韓國IT서비스學會誌
第19卷 第6號
2020年 12月, pp.83-95

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2020.19.6.083

보호동기이론에 기반한 조직구성원의 보안강화 : 보안정책에 대한 신뢰와 보안스트레스의 매개효과를 중심으로

최희영* · 강주영**

Security Enhancement of Public Organization Members Based on the Protection Motivation Theory

Heeyoung Choi* · Juyoung Kang**

■ Abstract ■

"I think security is only trying to make it uncomfortable."

"10% of my work is entering IDs and passwords, such as boot passwords, mobile phone authentication numbers, etc."

As reflected in the complaint above, stress caused by information security among organizations' members is increasing. In order to strengthen information security, practical solutions to reduce stress are needed because the motivation of the members is needed in order for organizations to function properly. Therefore, this study attempts to suggest key factors that can enhance security while reducing information security stress among members of organizations. To this end, based on the theory of protection motivation, trust and security stress from information security policies are set as mediating factors to explain changes in security reinforcement behavior. Furthermore, risk, efficacy, and reaction costs of cyberattacks are considered as prerequisites. Our study suggests a solution to the security reinforcement problem by analyzing the factors that influence the behavior of members of organizations. In turn, this can raise protection motivation among members.

Keyword : Protection Motivation Theory, Security Enhancements, Security Stress

Submitted : November 12, 2020 1st Revision : December 20, 2020 Accepted : December 24, 2020

* 아주대학교 경영대학 경영정보학과 박사과정
** 아주대학교 경영대학 e-비즈니스학과 교수, 교신저자

1. 서 론

최근 많은 공공기관 및 기업들이 정보 유출 사고 증가 및 개인 정보 강화로 인해 정보보안의 중요성 높아지면서 관리적·기술적·물리적 보안을 강화하고 있다. 이로 인해 조직구성원은 보안기술 적용 및 각종 지시사항 등으로 업무량이 늘어 다음과 같은 불만을 토로하며 보안 스트레스를 받고 있다(CCTV뉴스, 2019). “보안은 불편하게만 만들려고 하는 거 같아요.”, “부팅비밀번호, 윈도우 비밀번호, 네트워크 비밀번호, 이메일 접속 비밀번호, 이메일 접속 시 필요한 휴대폰 인증번호입력, 내 업무에 10%는 id와 비밀번호를 입력하는 겁니다.”, “매주 보안 검사를 해야 하는데 보안 검사를 할 때마다 시간도 오래 걸리고 PC가 너무 느려져서 업무를 재대로 수행할 수가 없어요, 파일이동 시에도 매번 결재를 받아야 해서 자료를 요청할 때나 받을 때마다 번거로움이 이만저만이 아니에요. 정작 보안문서는 몇 개 없는데 비효율적이네요.”, “보안 때문에 스트레스 받습니다. 필요한건 알겠는데 일 좀 합시다.”

이와 같이 조직 구성원이 정보 보안과 관련한 스트레스가 점점 높아지고 있으나 보안 침해 사고가 발생하는 피해 규모액 역시 증가하고 있기 때문에 보안 준수에 대한 스트레스를 감소시키면서 효율적으로 보안 정책을 집행하기 위한 실용적 해법이 더욱 필요한 상황이다. 오진욱, 백승익(2020)은 기업이 새로운 정보보호 정책을 도입할 때, 정보보호 정책에 대한 의도나 취지를 조직구성원들에게 이해시키는 것이 정보보호 준수의도에 영향을 준다고 주장하였다. 특히 보안팀에 근무해 본 경험을 토대로 조직구성원이 회사에서 시행 중인 보안 활동이 실제 회사의 정보 보호 능력을 강화시킬 수 있다고 신뢰하게 된다면 조금 더 능동적으로 보안 강화 조치 활동에 참여하고 보안 준수의도가 높아질 수 있을 것으로 예상된다.

본 연구는 이러한 조직구성원이 보안 준수 활동에 관련한 실무 사례에서 출발하여 실제 조직에서 일어날 수 있는 보안과 관련된 다양한 준수 활동들에 대해 조직구성원의 스트레스를 줄이면서 신뢰를 높이는 데 영향을 줄 수 있는 요인들을 살펴보고자 한다. 이를 위해 보호동기이론을 도입하여 조직구성원의 보안강화에 대한 새로운 접근 방법에 대해 제안하고자 한다.

정보 보안 사고의 발생은 행위주체 관점에서 인적/비인적 요인, 침입 경로 관점에서 내부/외부 침입으로 구분된다. 비인적측면의 경우 대표적인 예로 자연재해를 들 수 있으며, 조직 자체적으로 통제하기 쉽지 않다. 반면 인적측면의 경우 기술적인 해결책을 통해 해결 혹은 미연의 방지가 가능하다. 특히 조직 구성원이 사내에 수립되어 있는 보안 정책을 준수하도록 유도할 수 있다면 내부인에 의한 보안 사고를 미연에 예방할 수 있게 된다(Siponen and Vance, 2010). 하지만, 보안 정책 및 기술이 엄격해질수록, 조직은 정보보안에 대한 관리 및 통제가 수월해지나 조직구성원들은 기존 업무 이외에 추가적인 보안관련 요구사항이 발생되고, 관련 요구사항에 대한 적용과 관련된 보안스트레스를 형성하게 된다. 이렇게 발생된 스트레스는 정보보안 활동 준수의도를 감소시키게 된다(황인호, 김승욱, 2017). 따라서, 기술적 요인이 잘 마련되어 있을지라도 이를 사용하게 되는 조직구성원의 동기가 결여되어 있을 경우 조직에서 마련한 대안들이 제대로 효과를 발휘할 수 없기 때문에 인적요인에 대한 고려가 우선시 되어야 한다 (박철주, 임명성, 2012).

