제 업무에 적용할 수 있는 환경을 조성하기 위한 노력도 필요하다(Yang and Chung, 2006). 보안정책에 대한 교육훈련과 관련해서는, 교육훈련 과정에서 배운 보안정책 절차나 정보 또는 도구와 같은 것들을 실제 업무 상황에서 상시적으로 제공할 필요가 있다. 이러한 보안정책에 대한 조직지원은 조직구성원들의 보안정책 수용성에 영향을 미칠 수 있는 주요한 요인으로 사료된다. 본 연구에서는 이러한 관계를 실증적으로 규명하고 유용한 시사점들을 도출해보고자 한다.

3. 연구모형 및 가설

3.1 연구모형

본 연구는 건강신념모델의 변수들을 중심으로 보안정책 수용성을 높일 수 있는 방안을 모색하는 것을 목적으로 하고 있다. 이를 효과적으로 수행하기 위해 본 연구는 보안정책 수용성에 영향을 미치는 변수들을 부정적 측면과 긍정적 측면이 대비되도록 구성하였다. 이러한 맥락에서 Fig. 2의 연구모형에서 볼 수 있듯이, 보안 위협(지각된 위협 변수)이라는 부정적 측면과 대비하여 조직차원의 지원(보안정책 준수지원 변수)이라는 긍정적 변수에도 초점을 두었다. 지각된 위협은 원래 건강신념모델에서 지각된 심각성과 지각된 민감성으로 세분화되어 있었지만, 이 두 변수 모두 부정적 측면의 변수들이므로, 본 연구에서는 긍정적 측면의 조직지원 변수와의 효과적인 대비를 위해, 이 두 변수들의 상위변수인 지각된 위협을 사용하였다.

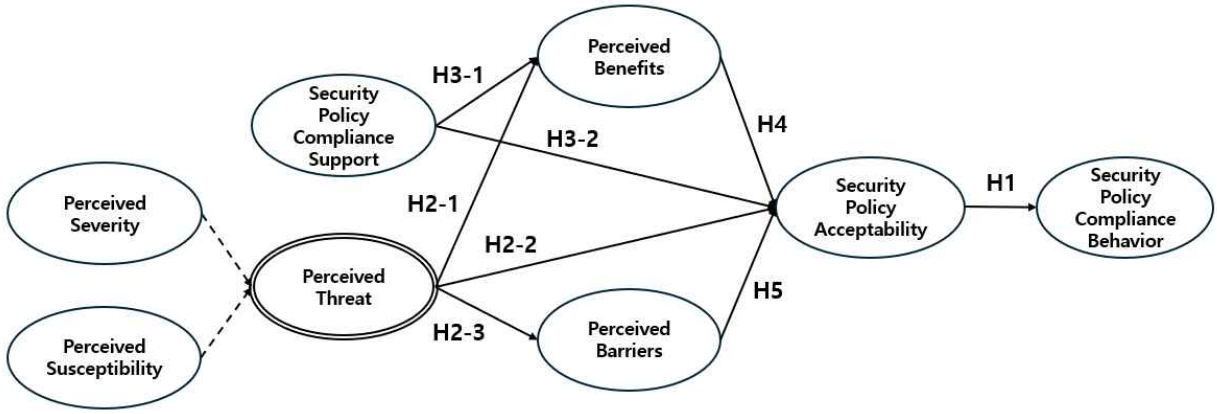


Fig. 2 Research Model

반면, 건강신념모델에서 질병예방에 대한 행위 평가 변수를 구성하고 있는 지각된 이익과 지각된 장애와 같은 구성 변수들은 각기 긍정과 부정의 상반된 측면들을 반영하고 있어서, 통합을 고려할 필요가 없었다. 이와 같은 행위 평가의 구성 변수들이 가지는 긍정과 부정의 상반된 측면들은 보안정책 수용성 증진을 위한 다양한 방안들을 모색하는 데 유용한 시사점을 줄 수 있을 것으로 기대된다. 이러한 연구모형을 통해, 본 연구에서는 우선 지각된 위협과 보안정책 준수에 대한 조직의 지원이 각각 지각된 이익과 지각된 장애 그리고 보안정책 수용성과 어떠한 영향 관계를 가지는지 규명해보고자 한다. 또한, 이러한 관계들 속에서 지각된 이익과 장애가 매개역할을 하는지에 대해서도 분석함으로써, 보안정책 사용자의 보안정책 수용성이 형성되는 메커니즘을 보다 심층적으로 밝혀보고자 한다.

3.2 보안정책 수용성과 보안정책 준수행위

보안정책의 성과 향상은 결국 조직구성원들이 보안정책 준수행위를 얼마나 충실히 하느냐에 달려있다. 이러한 관점에서, 본 연구에서 초점을 맞추고 있는 보안정책 수용성이 보안정책 준수행위에 긍정적인 영향을 미치지 못한다면, 보안정책 수용성을 강화시키는 방안을 모색하고자 하는 본 연구의 목적은 타당성을 잃게 될 것이다. 따라서, 본 연구에서는 우선 보안정책 수용성이 보안정책 준수행위에 실제 유의적인 영향을 미치는지부터 검증을 할 필요가 있다고 판단하여, 이에 대한 가설을 먼저 설정하였다. 가설의 근거에 대한 논의는 다음과 같다.

본 연구에서는 수용성의 개념을 태도와 의도라는 두 가지 측면을 복합적으로 가지고 있는 개념으로 정의하였다(2.2절 참조). 이러한 맥락에서 보안정책 준수태도나 준수의도가 준수행위에 유의적으로 긍정적인 영향을 미친다는 연구들을 많이 찾아볼 수 있다. 예를 들어, Heo and Ahn(2020)은 조직구성원들의 보안사고 대처방

안에 관한 연구를 통해, 태도와 행위가 높은 상관관계를 가지며 태도는 행위를 결정하는 중요한 요소 중 하나라고 강조하였다. Park(2019)은 청소년의 보안인식이 개인정보보호 활동에 미치는 영향 분석을 통해, 보안 태도가 보안 행위에 긍정적인 영향을 미친다는 점을 입증한 바 있다. 또한, Kim and Lim(2016)은 개인정보관리 준수의도가 개인정보관리 준수행위에 긍정적인 영향을 미친다는 분석결과를 제시하였고, Chen et al.(2012)도 보안정책에 대한 준수의도가 실제 행위에 영향을 미친다는 점을 입증한 바 있다. 이러한 연구결과들을 볼 때, 조직구성원의 보안정책 수용성이 보안정책 준수행위에 유의적인 영향을 미칠 것으로 추론할 수 있다. 이와 같은 논의를 바탕으로 본 연구에서는 다음과 같은 가설을 설정하였다.

H1: 조직구성원의 보안정책 수용성은 보안정책 준수행위에 정(+)의 영향을 미칠 것이다.

3.3 지각된 위협

본 연구의 초점 중 하나는 보안사고에 대한 불안감(지각된 위협)이 보안정책 준수를 통해 얻을 수 있는 이점(지각된 이익)과 보안정책 준수활동으로 인해 초래되는 부담감(지각된 장애), 그리고 보안정책 수용성에 미치는 영향들을 분석하는 것이다. 이를 위해, 우선 본 연구에서 설정한 가설에 사용된 변수들의 개념을 논의하면 다음과 같다. 본 연구에서 지각된 위협은 건강신념모델에 따라 지각된 심각성과 지각된 민감성, 이 두 하위요인으로 구성된 상위변수로 다루어지고 있다. 여기서 지각된 심각성이란 보안사고가 초래하는 결과의 심각성, 즉 구체적으로, 보안사고가 시스템과 데이터를 포함한 업무 요소 전반에 걸쳐 피해를 주는 정도에 대한 인식이라 할 수 있으며(Ng et al., 2009), 지각된 민감성은 개인이 보안사고를 당할 가능성에 대한 인식이라 할 수 있다(Ng et al., 2009; Cho et al., 2014). 이 두 가지의 개념을 복합한 지각된 위협은 간단히 보안사고에 대한 불안감으로도 해석될 수 있다. 한편, 본 연구에서 연구변수로 다루고 있는 지각된 이익은 보안정책 준수를 통해서 얻어질 수 있는 이점들, 예를 들면, 보안사고 발생 위험의 감소, 정보유출 가능성의 감소, 업무에 도움이 됨, 보안사고에 대한 불안감의 감소, 보안사고 예방효과 증대와 같은 요소들을 의미하는 개념이다(Ng et al., 2009; Hong et al., 2022).

