Journal of The Korea Convergence Society
Vol. 13. No. 1, pp. 283-295, 2022
e-ISSN 2713-6353
DOI : https://doi.org/10.15207/JKCS.2022.13.01.283

정보보안 중요성 인식에 관한 연구: 예방동기이론 관점에서

임명성
삼육대학교 경영학과 부교수

Information Security Importance Perception: Protection Motivation Theory Perpectives

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

요 약 본 연구는 조직 구성원들의 정보보안 중요성 인식에 영향을 미치는 요인을 탐색하고자 한다. 이를 위해 예방 동기 이론을 근간으로 인지된 처벌 확신성, 인지된 대응 비용, 묵인이 인지된 정보보안 중요성 인식에 미치는 영향을 살펴보았다. 분석 결과는 다음과 같다. 첫째, 인지된 처벌 확신성은 정보보안 중요성 인식에 유의한 영향을 미치는 것으로 나타났다. 또한, 인지된 처벌 확신성은 묵인에 부정적 영향을 미치는 것으로 나타났다. 둘째, 대응 비용은 정보보안 중요성 인식에 긍정적 영향을 미치는 것으로 나타났다. 또한, 대응 비용은 묵인에 긍정적 영향을 미치는 것으로 나타났다. 마지막으로 묵인은 정보보안 인식 중요성에 부정적 영향을 미치는 것으로 나타났다. 따라서, 구성원들의 정보보안 중요성 인식을 위해서 보안 위반 행위에 확실한 처벌이 뒤따를 수 있다는 것을 인식시킬 필요가 있다. 동시에, 조직은 구성원들이 보안 행동을 수행하는 데 있어서 장해가 되는 요소들을 제거하는 시도도 해야 한다. 마지막으로, 조직의 보안에 관한 열린 소통이 가능하도록 해야 한다.

주제어 : 예방 동기 이론, 정보보안, 묵인, 처벌, 대응 비용, 인지된 중요성

Abstract This study attempts to explore factors that influence the perception of importance of information security. Three possible exogenous variables including perceived certainty of punishment, perceived response cost, and acquiescense are suggested that are based on the protectiom motivation theory. As a result, we found followings. First, The perceived punishment certainty has a significant effect on the perceived importance of information security. Also, it influences a negative effect on acquiescence. Second, the response cost has a negative effect on the perceived importance of information security. In addition, the response cost positively effects on acquiescence. Finally, acquiescence negatively influences on the perceived importance of information security. The results show that, in order to increase the perceived importance of information security among employees, it is necessary to make them aware that a security violation can result in certain punishment. At the same time, organizations should also attempt to remove major obstacles accompanying security behaviors of employees. Finally, organizations encourage open communication relating to information security among employees.

Key Words : Protection Motivation Theory, Information Security, Acquiescence, Punishment, Response Cost, Perceived Importance

*Corresponding Author : Myung-Seong Yim(msyim@syu.ac.kr)

Received September 26, 2021
Revised January 12, 2022
Accepted January 20, 2022
Published January 28, 2022

1. 서론

ICTs(Information and Communication Technologies)의 발전과 함께 정보보안(InfoSec: Information Security) 사고는 감소하는 것이 아니라 기술의 발전에 비례해 증가하고 있다. 특히, 코로나19로 인해 기존과 다른 업무 환경 그리고 비대면의 확산으로 이전보다 더욱 심각해졌다. 2020년 2월 말, 대한민국 정부가 코로나19 대응 단계로 격상하면서 많은 기업이 재택근무를 시행했고, 원격 회의, 화상회의 앱 사용량이 급증했다. 하지만, 급증하는 사용량만큼 여러 가지 보안 취약점이 화두에 올랐다.

가트너에 따르면 코로나19 장기화로 인해 2020년 원격 근무는 전년 대비 41%나 높아졌다[1]. 한국인터넷진흥원이 발표한 '2020년 사이버 위협 동향 보고서'에 따르면 재택근무 시 사이버 위협 사례 경험에 대해 과반수(51.57%)가 해킹 및 악성 코드 감염 경험이 있거나 의심되는 정황이 있다고 응답했다.

정보보안에 있어서 사람의 행동이 가장 약한 고리(weakest link)이다[1]. 기술적 보안은 금전적, 상황적, 문화적 측면에서 완벽한 보안 대책이 될 수 없다[2]. 즉, 정보보안을 성공적으로 구현하기 위해서 구성원들의 행동이 핵심적 역할을 한다[2]. 보안 사고의 원인으로 시스템 오작동보다는 인적 오류가 주된 원인이 된다[3].

금융보안원이 발간한 "2020 사이버 보안 이슈 전망"에 따르면, 금융 클라우드 서비스의 주된 사고 원인으로 내부인의 과실을 지목했다[2]. 한국정보보호산업협회가 발간한 "2020년 정보보호 실태조사"에서도 개인정보 유출 원인으로 "내부자에 의한 고의 유출"이 42.8%로 높게 나타났다[3]. 이는 국내 기업에만 국한된 것이 아니다.

IBM이 전 세계 204개 기업, 964명의 보안 실무자들을 대상으로 조사한 자료에 따르면[4], 1년 동안 204개 기업에서 발생한 내부인에 의한 보안 사고는 4,716건이었으며, 이중 내부인의 태만에 의한 사고는 전체의 63%였고, 내부인의 의도적 범죄는 23%로 나타났다.

개인의 정보보안 예방 행동은 조직의 정보보안에 있어서 핵심이다[4]. PMT(Protection Motivation Theory)는 위협이라는 자극이 발생할 때 예방 행동에 참여하고자 하는 개인의 동기를 개념화한 모형이다[5].

Kim et al.[5]은 PMT를 기반으로 코로나19 상황에 소비자들의 의식적 소비, 보건 행동에 영향을 미치는 요인을 규명했다. Thompson et al.[6]은 가정용 컴퓨터뿐만 아니라 개인 모바일 장비의 보안 행동의 결정요인을 탐색하는 데 PMT를 활용했다. Workman et al.[2]은 조직 구성원들의 태만적 보안 행동에 영향을 미치는 요인을 탐구하기 위해서 PMT를 활용했다. Woon et al.[7]은 PMT를 기반으로 가정 무선 장비 보안 행위에 관해 연구했다. 이외에도 PMT는 사이버 보안, 바이러스 보호 행동, 보안 행동, 가정용 컴퓨터 보안 행동 의도, 인터넷 사용자의 보안 행동, 대학생들의 보안 행동, 청소년의 개인정보 온라인 보호 행동 등 다양한 분야에서 개인의 행동 의도를 설명해 주는 견고한 이론적 배경으로 사용되어왔음에도 불구하고, 개인의 인터넷 및 ICTs의 위험한 사용에 드물게 적용됐다[8]. 또한, PMT의 학술적 발전에도 불구하고, 선행연구에서 여러 불일치한 결과가 나타났다[9]. 따라서, 본 연구는 PMT를 기반으로 조직 구성원들의 정보보안 중요성 인식에 영향을 미치는 요인을 탐구하고자 한다.

정보보안에 있어서 구성원의 행동은 매우 중요한 역할을 한다. 따라서, 조직은 구성원의 올바른 보안 행동을 유도하는 과정에 관한 이해가 필요하다. 본 연구는 PMT를 기반으로 구성원들의 올바른 정보보안 행동을 유도할 수 있는 선행요인을 도출하고자 한다. PMT를 사용하는 이유는 선행연구에서 보안 사고라는 위협에 대한 구성원들의 반응 동기를 이해하는 데 적합한 이론이며, 정보보안 분야에서 본 이론을 검증할 기회이자 기존 연구의 불일치한 결과를 보완할 수 있기 때문이다. 본 연구의 연구 문제(RQ, Research Question)는 다음과 같다.