조직구성원의 정보보안 수준을 높이기 위한 방법과 관련된 선행 연구들은 대부분 조직구성원의 보안 준수와 관련된 동기적 측면에서의 접근을 시도하고 있다. 하지만 보안강화를 위해서는 정보보안 수준을 강화하면서 업무 목표 달성뿐 아니라 정보보안 정책 준수를 요구하는 상황에서 발생한 조직구성원의 스트레스를 감소시키기 위한 노력도 필요하다. 즉, 조직구성원의 보안강화행위에 영향을 미치는 다양한 설명 변인들을 찾고, 이를 바탕으로 사이버 보안 강화행위 특성을 분석하여 보안 정책에 반영하는 것이 필요하다. 즉, 조직 구성원 스스로가 사이버 보안을

강화하기 위해 능동적인 대처가 매우 중요해 진 것이다. 따라서 조직구성원의 보안 강화 행동을 이끌어 낼 수 있도록 인식 및 행동을 변화시키기 위한 접근이 필요하며, 행동을 변화시키기 위해 행동에 영향을 미치는 요인에 대한 이해가 중요하다.

본 연구에서는 다양한 분야에서 보호행동의 변화 과정을 설명하기 위한 대표적인 이론인 보호동기이론을 활용하여 조직 구성원의 보안강화 행동에 영향을 미치는 요인을 규명하고자 한다. 보호동기이론을 보안강화 조치 차원에서 살펴보면, 사이버 공격 위험에 대한 조직구성원의 평가인 위협 평가와 외부로부터 발생할 수 있는 위협에 대해 대처하는 능력에 대한 개인의 평가인 대처평가에 의해 인지적 매개과정이 일어난다. 위협평가와 대처평가는 보호동기를 유발하는 중요한 요인으로 보호행동에 영향을 미치게 된다(김종기, 김상희, 2013). 이러한 보호동기이론을 기반으로 보안강화 행동의 변화를 설명하기 위해 정보보안 정책에 대한 신뢰와 보안스트레스를 설정하고, 이에 영향을 미치는 요인으로 사이버공격에 대한 위험과 효능감, 반응비용을 변수로 설정하여 보안강화 행동의도에 어떠한 영향을 미치는지와 어떤 유의미성을 나타내는지 살펴보고자 한다.

2. 이론적 배경

2.1 정보보안 정책 준수의도

정보보안 정책은 조직의 중요한 정보 및 기술 자원들을 관리, 보호, 배포하는데 필요한 일련의 규칙과 실무지침을 규정해 놓은 것으로 조직구성원들에게 보안 기준을 제시하는 것이다(김상현, 송영미, 2011).

이러한 정보보안 정책의 적절한 사용은 최종사용자인 조직구성원 스스로 정보와 기술 자원에 대한 부적절한 활용을 막고 정보보안을 강화하며 정보보안 관련 사고의 확산과 재발 가능성을 억제한다(김상현, 송영미, 2011).

하지만 이 같은 정책들의 수립만으로는 조직구성원의 정보보안 정책 준수 행동을 이끌어 내기에 역부족이다. 조직구성원들이 조직의 정보와 기술 자원을 보호하기 위해 요구되는 활동들을 수행하는데 아무런 동기를 가지지 못하기 때문이다(Stanton et al., 2005).

정보보안 위협을 감소시키기 위해서는 조직원의 자발적인 정보보안 활동이 필요하며, 이러한 보안 준수 활동은 조직원의 정보보안 준수의도(Information Security Compliance Intention)로서 결정된다(Sohrabi Safa et al., 2016). 정보보안 정책 준수의도란 보안 위협으로부터 조직의 중요 정보 자원을 보호하기 위한 조직원들의 자발적인 의지이다(Bulgurcu et al., 2010). 따라서 조직의 정보보안 강화를 위해 조직구성원의 준수의도를 높일 수 있는 전략을 수립하고 조직원에게 정책적 지원을 실시하는 것이 중요하다.

2.2 보호동기이론

보호동기이론(Protection Motivation Theory)이란 개인이 공포에 반응하여 어떻게 태도가 바뀌는지를 설명하는 이론이다(Rogers, 1975). 보호동기이론에 의하면 개인이 심리적으로 위협을 느낄 만한 공포에 노출될 경우, 행위에 자극이 되는 몇 가지 심리적 보호동기들이 만들어진다. 보호동기는 위협평가(Threat Appraisal)와 대처평가(Coping Appraisal)라는 인지적 평가과정에서 비롯된다(Rogers, 1975).

위협평가란 위협적 사건에 의해 제기된 위험수준에 대한 개인의 평가이고, 대처평가는 위협으로부터 발생하는 잠재적인 손실을 방지하고 대처하는 능력에 대한 개인의 평가이다. 대처평가는 적응반응으로 위협적인 사건에 대해 제안된 행동을 수행하거나 대처할 수 있는 개인의 능력에 대한 믿음을 의미하는 자기효능감과 제안된 행동을 수행하였을 때 기대되는 능력에 대한 믿음을 의미하는 반응효능감, 그리고 제안된 행동을 수행할 때 지출된 시간, 노력 등의 인지된 기회비용인 반응비용으로 표현할 수 있다. 이러한 효능감 변수는 적응반응의 확률을 증가시키고 반응비용은 적응반응의 확률을 감소시켜 대처평가가 이루어지게 한다(Ifinedo, 2012).

Siponen et al.(2006)은 정보시스템 보안정책 준수를 설명하기 위해 보호동기이론을 적용하여 조직 보안에 대한 지각된 위협이 조직원들의 조직 보안정책을 준수하려는 의지에 영향을 미친다고 주장하였다.

본 연구에서는 선행연구에서 사용된 보호동기이론의 주요 요인을 중심으로 지각된 위험의 심각성과 효능감, 반응비용이 정보보안 정책 준수의도에 미치는 영향력을 알아보고자 한다.

