The Journal of the Convergence on Culture Technology (JCCT)
Vol. 9, No. 5, pp.463-474, September 30, 2023. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2023.9.5.463

JCCT 2023-9-56

협업시스템 담당자의 정보보안 인식이 SBOM (Software Bill Of Materials) 도입 의도에 미치는 영향 : 계획된 행동이론을 중심으로

The Effects of information security perceptions of collaborative system managers on intention to use SBOM(Software Bill Of Materials) : Focusing on the Theory of Planned Behavior

노혜영*, 이신복**

Noh Hyeyoung*, Lee Sin-Bok**

요 약 기술의 발전은 기업 간 손쉬운 정보공유 및 협업을 가능하게 하였다. 그러나 여러 주체가 정보를 공유하며 접속하는 협업을 위한 시스템은 보안에 취약할 수밖에 없다. SBOM은 소프트웨어 프로그램의 구성요소를 파악하고 투명하게 관리하여 정보보안을 강화하는 방안으로 소프트웨어 자재명세서(Software Bill Of Materials, SBOM)라는 개념으로 등장하였다. 본 연구는 이러한 SBOM의 국내 도입을 촉진하고자 협업시스템 담당자들을 대상으로 도입 의도를 연구하였다. 본 연구는 계획된 행동이론과 통합기술수용이론을 기반으로 하였다. 본 연구 결과, SBOM 도입으로 인한 성과기대가 도입 의도에 미치는 중요한 변수였으며, 보안에 대한 긍정적인 태도 또한 성과기대를 매개하여 간접효과를 나타내는 것으로 확인하였다. SBOM의 도입이 기업을 대상으로 한다는 특성상 성과와 중요한 인과관계가 있으며, 보안에 대한 긍정적인 태도나 사회적 분위기로 도입 의도에 강한 영향을 줄 수 있다는 것을 확인하였다.

주요어 : 정보보안, 계획된 행동이론, 도입 의도, Software Bill Of Materials

Abstract Advances in technology have made it easier for organizations to share information and collaborate. However, collaboration systems where multiple entities share and access information are vulnerable to security. The concept of Software Bill Of Materials (SBOM) has emerged as a way to strengthen information security by identifying and transparently managing the components of software programs. To promote the adoption of SBOM in Korea, this study investigated the intention to use of collaboration system managers. This study was based on the theory of planned behavior and the integrated technology acceptance theory. The results of this study confirmed that performance expectations from SBOM adoption were an important variable for intention to use, and positive attitudes toward security also had an indirect effect through performance expectations. We found that SBOM adoption has an important causal relationship with performance due to the fact that it is targeted at enterprises, and that positive attitudes toward security and social climate can have a strong effect on intention to use.

Key words : Information Security, Theory of Planned Behavior, Intention to Use, Software Bill Of Materials

*정회원, 가천대학교 경영학부 겸임교수 (제1저자)
**정회원, 나사렛대학교 경영학과 조교수 (교신저자)
접수일: 2023년 7월 25일, 수정완료일: 2023년 8월 10일
게재확정일: 2023년 9월 1일

Received: July 25, 2023 / Revised: August 10, 2023
Accepted: September 1, 2023
**Corresponding Author: sblee@kornu.ac.kr
Dept. of Assistant Professor, Business Administration, Nazarene University, Korea

Ⅰ. 서 론

최근 소프트웨어 공급망은 현대 기업 및 조직의 중요한 요소로 자리 잡았으며, 기업들은 소프트웨어 개발과 관리를 효율적으로 수행하기 위해 다양한 조치를 취하고 있다[1]. 특히 기업은 정보자산의 가치 보호를 위해 기업은 많은 돈과 인력을 투자하여 위험을 방지하고자 하고 있다. 이는 정보보안 관련 위험이 기업의 브랜드 가치나 신뢰성의 하락 그리고 정보 및 재무적 손실을 초래할 수 있기에 기업은 보안 관련 사고 예방에 심혈을 기울이고 있는 것이다[2]. 또한, 소프트웨어 공급망의 취약성은 지속적으로 논의되었으나, 소프트웨어 구성요소의 출처와 보안 취약성에 대한 부족한 투명성으로 인해 사이버 위협과 공격의 위험은 날로 증가하고 있는 상황이다[3]. 이로 인해 소프트웨어 공급망 산업에서는 소프트웨어 구성요소의 신뢰성과 보안을 향상하기 위한 다양한 대책이 필요한 시점이다.

이러한 환경에서 기업은 협업을 위해 여러 가지 협업시스템을 활용한다. 대표적으로 재고관리 시스템, 물류시스템, 공급망 관리 시스템, 업무관리 시스템 등 여러 시스템을 타인 또는 타 기업들과 함께 사용하며 정보를 공유하고 기업의 성과를 만든다[4][5][6][7]. 특히 기업의 수요나 재고와 관련된 정보공유는 기업의 공급망 비용을 최대 90%까지 절감할 수 있다고 한다[8][9]. 그러나 문제는 이러한 정보공유에서 온다. 2021년 애플의 협력업체인 대만의 Quanta는 랜섬웨어 공격을 받은 사건이 일어났다. 랜섬웨어 공격을 한 사이버 공격자는 애플의 공급망 협업시스템을 통해 정보를 훔치고 5천만 달러를 요구하기도 하였다[10][11]. 애플의 사례에서 볼 수 있듯이 다른 기업들과 협업하기 위한 시스템은 보안에 더욱 취약하고 그 피해도 클 수 밖에 없다. 전문가들은 협업시스템은 항상 보안에 취약성을 보이고 있으며, 글로벌 기업의 경우 국제 테러의 위험성도 존재한다고 하였다[11][12]. 그러나 기업의 입장에서 보안을 강화하고자 한다면 업무의 장애 또는 성과감소를 초래하게 된다[12][13].