RQ. 구성원들의 올바른 정보보안 행동의 선행요인인 정보보안 중요성 인식에 영향을 미치는 요인은 무엇인가?

본 연구에서는 PMT를 기반으로 위협 평가, 대응 평가, 부적응 반응이라는 세 가지 관점에서 정보보안 중요성 인식에 영향을 미치는 요인을 탐구하고자 한다.

2. 문헌연구

PMT는 개인이 보안 행동을 결정하는 과정을 설명해 주는 중요한 이론적 기반을 제공해 준다[10]. 하지만, 정보보안 분야에서 이 이론의 실증적 검증은 많이 이루

1) 서울경제. 재택근무에 허술해진 보안…노트북·줌도 '해커 먹잇감' 2021.04.25.
2) 금융보안원 (2020). 2020 사이버보안 이슈 전망.
3) 한국정보보호산업협회 (2021). 2020년 정보보호 실태조사.
4) IBM Security (2020). Cost of Insider Threats: Global Report 2020.

Table 1. Key Constructs and Definitions

Construct	Definition
Perceived Certainty of Punishment	an individual is less likely to be inclined to carry out a deviant act because organization is able to detect and punish the employee misbehavior
Perceived Response Cost	beliefs about how costly performing the recommended response will be
Acquiescence	withholding relevant ideas, information, or opinions, based on resignation
Perceived Importance of Information Security	the degree to which an individual perceives an information security or security behavior to be important

어지지 못했다[10]. PMT가 정보보안 분야에 적용 당위성을 확보하기 위해 본 이론을 기반으로 모형을 수립하고 실증적으로 검증할 필요가 있다.

2.1 예방 동기 이론

Rogers[11]가 소개한 PMT는 행동 변화의 수용과 유도를 위해 사용되는 이론 프레임워크이다[12]. 초기 PMT는 두려움 유발과 이에 대한 대응을 이해하고자 개발되었다[11,12]. 이후 설득 의사소통 이론(Persuasive Communication)으로 확장되었다[13].

Rogers[13]는 기대 가치 이론(EVT: Expectancy-Value Theory)을 반영하여 1983년에 포괄적으로 인지적 변화를 반영한 개선된 PMT를 제안했다. 본 모형은 두려움 대응 프로세스를 유발하는 다양한 정보 원천을 포함한다[14]. Rogers[13]는 수정 모형에 보상을 포함했다. 그는 위협에 대한 예방 행동을 취하지 않을 때 얻게 되는 가치 보상(예. 헬멧을 쓰지 않고 오토바이를 운전하면 자유로움/멋/시원함을 느낄 수 있음)을 수정 모형에 포함했다[14]. 하지만, 보상은 위협에 대한 예방 행동이 아니고 기존의 개념과 대조되는 행동으로 많은 연구에서 본 변수에 대한 논란은 여전하다[14].

PMT는 두려움 호소/유발에 관한 연구에서 확장되었다[14]. 추천 행동에 대한 메시지를 수용할 수 있도록 위험 통제 과정을 설명하는 것이 PMT이다[15]. 개인은 명확한 그리고 현실적 위협에 직면하게 되면, 위협 회피 혹은 위협의 피해를 줄이기 위해서 추천/대응을 취하게 된다[12]. 단, 추천/대응이 현실성 있고, 따르기 용이할 경우 추천 행동(recommended behavior)을 따른다[12].

두려움 유발은 개인의 웰빙(well-being)에 위협이 되는 내용에 관한 정보전달 의사소통이다[14]. 즉, 두려움 유발은 추천 행동을 취하지 않으면 발생하게 될 '무서운 일'을 기술하여 사람들에게 두려움을 유발하도록 작성된 설득 메시지이다[15]. 즉, 두려움 유발 소통을 통해 개인의 태도 변화, 행동 변화를 유발하는 것이다[14]. 선행연구에 따르면 두려움 유발 요소들이 인간의 태도 변화에 매우 효과적인 것으로 나타났다[16].

두려움 호소 연구에 있어서 문제점은 두려움 호소가 다양한 자극에 의해 유발됨에도 불구하고, 두려움을 자극하는 새로운 변수에 대한 탐구가 부족하고, 인지적 매개 효과(과정)에 관한 연구도 부족하다는 점이다[14].

PMT는 과거의 행동이 위협의 평가 과정과 개인의 위협 대응 능력에 강한 영향을 미친다고 제안한다[17]. 또한, PMT는 개인이 왜 그리고 어떻게 예방 행동을 수행할지 결정하는지를 설명해 준다[18].

예방 행동은 위협 평가와 대응 평가에 의해 유발된다[18]. 기대 가치 이론에 따르면, 어떠한 행동의 수용은 행동의 결과와 결과의 가치 간의 기대함수로 결정된다[14]. 기대 가치 이론에서 제시하는 두려움 유발을 위한 세 가지 자극 변수 1) 주어진 상황의 유해함 정도(인지된 심각성, perceived severity), 2) 현재 행동을 수정하거나 예방 행동을 취하지 않았을 경우 어떤 (유해한) 사건이 발생하게 될 확률(인지된 취약성, perceived vulnerability or certainty), 3) 유해한 자극을 감소 혹은 제거하기 위한 대응 반응의 가용성과 효과성(인지된 반응 효능감, perceived response efficacy or control) 등이다[11,19]. 이 세 가지 요인은 인지 매개 과정을 구성한다[14]. 인지된 심각성과 취약성은 위협 평가에 해당하고, 인지된 대응 효능감은 대응 평가에 해당한다[14].

위협 평가는 위협으로 발생하는 위험 수준에 대한 개인적 평가이다[7]. 위협 평가의 예로 인지된 취약성(위협 사건의 발생 가능성에 대한 개인적 평가), 인지된 심각성(위협 사건의 결과의 심각성), 보상(추천 대응 반응을 수용하지 않을 때 발생) 등이 있다[7,9].

두 번째 인지 프로세스인 대응 평가는 위험으로 인해 발생할 수 있는 잠재적 손실 혹은 손상에 대응 그리고 회피할 수 있는 개인의 능력 평가를 말한다[7]. 대응 평가에는 자기 효능감(self-efficacy, 추천 행동을 수행할

수 있는 개인의 능력에 대한 확신), 대응 효능감(response efficacy, 추천 행동에 대한 효능감), 대응 비용(response cost, 추천 행동을 취함에 있어서 발생할 수 있는 인지된 기회 비용(금전, 시간, 노력)) 등이 해당한다[7].

정보보안 분야에 PMT를 적용할 수 있는데, Ifinedo[20]는 PMT를 기반으로 정보보안 정책 준수 행동을 설명했다. 하지만, 본 모형의 확장과 정보보안 분야에서 본 이론에 대한 당위성을 확보하고 예방 행동을 이해 및 예측하기 위해서 본 모형의 효용성을 평가하는 것은 매우 중요하다[14].

2.2 정보보안 중요성 인식

Workman et al.[2]은 정보보안 분야에서 앎-실행 간의 격차를 해결하기 위해서 처벌, 상황적 윤리, 보안 인식 증가, 보안 절차 추가, 보안 정책 품질 향상, 조직의 보안 목표와 실천 간의 조화가 중요하다고 언급했다. 기존 연구에서 이와 같은 요인들에 관해 다양한 연구를 수행하였으나 자발적 보안 강화를 위해 필수적인 구성원들의 보안 인식 강화에 관해서는 상대적으로 관심이 부족했다.