2.3 신뢰-위험모델

지금까지 수많은 연구에서 개인의 태도 및 행동을 설명하고자 신뢰나 위험 개념을 사용해 왔으며, 신뢰와 위험 개념을 동시에 사용하여 설명하는 연구도 다수 존재한다.

심리적 상태 관점에 따른 신뢰는 불확실성 하에서 피신뢰자의 행동에 대해 신뢰자가 기꺼이 위험을 감수하고자 하는 의지로 정의된다(Kim and Kim, 2013). 심리적 상태 관점의 신뢰는 위험 및 위험감수와 직접적인 관계를 가지므로 개인행동을 설명하기 위해 위험 개념과 관련지어 연구가 진행되어 왔다. 이처럼 신뢰와 위험 간의 관계를 설명하고 있는 신뢰-위험 모델에서는 신뢰를 위험의 선행요인으로 보는 관점과 위험을 신뢰의 선행요인으로 보는 관점이 있다.

<표 1>과 같이 신뢰-위험 모델의 결과요인은 대부분 행동과 관련된 태도 및 의도로 연구되어 왔다. 신뢰와 위험 중 어떤 개념이 선행요인인지 상관없이 두 개념 모두 행동 의도에 있어 중요한 영향을 미친다는 것을 실증분석을 통해 확인 할 수 있다.

2.4 보안 스트레스

정보보안 관련 스트레스는 개인과 조직의 정보보안 요구사항에 따른 불균형에 의하여 발생한다. 조직구성원들은 보다 엄격해지는 정보보안 정책 및 난이도 높은 정보보안 기술로 보안관련 업무 스트레스를 받고 있고 이에 따라 정보보안 준수의도에 부정적 영향을 미치고 있음이 증명되었다(황인호, 김승욱, 2017).

조직은 정보보안 수준을 강화하면서 조직구성원에게 업무 목표 달성뿐 아니라 정보보안 정책준수를 요구하게 된다. 이때 조직구성원은 업무 목표 달성과 보안 목표 달성간의 갭으로 인하여 업무 갈등이 발생할 수 있다. 예를 들어 조직구성원이 업무상 협의 시 외부 협력사에게 내부 정보를 제공해야 할 경우가 발생할 때, 정보 제공에 대한 허가와 같은 정보보안 정책을 지키지 않는 것이 업무의 편의성과 빠른 성과 달성에 도움이 된다. 이러한 상황에서 조직구성원은 자신의 역할에 대한 갈등을 일으킬 수 있다(Tarafdar et al., 2007).

임광수, 권헌영(2016)은 기업마다의 정보보호활동 및 이에 수반되는 보안정책으로부터 수용자가 직간접적으로 체감하는 인지된 보안 스트레스 유발 요인을 알아내고자 보안정책 준수의도에 영향을 미치는 독립변수들과 보안스트레스를 종속변수로 하여 분석하였다.

〈표 1〉 신뢰 및 위험 관련 실증연구

신뢰 및 위험요인 설정	연구자	연구분야	선행요인	결과요인
신뢰 → 위험	Pavlou,et al.(2002)	온라인 시장	제도적 구조	거래의도
	Malhotra et al.(2004)	온라인 환경	프라이버시염려	개인정보 공개 의도
	장명희(2005)	인터넷 쇼핑몰	이해 타산적 믿음, 구조적 보장, 상황적 규범, 친숙함	구매의도
위험 → 신뢰	McKinght et al.(2002)	전자 상거래	지각된 평판, 지각된 품질, 구조적 보장	구매의도, 개인정보 공유의도
	Dinev et al(2006)	전자 상거래	-	개인정보 제공의도
	서보밀(2002)	인터넷 뱅킹	보안통제의 인지된 강도	사용태도, 사용의도, 실제 사용

본 연구에서는 보안스트레스를 매개로 하여 보안정책 준수의도에 영향을 미치는 독립변수와 인과관계를 분석하고 이 관계가 준수의도에 미치는 영향을 분석하고자 한다.

3. 연구모형 및 가설설정

기존 선행연구는 보안 규정이나 규범을 조직구성원에게 교육시켜 보안인식을 제고하는 일방향적 보안문화에 대하여 진행되었다. 하지만 양적·질적으로 변화하는 보안위협에 대한 대응을 위해서는 조직구성원들의 자발적인 참여에 의한 참여형 보안문화로의 전환이 필요한 시점이다. 따라서 본 연구에서는 보안정책준수의도에 영향을 주는 요인인 공포, 신뢰, 스트레스의 대한 연구로 연구모형 및 가설을 제시하여 조직구성원의 보안강화조치행동의도에 영향을 미치는 요인을 실증적으로 분석하고자 [그림 1]과 같은 연구 모형을 설계하였다.

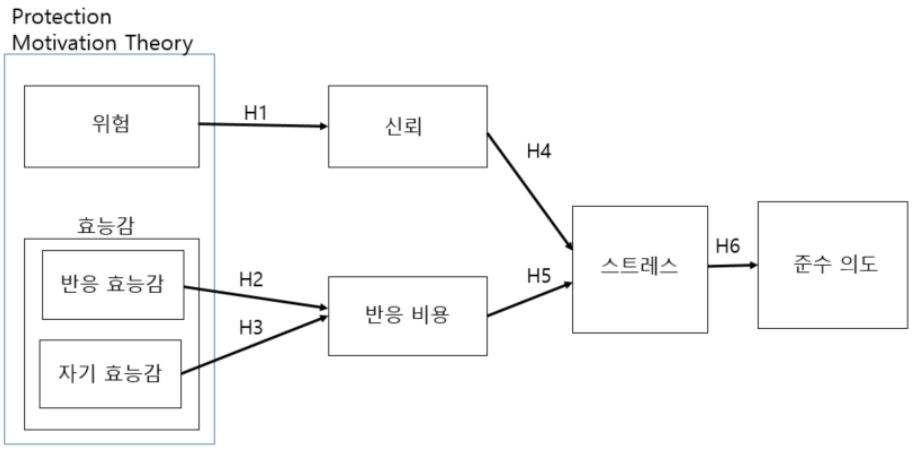
Ramachandran and Rao(2006)는 보안문화 모델을 발전시키기 위해서는 보안에 대한 신뢰가 직원들에게 보안 인식과 보안 준수를 이끌어 낼 수 있다고 하였다. 또한 신뢰는 보안 정책, 보안 표준 등의 요소에 의해 영향을 받아 보안준수 의도를 높일 수 있다고 주장하였다.