그러나 이러한 중요성에도 불구하고, 관련 연구가 충분히 진행되었다고 보기는 어려운 실정이다. 또한, 정보보안의 행동이나 보안위험에 관련한 연구는 실무에서 발생하는 다양한 현상을 중심으로 한 경험적 연구가 주를 이루고 있으며, 구체적인 이론적 논의가 진행되지는 않고 있다. 나아가 현재 실행되고 있는 기업의 정보 보안관련 대책은 그 실효성이 검증되고 있지 않고, 조직 구성원 측면의 고려 또한 상대적으로 미흡하다[14]. 기업에서 진행하는 보안 가이드라인은 보안관리의 가장 기초적인 단계일 뿐, 보안관리자의 적극적인 인식과 동기가 반영된 결과라고 보기 어려울 것이다.

이에 본 연구는 계획된 행동이론(TPB)을 바탕으로 기업 내 협업시스템 담당자의 정보보안 인식과 정보보안 행동 간의 관계를 확인하고자 하였으며, 구체적으로 시스템담당자의 정보보안 인식은 정보보안에 대한 태도, 주관적 규범, 지각된 행동 통제로 나누어 살펴보았으며, 정보보안 행동의 경우 구체적인 측정이 어려워 행동 의도로 그 관계를 살펴보고자 하였다. 즉, 적극적인 ICT 담당자의 정보보안 태도가 적극적인 정보보안 정책 도입 의도를 유발하고, 이는 결국 최종적으로 정보보안 관련 정책의 도입으로 이어질 것이다.

특히 본 연구는 단순히 계획된 행동이론을 바탕으로 행동 의도를 살펴보는 것이 아닌, 통합기술수용이론(UTAUT)에서의 정보보안 프로그램(정책)에 대한 성과기대(유용성)와 노력기대(용이성)의 매개효과를 통해 그 관계를 확인함으로써 정보보안행동에 중요한 영향을 미치는 요인에 대하여 검증하고자 하였다. 본 연구에서는 정보보안 관련 정책, 즉 정보보안 행동으로써 도입하게되는 방안으로 SBOM(Software Bill of Materials)의 도입 의도를 확인하고자 하였다.

여기에서의 SBOM은 소프트웨어 구성 요소 및 종속성을 명시적으로 문서화한 목록으로, 소프트웨어 개발 및 유지보수 과정에서 사용되는 여러 컴포넌트와 그 관계를 파악할 수 있도록 도와준다. 이에 기업들은 SBOM을 통해 소프트웨어 공급망의 투명성을 강화하고 있으며, 특히 SBOM은 개발자와 최종 사용자들에게 소프트웨어 구성 요소에 대한 정보를 제공하는 방법으로 주로 사용되고 있다.

즉, 본 연구를 통해 기업에게 위험관리 및 보안 강화, 공급망 보안을 향상하는 방법으로 기업 내 협업 시스템담당자의 정보보안 인식 제고 또한 적절한 전략임을 제시할 수 있으며, 이를 통해 기업과 정부가 보안위험을 더 잘 이해하고, 적절한 대응책을 수립할 것을 기대할 수 있다.

II. 이론적 배경

1. 협업시스템 담당자의 정보보안 인식

정보보안(Information security)은 다른 말로 '정보보호'라고 하며, 협의의 개념에서는 정보통신망에서의 기술적 측면에서 정보를 보호하는 것을 말하고, 광의의 개념에서는 기술적, 관리적, 제도적 차원에서의 정보보호를 의미한다[15][16]. 국내 연구에서는 정보보호(protection)와 정보보안(security)의 용어가 혼용되어서 사용하고 있지만, 궁극적으로는 정보 자체의 안정성(safety)과 무결성(integrity)의 보전을 의미한다고 볼 수 있다. 정보보안은 기업의 중요 자산인 정보에서 기밀성(confidentiality), 무결성(integrity), 가용성(availability)을 확보하는 것을 말하며, 이러한 정보자산에서 발생할 수 있는 다양한 침해 가능성을 최소화하고 위험을 관리하는 것이 정보보안의 목적이라고 볼 수 있다[17][18].

인식은 개인의 지각 또는 정해진 관심의 증가로 볼 수 있으며, 정보보안 인식(Information security awareness)은 정보보안에 대한 지각 및 정보보안 활동에 관련한 관심의 증가라고 할 수 있다[19]. 이러한 정보보안 인식과 정보보안 행동과의 관계는 주로 심리학에서 다루는 행동이론을 바탕으로 설명되고 있다. Dinevr과 Hu의 연구(2007)[20]에서는 데이터와 시스템을 보호하는 기술을 보호적 기술(protective technologies)로, 기술적 문제와 그러한 기술적 문제를 다루는 전략에 대한 지각을 기술적 인식(technology awareness)으로 정의하였다. 그리고 계획된 행동이론(TPB)을 바탕으로 이런 기술적 인식이 보호적 기술을 활용하고자 하는 의도를 형성한다고 제시하였다.