Rocha Flores et al.[21]는 구성원들의 정보보안 인식이나 지식의 결여는 낮은 수준의 정보보안 참여로 이어질 수 있다고 경고했다. Dincelli and Goel[22]은 사람들이 보안에 소홀한 이유는 보안 행동에 대한 인지된 중요성 수준이 낮거나 보안 지식 수준이 낮기 때문이라고 지적했다. Chai et al.[23]은 어떠한 행동을 취하고자 하는 개인의 동기에 중요한 영향을 미치는 요인 중 하나는 인지된 중요성(perceived importance)이라고 주장했다. Dang-Pham et al.[24]도 구성원들의 보안 인식을 위한 선행변수로 인지된 정보보안의 중요성이 핵심이라고 주장했다. Chai et al.[23]은 정보보안에 대한 인지된 중요성이 정보보안 행동에 유의한 영향을 미친다는 것을 규명했다. 따라서, 본 연구는 구성원들의 정보보안 중요성 인식에 영향을 미치는 요인을 탐색하고자 한다.

3. 가설설정 및 연구모형

예방 동기는 위협과 행동의 사이에 존재하는 핵심 매개변수이다[14]. 예방 동기란 어떠한 행동 수행 의도와 같은 개념이다[14]. 따라서, PMT의 핵심은 예방 동기에 대한 이해이다[28].

예방 동기는 두려움 유발에 상응하는 추천 행동(예. 두려움 회피, 두려움 감소 행동)을 취하도록 한다[14,28]. 즉, 예방 동기는 직접적으로 행동에 영향을 미치는 것이 아니라 행동 의도에 영향을 미침으로써 행동을 유발한다[7,28]. 따라서, 어떠한 행동을 유발하기 위해서는 행동의 핵심 선행변수인 동기에 대한 이해가 선행되어야 한다.

본 연구는 PMT의 인지 매개 프로세스를 기반으로 구성원들의 보안 행동의 예측 변수인 정보보안 중요성 인식에 영향을 미치는 요인을 탐색하고자 한다.

Fig. 1과 같이 본 연구의 이론적 기반이 된 PMT는 Milne et al.[14]이 제시한 확장된 PMT이다. 개선 모형에 인지 매개 프로세스는 적응 반응(adaptive responses)대 부적응 반응(maladaptive responses, 직접적으로 위협을 관리하는 것은 아님)으로 나뉜다[29].

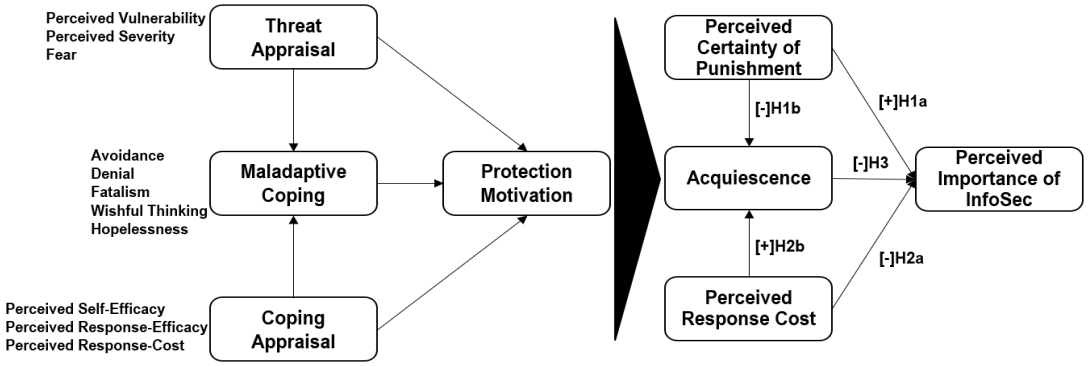

Fig. 1. Protection Motivation Model(Source: Milne et al.[16]) Fig. 2. Research Model

PMT의 핵심 요소인 위협 평가와 대응 평가는 인간의 적응 반응을 유도한다[28]. 위협 평가는 거부 혹은 회피와 같은 부적응 반응을 유발할 수 있다[1]. 반면, 대응 평가는 대응 비용과 같은 적응 반응을 유발할 수 있다[1]. 하지만, 두 평가가 모두 적응 반응과 부적응 반응을 유발하는 것은 아니다. 오히려, 적응 반응 보다는 부적응 반응을 유발할 수 있다. Floyd et al.[30]은 인간은 위협 평가과정에서 부적응 행동을 평가한다고 주장했다. 위협 평가 과정은 부적응 반응 보상(내적 그리고 외적)과 위협에 대한 인식(심각성, 취약성) 등을 포함한다[30]. 보상은 부적응 반응을 선택할 가능성을 높인다[30]. 반면, 위협은 부적응 반응을 선택할 가능성을 낮춘다[30].

3.1 인지된 처벌 확신

인간은 자신에게 심각한 위협이 발생할 것이라고 인지하면 두려움이라는 인지적 감정 반응을 보인다[28]. 여기서 발생한 두려움은 개인의 예방 동기를 활성화한다[28]. Hollinger and Clark[31]의 연구에 따르면, 처벌의 3대 요소인 심각성(severity), 확신성(certainty), 신속성(celerity) 중에 인지된 처벌의 확신성이 인간의 행동을 유도하는 데 가장 효과적인 수단이라는 것을 규명했다. Warr[32]와 Jackson[33]도 희생의 인지된 확신성이 범죄 희생으로 인한 두려움에 가장 중요한 영향을 미치는 요인이라고 주장했다. Kankanhalli et al.[34]도 이탈행동의 억제 노력은 개인의 이탈 행동이 외부/조직에 의해 발각될 수 있는 제재의 확신성에서 시작된다고 주장했다.

Roche et al.[35]은 억제 행동 연구에 있어서 인지된 제재의 확신성이 중요한 요인임에도 불구하고 이에 관한 학술적 탐구가 많이 이루어지지 않았다고 언급했다. 범죄 행위의 낮은 발각 가능성이 소프트웨어의 불법 복제 결정에 영향을 미치는 중요한 이유이다[25]. 정보보안 측면에서, 조직이 보안 행동에 대한 처벌을 강화한다면 구성원들이 부정행위에 신경을 쓸 가능성이 크다[25].

Roche et al.[35]은 처벌의 확신성이 범죄자의 체포 두려움에 영향을 미친다는 것을 발견했다. Burruss et al.[19]은 코로나19 상황에서 감염되었을 때 사망의 확신성은 두려움에 정(+)의 영향을 미치고, CDC(Centers for Disease Control and Prevention, 미국질병관리청)의 지침 준수 거부에 음(-)의 영향을 미친다는 것을 발견했다. Pickett et al.[36]은 인지된 확신성이 범죄 행위 시 체포에 대한 두려움에 긍정적 영향을 미친다는 것을 규명했다. Roche et al.[35]의 연구에서는 처벌의 확신성이 범죄 행위에 대한 두려움에 유의한 영향을 미치는 것으로 나타났다. Herath and Rao[25], Herath and Rao[26]의 연구에 따르면, 위반행위 적발/발견 확신성이 조직의 보안 정책 준수 의도에 유의한 영향을 미치는 것으로 나타났다. 마찬가지로, 조직에서 정보보안 정책을 위반한 사람을 처벌할 가능성이 크다고 인식할 경우, 처벌을 피하기 위해서 정보보안 행동을 취할 가능성이 크다. 또한, 업무 수행 순간마다 정보보안 행동 요소를 중요하게 생각할 가능성이 크다. 따라서, 다음의 가설을 제시할 수 있다.

H1a: 인지된 처벌 확신은 정보보안 중요성 인식에 긍정적 영향을 미칠 것이다.

H1b: 인지된 처벌 확신은 묵인에 부정적 영향을 미칠 것이다.