이러한 변수들의 개념을 바탕으로, 본 연구에서는 조직구성원의 지각된 위협이 지각된 이익에 영향을 미친다는 가설을 설정하였는데, 이에 대한 논의는 다음과 같다. Kim and Song(2011)에서 조직구성원이 보안사고에 대해 느끼는 불안감(지각된 위협)이 클수록 보안사고를 예방하려는 동기가 더욱 강화된다고 주장하였는데, 이러한 동기는 결국 보안사고를 예방함으로써 얻을 수 있는 이점(지각된 이익)을 추구하는 의도로 해석할 수 있다. 또한, 의료보건 분야의 연구이긴 하나, Jo and Han(2020)은 건강신념모델을 적용한 연구로서 질병에 대한 지각된 심각성과 민감성이 모바일 헬스케어 서비스의 유용성, 즉, 서비스를 통해 얻을 수 있는 이점에 유의적인 영향을 미친다는 점을 실증적으로 입증한 바 있다. 이와 같은 논의를 바탕으로 본 연구에서는 다음과 같은 가설을 설정하였다.

H2-1: 조직구성원이 지각하는 보안에 대한 위협(지각된 위협)은 보안정책 준수로 인해 얻을 수 있는 이점에 대한 인식(지각된 이익)에 정(+)의 영향을 미칠 것이다.

다음으로는 지각된 위협이 지각된 장애에 미치는 영향에 대한 가설을 설정하기 위한 논의를 하고자 한다. 본 연구에서는 보안 위협에 대한 인식(지각된 위협)이 보안정책 준수과정에서 요구되거나 발생되는 불편함이나 부담감(지각된 장애)을 증대시키는지에 대해서도 검증을 하고자 한다. 지각된 장애는 보안정책 준수활동으로 인해 발생할 수 있는 업무에 대한 불편함 초래, 업무 효율성 저하, 업무 지연, 자신의 노력 투자, 이러한 것들로 인한 심적 부담감과 같은 요소들을 포함하는 개념으로 설명될 수 있다(Ng et al., 2009). 조직의 입장에서는 보안 위협의

심각성을 인지하고 이를 예방하기 위한 대책을 마련하는 것은 바람직한 일이지만, 조직구성원들의 입장에서는 이러한 대책들이 업무 이외의 활동을 요구하는 것으로 느껴져서 부담감으로 다가올 수 있다(Hwang, 2021). 이러한 맥락에서, 보안 위협 인식, 즉 보안사고에 대한 심리적 불안감이 더 큰 조직구성원일수록 보안 활동에 더 관심을 가지고 더 많은 시간과 노력을 기울이는 경향이 있어서, 더 높은 수준의 지각된 장애를 경험하게 될 것으로 추론된다. 또한, 이러한 보안 위협에 대한 인식은 보안교육을 통해 강화될 수 있다. 즉, 보안교육에는 종종 보안 기술의 사용과 보안 책임에 대한 교육이 포함되므로, 이는 결국 업무 중 보안 활동을 수행하는 데 있어 기술 사용과 보안 책임감에 대한 부담감의 증가로 이어지는 경향이 있다는 것이다(Park and Yim, 2012a). 이와 같은 논의를 바탕으로 본 연구에서는 다음과 같은 가설을 설정하였다.

H2-2: 조직구성원이 지각하는 보안에 대한 위협(지각된 위협)은 보안정책 준수과정에서 초래되는 불편함이나 부담감(지각된 장애)에 정(+)의 영향을 미칠 것이다.

끝으로, 지각된 위협이 보안정책 수용성에 미치는 영향에 대한 가설을 설정하기 위한 논의는 다음과 같다. 본 연구에서는 수용성의 개념을 고찰하고 이에 따라 보안정책 수용성의 개념을 자신이 속한 조직의 보안정책 내용에 대한 태도 및 의도로 정의하였다(2.2절 참조). 이러한 맥락에서, 조직구성원이 인식하는 보안 위협이 보안정책에 대한 의도에 영향을 미친다는 연구들을 다수 찾아볼 수 있다. 예를 들어, Jung et al.(2016)은 지각된 심각성이 보안정책 준수의도에 긍정적인 영향을 미친다는 점을 실증적으로 입증하였으며, 이를 바탕으로 조직구성원으로 하여금 보안 위협을 심각하게 인지하도록 만드는 것이 조직구성원이 정책을 준수하도록 촉진하는 주요한 접근이 될 수 있음을 주장하였다. 이와 유사하게, Shin et al.(2016)에서는 SNS 사용과 관련하여 개인정보에 대한 사용자들의 지각된 심각성이 개인정보 보호행위 의도에 유의적인 영향을 미친다는 분석결과를 제시하였다. Kim and Song(2011)도 조직구성원이 인식하는 보안에 대한 심각성이 보안정책 준수의도에 유의미한 영향을 미친다는 점을 입증한 바 있다. 수용성이 태도 및 의도를 복합적으로 반영하고 있는 개념이라는 점과 지각된 위협이 지각된 심각성과 민감성으로 구성된 개념이라는 점을 고려할 때, 이러한 선행연구들의 결과들은 지각된 위협이 보안정책 수용성에 영향을 미친다는 주장을 뒷받침할 근거가 될 수 있을 것으로 사료된다. 이와 같은 논의를 바탕으로 본 연구에서는 다음과 같은 가설을 설정하였다.

H2-3: 조직구성원이 지각하는 보안에 대한 위협(지각된 위협)은 보안정책 수용성에 정(+)의 영향을 미칠 것이다.

3.4 보안정책 준수지원

본 연구의 초점 중 하나는 조직구성원들의 보안정책 준수에 대한 조직차원의 지원(보안정책 준수지원)이 보안정책 준수를 통해 얻을 수 있는 이점(지각된 이익)과 보안정책 수용성에 미치는 영향 관계들을 분석하는 것이다. 이러한 두 가지 관계 중에서 첫 번째 관계에 대한 가설을 설정하기 위해 논의를 하면 다음과 같다. 보안정책 준수지원은 조직이 조직구성원들에게 보안정책 준수에 필요한 분위기 조성과 교육 및 제도적 지원을 제공하는 것을 의미한다(Kim and Suh, 2024). 이러한 조직차원의 대표적인 지원의 예로는 교육지원을 들 수 있다. 조직의 교육지원과 관련된 기존의 여러 연구들은 학습에 대한 조직의 지원이 피훈련자의 학습동기에 긍정적인 영향을 미친다는 점을 실증적으로 입증해 오고 있다(Kim and Kim, 2003; Kwon and Shin, 2006; Yang and Chung, 2006). 학습동기는 학습의 필요성, 즉 학습이 추구하는 목표를 의미한다는 점을 고려해 볼 때, 이러한 연구결과를 보안교육 상황에 적용시켜 보면, 조직의 보안교육 지원은 조직구성원들이 보안교육에 대해 보다 긍정적인 동기를 가지도록 만들고, 이는 결

국 보안사고 예방 효과(지각된 이익)라는 보안 교육이 추구하는 목표를 더욱 명확하고 강하게 인식하도록 만드는 효과를 가져올 것으로 사료된다. 이와 같은 논의를 바탕으로 본 연구에서는 다음과 같은 가설을 설정하였다.

H3-1: 조직구성원들의 보안정책 준수를 위한 조직차원의 지원(보안정책 준수지원)은 보안정책 준수로 인해 얻을 수 있는 이점에 대한 인식(지각된 이익)에 정(+)의 영향을 미칠 것이다.

다음으로, 조직구성원들의 보안정책 준수에 대한 조직차원의 지원(보안정책 준수지원)이 보안정책 수용성에 미치는 영향에 대한 가설을 설정하기 위한 논의는 다음과 같다. 조직이 보안교육 참여를 높게 평가하고 장려하는 풍토를 조성하는 가운데 보안교육에 대한 지원을 제공하면, 학습자들은 교육 참여에 대한 동기가 강화되고(Kwon and Shin, 2006), 학습결과의 업무에 대한 적용도 적극적으로 수행하게 된다(Yang and Chung, 2006). 이러한 맥락에서, Park and Yim(2012b)은 조직의 정보보안 인식교육이 조직구성원들의 보안정책 준수태도와 준수의도 모두에 긍정적인 영향을 미친다는 분석결과를 제시하였다. 또한, Kim and Suh(2024)에서도 보안교육에 대한 조직차원의 지원이 조직구성원들의 보안정책 준수태도에 유의적으로 긍정적인 영향을 미친다는 점을 입증한 바 있다. 수용성이 태도와 의도의 개념을 복합적으로 반영하고 있는 개념이라는 점을 고려할 때, 이러한 연구결과는 보안정책에 대한 교육지원이 보안정책 수용성에 긍정적인 영향을 미친다는 추론을 가능케 한다. 이와 같은 논의를 바탕으로 본 연구에서는 다음과 같은 가설을 설정하였다.