시스템담당자의 정보보안 인식은 그들이 정보보안에 대한 중요성을 이해하고, 그에 따른 책임과 역할을 인식하는 것을 의미한다. 시스템담당자의 정보보안 인식이 높으면 정보보안 행동을 기대할 수 있으며, 담당자의 정보보안 행동으로 조직의 정보보안이 확립될 수 있다. 즉, 이러한 인식을 바탕으로 담당자가 조직의 정보자산을 효과적으로 보호하고, 보안 사고를 예방하며, 보안 위협에 대응하는 행동이 예상되며, 이는 조직의 정보자산을 보호하고 지키는 데 도움이 될 것이다. 따라서 본 연구는 기업의 실질적인 협업시스템 담당자들을 대상으로 연구를 진행하였다.

2. Software Bill Of Materials(SBOM)

많은 기업과 개발자는 하나의 소프트웨어 프로그램을 개발하기 위해 타사의 소스나 오픈소스를 사용하고 있다[11][21]. 그러나 통계에 따르면 2001년 당시 프로그램 1종당 평균 35개 정도의 결함이 있으며, 연간 1,000억 라인의 결함을 보유한 채로 프로그램이 공개된다고 한다[11][22]. 더 심각한 문제는 복잡한 소프트웨어의 구조상 이러한 결함을 발견하거나 관리하지 못하게 만든다는 것이다. 가장 큰 이슈로 2021년 Apache 'Log4j'사건을 들 수 있는데, Apache 'Log4j' 라이브러리(소프트웨어 구성요소)는 애플, 마이크로소프트를 포함한 대부분의 JAVA를 활용한 소프트웨어에서 사용되고 있었다[11]. 그러나 이 라이브러리에서 보안에 치명적인 취약점이 발견되어 세계적으로 큰 이슈를 불러왔음에도 어느 소프트웨어에서 이 라이브러리를 활용했는지 관리되지 않았기 때문에 정확한 피해 현황조차 파악할 수 없었다. 이 사건으로 2021년 12월 미국 정부는 물론 국내 과학기술정보통신부 또한 대대적으로 긴급 보안패치를 권고하기도 하였다.

이러한 배경에서 미국 정부는 2021년 정보보안에 관련하여 행정명령(Executive Order on Improving the Nation's Cybersecurity, EO 14028)을 발표하면서 모든 ICT 제품 조달시 SBOM의 의무화를 시작하였다. SBOM은 프로그램 내 여러 소스코드의 구성요소들을 파악하기 위해 1990년 후반부터 BOM(Bill Of Materials)이란 개념으로 적용된 '소프트웨어 프로그램의 모든 '구성요소'를 나타내는 목록표'이다[23][24]. 따라서 SBOM의 목적은 프로그램 내 소스코드의 구성요소와 종속성에 대하여 투명하게 정보를 제공하고 관리하는 것이 그 목적이다[25]. SBOM의 적용을 위해 미국 정부에서는 프로그램을 판매할 시 SBOM을 제공하거나 웹 사이트에 게시해야 한다고 하였다(EO 14028). 즉 미국 정부는 SBOM을 정보보안의 대안 중 하나의 방법으로 채택한 것이다.

그러나 국내에서는 SBOM이 제대로 도입된 사례나 움직임을 찾기 어렵다. 특히나 크고 작은 다수의 기업이 접속하는 협업시스템은 그 보안성이 더욱 취약한 현실에서 아직 뚜렷한 정보보안 대책이 나오지 않고 있다. 이에 미 정부의 선택처럼 SBOM이 하나의 대안으로 제시할 수 있을 것이다. 따라서 본 연구는 SBOM의 국내 도입 필요성을 가지고 본 연구를 진행하였다.

3. 계획된 행동이론

계획된 행동이론(Theory of Planned Behavior, TPB)은 Fishbein과 Ajzen의 연구(1975)[26]이 제시한 합리적 행동이론(Theory of Reasoned Action, TRA)을 바탕으로 발전된 이론으로, 사람의 행동을 예측하고 이해하기 위해 주로 사용된다[27][28]. 기존의 TRA는 행동에 대한 태도(Attitude toward Behavior, AB)와 주관적 규범(Subjective Norm, SN)에 의해 행동을 수행하고자 하는 행동 의도(Behavioral Intention, BI)를 결정짓고, 행동 의도대로 인간의 행동(Behavior, B)이 나타난다는 논리를 제시하였다. TRA는 사람이 의지로 인하여 행동 의도를 통제할 수 없는 경우에는 그 행동을 예측하기 어렵다는 한계점이 나타났으며, 이러한 한계를 보완하기 위해 TPB는 행동에 대한 지각된 통제력(Perceived Behavioral Control, PBC)을 추가로 살펴보게 되었다. 계획된 행동이론의 핵심 변수의 개념을 각각 살펴보면 다음과 같다.