3.2 인지된 대응 비용

인간은 자신에게 위협이 닥쳤을 때, 위협에 대한 대처 행동의 손익계산을 통해 취해야 할 행동을 결정한다[4]. 주어진 행동에 대한 보상은 부적응 대응이고, 비용은 적응 대응이다[2]. 인간은 자신의 행동을 결정하는 데 있어서 이익과 비용의 두 가지 측면을 평가한다. 정보보안 관점에서 대응 비용은 보안 대책을 실행하는 데 발생하는 비용과 보안 대책의 잠재적 이익의 관점에서 평가된다[2]. 만약, 조직의 정보자산을 보호하기 위해 예방 행동을 취하는 것이 개인의 업무 생산성에 장해가 된다면 인지된 비용이 더 크기 때문에 해당 행동을 수용하지 않을 수 있다[2]. 반면, 예방 행동을 수행하는 데 소비되는 비용이 적었지만, 보안 효과가 크다면 구성원들이 예방 행동을 받아들일 가능성은 커진다[2].

Ifinedo[20]는 보안 행동을 수용하는 데 개인의 자원이 많이 소요된다면 해당 행동의 수행을 망설일 가능성이 커진다고 주장했다. Thompson et al.[6]의 연구에서 대응 비용이 가정용 컴퓨터뿐만 아니라 모바일 기기의 보안 행동에 모두 유의한 영향을 미치는 것으로 나타났다. Vance et al.[17]은 대응 비용이 조직의 정보보안 정책 준수 의도에 부정적 영향을 미친다는 것을 규명했다. Herath and Rao[26]도 대응 비용이 보안 정책 준수 태도에 유의한 영향을 미친다는 것을 규명했다.

Herath and Rao[25]는 인지된 심각성, 자기 효능감, 대응 효능감, 대응 비용이 구성원들의 보안 정책 준수 의도에 영향을 미친다는 것을 발견했다. Marett et al.[8]의 연구에 따르면 대응 비용이 회피와 절망과 같은 부적응 반응에 모두 정(+)의 영향을 미친다는 것을 규명했다. 반면, Ifinedo[20]는 인지된 위협의 심각성과 대응 비용이 IT 전문가의 정보보안 정책 준수 의도에 유의한 영향을 미치지 못한다는 상반된 결과를 발견했다. 이러한 불일치한 결과의 원인을 규명하기 위해서는 대응 비용을 역할을 다시 검증해 볼 필요가 있다. 따라서, 다음의 가설을 제시할 수 있다.

H2a: 인지된 대응 비용은 정보보안 중요성 인식에 부정적 영향을 미칠 것이다.

H2b: 인지된 대응 비용은 묵인에 긍정적 영향을 미칠 것이다.

3.3 묵인

PMT에 따르면, 부적응 대응은 행동 의도에 부정적 영향을 미친다[29]. 부적응 대응(maladaptive coping)은 보안 사고 위협에 대한 간접적 대응 행동이다[19]. 대부분의 부적응 대응(maladaptive coping)은 회피적 사고(avoidant thinking)와 밀접한 관련이 있다[29]. 예를 들어, 외부 위협의 위험성을 부정하는 것과 같은 부적응 대응은 예방 동기를 감소시킨다[19].

Chenoweth et al.[29]은 회피(avoidance), 현실 부정(denial), 숙명(fatalism), 절망(hopelessness)과 같은 부적응 대응이 행동 의도에 부정적 영향을 미친다는 것을 규명했다. Yim[27]은 정보보안에 대한 구성원의 침묵 행위(employee silence behavior)가 정보 보안의 인지된 중요성에 긍정적(+) 영향을 미친다는 것을 실증적으로 규명했다. 따라서, 다음의 가설을 제시할 수 있다.

H3: 묵인은 정보보안 중요성 인식에 부정적 영향을 미칠 것이다.

지금까지 제시한 가설을 기반으로 연구모형을 제시하면 Fig. 2와 같다.

4. 분석

4.1 자료 수집

PMT는 정보보안 영역에서 최종 사용자, 구성원, 소비자와 같은 개인적 차원에서 접근해야 왔다[28]. 본 연구도 개인적 차원에 적합한 설문을 개발하여 제한 모형 검정에 필요한 데이터를 수집하고자 한다.

설문에 사용된 항목은 선행연구에서 신뢰성이 확보된 항목을 차용했다. 각 잠재변수를 측정하기 위한 관측변수의 출처는 다음과 같다. 인지된 처벌 확신은 Herath and Rao[26], Rajab and Eydgahi[34]의 연구에서 4개의 항목을 차용했다. 인지된 대응 비용은 Herath and Rao[26], Rajab and Eydgahi[34]의 연구에서 6개의 항목을 차용했다. 묵인은 Knoll and Dick[37]의 연구에서 6개의 항목을 차용했다. 정보보안 중요성 인식은 Chai et al.[23], Pajares and Graham[38], Yim[27]의 연구에서 8개의 항목을 차용했다.

Table 2. Demographic Information of Respondents

Classification		Freq.	%	Classification		Freq.	%
Gender	Male	195	84.4	Age	~29	14	6.1
	Female	33	14.3		30~39	86	37.2
	No Response	3	1.3		40~49	96	41.6
Position	Rank-and-Fire	19	8.2		50~59	30	13.0
	Assistant Manager	45	19.5		60~	1	0.4
	Section Chief	46	19.9		No Response	4	1.7
	Deputy Head	44	19.0	Industry Type	IT/SI	82	35.5
	Head of Dept	49	21.2		Manufacturing	57	24.7
	Director	22	9.5		Finance	26	11.3
	Executive Director	2	0.9		Transportation	4	1.7
	No Response	4	1.7		Education	1	0.4
Employment Type	Permanent	222	96.1		Construction	46	19.9
	Contract	7	3.0		Other Services	5	2.2
	Dispatched	1	0.4		ETC	7	3.0
	No Response	1	0.4		No Response	3	1.3
	Sum	231	100	Years of Service(Avg.)		10.8738 yrs	

설문의 응답은 Likert-type 7점 척도법을 사용했다. 1점은 전혀 동의하지 않음을 의미하여, 7점은 전적으로 동의함을 의미한다. 응답자의 특성은 Table 2와 같다.

4.2 측정모형 검정

4.2.1 요인 분석 및 CMB 검정

다음으로 수집된 자료 속 요인구조를 탐색하기 위해서 EFA(Exploratory Factor Analysis)를 수행했다. 요인 회전은 사각회전 기법을 사용했다. 요인 추출 기법은 PAF(Principal Axis Factoring)를 사용했다. 요인 선별은 적재값(loading)이 0.5 이상되며, 교차요인(0.4 ≥ cross-loadings)이 없으며, eigenvalue ≥ 1, 총 분산은 60% 이상 기준을 사용했다[39]. 이 기준에 따라 총 4개의 요인을 추출했다.

다음으로 CMB(Common Method Bias) 검정을 수행했다. CMB의 영향력을 검토하기 위해 Harman의 일요인 검정(Harman's one-factor test)을 수행했다[41]. Fuller et al.[42]에 따르면, 첫 번째 요인의 분산이 50% 이상 될 경우 CMB의 영향이 크다고 본다. Table 3을 보면 첫 번째 요인의 분산이 44.777로 50%를 넘지 않기 때문에 CMB의 영향이 심각하지 않다고 판단된다.

다음으로 개념 타당성(construct validity)을 평가하기 위해서 CFA(Confirmatory Factor Analysis)를 수행했다. Table 4에 제시된 바와 같이 EFA에서 식별된 모든 요인이 통계적으로 유의하게 나타났다.