Mayer et al.(1995)은 신뢰를 신뢰자(trustor)가 피신뢰자(trustee)에게 필요한 업무 등을 안전하고 정확하게 수행할 것이라는 기대감을 바탕으로 하여 피신뢰자의 행동을 기꺼이 믿으려는 의지로 정의하였다.

본 연구에서는 이러한 신뢰를 조직에서 조직구성원과 보안정책에 대입하여 조직구성원이 보안정책이 안전하고 정확하게 수행할 것이라는 기대감을 신뢰로 정의 하였다. Huigang and Yajiong(2010)은 인지된 위협이 이러한 위협을 회피하고자 하는 행동에 변화를 가져 온다고 가정하고 실증분석을 통해 검증하였다. 본 연구에서는 이러한 선행연구와 신뢰-위험모델에서 위험을 신뢰의 선행요인으로 보는 관점을 바탕으로 사이버 공격의 대한 인지된 위험이 조직 내에서 이를 회피할 수 있게 만들어주는 수단인 보안정책에 대한 신뢰에 영향을 미친다는 연구가설을 설정하였다.

H1 : 사이버공격에 대한 위험은 보안강화조치에 대한 신뢰의 정(+)의 영향을 미칠 것이다.

반응효능감이란 보안강화조치 활동 시, 이 예방조치가 얼마나 효과적인지의 정도이고 자기효능감은 보안강화조치를 할 수 있는 자신의 능력에 대한 믿음의 정도로(Johnston and Warkentin, 2010), 이러한 효능감이 보안강화조치를 업무에 적용함으로써 드는 반응비용으로 인한 부정적 인식을 줄일 수 있다고 가정하였다(Woon et al., 2005).



[그림 1] 연구모형

H2 : 보안강화조치 반응효능감은 반응비용의 부(-)의 영향을 미칠 것이다.

H3 : 보안강화조치 자기효능감은 반응비용의 부 (-)의 영향을 미칠 것이다.

보안강화조치에 따른 통제와 이로 인한 스트레스는 보안강화조치 행동 의도에 영향을 준다고 가정한 요인인 신뢰에는 부정적인 영향을 주게 되고, 반응비용으로부터 오는 부정적 인식은 더 높인다고 가정할 수 있다(Johnston and Warkentin, 2010). 따라서 이러한 스트레스가 보안강화조치 의도에 영향을 주는 변수와 준수의도 사이에 미치는 영향에 대해 파악하고자 하였다.

H4 : 보안강화조치에 대한 신뢰는 보안스트레스의 부(-)의 영향을 미칠 것이다.

H5 : 반응비용은 보안스트레스의 정(+)의 영향을 미칠 것이다.

H6 : 보안스트레스는 보안강화조치 준수의도에 부(-)의 영향을 미칠 것이다.

4. 실증분석

4.1 자료수집 및 연구방법

본 연구는 조직구성원들의 보안 행동에 대한 이해를 돕기 위함이므로 보안정책이나 규제가 민간기업보다 빠르고 엄격하게 적용되고 있는 공공기관에서 근무하는 조직구성원들을 대상으로 설문조사를 실시하였다. 설문조사 결과 총 144부를 회수하여 본 연구에서 제안한 연구모형의 분석을 위해 사용하였다. 기초적인 자료 분석은 SPSS23으로 진행하였고, 구조방정식 모형분석은 SmartPLS 3.0을 분석도구로 활용하였다.

<표 2>와 같이 연구모형의 변수들을 측정하기 위해 국내외 선행연구들을 바탕으로 도입된 측정항목을 본 연구의 목적에 맞게 수정·보완하였다. 도출된 모든 측정항목은 7점 리커트 척도를 사용하였다(1점 전혀 그렇지 않아 -7점 매우 그렇다).

〈표 2〉 변수의 조작적 정의

잠재변수	측정변수	측정항목	출처
위험	SEV1	내가 PC보안 강화 조치 절차를 준수하지 않을 경우 우리 회사에 보안이 취약해질 수도 있다는 사실을 알고 있다	임광수 외 (2016)
	SEV2	내가 PC보안 강화 조치 절차를 준수하지 않는다면 해킹을 당할 수 있다	
	SEV3	내가 PC보안 강화 조치 활동에 관심을 기울이지 않는다면 우리 회사 정보가 위태로워질 수 있다.	
반응 효능감	REFF1	PC보안 강화 조치 준수는 내 정보에 불법적 접근(해킹)이 이루어지지 않게 예방하는데 도움이 된다고 생각한다.	황성민 (2018)
	REFF2	PC보안 강화 조치 준수는 악성코드나 바이러스 침해를 예방하는데 도움이 된다고 생각한다.	
자기 효능감	SEFF1	나는 PC보안 강화 조치를 마음먹으면 진행 할 수 있다.	우형진 (2014)
	SEFF2	나는 PC보안 강화 조치를 위해 여러 가지 사이버 보안 장치를 업데이트 할 수 있다.	
	SEFF3	나는 PC보안 강화 조치를 위해 다양한 소프트웨어와 기술을 설치할 수 있다.	
신뢰	TST1	PC보안 강화 조치 활동에 참여는 보안제도 운영과 보안 규정의 확실한 준수에 도움이 된다	황성민 (2018)
	TST2	PC보안 강화 조치로 업무내용의 기밀성이 철저히 보장되고 있다.	
스트레스	SSTSS1	PC보안 강화 조치 활동으로 인해 나는 부담을 느낀다.	임광수 외 (2016)
	SSTSS2	PC보안 강화 조치 활동으로 인해 나는 압박을 받는다고 느낀다.	
반응 비용	RCOS1	PC보안 강화 조치 절차에 따르지 않을 경우, 나의 업무 성과가 향상된다.	임광수 외 (2016)
	RCOS2	PC보안 강화 조치 절차에 따르지 않을 경우, 정해진 시간 동안 더욱더 많은 일을 해낼 수 있다.	
	RCOS3	PC보안 강화 조치 절차에 따르지 않을 경우, 나의 업무를 더욱더 빨리 끝낼 수 있다.	
준수 의도	INTN1	나는 PC보안 강화 조치 절차를 따를 의향이 있다.	임광수 외 (2016)
	INTN2	나는 PC보안 강화 조치 방안에 명시된 나의 책임을 준수할 의도가 있다.	
	INTN3	나는 나의 의도에 의해 PC보안 강화 조치 절차를 따른다.	