첫 번째는 행동에 대한 태도(AB)이다. 태도는 사람이나 사물과 같은 대상에 대하여 가지는 호의적·비호의적 반응을 보이는 경향이며, 행동에 대한 태도는 행동에 대한 일관성 있는 긍정적·부정적 평가를 말한다[29]. TPB에서 태도를 통해 이후 행동이 어떻게 나타나는지에 대한 경향을 예측할 수 있기에 행동 의도를 예측할 수 있는 중요한 요인으로 제시되고 있다[30].

두 번째는 주관적 규범(SN)이다. 주관적 규범은 준거인이 특정 행동에 대하여 어떠한 의견을 가지는지를 의미하며[31], 사회적인 영향에 의해 표현될 수도 있고, 변화될 수도 있다[32]. 어떠한 행동을 하고자 할 때, 자신에게 사회적인 영향을 미치는 준거인이 나의 행동에 대하여 찬성·반대의 반응을 보임으로써 행동에 영향을 미치게 된다.

세 번째는 지각된 행동 통제력(PBC)이다. 지각된 행동 통제력은 행동을 수행하는 것이 쉽다고 인식하는 믿음이나 신념을 의미한다. 이러한 믿음과 행동 기회가 많을수록 지각된 행동 통제력은 향상한다[32]. 지각된 행동 통제력은 사회인지 이론에서 주장하는 지각된 자기효능감(perceived self-efficacy)과 유사한 개념으로[33], 행동의 실행이 통제하에 있다고 믿는 정도라고 볼 수 있다[34].

마지막으로 의도(Intention)는, 특정 행동을 하기로 결정 한 의지나 계획이다. 즉, 의도는 실제 행동의 예측변수로 사용된다.

계획된 행동이론은 이러한 개념들을 바탕으로 의도와 실제 행동 사이의 관계를 설명한다. 예를 들어, 시스템담당자의 정보보안 인식을 이해하기 위해 계획된 행동이론을 적용할 수 있다. 개인의 정보보안에 대한 태도, 주관적 규범, 행동 통제에 대한 인식은 개인이 정보보안을 어떻게 인식하고 행동할지에 영향을 미칠 수 있다. 이를 기반으로 조직은 개인의 태도와 인식을 개선하고, 정보보안 인식을 증진하기 위한 적절한 교육 및 인식 활동을 계획함으로써 협업시스템 담당자의 정보보안 행동을 유발할 수 있다.

4. 통합기술수용이론(UTAUT)

기술수용 관련 이론 중 가장 대표적이면서도 전통적인 이론인 기술수용모델(Technology Acceptance Model, TAM)은 조직 구성원들의 정보기술 수용에 영향을 미치는 요인에 대한 탐색 끝에 개발된 이론적 틀로, 사용자들이 새로운 정보기술을 어떻게, 왜 수용하는지를 설명하고 예측하는 이론이다[35]. 계획된 행동이론은 합리적 행동이론(TRA)의 신념-태도-행동의도-행동 간의 관계를 바탕으로 발전해왔으며, 새로운 정보기술에 대한 수용은 결국 신기술에 대한 인지된 유용성(Perceived Usefulness)과 인지된 용이성(Perceived Ease of Use)의 신념에서 시작된다고 제시하였다[35]. 그러나 발전하는 정보통신 기술에 따라 기존의 간소화되어있는 계획된 행동이론 모형으로는 신기술에 대한 수용을 명확하게 설명하기엔 한계를 마주하게 되었다. 이에 Venkatesh의 연구(2003)[36]에서는 기존의 계획된 행동이론 모형에 더하여, 합리적 행동이론, 계획된 행동이론, 통합된 TAM-TPB모형, 동기모형(MM), PC활용모델(MPCU), 혁신확산이론(IDT), 사회인지이론(SCT)의 이론을 바탕으로 각각의 구성개념을 분석하고 이를 바탕으로 하나의 통합적인 모형을 구성하여 이를 바탕으로 통합기술수용이론(Unified Theory of Acceptance and Use of Technology, UTAUT)을 제시하였다[36].

통합기술수용이론(UTAUT)은 행동의도에 영향을 미치는 핵심 변수로 성과기대(Performance Expectation), 노력기대(Effort Expectation), 사회적 영향(Social Influence)을 제시하고, 촉진조건(Facilitating Condition)은 사용행동에 영향을 미치는 것을 제시하였다. UTAUT의 핵심 변수 개념을 각각 살펴보면 다음

과 같다.

첫 번째는 성과기대로, 계획된 행동이론의 지각된 유용성이 발전한 개념이며, 시스템을 사용함으로써 업무의 성과가 향상될 것이라고 믿는 믿음을 의미한다.

두 번째는 노력기대로, 계획된 행동이론의 지각된 용이성이 발전한 개념이며, 시스템의 사용이 얼마나 용이한지 정도를 의미한다. 즉, 신기술을 수용하는 부분에 있어서 사용자가 쉽게 사용할 수 있고, 어려움 없이 사용 방법을 익혀야 사용 행동으로 이어질 수 있음을 말한다.

세 번째는 사회적 영향으로, TRA, TPB에서 제시하는 주관적 규범이 발전한 개념이며, 사용자의 중요한 주변 사람들에 의해 사용자의 행동이 정해질 수 있음을 제시한다.

네 번째는 촉진조건으로, TPB의 지각된 행동 통제력이 발전한 개념이며, 시스템을 사용하는 것을 돕는 기술적 인프라와 지원이 존재한다고 믿는 정도를 의미한다.