H3-2: 조직구성원들의 보안정책 준수를 위한 조직차원의 지원(보안정책 준수지원)은 보안정책 수용성에 정(+)의 영향을 미칠 것이다.

3.5 지각된 이익

본 연구는 보안정책 수용성에 영향을 미치는 요인들을 규명하는 데 초점을 두고 있다. 이러한 관점에서 본 연구에서는 보안정책 준수로 인해 얻을 수 있는 이점(지각된 이익)이 미치는 영향에 대한 분석을 수행한다. 이에 관한 가설을 설정하기 위한 논의는 다음과 같다. 지각된 이익의 개념은 보안사고 발생 위험의 감소나 정보유출 가능성의 감소와 같이 보안행위를 통해 기대할 수 있는 보안사고 예방 효과에 대한 개인의 믿음이라 할 수 있다(Ng et al., 2009). 조직구성원은 이러한 믿음이 클수록 보안정책을 더욱 적극적으로 수용하려는 의도를 갖게 될 것으로 추론할 수 있다. 이러한 맥락에서, Lee et al.(2016)은 보안정책을 준수함으로써 얻을 수 있는 이익, 즉 개인이 기대할 수 있는 혜택이 준수태도에 유의적으로 긍정적인 영향을 미친다는 점을 실증적으로 입증한 바 있다. 이와 같은 논의를 바탕으로 본 연구에서는 다음과 같은 가설을 설정하였다.

H4: 보안정책 준수로 인해 얻을 수 있는 이점에 대한 조직구성원들의 인식(지각된 이익)은 보안정책 수용성에 정(+)의 영향을 미칠 것이다.

3.6 지각된 장애

보안정책 준수를 위한 노력과 비용에 대한 조직구성원들의 인식(지각된 장애)이 보안정책 수용성에 미치는 영향에 대한 가설을 설정하기 위한 논의는 다음과 같다. 지각된 장애는 보안정책 준수활동으로 인해 초래될 수 있는 업무에 대한 불편함 초래, 업무 효율성 저하, 업무 지연과 같은 부정적인 결과들에 대한 개인의 인식이라 할 수 있다(Ng et al., 2009; Cho et al., 2014). 조직구성원의 이러한 인식은 보안정책 수용 의도를 약화시킬 것으로 추론할 수 있다. 이러한 맥락에서, Lee et al.(2018)은 보안행위를 실천하는 데 있어서 장애가 되는 요인을 더 크게 지각할수록 개인의 보안행위 의도가 낮아지는 경향이 있음을 입증한 바 있다. 또한, Bulgurcu et al.(2010)은 보안정책 실행으로 인해 추가적으로 발생하는 업무 과정 및 행동에 대한 요구가 조직구성원에게 업무에 대한 시간 소모와 부담감

을 초래할 수 있으며, 이와 같은 부정적 결과가 조직구성원들의 보안정책 준수태도에 강한 부정적 영향을 준다는 점을 실증적으로 입증한 바 있다. 수용성의 개념이 태도와 의도가 복합된 개념이라는 점을 고려할 때, 보안정책을 준수하는 과정에서 겪게 되는 불편함이나 부담감과 같은 장애 요인들이 보안정책 수용성을 약화시킬 수 있을 것으로 사료된다. 이와 같은 논의를 바탕으로 본 연구에서는 다음과 같은 가설을 설정하였다.

H5: 보안정책 준수에 따르는 불편함이나 부담감(지각된 장애)은 보안정책 수용성에 음(—)의 영향을 미칠 것이다.

4. 연구방법

4.1 변수측정

본 연구에서는 지각된 심각성과 지각된 민감성으로 구성된 지각된 위협, 보안정책 준수지원, 보안정책 수용성, 지각된 이익, 지각된 장애, 보안정책 준수행위로 구성된 연구모형을 제안하였다. 연구모형을 검증하기 위해 본 연구의 변수들을 모두 리커드(Likert) 7점 척도로 측정하였으며, 모든 설문항목들은 관련 문헌에서 신뢰성과 타당성이 확인된 문항들을 수정하여 사용하였다. 본 연구에서 사용된 변수들의 조작적 정의와 측정항목은 Table 1과 같다.

Table 1 Constructs and Measurement Items

Constructs	Codes	Operational Definitions and Measurement Items	Sources
Security Policy Acceptance	The degree of willingness to agree with and follow the contents of the security policy of the organization to which one belongs		
	SPA1	I accept our organization's security policies.	Chung(2017)
	SPA2	I have no objections to our organization's security policies.	
	SPA3	I intend to actively follow our organization's security policy.	
	SPA4	I agree with our organization's security policies.	
Security Policy Compliance Behavior	The degree to which organizational members comply with the guidelines required by the organization's security policies		
	SPCB1	I do not take any action that violates our organization's security policy.	Jee et al.(2011) Liand and Xue(2010) Suh(2020)
	SPCB2	I am practicing the guidelines outlined in our organization's security policies.	
	SPCB3	I am faithfully carrying out the security incident prevention guidelines required by our organization's security policy.	
Perceived Severity	The degree of awareness of the severity of security incidents related to one's work		
	SEV1	If a security incident related to my work occurs, it will be a serious issue for me.	Ng et al.(2009)
	SEV2	If important information related to my work is leaked, it will be a serious problem for me.	
	SEV3	If a security incident related to my work occurs in our organization, it will significantly disrupt my work.	
Perceived Susceptibility	The degree of awareness of the possibility of security incidents occurring in relation to one's work		
	SUS1	When I work in our organization, I often think that information related to my work might be leaked without my knowledge.	Cho et al.(2014) Ng et al.(2009)

	SUS2	When I work in our organization, I often think that there is a possibility of a security incident related to my work occurring.	
	SUS3	When I work in our organization, I often think that there is a possibility that I may experience a security incident.	
Security Policy Compliance Support	The degree to which the organization creates an environment for compliance with security policies and provides training and institutional support to its members		
	SPCS1	Our organization places a high value on compliance with security policies.	Kim and Kim(2003)
	SPCS2	Our organization assigns responsibility to members for compliance with security policies.	
	SPCS3	Our organization provides adequate training and institutional support necessary for members to comply with security policies.	
Perceived Benefits	The degree of awareness of the positive outcomes that can be obtained in relation to one's work by faithfully complying with the organization's security policy		
	BEN1	If I faithfully comply with our organization's security policy, the risk of security incidents related to my work will decrease.	Hong et al.(2022) Ng et al.(2009)
	BEN2	If I faithfully comply with our organization's security policy, the possibility of important information related to my work being leaked will decrease.	
	BEN3	If I faithfully comply with our organization's security policy, this will ultimately help my work.	
	BEN4	If I faithfully comply with our organization's security policy, I will be able to free myself from anxiety about security incidents.	
	BEN5	If I faithfully comply with our organization's security policy, this will be of great help in preventing security incidents related to my work.	
Perceived Barriers	The degree of awareness of the negative outcomes that can occur in relation to one's work in the process of faithfully complying with the organization's security policy		
	BAR1	If I faithfully comply with our organization's security policy, this may cause inconvenience in my work.	Ng et al.(2009)
	BAR2	If I faithfully comply with our organization's security policy, this may cause my work efficiency to decrease.	
	BAR3	If I faithfully comply with our organization's security policy, this may cause my work to be delayed.	
	BAR4	I will have to invest considerable effort to faithfully comply with our organization's security policy.	
	BAR5	If I faithfully comply with our organization's security policy, this may cause me to experience considerable psychological burden..	

4.2 데이터 수집

본 연구는 연구모형 검증을 위해 국내 민간 및 공공 부문에서 종사하는 조직구성원들을 대상으로 온라인 방식의 설문조사를 통해 데이터를 수집하였다. 데이터 수집은 2024년 6월 4일부터 6월 18일까지 수행되었다. 설문지 링크를 전달하는 방식으로 총 569부를 배부한 결과 540부가 회수되었으며, 이 중 불성실 응답으로 판단되는 것들을 제거하고 최종적으로 477부를 연구모형 검증에 사용하였다. 응답자의 인구통계학적 특성은 Table 2와 같다.