〈표 3〉 인구통계학적 특성

구분		빈도(명)	비율(%)
직종	사무	64	38.6
	기술	80	48.2
근무 년수	3년 이하	22	13.3
	3년 이상~7년 이하	23	13.9
	7년 이상~10년 이하	11	6.6
	10년 이상~15년 이하	15	9.0
	15년 이상	74	44.6
해킹피해경험	있음	6	3.6
	없음	138	83.1

응답 결과의 인구통계학적 특징은 <표 3>과 같다. 직종은 사무 64명(38.6%), 기술 80명(48.2%)으로 나타났으며, 근속년수는 3년 이하 22명(13.3%), 3년 이상~7년 이하 23명(13.9%), 7년 이상 10년 이하 11명(6.6%), 10년 이상~15년 이하 15명(9%), 15년 이상이 74명(44.6%)으로 가장 많았다. 해킹 피해 경험은 6명(3.6%)만 있다고 응답하였고, 응답자의 대부분인 138명(83.1%)은 없는 것으로 나타났다.

측정 모형을 추정하여 측정변수의 질을 평가한 후 구모모형을 추정하여 연구모형에 대한 가설검증을 수행하는 2단계 분석법(Two-step Analysis)으로 연구모형을 검증하였다. 2단계로 측정모형과 구조모형을 구분하여 분석함으로써 측정변수의 신뢰성을 정확히 추정하여 해석상 혼동을 줄이고자 하였다(James and David, 1988).

4.2 측정모형 분석

2단계 분석법에 따라 구조모형을 분석하기 전에 측정변수의 신뢰성 및 타당성을 평가하기 위하여 측정모형을 분석하였다. 측정모형의 신뢰성을 평가하기 위해 Cronbach's α, 평균분산추출(AVE : Average Variance Extracted), 합성신뢰도(CR : Composite Reliability)를 이용하였다.

Cronbach's α는 한 구성개념을 이루고 있는 측정변수들의 내적일관성을 측정하기 위한 값이고, 평균분산추출은 한 구성개념을 이루고 있는 측정변수들이 설명되는 분산의 비율을 의미하며 합성신뢰도는 측정변수들 간의 공유분산을 의미한다. 일반적으로 Cronbach's α가 0.7 이상, 평균분산추출이 0.5 이상, 합성신뢰도가 0.7 이상이면 신뢰성이 있다고 평가한다(Nunally, 1978).

<표 4>와 같이 각 요인들은 Cronbach's α가 0.7 이상, 평균분산 추출이 0.5 이상, 합성신뢰도가 0.7 이상으로 나타났으며, 각 구성개념의 추정치도 모두 0.5 이상으로 나타나 측정모형의 신뢰성과 집중타당성이 확보된 것으로 평가할 수 있다.

〈표 4〉 측정 변수의 신뢰성 및 집중타당성 분석

잠재변수	측정변수	Factor Loading	Cronbach's α	AVE	Composite reliability
위험	SEV1	0.918	0.924	0.864	0.950
	SEV2	0.938			
	SEV3	0.933			
반응효능감	REFF1	0.974	0.929	0.933	0.965
	REFF2	0.958			
자기효능감	SEFF1	0.937	0.934	0.883	0.958
	SEFF2	0.949			
	SEFF3	0.933			
신뢰	TST1	0.978	0.956	0.958	0.978
	TST2	0.979			
스트레스	SSTSS1	0.985	0.970	0.971	0.985
	SSTSS2	0.986			
반응비용	RCOS1	0.916	0.941	0.896	0.963
	RCOS2	0.972			
	RCOS3	0.951			
준수의도	INTN1	0.968	0.956	0.919	0.971
	INTN2	0.960			
	INTN3	0.948			

또한 판별타당성 분석을 수행한 결과, <표 5>에서 나타난 바와 같이 평균분산추출의 제곱근이 모두 0.7 이상이고 다른 구성개념과의 상관계수보다 큰 것으로 나타나 판별타당성이 있는 것으로 평가할 수 있다.

4.3 구조모형 평가 및 가설검증

구조모형의 평가는 연구모형을 최종적으로 확정하고 구조모형이 적합한 모형임을 확인하는 절차이다. PLS-SEM에서는 구조모형의 평가를 위해 다중공선성, 결정계수(R^2), 효과크기(f^2), 예측적합성(Q^2)을 검토해야 한다.

연구 변수간의 다중공선성은 내부VIF값으로 평가하게 되는데 모두 5 미만으로 다중공선성이 없다고 판명되었다. 외생연구변수의 내생연구변수에 대한 설명력을 평가하는 결정계수(R^2) 값은 0.082~0.477의 값을 가진다. 외생 잠재변수의 내생잠재변수에 대한 효과크기를 나타내는 f^2은 반응 비용t의 내생연구변수에 대한 보안스트레스 R^2에 기여하는 f^2가 0.626으로 큰 효과 크기를 나타내며 본 연구에서 가장 큰 기여를 하는 것으로 나타났다. 구조모형이 특정 내생연구변수에 대해 예측적 적합성을 가지고 있는지 평가하는 Q^2은 모든 내생잠재 변수들의 값이 0보다 크게 나와 본 연구의 구조모형의 예측 적합성을 지지한다고 판단한다.