그러나 본 연구에서는 TPB의 주관적 규범과 지각된 행동 통제를 변수로 사용하기에 UTAUT에서 사회적 영향과 촉진조건을 제외하였다. 그리고 보안의 중요성 및 인식에 대한 특성을 고려할 때, 주요변수인 성과기대, 노력기대가 핵심적인 요인으로서 작용할 것으로 보고 정보보안인식과 SBOM 도입 의도와의 관계에서 그 영향력을 보고자 하였다.

5. SBOM 도입 의도

SBOM은 소프트웨어의 각 구성요소에 대한 종속 관계를 표현함으로써 소프트웨어 구성요소의 투명성을 증가시키고, 활발한 SBOM의 유통으로 인해 공급망 체계에서의 신뢰도를 향상할 수 있다는 목표를 지니고 있다[37]. 이는 디지털 인프라에 대한 의존도가 점점 높아지고 있는 현 사회에서, 소프트웨어의 각 구성요소에 대한 신뢰성과 투명성이 부족하다는 인식에서 기인한다.

이러한 배경에 SBOM 도입 의도는 조직이 소프트웨어 생태계의 투명성과 보안을 강화하기 위해 SBOM을 도입하려는 의지나 계획을 나타낸다. 기업의 입장에서 SBOM의 도입으로 인해 정보자산을 보호할 수 있고, 보안위험을 감소시킬 수 있으며, 국내외의 여러 규정 준수 요구를 충족하는데 도움이 될 수 있을 것이다. 따라서 본 연구는 TPB의 의도를 SBOM의 도입으로 이어지는 행동 의도로 간주하여 SBOM 도입 의도를 종속변수로 활용하였다.

III. 연구 방법

1. 표본설계와 측정도구

본 연구는 제조기업의 협업시스템을 담당하는 실무 담당자들로 구성하였다. 업무의 전문성을 보유한 담당자를 대상으로 하기 위해 관련 경력 5년 이상자들로 구성하였다. 조사 기간은 2023년 1월 23일부터 2월 17일까지 진행되었다. 본 연구에는 결측 데이터 및 불성실 응답 데이터를 제외한 349개의 데이터가 활용되었다.

먼저 계획된 행동이론에서 행동을 예측하기 위한 핵심 변수인 행동 태도는 '행동에 대한 일관성 있는 긍정적·부정적 평가'를 의미하고[29], 주관적 규범은 '준거인이 특정 행동에 대하여 어떠한 의견을 가지는지'를 의미하며[31][32], 지각된 행동 통제는 '행동을 수행하는 것이 쉽다고 인식하는 믿음이나 신념'을 의미한다[32][33][34]. 이에 세 가지 각 변수를 독립변수로 설정하고 선행연구들의 측정 항목에서 정보보안을 대입하여 <표 1>과 같이 설정하였다[38][39][40][41][42][43].

통합기술수용이론의 핵심 변수인 성과기대와 노력기대는 각 '시스템을 사용함으로써 업무의 성과가 향상될 것이라고 믿는 믿음'과 '시스템의 사용이 얼마나 용이한지 정도'를 의미한다[39][41][44][45]. 본 연구에서는 SBOM이라는 ICT 정보보안 방안 도입에 대하여 계획된 행동이론의 행동을 예측하게 하는 세 가지 변수가 기업에서의 성과, 기업에서의 활용 용이성을 매개하여 도입 의도에 이른다고 보고 있다. 따라서 통합기술수용이론의 성과기대와 노력기대라는 두 변수를 매개변수로 설정하고 선행연구의 측정 항목에서 SBOM 도입으로 이루는 기대를 대입하여 <표 1>과 같이 설정하였다.

마지막으로 도입 의도는 계획된 행동이론의 행동 할 것이라 예측 할 수 있는 변수로서 선행연구의 측정 항목에 SBOM을 적용하여 <표 1>과 같이 측정하였다[38][44][45].

2. 분석방법

본 연구는 <표 1>의 6개 요인에 대한 타당성 분석

표 1. 측정항목
Table 1. list of measurement

변수	측정 항목
행동 태도	정보보안 정책을 준수하는 것은 좋은 생각이다.
	시스템을 안티바이러스 프로그램, 소프트웨어, 방화벽 등 보안을 위한 노력이 필요하다고 생각한다.
	조직의 시스템을 보호하기 위한 보안 조치가 중요하다고 생각한다.
	조직의 시스템을 보호하기 위한 보안대책을 수립하는 것이 옳다고 생각한다.
주관적 규범	나에게 영향을 주는 사람은 내가 SBOM을 도입해야 한다고 생각할 것이다.
	시스템과 연관된 중요한 사람은 SBOM을 사용하는 것이 당연하다고 생각할 것이다.
	SBOM이 소프트웨어 산업계 내에서 기업 경쟁력에 영향을 준다고 생각한다.
	경쟁사가 SBOM을 사용한다면 우리 조직도 도입을 검토해야 한다고 생각한다.
지각된 행동 통제	나는 대부분의 정보보안 정책을 준수하는 데 전혀 불편함이 없다.
	나는 정보보안정책 준수에 필요한 역량을 가지고 있다.
	나는 주변에 도와줄 사람이 없어도 정보보안정책을 준수할 능력이 있다.
	만일 내가 원한다면 정보보안정책을 준수하는 것은 매우 쉬운 일이다.
성과 기대	SBOM의 도입으로 정보보안 업무(소프트웨어 보안 및 라이선스 관리 등)를 보다 빨리 처리할 수 있을 것으로 생각한다.
	SBOM의 도입으로 정보보안 업무에 질적 향상이 있을 것으로 생각한다.
	SBOM의 도입으로 정보보안 업무를 보다 쉽게 처리할 수 있을 것으로 생각한다.
	SBOM의 도입으로 정보보안 업무의 가치를 높여 줄 것으로 생각한다.
노력 기대	SBOM에 대해 명확하게 이해하는 데 어려움이 없을 것으로 생각한다.
	SBOM을 잘 사용할 수 있을 것으로 생각한다.
	SBOM을 사용하는 데 익숙해질 것으로 생각한다.
	SBOM을 도입한 후 받아야 하는 사용 교육은 쉬울 것으로 생각한다.
도입 의도	SBOM 도입을 추천할 의향이 있다.
	SBOM을 도입할 것으로 예측할 수 있다.
	SBOM을 도입하여 사용할 의사가 있다.
	SBOM을 도입하여 사용법을 학습할 계획이 있다.