Table 3. Results of Exploratory Factor Analysis

Construct	Items	Factor				Communality	
		1	2	3	4	Initial	Extraction
Response Cost	sc1	-0.023	0.797	0.068	0.006	0.713	0.696
	sc2	-0.007	0.893	-0.022	0.014	0.769	0.796
	sc3	0.015	0.882	-0.021	0.014	0.782	0.760
	sc4	0.088	0.906	-0.017	0.069	0.788	0.776
	sc5	-0.118	0.814	0.051	0.006	0.793	0.795
	sc6	-0.085	0.830	0.061	-0.020	0.777	0.787
Perceived Importance	aw1	0.611	0.114	-0.079	-0.193	0.757	0.556
	aw2	0.655	0.103	-0.113	-0.217	0.815	0.687
	aw3	0.846	0.033	0.025	-0.010	0.699	0.686
	aw4	0.854	0.053	-0.037	-0.012	0.757	0.735
	aw5	0.807	-0.183	0.047	0.045	0.724	0.725
	aw6	0.842	-0.095	0.040	0.059	0.758	0.697
	aw7	0.891	-0.058	-0.020	0.050	0.799	0.801
	aw8	0.719	-0.024	-0.025	-0.062	0.717	0.608
Perceived Certainty	br1	0.079	0.006	-0.035	-0.692	0.609	0.576
	br2	-0.027	-0.084	0.040	-0.952	0.817	0.879
	br3	0.019	0.004	-0.031	-0.884	0.824	0.828
	br4	0.022	-0.030	-0.006	-0.881	0.804	0.818
Acquiescence	abr1	0.060	0.017	0.662	0.089	0.524	0.471
	abr2	-0.002	0.089	0.864	-0.062	0.771	0.762
	abr3	-0.067	-0.007	0.939	-0.082	0.876	0.865
	abr4	-0.010	-0.004	0.941	-0.018	0.866	0.876
	abr5	0.048	-0.002	0.885	0.002	0.770	0.750
	abr6	-0.063	-0.026	0.773	0.066	0.686	0.684
Eigenvalue		10.746	3.502	2.904	1.449		
% of Variance		44.775	14.593	12.099	6.039		
Cumulative %		44.775	59.367	71.467	77.506		
KMO and Bartlett's Test							
Kaiser-Meyer-Olkin Measure of Sampling Adequacy					0.925		
Bartlett's Test of Sphericity		Approximate Chi-Square			5470.790		
		Degree of Freedom			276		
		Significance			0.000		

Extraction Method: Principal Axis Factoring

Rotation Method: Oblimin with Kaiser Normalization

Table 4. Confirmatory Factor Analysis

constructs	items	estimate	Standard Error	t value	p value	SMC	Cronbach's alpha≥0.7	CR ≥0.7	AVE ≥0.5
Response Cost	sc1	0.958	0.054	17.910	0.000	0.709	0.950	0.973	0.763
	sc2	0.990	0.050	19.883	0.000	0.788			
	sc3	1.058	0.057	18.566	0.000	0.745			
	sc4	1.014	0.054	18.694	0.000	0.751			
	sc5	0.988	0.049	20.308	0.000	0.792			
	sc6	1.000	-	-	-	0.792			
Perceived Importance	aw1	1.000	-	-	-	0.510	0.942	0.966	0.667
	aw2	1.078	0.090	11.960	0.000	0.618			
	aw3	1.394	0.115	12.111	0.000	0.677			
	aw4	1.343	0.107	12.544	0.000	0.723			
	aw5	1.205	0.099	12.238	0.000	0.697			
	aw6	1.394	0.115	12.092	0.000	0.694			
	aw7	1.326	0.101	13.063	0.000	0.793			
	aw8	1.101	0.094	11.725	0.000	0.622			
Perceived Certainty	br1	1.000	-	-	-	0.569	0.930	0.962	0.776
	br2	1.189	0.079	15.000	0.000	0.823			
	br3	1.282	0.085	15.041	0.000	0.864			
	br4	1.194	0.080	14.949	0.000	0.847			
Acquiescence	abr1	0.878	0.079	11.110	0.000	0.437	0.940	0.966	0.728
	abr2	1.143	0.071	16.062	0.000	0.749			
	abr3	1.194	0.065	18.383	0.000	0.880			
	abr4	1.184	0.064	18.574	0.000	0.889			
	abr5	1.048	0.065	16.097	0.000	0.745			
	abr6	1.000	-	-	-	0.665			

Table 5. Correlations Analysis

Pearson Correlation	Mean	Std. Deviation	Punish Certainty	Acquiesence	Response Cost	Perceived Importance
Punish Certainty	5.4102	1.11184	**.881**	-.448**	-.262**	.627**
Acquiesence	2.5971	1.32255	-.448**	**.853**	.367**	-.437**
Response Cost	3.4268	1.44286	-.262**	.367**	**.873**	-.436**
Perceived Importance	5.3734	1.05239	.627**	-.437**	-.436**	**.817**

Diagonal elements are the square root of Average Variance Extracted
**. Correlation is significant at the 0.01 level (2-tailed)

4.2.2 신뢰성 분석

신뢰성을 위해 가장 널리 사용되는 지표이자 내적 일관성 신뢰성 지표인 Cronbach's alpha와 CR(Composite Reliability)을 검토했다[40]. Nunnally and Bernstein[43]에 따르면, 내적 일관성은 최소 0.7 이상 되어야 한다. 반면, 0.95를 넘지 말아야 한다[44]. Table 4를 보면 Cronbach's alpha의 범위는 0.930~0.950으로 나타났으며, CR의 범위는 0.962~0.973으로 나타났다. 따라서, 신뢰성 기준을 충족하고 있다.

4.2.3 타당성 분석

Fornell and Larcker[45]에 따르면, AVE 값이 0.5 이상일 경우 수렴 타당성이 확보되었다고 본다. Table 5를 보면 AVE의 범위가 0.667~0.776으로 기준을 충족하고 있다.

판별 타당성은 Fornell and Larcker[45]의 기준에 따라 잠재변수 간의 상관관계 분석값과 AVE의 제곱근 값을 비교했다. Table 5를 보면 대각선에 AVE 제곱근 값을 제시했다. 분석 결과, 모든 AVE 제곱근 값이 변수 간의 상관관계 계수보다 크게 나타나서 판별 타당성이 확보되었다고 볼 수 있다.

4.3 구조모형 검정

4.3.1 정규성 검정

본 연구는 제안 모형을 검정하기 위해서 CB-SEM(Covariance-based Structural Equation Model)을 활용했다. CB-SEM은 MLE(Maximum Likelihood Estimation)를 사용하기 때문에 정규성 가정에 엄격하다[44]. 단변량 정규성(univariate normality)을 평가하기 위한 기준으로 왜도가 3.0이며 첨도가 8.0을 사용한다[46].

Table 6. Test of Normality

	Kolmogorov-Smirnov			Shapiro-Wilk			Skewness		Kurtosis		Collinearity	
	Statistic	df	Sig.	Statistic	df	Sig.	Statistic	Std. Error	Statistic	Std. Error	Tolerance	VIF
Punish Certainty	0.129	227	0.000	0.952	227	0.000	-0.448	0.160	-0.248	0.319	0.787	1.271
Acquiesence	0.112	227	0.000	0.932	227	0.000	0.751	0.160	0.259	0.320	0.728	1.374
Responce Cost	0.073	227	0.005	0.974	227	0.000	0.036	0.160	-0.746	0.320	0.833	1.201
Perceived Importance	0.075	227	0.003	0.967	227	0.000	-0.169	0.161	-0.784	0.320	-	-

본 연구에서 왜도는 |0.036|~|0.751|로 나타났으며, 첨도는 |0.248|~|0.0.784|로 나타나 정규분포를 심각하게 위배하고 있다고 볼 수 없다[47].

다중공선성(multicollinearity)을 평가하기 위해서 VIF(Variance Inflation Factors)를 확인했다. VIF는 VIF<3이 이상적 기준이다[44]. 본 연구에서 VIF는 1.201~1.374로 공선성이 문제가 없다고 판단된다.