Table 2 Sample Characteristics

Characteristics	Options	Count	Percentage
Gender	Male	235	49%
	Female	242	51%
Education	High school or Less	70	15%
	College Graduate (Including Current Students)	350	73%
	Master's Degree (Including Current Students)	49	10%
	Doctoral Degree (Including Current Students)	8	2%
Age	20s	38	8%
	30s	111	23%
	40s	159	34%
	50s	143	30%
	60s and Above	26	5%
Job	Public Sector (Including Public Enterprises)	48	10%
	Management	10	2%
	Office Worker	302	63%
	Production/Technical/Labor	62	13%
	Service/Sales	55	12%
Industry	Manufacturing	108	22%
	Construction	54	11%
	Energy	10	2%
	Retail/Wholesale	47	10%
	Public Sector/Defense	46	10%
	Finance/Insurance	23	5%
	Science Technology	8	2%
	Education	48	10%
	Arts/Sports	13	3%
	Information Technology	42	9%
	Other	78	16%
Organization Type	Large Enterprise	54	11%
	Mid-Sized Company	74	14%
	Small Company	231	48%
	Government Agency (Including Central and Local)	33	7%

	Public Institution(Public Enterprises, Quasi-Governmental, Other Public Institutions)	49	10%
	Educational Institution	14	3%
	Other	22	7%
Position	Entry-Level	156	33%
	Junior/Assistant Manager	101	21%
	Manager/Senior Manager	135	28%
	Director	51	11%
	Executive	19	4%
	Other	15	3%
Current Job Duration	Less than 5 years	194	41%
	5 to 10 years	120	25%
	10 to 15 years	68	14%
	15 to 20 years	41	9%
	More than 20 years	54	11%
Total		477	100%

5. 분석 및 결과

5.1 측정모형 분석

본 연구의 연구모형은 지각된 위협이 지각된 심각성, 지각된 민감성과 같은 두 가지의 구성개념들을 하위변수로 가지고 있는 위계적성분모형(hierarchical component model, HCM)의 구조를 가진다. 본 연구모형에서 2차변수(second-order construct)인 지각된 위협은 지각된 심각성 및 지각된 민감성과 형성적(formative) 관계를 가지고 있으며, 이 두 가지의 1차변수들(first-orders)은 반영적(reflective) 측정항목들로 측정되므로, 본 연구모형은 반영적-형성적(reflective-formative) HCM이라 할 수 있다(Hair et al., 2018). 이러한 연구모형을 분석하기 위해, 본 연구에서는 모든 1차변수들에 대한 측정모형을 평가하고, 이를 바탕으로 생성된 잠재변수값을 이용하여 2차변수인 지각된 위협의 측정모형을 평가하는 '2단계 접근법(two-stage approach)'을 사용하였다(Hair et al., 2014). 본 연구는 이러한 통계적 분석을 위해 PLS-SEM(partial least squares-structural equation modeling) 기법을 사용하였으며, 분석 소프트웨어로는 SmartPLS 4.0을 사용하였다.

우선 1차변수들에 대한 측정모형 평가를 위해 신뢰성과 타당성을 분석하였다. 변수들의 신뢰성을 확보하기 위해서는 내적일관성을 나타내는 크론바흐알파값(Cronbach's alpha)과 복합신뢰도(composite reliability)의 값이 각각 0.7 이상이어야 한다(Sosik et al., 2009). Table 3에서 볼 수 있듯이, 변수들의 크론바흐알파값은 모두 0.8 이상으로 그리고 복합신뢰도는 모두 0.9 이상으로 나타나 본 연구에서 사용한 측정도구는 구성개념에 대한 신뢰성이 확보된 것으로 평가되었다.

Table 3 Results of the Reliability and Convergent Validity

Constructs	Items	Outer Loadings	Cronbach's Alpha	Composite Reliability	AVE
Security Policy Acceptance	SPA1	0.893	0.928	0.949	0.823
	SPA2	0.902			
	SPA3	0.926			
	SPA4	0.908			
Security Policy Compliance Behavior	SPCB1	0.928	0.933	0.957	0.881
	SPCB2	0.942			
	SPCB3	0.946			
Perceived Severity	SEV1	0.949	0.954	0.970	0.916
	SEV2	0.965			
	SEV3	0.956			
Perceived Susceptibility	SUS1	0.947	0.948	0.967	0.906
	SUS2	0.958			
	SUS3	0.950			
Security Policy Compliance Support	SPCS1	0.940	0.926	0.953	0.871
	SPCS2	0.935			
	SPCS3	0.925			
Perceived Benefits	BEN1	0.916	0.953	0.963	0.841
	BEN2	0.915			
	BEN3	0.900			
	BEN4	0.920			
	BEN5	0.933			
Perceived Barriers	BAR1	0.904	0.948	0.960	0.826
	BAR2	0.925			
	BAR3	0.924			
	BAR4	0.888			
	BAR5	0.904			

타당성은 집중타당성(convergent validity)과 판별타당성(discriminant validity), 이 두 가지 관점으로 나누어 평가하였고(Malhotra et al., 2004), 집중타당성은 외부적재치(outer loading)와 평균분산추출값(average variance extracted, AVE)를 통해 평가하였다. 요인적재값이 모두 0.7 이상, 평균분산추출값이 모두 0.5 이상으로 나타나 집중타당성이 확보된 것으로 판단하였다(Hair et al., 2022). 판별타당성은 Fornell-Larcker 기준과 HTMT(heterotrait-monotrait) 비율로 평가하였다. Fornell-Larcker 기준에 따른 결과는 Table 4에서 볼 수 있는데, 평균분산추출값의 제곱근들이 다른 변수들과의 상관관계 계수보다 높은 것으로 나타나 판별타당성이 확보된 것으로 판단하였다(Fornell and Larcker, 1981). HTMT 비율 기준에 따른 분석 결과는 Table 5에서 볼 수 있는데, HTMT 비율값들이 모두 0.9 이하로 나타나 판별타당성이 확보된 것으로 판단하였다(Hair et al., 2015). 이상과 같이, '2단계 접근법'의 첫 번째 단계에서는 모든 1차변수들이 측정모형이 신뢰성과 타당성을 가지는 것을 확인할 수 있었다.

Table 4 Results of Fornell-Larcker Criterion Analysis for Discriminant Validity Assessment

Constructs	SPA	SPCB	SEV	SUS	SPCS	BEN	BAR
Security Policy Acceptance (SPA)	**0.907**						
Security Policy Compliance Behavior (SPCB)	0.720	**0.939**					
Perceived Severity (SEV)	0.415	0.329	**0.957**				
Perceived Susceptibility (SUS)	0.060	-0.049	0.395	**0.952**			
Security Policy Compliance Support (SPCS)	0.537	0.487	0.389	0.135	**0.933**		
Perceived Benefits (BEN)	0.583	0.484	0.573	0.222	0.430	**0.917**	
Perceived Barriers (BAR)	0.019	-0.022	0.395	0.510	0.117	0.160	**0.909**

Note: Diagonal elements are square root of AVEs.

Table 5 Results of HTMT Analysis for Discriminant Validity Assessment

Construct	SPA	SPCB	SEV	SUS	SPCS	BEN	BAR
Security Policy Acceptance (SPA)							
Security Policy Compliance Behavior (SPCB)	0.773						
Perceived Severity (SEV)	0.441	0.349					
Perceived Susceptibility (SUS)	0.063	0.052	0.415				
Security Policy Compliance Support (SPCS)	0.577	0.522	0..413	0.144			
Perceived Benefits (BEN)	0.618	0.512	0.602	0.233	0.456		
Perceived Barriers (BAR)	0.064	0.063	0.273	0.536	0.120	0.162	

Table 6 Resutls of Significance and Multicollinearity Analysis for Perceived Threat

Constructs	Items	Outer Weights	t-value	p-value	Outer Loadings	VIF
Perceived Severity (SEV)	THR_LV 1	0.909	1.165	0.000	0.985	1.185
Perceived Susceptibility (SUS)	THR_LV 2	0.191	14.192	0.106	0.550	1.185

다음으로 '2단계 접근법'의 두 번째 단계의 분석, 즉 2차변수인 지각된 위협에 대한 측정모형 분석을 실시하였다. 이를 위해 우선 '2단계 접근법'에 따라 모든 1차변수들을 대상으로 잠재변수값들로 구성된 데이터셋을 생성하였다(Hair et al., 2018; Piaw, 2023). 형성적 변수의 측정모형을 평가하기 위해서는 구성 요인에 대한 다중공선성 및 각 요인에 대한 유의성을 분석해야 한다(Hair et al., 2022). 다중공선성은 분산팽창지수(variance inflation factor, VIF)값이 5를 넘지 않으면 다중공선성에 문제가 없는 것으로 판단할 수 있다(Hair et al., 2022). 분석 결과, Table 6에서 볼 수 있듯이, 지각된 위협의 구성요인인 지각된 심각성과 지각된 민감성 모두 임계치인 5 미만으로 나타나 다중공선성에 문제가 없음을 확인할 수 있었다.