과 인과관계를 설명하고자 하였다. 따라서 인과관계를 분석하기 위해 공분산 구조분석(covariance structure analysis)을 활용하여 진행하였다. 또한, 매개효과를 측정하기 위해 부트스트랩 간접효과 유효성 검증과 팬텀 변수를 활용한 각 경로별 간접효과도 측정하였다. 분석을 위한 도구로 구조방정식 모형 소프트웨어인 IBM의 SPSS 18.0과 Amos 18.0을 활용하여 검증하였다.

3. 가설 설정

이론적 배경에서 언급한 것처럼 합리적 행동이론을 바탕으로 발전한 계획된 행동이론은 행동 태도와 주관적 규범 그리고 지각된 행동 통제로 행동을 예측할 수 있다고 하였다[29][30][33]. 그리고 통합기술수용이론에 따르면 기술에 대하여 기대할 수 있는 성과와 노력으로 행동이 정해진다고 하였다[35][36]. 이에 정보보안을 위한 SBOM에 대한 태도, 주관적 규범, 지각된 행동 통제가 정보보안 성과와 SBOM 활용 용이성을 매개로 도입 의도까지 나타날 것이라 기대하여 다음과 같은 가설을 수립하였다.

H1. 계획된 행동이론의 행동 태도, 주관적 규범, 지각된 행동 통제는 성과기대에 정(+)의 영향을 미칠 것이다.

H2. 계획된 행동이론의 행동 태도, 주관적 규범, 지각된 행동 통제는 노력기대에 정(+)의 영향을 미칠 것이다.

H3. 계획된 행동이론의 행동 태도, 주관적 규범, 지각된 행동 통제는 도입 의도에 정(+)의 영향을 미칠 것이다.

H4. 성과기대는 도입 의도에 정(+)의 영향을 미칠 것이다.

H5. 노력기대는 도입 의도에 정(+)의 영향을 미칠 것이다.

H6. 성과기대와 노력기대는 계획된 행동이론의 행동 태도, 주관적 규범, 지각된 행동 통제와 도입 의도 간 관계에서 매개효과가 있을 것이다.

Ⅳ. 분석 결과

1. 표본의 특성

본 연구에 활용된 표본의 인구 통계학적 특성은 <표 2>와 같다. 먼저 성별로는 남성이 211명(60.5%), 여성이 138명(39.5%)로 나타났다. 연령으로는 30대와 40대가 249명으로 전체의 71.3%를 차지하였다. 학력은 대학 졸업자가 275명(78.8%)로 가장 높게 나타났다. 직무로는 Staff와 Junior manager가 316명으로 전체의 90.6%로 나타났다. 마지막으로 응답자의 중요한 조건 중 하나였던 경력은 5년 이상부터 15년 미만이 237명으로 전체의 68.6%를 차지하였다. 추가적으로 21년 이상 경력자도 61명(17.5%)로 낮지 않은 결과를 나타내었다.

표 2. 인구 통계
Table 2. Demographics of the Survey Respondents

구분		N	%
성별	남성	211	60.5
	여성	138	39.5
나이	30 - 39세	102	29.2
	40 - 49세	147	42.1
	50 - 59세	72	20.6
	60세 이상	28	8.1
학력	고등학교 졸업	25	7.2
	대학교 졸업	275	78.8
	대학원 졸업	43	12.3
	기타	6	1.7
직급	사원	106	30.4
	선임	210	60.2
	주임 이상	33	9.4
경력	5 - 10년	107	30.7
	11 - 15년	133	38.1
	16 - 20년	48	13.7
	21년 이상	61	17.5

2. 측정 항목의 신뢰성과 타당성

가설을 검증하기 전, 각 변수의 측정 항목에 대한 신뢰성과 타당성 검증을 시행하여 결과를 <표 3>과 같이 제시하였다. 분석방법은 AMOS를 통한 확인적 요인분석을 진행한 후 CR(Composite Reliability)과 AVE(Average Variance Extracted)를 계산하였다. 신뢰성 분석을 위한 Cronbach's α는 SPSS로 계산되었다.