측정모형의 신뢰성 및 타당성을 평가한 후 연구가설을 검증하기 위해 구조모형의 분석을 실시하였다.

구조모형의 각 경로에 대한 유의성을 검정하기 위해 반복적인 샘플링을 통해 t-값을 제시하는 부트스트랩핑(Bootstraping)을 실시하였고, 반복샘플링의 수는 500회로 설정하였다(Efron and Tibshirani, 1997).

본 연구의 구조모형에 대한 경로분석을 실시한 결과는 <표 6>과 같다. 연구모형의 각 경로를 살펴보면, 자기효능감과 반응비용간의 경로를 제외한 다른 모든 경로들은 통계적으로 유의한 것으로 분석되었다.

가설 1인 위험과 신뢰간의 관계에서는 경로계수가 0.496으로 긍정적 영향($t = 5.389$, $p > 0.05$)을 미치는 것으로 나타났다. 가설 2와 가설 3인 반응효능감과 자기효능감이 반응비용의 미치는 영향에서 가설 2는 경로계수 -0.283으로 반응 비용에 부정적인 영향을 미치는 것으로 나타났으나 가설 3은 -0.063으로 부정적인 관계는 가지나 통계적으로 유의하지 않은 것으로 나타났다. 이 같은 결과는 준수 행동을 충분히 지킬 수 있는 개인의 자신감이나 역량은 개인적 행위를 하는 것에 있어서는 의도에 영향을 미치게 되지만, 조직구성원으로써 조직의 정책을 따르는 행위에는 영향을 미치지 못함을 나타낸다.

스트레스의 영향을 미친다고 가정한 가설4의 신뢰와 가설 5의 반응비용 효과에서는 신뢰는 경로계수 -0.136으로 스트레스의 부정적인 영향($t = 1.799$, $P < 0.01$)을 주는 것으로 나타났고, 반응비용은 경로계수 0.625로 반응비용과 스트레스간의 정의 효과($t = 8.892$, $P > 0.05$)가 있는 것으로 나타났다. 보안강화조치의도의 영향을 미치는 요인과 스트레스의 관계를 알아보기 위한 가설 6은 경로계수 -0.286으로 스트레스가 의도에 부정적인 영향($t = 2.564$, $P > 0.05$)을 주는 것으로 나타났다.

〈표 6〉 가설 검증 결과

Hypothesis	Path coefficient(O)	T Statistics	Results
H1 : 사이버공격에 대한 위험은 보안강화조치에 대한 신뢰의 정(+)의 영향을 미칠 것이다.	0.496	5.389	Supported
H2 : 보안강화조치 반응효능감은 반응비용의 부(-)의 영향을 미칠 것이다.	-0.283	3.315	Supported
H3 : 보안강화조치 자기효능감은 반응비용의 부(-)의 영향을 미칠 것이다.	-0.063	0.713	Not Supported
H4 : 보안강화조치에 대한 신뢰는 보안스트레스의 부(-)의 영향을 미칠 것이다.	-0.136	1.799	Supported
H5 : 반응비용은 보안스트레스의 정(+)의 영향을 미칠 것이다.	0.625	8.892	Supported
H6 : 보안스트레스는 보안강화조치 준수의도에 부(-)의 영향을 미칠 것이다.	-0.286	2.564	Supported

5. 결 론

본 연구는 조직구성원의 보안강화조치 행동 의도에 영향을 미치는 요인을 보호동기이론을 기반으로 보안정책에 대한 신뢰와 보안규율 강화에 따른 스트레스를 매개로 살펴보고자 하였다.

먼저 보안강화조치 행동의도에 영향을 미치는 요인으로 사이버공격에 대한 위험과 보안강화조치 활동 시 예방조치가 얼마나 효과적인지의 정도를 나타내는 반응효능감을 살펴보았다. 그리고, 보안강화조치를 할 수 있는 자신의 능력에 대한 믿음의 정도인 자기효능감과 보안강화조치를 업무에 적용함으로써 드는 반응비용을 설정하여 인과관계를 살펴볼 수 있도록 연구 모형을 설계하였다. 보호동기를 유발하는 요인인 신뢰와 보호동기를 저해하는 요인인 스트레스를 매개요인으로 설정하였다.

본 연구의 분석결과는 다음과 같다. 총 6가지 가설 중 자기효능감과 반응비용간의 관계를 설정한 가설을 제외한 5가지의 가설이 채택되었다.

첫째, 보호동기요인의 영향력은 사이버공격에 대한 위험과 보안강화조치에 대한 신뢰 간의 관계에서는 유의한 설명력을 가지는 것으로 나타났다. 효능감에서는 반응효능감만이 반응비용과의 관계에서 유의미한 설명력을 가지는 것으로 나타났고 자기효능감은 유의한 설명력을 가지지 않는 것으로 분석되었다. 조직의 보안조치행동에 미치는 영향은 개인의 능력에 따른 효능감보다는 보안정책으로 인해 행해지는 보안절차가 효과적인지의 여부가 보안강화조치를 업무에 적용함으로써 드는 반응비용에 대한 부정적 인식을 줄어들게 하는 효과를 가진다고 할 수 있다.

둘째, 보안스트레스의 매개효과를 보호동기요인과 의도, 보안강화조치에 대한 신뢰 사이에서 확인할 수 있었다. 보안강화조치에 따른 통제로부터 오는 스트레스는 보안강화조치 활동이 사이버 공격을 예방하기 위하여 올바르게 진행되고 있다고 믿는 신뢰가 높아질수록 낮아지고, 보안강화조치에 따른 반응비용이 높아질수록 스트레스 또한 증가하였다. 또한 이러한 스트레스는 보안강화조치 행동을 하고자 하는 의도에 부정적인 영향을 미치는 것으로 분석되었다.