그다음 지각된 위협의 두 가지 형성적 요인들에 대한 유의성 분석을 수행하였다. 형성적 측정모형에서 유의성은 외부가중치(outer weights)를 기준으로 판단할 수 있는데, 분석 결과 외부가중치가 유의하지 않게 나오더라도 외부적재치(outer loadings)가 0.5이상이면 해당 요인의 유의성은 인정받을 수 있다(Hair et al., 2022). 분석 결과, Table 6에서 볼 수 있듯이, 지각된 심각성은 외부적재치가 유의적인 것으로 확인되었다. 반면, 지각된 민감성은 외부가중치가 유의적이지 않았으나 외부적재치가 0.5 이상으로 확인되어, 결국 유의성을 확보한 것으로 평가할 수 있었다. 지금까지의 측정모델 분석 결과를 종합하면, 반영적 지표들을 가지는 모든 1차변수들은 신뢰성과 타당성의 요건을 충족하였고, 형성적 지표들을 가지는 2차변수인 지각된 위협도 측정모형 평가에서 요구하는 다중공선성과 유의성의 요건을 모두 충족하였다.

5.2 구조모형 분석

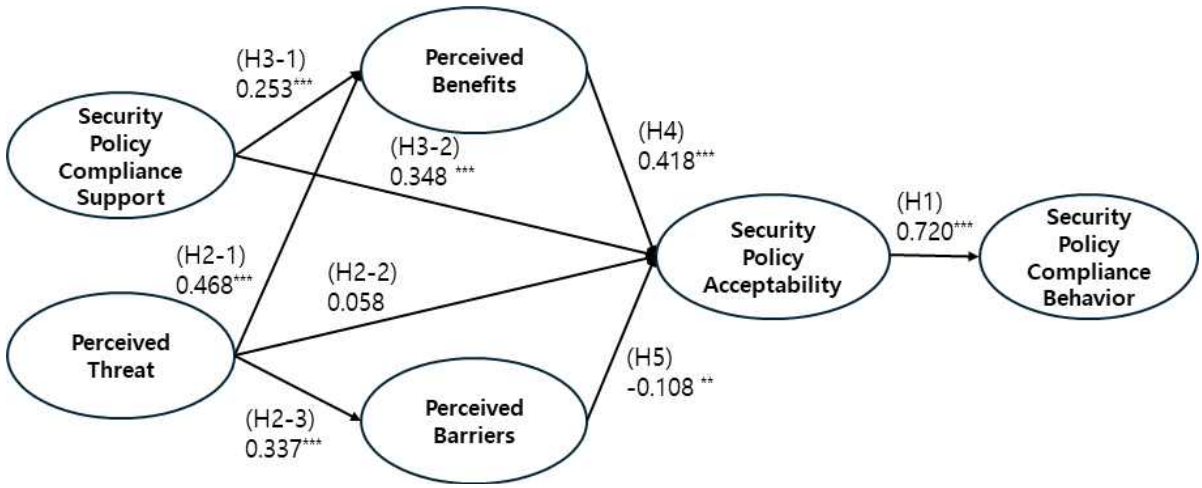
본 연구에서는 부트스트래핑(resampling 5000회)을 통한 구조모형 분석을 통해, 가설검정을 수행하였으며, 그 결과는 Table 7과 같다. 결과를 보면, 조직구성원의 보안정책 수용성은 보안정책 준수행위에 유의적으로 정(+)의 영향을 미치는 것으로 나타났다. 이는 보안정책 수용성을 높이기 위한 방안들을 모색하고자 하는 본 연구의 결과가 결국 보안준수 행위에 영향을 미쳐 보안성과로 이어질 수 있음을 보여주는 것으로 해석할 수 있다.

한편, 조직구성원이 보안에 대한 위협을 느끼는 인식의 정도가 보안정책을 준수함으로써 얻을 수 있는 이익이나 이점들에 대한 기대에 정(+)의 유의적인 영향을 미치고, 보안정책 준수로 인해 겪게 될 것으로 예상되는 불편함 등의 부정적 측면(지각된 장애)에도 정(+)의 영향을 미치는 것으로 나타났다. 이와 동시에 조직구성원의 지각된 위협이 보안정책 수용성에 직접적으로 유의적인 영향을 미치지 못하는 것으로 나타났다. 그러나 Table 8의 1, 2번 간접효과에서 볼 수 있듯이, 지각된 위협이 지각된 이익과 지각된 장애를 거쳐 보안정책 수용성에 미치는 간접효과들은 모두 유의적인 것으로 나타났다. 이는 지각된 위협은 지각된 이익과 지각된 장애의 매개역할을 통해서만 보안정책 수용성에 영향을 준다는 것을 의미한다(즉, 완전매개).

조직구성원들에 대한 조직차원의 보안정책 준수에 대한 지원은 지각된 이익과 보안정책 수용성에 모두 유의적으로 정(+)의 영향을 미치는 것으로 나타났다. 이와 동시에 보안정책 준수지원은 Table 8의 6번 간접효과에서 볼 수 있듯이, 지각된 이익의 매개역할을 통해서도 보안정책 수용성에 영향을 미치는 것으로 나타났다(즉, 부분매개). 또한, 지각된 이익과 장애 모두 보안정책 수용성에 유의적으로 영향을 미치는 것으로 나타났는데, 지각된 장애는 지각된 이익과는 반대로 보안정책 수용성에는 부정적인 영향을 미치는 것으로 나타났다.

또한, 본 연구는 구조모형의 설명력과 예측력을 평가하기 위해 R^2값과 Q^2값을 함께 분석하였다. 먼저, 설명력 지표인 R^2값은 보안정책 수용성이 0.451, 보안정책 준수행위가 0.518, 지각된 이익이 0.372 그리고 지각된 장애가 0.113으로 확인되었다. R^2값이 0.5 정도면 중간 수준이고 0.25 정도면 낮은 수준으로 볼 수 있다는 점을 고려할 때(Hair et al., 2011), 지각된 장애를 제외한 나머지 변수들은 무난한 수준으로 사료

된다. 한편, Q^2값은 0보다 크면 예측력이 있음을 나타내는데(Hair et al., 2022), 본 연구에서 검증한 Q^2값은 보안정책 수용성이 0.316, 보안정책 준수행위는 0.234, 지각된 이익은 0.360 그리고 지각된 장애는 0.105로서, 모두 양수로 확인되었다. 또한, 본 연구에서는 보안정책 수용성에 대한 통제변수들(연령, 산업, 직무, 조직유형)에 대한 유의성 분석도 수행하였는데, 그 결과, 모든 통제변수들이 보안정책 수용성에 유의적인 영향을 미치지 않는 것으로 나타나, 각 통제변수의 세부 그룹 간 수용성에는 차이가 없음을 확인할 수 있었다.



Note: *p<0.05, **p<0.01, ***p<0.001

Fig. 3 Results of Structural Model Analysis

Table 7 Results of Structural Model Path Coefficient Test

Hypotheses	Paths	Path Coefficients	t-value	p-value	Supported?
H1	Security Policy Acceptability → Security Policy Compliance Behavior	0.720	18.483	0.000	Yes
H2-1	Perceived Threat → Perceived Benefits	0.468	8.565	0.000	Yes
H2-2	Perceived Threat → Security Policy Acceptability	0.058	0.948	0.343	No
H2-3	Perceived Threat → Perceived Barriers	0.337	4.058	0.000	Yes
H3-1	Security Policy Compliance Support → Perceived Benefits	0.253	4.500	0.000	Yes
H3-2	Security Policy Compliance Support → Security Policy Acceptability	0.348	5.972	0.000	Yes
H4	Perceived Benefits → Security Policy Acceptability	0.418	6.876	0.000	Yes
H5	Perceived Barriers → Security Policy Acceptability	-0.108	2.642	0.008	Yes