모형의 설명력을 나타내는 지표인 R^2을 살펴보았다. 모형의 복잡성을 반영한 Adjusted R^2도 살펴보았다[40]. R^2은 0.20(20%) 이상일 경우 높은 수준이라고 본다[40]. 회귀분석 결과, 정보보안 중요성 인식의 R^2는 0.476, Adjusted R^2는 0.469로 나타났다. 묵인의 R^2는 0.269, Adjusted R^2는 0.262로 나타났다.

다음으로 수집된 데이터와 모형 간의 적합도(Goodness-of-Fit Indices)를 살펴보았다.

Table 7에 제시된 바와 같이 χ^2를 제외하고 나머지 적합도 지표가 모두 만족스러운 수준으로 나타났다. 다음으로 제안 모형을 검정한 결과는 Fig. 3과 Table 8과 같다.

Table 7. Classification of Goodness of Fit Indices[5)]

Fit Indices	Minimum Thresholds	Proposed Model Estimated
x^2(p)	p>0.05	728.269(p=0.000)
x^2/df	≤2 or 3	2.960
CFI	≥0.90	0.9121
PCFI	≥0.50	0.813
NFI	≥0.80	0.873
NNFI	≥0.90	0.901
IFI	≥0.90	0.912
GFI	≥0.80	0.781
AGFI	≥0.70	0.733
PGFI	≥0.50	0.640
RMSEA	<0.10	0.092
SRMR	≤0.08	0.0548

5) RMSR= Root Mean Square Residual; SRMR=Standardized RMSR; GFI= Goofness of Fit; AGFI= Adjusted GFI; NFI= Normed Fit Index; NNFI= Non-NFI; TLI= Tucker-Lewis Index; CFI= Comparative Fit Index, PCFI= Parsimony CFI; RMSEA= Root Mean Square Error of Approximation; RNI= Relative Noncentrality Index; AIC= Akaike Information Criterion; l= The Estimate of Noncentrality Parameter; d= The Estimate of Monimized Population Discrepancy Function; Mc= McDonald's Centrality Index

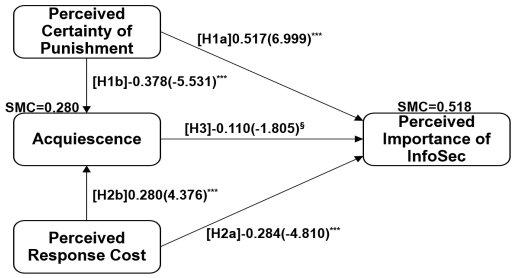

Fig. 3. Results of Structural Equation Modelling

확률(probability)이라는 단어에서 기원한 p 값은 모든 과학 문헌에서 변수들 간의 통계적 유의성을 나타내기 위해 Fischer에 의해 제시된 0.05의 α 수준을 일반적으로 사용하지만, α 수준은 임의적이다[48].

Paoletti and Grulke[49]은 0.05≤p<0.1도 유의하게 해석해야 한다고 주장했다. Boos and Stefanski[50]은 실증적으로 고려해야 하는 p-values의 범위는 0.00001~0.1까지라고 보았다. Bruns et al.[51]는 유의성의 기준은 α=0.01, 0.05, 0.1이라고 주장했다. Bayarri et al.[52]도 유의수준의 기준은 0.1부터라고 주장했다. 따라서, 본 연구는 0.1을 가설검정을 위한 유의수준으로 사용했다.

구조모형 검정 결과, 인지된 처벌 확신은 인지된 정보보안 중요성 인식에 유의한 영향을 미치는 것으로 나타났다(β=0.517, t=6.999, p<0.001). 또한, 인지된 처벌 확신은 묵인에도 유의한 영향을 미치는 것으로 나타났다(β=-0.378, t=-5.531, p<0.001).

인지된 대응 비용은 인지된 정보보안 중요성 인식에 유의한 영향을 미치는 것으로 나타났다(β=-0.284, t=-4.810, p<0.001). 인지된 대응 비용은 묵인에도 유의한 영향을 미치는 것으로 나타났다(β=0.280, t=4.376, p<0.001). 주목할 점은 선행연구에서는 대응평가 요소가 위협 평가 요소보다 행동 의도와 실제 행동에 더 큰 영향을 미친다고 주장하였으나[1], 본 연구에서는 대응 평가보다는 위협 평가가 더 강한 영향을 미치는 것으로 나타났다는 점이다.

Table 8. Results of Hypotheses Tests

Hypotheses	Estimate	S.E.	C.R.	p value	Results
H1a.Perceived Certainty→InforSec Imfortance	0.465	0.066	6.999***	0.000	Supported
H1b.Perceived Certainty→Acquiescence	−0.488	0.088	−5.531***	0.000	Supported
H2a.Response Cost→InforSec Imfortance	−0.167	0.035	−4.810***	0.000	Supported
H2b.Response Cost→Acquiescence	0.237	0.054	4.376***	0.000	Supported
H3.Acquiescence→InforSec Imfortance	−0.077	0.042	−1.805§	0.071	Supported

§ p<0.1, *p<0.05, **p<0.01, ***p<0.0001

마지막으로 묵인은 인지된 정보보안 중요성 인식에 유의한 영향을 미치는 것으로 나타났다(β=-0.110, t=-1.805, p<0.1).

인지된 처벌 확신이 정보보안 중요성 인식에 유의한 영향을 미치는 것으로 나타났다. 또한, 처벌 확인은 묵인에도 영향을 미치는 것으로 나타났다. 구성원이 정보보안 정책을 위반했을 때 본인이 처벌받을 것이라는 확신이 든다면 정보보안이 중요하다고 생각할 뿐만 아니라 보안 위반 사례에 대해 묵인하지 않으리라는 것을 알 수 있다. 반대로, 인지된 대응 비용은 인지된 정보보안 중요성 인식에 부정적 영향을 미치지만, 묵인에는 긍정적 영향을 미치는 것으로 나타났다. 즉, 구성원들이 보안 행동을 취하는 데 있어서 어려움이 있거나 자신의 업무 생산성과 상충한다고 느끼게 되는 경우 정보보안이 중요하다고 인식할 가능성이 작다는 것을 알 수 있다. 심지어, 정보보안 사고나 정보보안 관련 이슈에 대해 심각하게 생각하지 않을 가능성도 있다. 마지막으로, 정보보안에 대한 묵인은 정보보안 중요성 인식에 부정적 영향을 미치는 것으로 나타났다. 조직이 구성원의 보안 정책 위반 행동에 대해 지나치게 관대하거나 피상적으로 다룰 경우, 정보보안에 대한 중요성 인식 수준이 낮아질 수 있다는 것을 알 수 있다.

5. 결론 및 논의

본 연구는 구성원들의 정보보안에 대한 중요성 인식에 영향을 미치는 선행요인을 규명하고자 진행되었다. PMT를 기반으로 수립한 제안 모형을 실증적으로 분석한 결과에 대한 함의는 다음과 같다.

개인의 자발적 행동뿐만 의무적 행동에 있어서 중요성 인식이 선행되어야 한다. 어떠한 행동을 취하는 데 있어서 그 행동을 왜 해야 하는지 이유를 모른다면 행동이 반복될 것으로 예상하기 힘들다.