본 연구의 시사점은 다음과 같다. 정보보안과 관련된 정책을 배포하고 있는 기업의 이러한 정책을 업무에 적용함으로써 스트레스를 받고 있는 조직구성원들을 대상으로 정보보안 정책 준수 의도에 영향을 주는 요인들에 대한 실증적 연구를 하였다. 다양한 분야에서 보호행동 변화를 설명하고자 제시된 보호동기이론을 정보보안활동의도에 적용하여 보안강화조치의도에 미치는 영향에 대한 접근을 시도하였다. 보호동기이론을 기반으로 조직구성원의 인지적 평가 과정을 통하여 보호동기가 형성됨으로 인해 보안강화조치를 수행하고자 하는 보호행동의 변화가 일어난다고 보았다. 본 연구에서는 다양한 선행연구에서 행동을 설명하기 위해 사용되어온 개인의 신념 및 태도를 나타내는 신뢰와 위험의 상호작용 관계를 보호동기요인으로 설정하여 실증적인 분석을 시도하였다는 점에서 의의를 찾을 수 있다. 또한 정보보안 준수행동 수준을 높이기 위해 보안관련 스트레스를 설정하여 정보보안 행동 의지 감소 관점에서 접근하였다.

따라서 본 연구는 조직구성원들의 정보보안 행동과 관련된 문제들을 이해하는데 유용한 이론적 자료가 될 수 있다. 또한 이 같은 동기 요인들의 유효성을 검증하고 조직의 관리자들에게 정보보안 정책 준수를 강화시킬 수 있는 방법을 제안한다는 데 본 연구의 의의가 있다.

정보보안에 대한 관심 및 투자가 지속적으로 높아지면서, 조직구성원들은 자신의 고유 업무에 조직에서 요구하는 정보보안 기술 및 정책 준수를 이행해야하는 부담감의 수준이 높아지고 있으며, 변화하고 증가하는 보안요구 수준과 고유 업무 이행간의 갈등으로 인한 보안 관련 스트레스가 높아지게 되는 현상이 발생하고 있다.

따라서 조직구성원에게 보안강화조치행동이 불필요하고 추가적인 업무를 야기하는 것이 아니라 실제적으로 보안공격을 예방하는 효과가 있다고

믿는 신뢰와 사이버 공격에 대한 위험성에 대한 인식을 높임으로써 상호조절 효과를 낼 수 있는 대책이 필요하다.

이러한 정보보안 정책 행동을 유발할 수 있는 동기요인들에 대한 실증적 연구는 부족한 실정이다. 본 연구는 이전 연구에서 실증적으로 연구되지 않은 이러한 요인들과의 인과관계를 이론화하여 증명했다는데 그 의미가 있다.

기술발달에 따라 기업들의 정보시스템에 대한 의존도가 높아지고 있는 만큼 기업은 정보 보안 정책을 강화하고 관련 행동을 구성원들에게 요구하면서 조직구성원들 스스로 이러한 보안스트레스를 받지 않고 능동적으로 참여 할 수 있게 정보보안에 대한 인식 향상과 조직 문화의 변화가 어느 때보다 요구되고 있다. 따라서 본 연구를 통해 조직구성원들의 정보보안 행동에 결정적 영향 요인이라 판단되는 정보보안 정책 준수의도에 어떤 동기 요인들이 작용하는지에 대한 이해를 높이고 기업의 정보보안 관련 실무자들이 정보보안 문제에 대한 예방책과 해결책 제시를 위한 학문적 기반이 될 수 있다.

또한 이러한 시도는 향후 기업 내 정보보안에 대한 조직구성원의 행동을 설명하는 이론적 배경이 될 것이며 실무적으로는 기업의 정보보안 정책 수립 및 강화에 이론적 기반이 될 수 있을 것이다.

본 연구는 몇 가지 제약사항이 있으며. 향후 연구에서 보완될 필요성이 있다.

최초 설문 문항에는 보안강화조치 미준수로 인한 사이버 해킹 위험을 위험 발생가능성과 위험 심각성으로 나누어 각각의 영향력을 확인하고자 하였으나, 잠재변수들 간의 집중타당도 분석결과 외부적재치의 적합성검증에서 유의한 결과를 내지 못하여위험 발생가능성 항목을 삭제 하였다. 이는 조직구성원들이 사이버 공격 위험에 대한 심각성은 인지하고 있지만 이러한 공격이 실제로 자신들에게는 발생하지 않을 거란 인식을 볼 수 있다. 따라서 조직구성원에게 정보보안교육 활동 등을 통하여 사이버공격이 실제로 본인들이 근무하는 기업에 동료에게 발생하였고, 앞으로도 자신을 포함한 누군가에게 발생 할 수 있으며, 이러한 사이버 공격의 발생을 보안강화조치 행동을 준수하는 것만으로도 예방할 수 있다는 점을 인지시켜야 할 것이다.

향후 연구에는 업종 및 기업 마다 상이한 보안환경과 상황 등을 고려하여 보안인식 수준을 조절함으로써 기업별, 업종별 조직문화 분위기에 따른 보안인식의 차이를 추가로 분석하여 또 다른 시사점을 도출 해 낼 수 있을 것이다.

또한 보호동기에 영향을 주는 요인들이 보호동기 뿐 아니라 실제 행동으로 연계되는 부분을 추가로 검증하여 조직구성원들이 업무를 수행함에 있어 의도를 가지고 있더라도 실제로 행동까지는 얼마나 미치게 되는지를 추가로 분석하여 조직구성원들의 정보보안 행동과 관련된 문제를 풀어 나갈 수 있을 것이다.