Table 8 Results of Indirect Effect Test

No.	Indirect Effect Paths	Path Coefficients	t-value	p-value	Supported?
1	Perceived Threat → Perceived Benefits → Security Policy Acceptability	0.196	5.381	0.000	Yes
2	Perceived Threat → Perceived Barriers → Security Policy Acceptability	-0.036	2.134	0.033	Yes
3	Perceived Threat → Perceived Benefits → Security Policy Acceptability → Security Policy Compliance Behavior	0.141	5.613	0.000	Yes
4	Perceived Threat → Perceived Barriers → Security Policy Acceptability → Security Policy Compliance Behavior	-0.026	2.098	0.036	Yes
5	Perceived Threat → Security Policy Acceptability → Security Policy Compliance Behavior	0.042	0.952	0.341	No
6	Security Policy Compliance Support → Perceived Benefits → Security Policy Acceptability	0.106	3.563	0.000	Yes
7	Security Policy Compliance Support → Perceived Benefits → Security Policy Acceptability → Security Policy Compliance Behavior	0.076	3.472	0.001	Yes
8	Security Policy Compliance Support → Security Policy Acceptability → Security Policy Compliance Behavior	0.250	5.134	0.000	Yes
9	Perceived Benefits → Security Policy Acceptability → Security Policy Compliance Behavior	0.301	6.987	0.000	Yes
10	Perceived Barriers → Security Policy Acceptability → Security Policy Compliance Behavior	-0.078	2.538	0.011	Yes

6. 토의 및 결론

본 연구는 조직구성원들의 보안정책 수용성을 높일 수 있는 방안을 모색하기 위해 건강신념모델의 변수들을 중심으로 연구모형을 개발하고 분석하였다. 이를 통해 본 연구는 조직구성원들

이 느끼는 보안에 대한 위협감과 보안정책 준수를 위한 조직의 지원이 그들의 보안정책 수용성에 미치는 영향을 규명하였다. 특히 보안정책 준수행위로 인한 이익 및 손실에 대한 인식이 매개역할을 하는지를 분석함으로써 조직구성원들의 보안정책 수용성이 형성되는 메커니즘을 보다 구체적으로 규명하였다. 이러한 분석과정을 통해 여러 가지의 시사점들을 도출할 수 있었는데, 우선 실무적 시사점에 대해 논의하면 다음과 같다.

첫째, 본 연구에서는 우선 보안정책 수용성이 보안정책 준수행위에 미치는 영향을 분석하였는데, 그 결과, 보안정책 수용성이 강할수록 보안정책 준수행위를 더욱 적극적으로 수행한다는 점을 확인할 수 있었다(H1). 조직의 보안성과는 결국 조직구성원들의 행위를 통해 얻어질 수 있으므로, 이와 같은 결과는 조직이 보안행위에 긍정적인 영향을 미치는 보안정책 수용성을 높이기 위한 노력을 기울일 필요가 있음을 시사한다. 본 연구가 보안정책 수용성에 관심을 가지는 이유는 궁극적으로 이것이 조직구성원들의 보안정책 준수행위를 촉진시킬 수 있을 것이라는 믿음 때문이다. 이러한 믿음이 실증적으로 입증되었다는 점은 보안정책 수용성을 높이는 방안을 모색하고자 하는 본 연구의 목적이 타당성을 가질 수 있음을 의미한다. 특히, 분석결과에서 볼 수 있는 경로계수들 중에서 보안정책 수용성과 보안정책 준수행위 간의 경로계수가 큰 것으로 나타났는데, 이는 본 연구 목적의 타당성을 더욱 견고하게 지지해주는 의미로 해석될 수 있을 것으로 사료된다.

둘째, 본 연구에서는 조직구성원이 보안에 대해 지각한 위협감이 클수록 보안정책 준수를 통해 기대할 수 있는 이익이나 이점도 더욱 크게 인식한다는 점을 확인할 수 있었다(H2-1). 즉, 조직구성원은 보안 위협을 크게 인식할수록 보안정책 준수의 가치도 더욱 크게 평가한다는 것이다. 이는 조직구성원들의 보안정책 준수의 가치와 필요성에 대한 인식을 증진시키기 위해서는 조직구성원들이 보안 위협이 초래하는 결과의 심각성을 명확하게 인식할 수 있는 방안들을 강구할 필요가 있다는 점을 시사한다. 이러한 방안으로는 대표적으로 보안교육을 들 수 있다. 이러한 교육을 통해 동종 업계의 조직들이나 해당 조직이 직접 겪었던 실제 보안사고 사례들을 중심으로 재정적, 법적 측면의 손실 내역들을 구체적으로 전달할 필요가 있다. 또한, 해당 조직을 대상으로 조사한 잠재적 위협들에 대한 구체적인 정보도 함께 제공할 필요가 있다. 조직의 이러한 노력은 조직구성원들이 보안 위협을 단순한 논리가 아닌, 자신의 업무와 관련된 위협 가능성과 그 결과를 구체적으로 인식할 수 있도록 하는 계기가 될 것으로 사료된다.

셋째, 본 연구에서는 지각된 위협이 보안정책 수용성에 직접적으로 유의미한 영향을 미치지 않음을 확인할 수 있었다(H2-2). 이는 단순히 위협을 인식하는 것만으로는 보안정책을 수용하려는 의도를 형성하기 어렵다는 것을 보여준다. 조직구성원들이 보안사고의 심각성과 발생 가능성을 인지하더라도, 보안정책 준수가 자신의 업무 및 생활에 어떤 실질적인 변화를 가져올지 인식하지 못하면 해당 정책을 수용하지 않을 가능성이 크다는 것을 시사한다. 하지만 지각된 위협이 지각된 이익의 매개역할을 통해 결국 보안정책 수용성에 유의적으로 긍정적인 영향을 미치는 것(즉, 완전매개)을 확인할 수 있었다(Table 8의 1번). 이는 보안정책 수용성을 효과적으로 증대시키기 위해서는 이러한 지각된 이익의 매개효과를 더 높일 수 있는 방안을 모색할 필요가 있음을 시사한다. 이러한 관점에서, 앞에서 논의한 보안 위협 인식을 고취하기 위한 교육 프로그램을 설계할 때에는 보안정책을 충실히 준수할 때 얻을 수 있는 긍정적인 측면들도 함께 다루는 방안을 고려할 필요가 있다.

넷째, 지각된 이익이 보안정책 수용성에 직접적으로 유의적인 영향을 미친다는 결과도 확인할 수 있었다(H4). 즉, 조직구성원이 보안정책 준수를 통해 얻을 수 있는 이익을 크게 느낄수록 보안정책에 대해 더 높은 수용성을 보인다는 것이다. 이는 조직구성원들의 보안정책 수용성을 높이기 위해서는 보안정책 준수를 통해 얻을 수 있는 이익을 적극적으로 인식시킬 필요가 있음을 시사한다. 조직구성원들 중에는 보안정책을 충실히 따르는 것이 자신에게 어떠한 도움이

되는지 명확하게 인식하지 못하는 경우가 적지 않게 있을 것으로 사료된다. 따라서, 조직은 정보유출과 같은 보안사고의 불안 탈피, 보안사고 예방효과, 업무 손실 방지와 같은 이점들을 중심으로 보안정책 준수의 이점과 가치를 사내 메일이나 포털사이트의 공지사항과 같은 사내 소통 채널들을 통해 지속적으로 전달하는 방안을 고려할 필요가 있다.

다섯째, 조직구성원이 보안 위협을 더 크게 느낄수록, 이를 방지하기 위해 더 많은 노력의 필요성을 느끼고, 이로 인해 더 많은 불편함과 부담감을 느끼게 된다는 점을 확인할 수 있었다(H2-3). 또한 자신의 노력 투자 과정에서 겪게 되는 불편함과 부담감(지각된 장애)은 보안정책 수용성에 유의적으로 부정적인 영향을 미친다는 점도 확인할 수 있었다(H5). 이러한 두 가지의 결과를 함께 고려해 볼 때, 앞에서 논의했듯이 조직구성원들에게 보안 위협에 대해 명확히 인식시키는 것은 필요한 일이지만, 이는 조직구성원이 보안 위협에 대응하기 위한 노력의 부담을 가중시키고, 결과적으로 보안정책 수용성에 부정적인 영향을 줄 수 있다는 해석이 가능하다. 이는 조직구성원들이 보안정책 준수행위가 업무에 부담을 주거나 방해가 될 것이라는 인식(지각된 장애)에서 벗어날 수 있도록 노력할 필요가 있다는 점을 시사한다. 지각된 장애의 개념은 보안정책 준수로 인해 유발되는 심적 부담 외에도 업무의 불편함 또는 효율성 저하에 대한 우려를 포함한다. 이러한 부정적 인식들을 줄이기 위해서는 보안정책에 대한 실무교육 프로그램을 개발하고 운영할 필요가 있다. 이러한 교육의 목표는 조직구성원들이 보안정책 준수행위를 이해하는 데 있어 높은 자기효능감을 가지도록 하는 것에 맞출 필요가 있다. 이를 위해서는 조직구성원들이 보안정책 지침들에 대한 구체적인 이행 방법들을 충분히 연습해볼 수 있는 실습 중심의 교육과정으로 설계할 필요가 있다. 또한, 교육과 홍보를 통해 보안정책 준수로 얻을 수 있는 이점을 강하게 인식시킴으로써 지각된 장애와 같은 부정적 인식을 상쇄시킬 수 있는 긍정적 인식과 의도를 가지도록 유도하는 것도 하나의 방안으로 고려할 수 있을 것으로 사료된다.