본 연구는 정보보안 중요성 인식에 미치는 선행요인을 탐색했다. 분석 결과, 인지된 처벌 확신은 정보보안 중요성 인식에 긍정적 영향을 미치는 반면, 인지된 대응 비용은 정보보안 중요성 인식에 부정적 영향을 미치는 것으로 나타났다. 이와 같은 두 변수의 반대 영향은 묵인에 미치는 영향도 동일했다. 즉, 인지된 처벌 확신은 묵인에 부정적 영향을 미치는 반면, 인지된 대응 비용은 묵인에 긍정적 영향을 미치는 것으로 나타났다. 본 결과는 정보보안 위반행위로 인해 조직의 정보자산에 치명적 영향을 미칠 수 있을 것으로 판단되고 그에 상응하는 개인적 처벌이 뒤따를 수 있다는 것을 구성원들이 인식하게 된다면 정보보안에 대한 중요성 인식 수준은 높아질 수 있다.

그동안 많은 조직은 업무 생산성은 수익, 정보보안은 비용이라는 고정관념으로 인해 보안 투자에 소극적이었다. 따라서, 보안 사고 대처 방안도 제대로 마련되지 못한 경우가 많고 그나마 보안 사고가 발생하였을 때 보안 대책이 마련되는 사후약방문식 대책이 많았다. 이와 같은 환경은 구성원들이 보안의 중요성을 인식하거나 보안이 자신의 조직에 얼마나 중요한지 인식시키는 데 실패했다.

정보보안은 '현재의 비용'이 아니다. 인간에게 백신접종은 비용이 아니라 지신의 건강을 위한 투자이다. 조직도 보안에 대한 비용과 관심은 향후 발생할 수 있는 잠재적 위협을 제거할 수 있는 미래투자이다. 이러한 관점에서 조직은 보안 투자와 보안 인력 관리, 그리고 구성원의 정보보안 인식 강화에 투자를 아끼지 말아야 한다. 이를 위한 첫걸음으로 보안 정책을 위반할 때 발생할 수 있는 처벌에 대해 명확히 규정하는 것이 필요하다. 물론 무조건적 처벌이 아니라 당위적 처벌이어야 한다. 조직 자산에 대한 위협이 되었고, 회사의 이미지에 부정적 영향을 끼쳤으며, 해당 행동이 반복적일 경우 엄중한 처벌이 뒤따를 수 있다는 것을 명확히 해야 한다. 또한, 무의식적 사고뿐만 아니라 의식적 사고의 경우 처벌 수위가 다를 수 있다는 점도 명시할 필요가 있다. 하지만, 처벌을 위한 처벌이 아니라 조직의 정보 자산 보호를 위한 처벌이어야 한다.

보안 행동 수행에 수반되는 비용도 감소시킬 필요가 있다. 예를 들어, 보안 절차 준수가 복잡하거나, 보안 준수 절차가 너무 복잡할 경우, 혹은 구성원들이 불필요한 절차라고 생각할 경우 보안 행동의 부작용을 유발할 수 있다. 보안 행동이 자신의 업무 생산성에 방해가 되거나, 업무 수행에 방해가 된다고 생각된다면 구성원들의 보안 행동을 유도하기 어렵다. 따라서, 조직이 의도하는 구성원의 보안 행동을 유도하기 위해서 구성원의 관점에서 명확한 보안 행동 지침을 마련해야 한다. 또한, 구성원의 업무 생산성과 보안 행동 간에 상충 혹은 보안 행동이 업무 수행에 장해가 되는지도 사전에 검토해야 한다.

REFERENCES

[1] R. van Bravel, N. Rodríguez-Priego, J. Vila & P. Briggs. (2019). Using Protection Motivation Theory in the Design of Nudges to Improve Online Security Behavior. *International Journal of Human-Computer Studies, 123,* 29-39.
DOI : 10.1016/j.ijhcs.2018.11.003

[2] M. Workman, W. H. Bommer & D. Straub (2008). Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. *Computers in Human Behavior*, 24, 2799-2816.
DOI : 10.1016/j.chb.2008.04.005

[3] V. Cho & W. H. Ip (2018). A Study of BYOD Adoption from the Lens of Threat and Coping Appraisal of Its Security Policy. *Enterprise Information Systems, 12(6),* 659-673.
DOI : 10.1080/17517575.2017.1404132

[4] T. Sommestad, H. Karlzén & J. Hallberg (2015). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *International Journal of Information Security and Privacy*, *9(1),* 26-46.
DOI : 10.4018/IJISP.2015010102

[5] J. Kim, K. Yang, J. Min & B. White (2021). Hope, Fear, and Consumer Behavioral Change amid COVID-19: Application of Protection Motivation Theory. *International Journal of Consumer Studies*, Early View, 1-17.
DOI : 10.1111/ijcs.12700

[6] N. Thompson, T. J. McGill & X. Wang (2017). "Security Begins at Home": Determinants of Home Computer and Mobile Device Security Behavior. *Computers & Security*, *70*, 376-391.
DOI : 10.1016/j.cose.2017.07.003

[7] I. M. Y. Woon, G. W. Tan & R. T. Low (2005). A Protection Motivation Theory Approach to Home Wireless Security. 26th International Conference on Information Systems, 367-380.

[8] K. Marett, A. L. McNab & R. B. Harris (2011). Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory. *AIS Transactions on Human-Computer Interaction*, *3(3)*, 170-188.

[9] D. Arthur & P. Quester (2004). Who's Afraid of That Ad? Applying Segmentation to the Protection Motivation Model. *Psychology & Marketing*, *21(9)*, 671-696.
DOI : 10.1002/mar.20024

[10] R. Crossler & F. Bélanger (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *DATABASE for Advances in Information Systems*, *45(4),* 51-71.
DOI : 10.1145/2691517.2691521

[11] R. W. Rogers (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology*, *91*, 31-114.
DOI : 10.1080/00223980.1975.9915803

[12] M. Cismaru, R. Cismaru, T. Ono & K. Nelson. (2011). "Act on Climate Change": An Application of Protection Motivation Theory. *Social Marketing Quarterly, 17(3),* 61-84.
DOI : 10.1080/15245004.2011.595539

[13] R. W. Rogers. (1983). Cognitive and Psysicological Processes in Fear Appreals and Attitude Change: A Revised Theory of Protection Motivation. In B. L. Cacioppo & L. L. Pretty (eds.), *Social Psychophysiology: A Sourcebook*, London, UK:Guilford.

[14] S. Milne, P. Sheeran & S. Orbell (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology, 30(1),* 106-143.
DOI : 10.1111/j.1559-1816.2000.tb02308.x

[15] K. Witte. (1992). Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. *Communication Monographs, 59(4),* 329-349.
DOI : 10.1080/03637759209376276

[16] J. E. Maddux & R. W. Rogers. (1983). Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology, 19(5),* 469-479.
DOI: 10.1016/0022-1031(83)90023-9

[17] A. Vance, M. Siponen & S. Pahnila. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 40,* 190-198.
DOI : 10.1016/j.im.2012.04.002

[18] H. S. Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon & S. R. Cotten. (2016). Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective. *Computers & Security*, *59,* 138-150.
DOI : 10.1016/j.cose.2016.02.009

[19] G. W. Burruss, C. M. Jaynes, R. K. Moule Jr. & R. E. Fairchild. (2021). Modeling Individual Defiance of COVID-19 Pandemic Mitigation Strategies. *Criminal Justice and Behavior, 48(9),* 1317-1338.
DOI : 10.1177/00938548211010315

[20] P. Ifinedo. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security*, *31(1),* 83-95.
DOI : 10.1016/j.cose.2011.10.007

[21] W. Rocha Flores, E. Antonsen & M. Ekstedt. (2014). Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture. *Computers & Security*, *43,* 90-110.
DOI : 10.1016/j.cose.2014.03.004

[22] E Dincelli & S. Goel (2017). Can Privacy and Security be Friends? A Cultural Fraemwork to Differentiate Security and Privacy Behaviors on Online Social Networks. *Proceedings of the 50th Hawaii International Conference on System Sciences,* 4011-4020.