참고문헌

김상현, 송영미, “조직구성원들의 정보보안 정책 준수 동기요인에 관한 연구”, *e-비즈니스연구*, 제12권, 제3호, 2011, 327-349.

김종기, 김상희, “온라인 환경에서 프라이버시 행동의도에 미치는 영향-보호동기이론을 중심으로”, *정보화정책*, 제20권, 제3호, 2013, 63-85.

박철주, 임명성, “보안 대책이 지속적 보안 정책 준수에 미치는 영향”, *디지털융복합연구*, 제10권, 제4호, 2012, 23-35.

오진욱, 백승익, “정보보호 정책의 전유과정이 정보보호 준수의도에 미치는 영향에 대한 탐색적 연구 : 콜센터와 병원 종사자들을 중심으로”, *한국IT서비스학회지*, 제19권, 제5호, 2020, 15-31.

우형진, “지각된 사이버 보안 위험이 개인정보보호 증진을 위한 기술채택 및 지속이용 행위의도에 미치는 영향에 관한 연구 : 관여도, 보호동기, 비용지불의사를 중심으로”, *언론과학연구*, 제14권, 제2호, 2014, 220-257.

임광수, 권헌영, “통제수용자에 의해 인지된 정보보안정책 특성요인이 보안스트레스와 보안준수의도에 미치는 영향에 대한 연구”, *한국인터넷방송통신학회 논문지*, 제16권, 제6호, 2016, 243-253.

황성민, “보안관제에서의 보호동기요인이 자기효능감과 보안신뢰를 통해 정보보안성과에 미치는 영향”, 건국대학교 정보통신대학원 석사학위논문, 2018.

황인호, 김승욱, “조직원의 정보보안 관련 업무 스트레스에 대한 억제 및 업무대처에 대한 연구”, *e-비즈니스연구*, 제18권, 제3호, 2017, 147-164.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat, “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness”, *MIS Quarterly*, Vol.34, No.3, 2010, 523-555.

CCTV뉴스, “개인 직무효율성 떨어뜨리는 정보보안 테크노스트레스”, 2019, https://www.cctvnews..co.kr/news/articleView.html?idxno=108330

Efron, B. and R. Tibshirani, “Improvements on Cross-Validation : The .632+ Bootstrap Method”, *Journal of the American Statistical Association*, Vol.92, No.438, 1997, 548-560.

Huigang, L. and X. Yajiong, “Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective”, *Journal of the Association for Information Systems*, Vol.11, No.7, 2010, 394-414.

Ifinedo, P., “Understanding Information Systems Security Policy Compliance : An Integration of the Theory of Planned Behavior and the Protection Motivation Theory”, *Computers and Security*, Vol.31, No.1, 2012, 83-95.

James, C.A. and W.G. David, “Structural Equation Modeling in Practice : A Review and Recommended Two-Step Approach”, *Psychological Bulletin*, Vol.103, No.3, 1988, 411-412.

Johnston, A.C. and M. Warkentin, “Fear Appeals and Information Security Behaviors : An Empirical Study”, *MIS Quarterly*, Vol.34, No.3, 2010, 549-570.

Kim, J. and S. Kim, “Privacy Behavioral Intention in Online Environment : Based on Protection Motivation Theory”, *Informatization Policy*, Vol.20, No.3, 2013, 63-85.

Mayer, R.C., J.H. Davis, and F.D. Schoorman, “An Integrative Model of Organizational Trust”, *Academy of Management Review*, Vol.20, No.3, 1995, 709-734.

Nunally, J.C., Psychometric Theory, 2nd ed, New York, NY : McGraw-Hill, 1978.

Ramachandran, S. and S. Rao, “Security Cultures in Organizations : A Theoretical Model”, *AMCIS 2006 Proceedings*, 2006.

Rogers, R.W., “A Protection Motivation Theory of Fear Appeals and Attitude Change”, *Journal of Psychology*, Vol.91, No.1, 1975, 93-114.

Siponen, M., S. Pahnila, and A. Mahmood, “Factors Influencing Protection Motivation and Is Security Policy Compliance”, *Proceedings of 2006 Innovations in Information Technology*, 2006.

Siponen, M. and A. Vance, “Neutralization : New Insights into the Problem of Employee Information Systems Security Policy Violations”, *MIS Quarterly*, Vol.34, No.3, 2010, 487-502.

Safa, S.N., R. Von Solms, and S. Furnell, “Information Security Policy Compliance Model in Organizations”, *Computers and Security*, Vol.56, 2016, 70-82.

Stanton, J.M., K.R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of End User Security Behaviors", *Computers and Security*, Vol.24, No.2, 2005, 124-133.

Tarafdar, M., Q. Tu, S. Ragu-Nathan Bhanu, and T.S. Ragu-Nathan, "The Impact of Technostress on Role Stress and Productivity", *Journal of Management Information Systems*, Vol.4, No.1, 2007, 301-328.

Woon, I., G.-W. Tan, and R. Low, "A Protection Motivation Theory Approach to Home Wireless Security", *ICIS 2005 Proceedings*, 2005.

About the Authors

최 희 영 (hy2748@ex.co.kr)

아주대학교 경영정보학 석박사 통합과정을 수료하였고, 인하대학교 컴퓨터공학과에서 학사를 취득하였다. 현재 한국도로공사 대전충남본부에서 경영정보업무를 담당하고 있으며, 주요 관심분야는 정보화전략, 정보시스템 보안관리, 빅데이터, 텍스트마이닝 등의 관한 연구이다.

강 주 영 (jykang@ajou.ac.kr)

현재 아주대학교 경영대학 e-비즈니스학과 교수로 재직 중이며, 포항공과대학교 컴퓨터공학과에서 학사, 서울대학교 컴퓨터공학과에서 석사, 한국과학기술원 경영공학전공에서 공학박사학위를 취득하였다. 주요 관심분야는 빅데이터, 텍스트마이닝, 시맨틱 웹, 지능형 정보시스템 등이다.