여섯째, 본 연구에서는 조직의 보안정책에 대한 지원이 보안정책 준수를 통해 얻을 수 있는 이점과 보안정책 수용성에 유의적으로 긍정적인 영향을 미친다는 점을 확인할 수 있었다(H3-1, H3-2). 이는 조직구성원들이 보안정책 준수로 인해 얻을 수 있는 긍정적인 효과들에 대한 인식을 증대시키기 위해서는 조직차원의 지원 노력이 중요하다는 점을 시사한다. 조직차원의 지원으로는 우선 보안가치를 중시하는 조직문화 구축을 위한 조직의 투자와 노력을 들 수 있다. 이를 위해 조직은 조직구성원들이 보안정책의 준수가 매우 높은 가치를 가진다는 점을 인식할 수 있도록, 다양한 사내 매체를 통해 홍보 활동을 지속적으로 해나갈 필요가 있다. 또한 조직구성원들의 보안정책 준수 노력을 평가할 수 있는 기준을 마련하고 이에 대한 보상을 제공하는 제도를 개발하고 운영하는 것도 고려할 필요가 있다. 또한, 앞에서 논의한 교육훈련 기회의 제공을 들 수 있다. 이 외에도 조직구성원들이 보안정책 행위를 효율적으로 수행할 수 있도록 도와줄 수 있는 보기 쉬운 매뉴얼의 제공과 궁금증이나 문제가 발생했을 때 보안상담팀이나 기술지원팀을 통해 즉각적으로 도움을 줄 수 있는 지원체계의 구축도 고려할 필요가 있다.

한편, 본 연구의 동기와 분석결과를 종합적으로 고려해 볼 때, 본 연구의 주요한 이론적 시사점은 다음과 같이 설명할 수 있다. 건강신념모델은 그동안 설명변인들을 서로 인과관계가 없는 수평적 관점으로 바라보는 가운데, 이것들을 통해 연구대상 행위를 설명하는 데에만 초점을 맞춰왔다. 그러나, 본 연구에서는 건강신념모델의 설명변인인 지각된 위협이 다른 설명변인인 지각된 이익과 지각된 장애 모두에 대해 인과관계를 가진다는 점을 통계적으로 규명하였다. 이는 건강신념모델을 어떤 현상에 적용함에 있어 그 현상을 보다 체계적이고 정교하게 바라볼 수 있는 시각을 제공한다는 점에서, 이 모델의 설명력을 향상시키는 데 기여했다는 의의를 가질 수 있을 것으로 사료된다. 또한, 건강신념모델은 질병이나 보안과 같은 관심 대상으로부터 직접적으로 초래되는 결과나 현상에 대한 인

식들에 초점을 맞추고 있지만, 본 연구는 조직차원의 지원이라는 변수를 건강신념모델과 결합시킴으로써 환경적 차원의 현상까지 고려할 수 있는 프레임워크를 제시했다는 점을 또 하나의 이론적 기여점으로 고려할 수 있을 것으로 사료된다.

본 연구의 한계점과 향후 연구 방향은 다음과 같다. 본 연구에서는 보안정책 준수에 대한 조직차원의 지원을 하나의 개념으로 다루었는데, 이 개념은 지원의 내용에 따라 세분화될 수 있을 것으로 사료된다. 따라서 향후에는 조직차원의 지원 유형별로 보안정책 수용성에 대한 영향력에 어떤 차이가 있는지를 분석함으로써 보안정책 수용성 향상을 위한 보다 깊이 있는 지원 전략들을 모색해볼 필요가 있다. 또한, 본 연구의 접근관점은 보안정책 수용성과 이에 대한 영향 요인들 간의 관계에만 국한되어 있다. 그러나 향후에는 이러한 영향 관계들을 바람직한 방향으로 강화 또는 약화시키는 데 유용하게 활용할 수 있는 조절요인들을 식별하고 검증하는 연구도 수행할 필요가 있다.

References

Ahn, H. J., Kim, S. J. and Kwon, D. S. (2016). A Study on Security Independent Behavior in Social Game Using Expanded Health Belief Model, *Management & Information Systems Review*, 35(2), 99-118.

Boannews. (2023). *Insiders: The Other Culprits Behind Security Breaches and Data Leaks... The Threat is Within*, https://m.boannews.com/html/detail.html?idx=115440 (Accessed on July. 21th, 2024).

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information Security Policy Compliance: an Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, 34(3), 523-548.

Cho, S. B., Kwon, D. S. and Lee, M. Y. (2014). A Study on the Information Security Behavior of Corporations Using Health Belief Model, *Asia Pacific Journal of Small Business*, 36(2), 241-263.

Chung, W. (2017). A Study of Policy Acceptance - Based on the Case of the Korea-China Free Trade Agreement (FTA), *The Korean Journal of Advertising and Public Relations*, 19(3), 99-135.

Douglass, R. B. (1977). Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research, *Philosophy & Rhetoric*, 10(2), 130-132.

Etnews. (2023). *25 Trillion Won Lost to Industrial Technology Leaks Over 5 Years... Only 9 Prison Sentences*, *https://www.etnews.com/*20230930000014 (Accessed on July. 21th, 2024).

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

GTT Korea. (2024). *56% of Insider Security Incidents Due to 'Negligence'*, *https://www.gttkorea.com/*news/articleView.html?idxno=9139 (Accessed on July. 21th, 2024).

Guo, K. H. (2013). Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis, *Computers & Security*, 32, 242-251.

Hair, J. F., Hult, G. T. M., Ringle, C. M. and Sarstedt, M. (2022). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) (3rd ed.)*, Thousand Oaks, CA: Sage Publication Inc.

Hair, J. F., Ringle, C. M. and Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet, *Journal of Marketing Theory and Practice*, 19, 139-151.

Hair, J. F., Ringle, C. M. and Sarstedt, M. (2015). A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling, *Journal of the Academy of Marketing Science*, 43(1), 115-135.

Hair, J. F., Sarstedt, M., Hopkins, L. and

Kuppelwieser, V. G. (2014). Partial Least Squares Structural Equation Modeling (PLS-SEM): An Emerging Tool in Business Research, *European Business Review*, 26(2), 106 - 121.

Hair, J. F., Sarstedt, M., Ringle, C. M. and Gudergan, S. P. (2018). *Advanced Issues in Partial Least Squares Structural Equation Modeling*, Thousand Oaks, CA: Sage Publication Inc.

Hankyung. (2023). *Semiconductor Secrets Leaked to China: Samsung Employee Under Investigation for Hundreds of Billions in Bribes*, https://www.hankyung.com/article/202312157871i (Accessed on July. 21th, 2024).

Heo, J. and Ahn, S. (2020). Effects of Biased Awareness of Security Policies on Security Compliance Behavior, *The Journal of Korean Association of Computer Education*, 23(1), 63-75.

Hong, M. J., Lee, Y. J., Lee, K. M., Heo, J. and Yoon, N. (2022). Factors Influencing COVID-19 Vaccination Intention among Korean College Students, *Korean Journal of Health Education and Promotion*, 39(1), 1-10.

Hwang, I. (2021). A Study on the Effects of Organization Justice and Organization Trust on Mitigation of Techno-stress Related to Information Security, *Journal of the Korea Academia-Industrial Cooperation Society*, 22(7), 435-448.

Hwang, I. and Hu, S. (2021). The Influence of Security Motivation and Organization Trust on Information Security Compliance: Focusing on Moderation Effects of Work Promotion Focus, *Journal of Korea Society of Industrial Information Systems*, 26(3), 23-39.

ITBizNews. (2023). *Considerations When Establishing Cybersecurity Operations Policies: 'Both Security Enhancements and Human Factors are Crucial'*, https://www.itbiznews.com/news/articleView.html?idxno=94563#google_vignette (Accessed on July. 21th, 2024).

Jang, C. and Sung, W. (2022). A Study on Policy Acceptance Intention to Use Artificial Intelligence-Based Public Services: Focusing on the Influence of Individual Perception & Digital Literacy Level, *Informatization Policy*, 29(1), 60-83.

Janz, N. K. and Becker, M. H. (1984). The Health Belief Model A Decade Later, *Health Education Quarterly*, 11(1), 1-47.