[23] S. Chai, S. Bagchi-Sen, C. Morrel, H. R. Rao & S. Upadhyaya. (2006). Role of Perceived Importance of Information Security: An Exploratory Study of Middle School Children's Information Security Behavior. *Issues in Informing Science and Information Technology*, 3, 127-135.
DOI : 10.28945/2956

[24] D. Dang-Pham, S. Pittayachawan & V. Bruno. (2015). Investigating the Formation of Information Security Climate Perceptions with Social Network Analysis: A Research Proposal. Pacific Asia Conference on Information Systems.

[25] T. Herath & H. R. Rao. (2009). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems, 47,* 154-165.
DOI : 10.1016/j.dss.2009.02.005

[26] T. Herath & H. Rao. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems, 18(2),* 106-125.
DOI : 10.1057/ejis.2009.6

[27] M. S. Yim. (2018). An Exploratory Research on Factors Influence Perceived Compliance Cost and Information Security Awareness in Small and Medium Enterprise. *Journal of the Korea Convergence Society*, *9(9),* 69-81.
DOI : 10.15207/JKCS.2018.9.9.069

[28] S. R. Boss, D. F. Galletta, F. B. Lowry, G. D. Moody & P. Polak. (2015). What Do Systems Users Have to Fear? Using Fear Appeals Engender Threats and Fear That Motivate Protective Security Behaviors. *MIS Quarterly*, *39(4),* 837-864.
DOI : 10.25300/MISQ/2015/39.4.5

[29] T. Chenoweth, R. Minch & T. Gattiker. (2009). Application of Protection Motivation Theory to Adoption of Protective Technologies. *Proceedings of the 42nd Hawaii International Conference on System Sciences*, 1-10.

[30] D. L. Floyd, S. Prentice-Dunn & R. W. Rogers (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30(2)*, 407-429.
DOI : 10.1111/j.1559-1816.2000.tb02323.x

[31] R. C. Hollinger & J. P. Clark. (1983). Deterrence in the Workplace: Perceived Certainty, Perceived Severity, and Employee Theft. *Social Forces*, *62(2),* 398-418.
DOI : 10.1093/sf/62.2.398

[32] M. Warr. (1987). Fear of Victimization and Sensitivity to Risk. *Journal of Quantitative Criminology, 3(1)*, 29-46.
DOI : 10.1007/bf01065199

[33] J. Jackson. (2011). Revisiting Risk Sensitivity in the Fear of Crime. *Journal of Research in Crime and Delinquency, 48(4),* 513-537.
DOI : 10.1177/0022427810395146

[34] A. Kankanhalli, H. -H. Teo, B. C. Y. Tan & K. -K. Wei. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management, 23(2),* 139-154.
DOI : 10.1016/S0268-4012(02)00105-6

[35] S. P. Roche, T. Wilson & J. T. Pickett. (2020). Perceived Control, Severity, Certainty, and

Emotional Fear: Testing an Expanded Model of Deterrence. *Journal of Research in Crime and Delinquency*, 57(4), 493-531.
DOI : 10.1177/0022427819888249

[36] J. T. Pickett, S. P. Roche & G. Pogarsky. (2018). Toward a Bifurcated Theory of Emotional Deterrence. *Criminology*, *56(1),* 27-58.
DOI : 10.1111/1745-9125.12153

[37] M. Knoll & R. van Dick. (2013). Do I Hear the Whistle…? A First Attempt to Measure Four Forms of Employee Silence and Their Correlates. *Journal of Business Ethics, 113(2),* 349-362.
DOI : 10.1007/s10551-012-1308-4

[38] F. Pajares & L. Graham. (1999). Self-efficacy, Motivation Constructs, and Mathematics Performance of Entering Middle School Students. *Contemporary Educational Psychology*, *24,* 124-139.
DOI : 10.1006/ceps.1998.0991

[39] M. S. Yim. (2015). Factor Analysis for Exploratory Research in the Distribution Science Field. *Journal of Distribution Science*, *13(9),* 103-112.
DOI : 10.15722/jds.13.9.201509.103

[40] D. Russo & K. -J. Stol. (2021). PLS-SEM for Software Engineering Research: An Introduction and Survey. *ACM Computing Surveys, 54(4),* Article #1.
DOI : 10.1145/3447580

[41] S. -J. Chang, A. van Witteloostuijn & L. Eden (2010). From the Editors: Common Method Variance in International Business Research. *Journal of International Business Studies, 41,* 178-184.
DOI : 10.1057/jibs.2009.88

[42] C. M. Fuller, M. J. Simmering, G. Atinc, Y. Atinc & B. J. Babin. (2016). Common Methods Variance Detection in Business Research. *Journal of Business Research, 69(8),* 3192-3198.
DOI : 10.1016/j.jbusres.2015.12.008

[43] B. Nunnally & I. R. Bernstein. (1994). *Psychometric Theory*. New York: Oxford Univer Press.

[44] J. F. Hair, J. J. Risher, M. Sarstedt & C. M. Ringle. (2019). When to Use and How to Report the Results of PLS-SEM. *European Business Review*, *31(1),* 2-24.
DOI : 10.1108/EBR-11-2018-0203

[45] C. Fornell & D. F. Larcker. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18(1)*, 39-50.
DOI : 10.1177/002224378101800104

[46] R. B. Kline. (2005).. *Principles and Practice of Structural Equation Modeling*. Guilford Press.

[47] E. K. Pellegrini & T. A. Scandura. (2005). Construct Equivalence Across Groups: An Unexplored Issue in Mentoring Research. *Educational and Psychological Measurement*, *65(2),* 323-335.
DOI : 10.1177/0013164404268665

[48] M. S. Thiese, B. Ronna & U. Ott. (2016). P Value Interpretations and Considerations. *Journal of Thoracic Disease*, *8(9),* 929-931.
DOI : 10.21037/jtd.2016.08.16.

[49] E. Paoletti & N. E. Grulke. (2010). Ozone Exposure and Stomatal Sluggishness in Different Plant Physiognomic Classes. *Environmental Pollution*, *158,* 2664-2671.
DOI : 10.1016/j.envpol.2010.04.024

[50] D. D. Boos & L. A. Stefanski. (2011). P-Value Precision and Reproducibility. *American Statistician*, *65(4),* 213-221.
DOI : 10.1198/tas.2011.10129

[51] S. B. Bruns, I. Asanov, R. Bode, M. Dunger, C. Funk, S. M. Hassan, J. Hauschildt, D. Heinisch, K. Kempa, J. König, J. Lips, M. Verbeck, E. Wolkfschütz & G. Buenstorf. (2019). Reporting Errors and Biases in Published Empirical Findings: Evidence from Innovation Research. *Research Policy*, *48,* 103796.
DOI : 10.1016/j.respol.2019.05.005

[52] M. J. Bayarri, D. J. Benjamin, J. O. Berger & T. M. Sellke. (2016). Rejection Odds and Rejection Ratios: A Proposal for Statistical Practice in Testing Hypotheses. *Journal of Mathematical Psychology*. *72,* 90-103.
DOI : 10.1016/j.jmp.2015.12.007

임 명 성(Myung-Seong Yim) [정회원]

· 2002년 2월 : 삼육대학교 경영정보학과(BBA)
· 2004년 2월 : 한국외국어대학교 경영정보대학원(MBA)
· 2011년 8월 : 서강대학교 경영전문대학원(Ph.D.)
· 2011년 9월 ~ 2012년 2월 : 서강대학교 경영대학 대우교수
· 2012년 3월 ~ 현재 : 삼육대학교 경영학과 부교수
· 관심분야 : Side Effect of ICTs, Service Innovation
· E-Mail : msyim@syu.ac.kr