먼저 집중 타당성(convergent validity) 검증을 위해 Standard Loading 값을 확인한 결과 모두 0.7 이상으로 통상적으로 제시하는 기준치인 ±0.4보다 높게 나타났다. 각 변수들의 수렴타당성 확보를 위해 CR과 AVE 검증을 진행하였다[46]. 일반적으로 Composite Reliability의 기준으로 0.70이 제시되고 있으며, Average Variance Extracted는 0.05 이상을 적정으로 보고 있다[47][48]. 본 분석결과는 CR 값이 모두 0.8 이상, AVE 값이 모두 0.6 이상으로 타당성을 확보하였다.

판별 타당성을 검증하기 위해 SPSS에서 상관관계분석을 진행한 후 AVE와 비교한 결과를 <표 4>로 제시하였다. 판별 타당성은 각 구성에 대한 AVE를 상관계수의 제곱근을 비교하여 평가한다[46][48]. 상관계수 ±2*S.E.의 계산 결과가 모두 1을 포함하지 않으며,

표 3. 측정 항목의 신뢰성과 타당성
Table 3. Reliability and validity of measurement items

변수	측정항목	요인 적재량	Cronbach's α	C.R	AVE
행동 태도 (Attitude toward Behavior)	AB1	0.852	0.911	0.911	0.720
	AB2	0.863			
	AB3	0.856			
	AB4	0.822			
주관적 규범 (Subjective Norm)	SN1	0.819	0.906	0.906	0.707
	SN2	0.851			
	SN3	0.863			
	SN4	0.829			
지각된 행동 통제 (Perceived Behavioral Control)	PBC1	0.825	0.900	0.901	0.695
	PBC2	0.896			
	PBC3	0.840			
	PBC4	0.770			
성과기대 (Performance Expectation)	PE1	0.871	0.907	0.907	0.709
	PE2	0.846			
	PE3	0.852			
	PE4	0.797			
노력기대 (Effort Expectation)	EE1	0.792	0.897	0.897	0.687
	EE2	0.846			
	EE3	0.856			
	EE4	0.819			
도입 의도 (Intention to Use)	ITU1	0.930	0.948	0.948	0.819
	ITU2	0.878			
	ITU3	0.932			
	ITU4	0.879			

AVE 결과도 모두 상관계수 값을 초과하므로 판별 타당성을 확보하였다.

본 연구를 위한 측정 항목의 신뢰성과 타당성이 모두 확보됨을 확인하고 가설검증을 진행하였다.

표 4. 구성개념의 상관관계, 평균, 표준편차
Table 4. Correlations among Constructs

요인	요인 간 상관계수					
	1	2	3	4	5	6
행동 태도	(0.720)					
주관적 규범	0.485	(0.707)				
지각된 행동 통제	0.173	0.318	(0.695)			
성과기대	0.658	0.531	0.276	(0.709)		
노력기대	0.393	0.296	0.417	0.458	(0.687)	
도입 의도	0.504	0.490	0.234	0.596	0.292	(0.819)
평균	5.689	5.190	4.727	5.476	5.026	6.006
표준편차	0.887	0.963	1.035	0.835	0.877	0.81

(): AVE 값

3. 측정모형의 적합도 검증

본 연구의 가설을 검증하기 위해 분석 도구로 AMOS를 활용하였으며, 구조방정식으로 인과관계를 분석하였다. 먼저 구조방정식 모형의 적합도를 살펴본 결과를 <표 5> 하단에 제시하였다. 모형 적합도 결과는 χ2값 418.176로 p<=0.001로 나타났으며, CMIN/DF값이 1.757으로 수용가능 영역인 3미만으로 나타났다. Root Mean-Square Residual인 RMR은 0.05 이하까지 수용하는데, 본 연구모델은 0.04로 적합하게 나타났다. Root Mean Square Error of Approximation인 RMSEA는 0.047로 기준치인 0.8이하로 적합함으로 나타났다. 이 외에도 모형의 적합도를 검증하는 GFI(goodness of fit index), NFI(normed fit index), IFI(Incremental fit index), TLI(Turker-Lewis index), CFI(comparative fit index) 모두 기준치인 0.9를 넘어 모델 적합성을 검증하였다

4. 연구가설 검증 결과

본 연구의 가설검증을 위한 경로 분석 결과를 <표 5>와 같이 제시하였다. 먼저 가설1인 계획된 행동이론의 행동 태도, 주관적 규범, 지각된 행동 통제는 성과기대에 정의 영향을 미친다는 가설은 P값 0.05 기준 내에서 모두 채택되었다. 그중 행동 태도가 경로계수 0.581(P<0.001)에서 가장 높게 나타났다. 협업시스템 담당자의 보안에 대한 태도는 업무의 성과 향상 기대에 가장 많은 영향을 준다는 것을 알 수 있었다.

가설2인 계획된 행동이론의 행동 태도, 주관적 규범, 지각된 행동 통제가 노력기대에 미치는 영향에서는 주관적 규범만 기각되고 나머진 채택되었다. 노력기대는 기술 활용의 용이성을 의미하는데, 보안에 대한 긍정적 행동 태도와 수행의 어려움을 느끼지 않는 지각된 행동 통제는 SBOM 활용의 이해나 사용에 긍정적인 영향을 미친다는 결과인 것이다. 그러나 주관적 규범은 준거인인 타인의 영향으로서 타인의 영향이 SBOM을 용이하게 활용하는것과 관련성을 가지기 어렵다는 결론인 것이다.