Jee, B. S., Fan, L., Lee, S. C. and Suh, Y. H. (2011). Personal Information Protection Behavior for Information Quality: Health Psychology Theory Perspectives, *Journal of the Korean Society for Quality Management*, 39(3), 432-443.

Jo, S. C. and Han, Y. J. (2020). A Study on the Effect of Health Belief Factors on the Acceptance of Mobile Healthcare: Focusing on Mediating Effects of Perceived Usefulness, *Regional Industry Review*, 43(2), 263-280.

Jung, J., Lee, J. H. and Kim, C. R. (2016). A Study on the Influence of Firm's Information Security Activities on the Information Security Compliance Intention of Employees, *Convergence Security Journal*, 16(7), 51-59.

Kang, D. and Chang, M. (2014). An Analysis of Compliance with Information Security Policy Effects on Information Security Ability and Behavior: Focused on Workers of Shipping and Port Organization, *Journal of Korea Port Economic Association*, 30(1), 97-118.

Kim, D. J., Hwang, I. H. and Kim, J. S. (2016). A Study on Employee's Compliance Behavior towards Information Security Policy: A Modified Triandis Model, *Journal of Digital Convergence*, 14(4), 209-220.

Kim, H. H., Kang, H. and Choi, Y. J. (2017). A Study on The Effects of HRM in Industrial Security on Job Attitude, *Korean Journal of Industrial Security*, 7(2), 7-31.

Kim, J. and Lim, S. H. (2016). A Preliminary

Research on the Impact of Perception of Personal Information Leakage Incidents on the Behavior of Individual Information Management in the Mobile Banking Contexts, *Journal of The Korea Institute of Information Security & Cryptology*, 26(3), 735-744.

Kim, J. and Suh, W. (2024). An Empirical Study for Enhancing Security Training Effectiveness: From the Perspective of Transfer of Training Theory, *Korean Security Journal*, 78, 1-28.

Kim, J. K. and Jeon J. H. (2006). A Security Behavior Intention Model for Controlling Computer Viruses, *Informatization Policy*, 13(3), 174-196.

Kim, J. K. and Kang, D. Y. (2008). The Effects of Security Policies, Security Awareness and Individual Characteristics on Password Security Effectiveness, *Journal of the Korea Institute of Information Security & Cryptology*, 18(4), 123-133.

Kim, M. J. and Lee, S. B. (2017). The Effect of the Innovativeness of Delivery Application Users on Perceived Traits, Satisfaction, and Continuous Usage Intention: Using the Extended Technology Acceptance Model (ETAM), *International Journal of Tourism and Hospitality Research*, 31(1), 199-214.

Kim, S. and Song, Y. (2011). An Empirical Study on Motivational Factors Influencing Information Security Policy Compliance and Security Behavior of End Users (employees) in Organizations, *The e-Business Studies*, 12(3), 327-349.

Kim, S. W. and Kim, J. H. (2003). An Exploratory Study for Development of Learning Transfer Model in Corporate Training, *Journal of Corporate Education and Talent Research*, 5(1), 83-105.

Kruger, H. A. and Kearney, W. D. (2006). A Prototype for Assessing Information Security Awareness, *Computers & Security*, 25(4), 289-296.

Kwon, Y. and Shin, J. H. (2006). A Study on the Effects of Transfer on Training of Hotel Employees, *Journal of Hospitality and Tourism Studies*, 8(2), 27-43.

Lee, B. K., Oh, H. J., Shin, K. A. and Ko, J. Y. (2008). The Effect of Media Campaign as a Cue to Action on Influenza Prevention Behavior: Extending Health Belief Model, *The Korean Journal of Advertising and Public Relations*, 10(4), 108-138.

Lee, D. H., Kim, T. S. and Jun, H. J. (2018). Factors that Affect the Intention of Password Security Behavior, *Journal of the Korea Institute of Information Security & Cryptology*, 28(1), 187-198.

Lee, J. C. (2010). The Effects of Perceived Organizational Support on Affective Commitment, Turnover Intention and Organizational Citizenship Behavior, *Korean Journal of Business Administration*, 23(2), 893-908.

Lee, K. H., Han, K. S. and Jung, J. S. (2016). A Study of Influencing Factors for Compliance Intention of Personal Information Protection Policy of Public Institution Employees, *Entrue Journal of Information Technology*, 15(1), 75-94.

Lee, M. J., Chung, J. S. and Park, G. S. (2014). The Influence of the Perceived Risk, Perceived Usefulness, and Transparency in the Development of Nuclear Power on Public Acceptability: Using the Trust of Korea Hydro and Nuclear Power (KHNP) Company as a Mediator, *Korean Corporation Management Association*, 21(4), 253-279.

Lee, S. C. and Kwon, Y. J. (2011). The Effect of the Organizational and Individual Characteristics on the Acceptance of the Revised Acts on the Industrial Relations in the Public Institutions: Focused on the Multiple Unions System, *Korean Public Administration Quarterly*, 23(3), 671-692.

Lim, C. H. (2006). Effective Strategies for

Enhancing Information Security Awareness, *Korea Institute of Information Security & Cryptology*, 16(2), 30-36.

Malhotra, N. K., Kim, S. S. and Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model, *Information Systems Research*, 15(4), 336-355.

Ng, B. Y., Kankanhalli, A. and Xu, Y. C. (2009). Studying Users' Computer Security Behavior: A Health Belief Perspective, *Decision Support Systems*, 46(4), 815-825.

Park, C. J. and Yim, M. S. (2012a). An Investigation into the Role of Technostress in Information Security Context, *Journal of Digital Convergence*, 10(5), 37-51.

Park, C. J. and Yim, M. S. (2012b). An Understanding of Impact of Security Countermeasures on Persistent Policy Compliance, *Journal of Digital Convergence*, 10(4), 23-35.

Park, K. (2019). A Study on the Influence of the Perception of Personal Information Security of Youth on Security Attitude and Security Behavior, *Journal of Korea Society of Industrial Information Systems*, 24(4), 79-98.

Piaw, C. Y. (2023). *A Step By Step Guide PLS-SEM Data Analysis Using SmartPLS 4*, Researchtree Education.

Rosenstock, I. M. (1974). Historical Origins of the Health Belief Model, *Health Education Monographs*, 2(4), 329.

Rosenstock, I. M. (2005). Why People Use Health Services, *The Milbank Quarterly*, 83(4).

Shin, S. M., Kim, S. J. and Kwon, D. S. (2016). Study on Personal Information Protection Behavior in Social Network Service Using Health Belief Model, J*ournal of the Korea Institute of Information Security & Cryptology*, 26(6), 1619-1637.

Soh, H. C. and Kim, J. K. (2017). Influence of Information Security Activities of Financial Companies on Information Security Awareness and Information Security Self Confidence: Focusing on the Mediating Effect of Information Security Awareness, *Journal of Korea Society of Industrial Information Systems*, 22(4), 45-64.

Sosik, J. J., Kahai, S. S. and Piovoso, M. J. (2009). Silver Bullet or Voodoo Statistics? A Primer for Using the Partial Least Squares Data Analytic Technique in Group and Organization Research, *Group & Organization Management*, 34(1), 5-36.

Suh, K. H. (2020). Verification of a Theory of Planned Behavior Model of Medication Adherence in Korean Adults: Focused on Moderating Effects of Optimistic or Present Bias Delay Discounting, *The Korean Journal of Health Psychology*, 25(5), 1007-1024.

Sung, W. (2013). A Study on the Acceptance Factors of Smart Work Policy in Korea: Using the User Survey of Smart Work Center, *Korean Policy Studies Review*, 22(1), 331-359.

Yang, E. H. and Chung, J. S. (2006). In Search of Diagnostic Tools for Learning Transfer, *Journal of Corporate Education*, 8(2), 101-122.

Yim, M. S. (2013). The Effect of Characteristics of Information Security Policy on Security Policy Compliance Intention of Employees, *Journal of Digital Convergence*, 11(1), 27-38.

A Study on Improving the Acceptability of Security Policies among Organizational Members: Based on the Health Belief Model

김 보 영 (Boyoung Kim)

- 인하대학교 경영학과 학사
- (현재) 인하대학교 대학원 산업보안거버넌스전공 석사과정
- 관심분야: 보안관리, 보안정책, 인적자원관리

서 우 종 (Woojong Suh)

- 정회원
- 연세대학교 응용통계학과 경제학사
- 연세대학교 응용통계학과 경제학 석사
- KAIST 경영공학과 공학박사
- (현재) 인하대학교 경영학과 교수
- 관심분야: 디지털 비즈니스, 융합보안, 스마트시티