가설3인 계획된 행동이론의 행동 태도, 주관적 규범, 지각된 행동 통제가 도입 의도에 미치는 영향은 주관적 규범만 유의미한 결과를 도출하였고 행동 태도와 지각된 행동 통제는 기각되었다. 이는 실질적으로 기업에 SBOM 도입 의도를 가지게 되는 요인으로 담당자의 태도나 지각된 행동 통제가 아닌 준거인의 영향이 가장 크다는 것이다. 이러한 결과는 SBOM이 개인의 의지로 도입되는 것이 아닌 기업의 의사결정이 필요한 부분이기 때문에 나타난 결과로 보인다. 아마도 여기서 영향을 미치는 준거인은 기업에 관련한 경영진이나 여론 등 개인이 아닌 기업에 영향을 미치는 준거인의 영향을 의미할 것으로 예측된다.

가설4인 SBOM 도입으로 인한 성과기대가 도입 의도에 미치는 영향은 경로계수 0.438(P<0.001)의 높은 수치로 채택되었다. 그러나 가설5인 SBOM 도입의 노력기대가 도입 의도에 미치는 영향은 P값 0.472로 기각되었다. 이는 기업에 도입하는 입장에서 SBOM 도입한 활용이 얼마나 용이한지 보다는 SBOM을 도입하는 목적이 정보보안 향상이라는 성과라는 측면에서 나타난 결과로 나타났다.

표 5. 가설검증 결과
Table 5. Result of Research Model

가설		Estimate	S.E.	C.R.	P	결과
H1.1	AB → PE	0.581	0.055	10.480	***	채택
H1.2	SN → PE	0.216	0.051	4.238	***	채택
H1.3	PBC → PE	0.101	0.036	2.842	0.004	채택
H2.1	AB → EE	0.358	0.061	5.858	***	채택
H2.2	SN → EE	-0.005	0.058	-0.081	0.936	기각
H2.3	PBC → EE	0.301	0.044	6.766	***	채택
H3.1	AB → ITU	0.121	0.076	1.590	0.112	기각
H3.2	SN → ITU	0.189	0.056	3.352	***	채택
H3.3	PBC → ITU	0.041	0.043	0.936	0.349	기각
H4	PE → ITU	0.438	0.079	5.565	***	채택
H5	EE → ITU	-0.043	0.059	-0.719	0.472	기각
χ2: 418.176***, CMIN/DF: 1.757, RMR: 0.040, GFI: 0.913, NFI: 0.939, RFI: 0.930, IFI: 0.973, TLI: 0.968, CFI: 0.973, RMSEA: 0.047						

*p<=0.05, **p<=0.01, ***p<=0.001.

표 6. 간접효과 검증 결과
Table 6. Results of Mediating Effect Analysis

가설		직접효과	간접효과	총간접효과	총효과	결과
H6.1	AB PE ITU EE	0.121	0.255*** -0.015	0.239***	0.361***	채택
H6.2	SN PE ITU EE	0.189**	0.095*** 0.000	0.095***	0.283***	채택
H6.3	PBC PE ITU EE	0.041	0.044** -0.013	0.032	0.072	기각

*p<=0.05, **p<=0.01, ***p<=0.001.

마지막으로 본 연구에서 기업의 도입이라는 측면을 고려하여 계획된 행동이론을 그대로 활용하기보다 기업의 성과나 활용 기대를 매개할 것이라는 예측으로 수립한 가설6의 결과는 <표 6>과 같다. 매개변수가 성공기대와 노력기대로 다수인 점을 고려하여 다중매개의 경로별 간접효과를 볼 수 있는 Phantom variable modeling으로 그 영향도와 유의성을 검증하였다. 그 결과 행동 태도와 주관적 규범이 도입 의도에 미치는 영향에 성과기대와 노력기대의 간접효과는 유의한 결과가 나타났으나, 지각된 행동 통제가 도입 의도에 미치는 영향에서 매개효과는 기각되었다. 가설3에서 주관적 규범이 도입 의도에 미치는 직접적 영향에서 경로계수 3.352(P<0.001)의 값으로 채택되었으며, 성과기대와 노력기대를 매개하여 더 큰 영향을 미친다는 결과가 나타났다. 그러나 행동 태도의 경우 도입 의도에 직접적인 영향을 미치지 못하지만 매개변수 중 특히 성공기대를 매개할 경우 유의미한 영향을 미친다는 것을 알 수 있다.

Ⅴ. 결 론

기술의 발전은 기업에게 많은 발전을 가져왔다. 특히 기업은 기업 내 또는 타 기업들과 협업시스템을 활용하여 정보를 공유하고 성과를 만든다[4][5][6][7]. 이러한 협업시스템 활용은 기업에게 글로벌 진출 또는 파트너쉽 등 다양한 역량으로 활용되었지만, 문제는 이러한 협업시스템은 정보유출, 사이버 테러 등 나아가 국제테러의 위험성도 존재할 정도로 보안에 취약하다는 것이다[11][12]. 하지만 기업의 입장에서 보안을 강화하고자 한다면 업무의 장애 또는 성과감소를 초래하게 된다[13][12]. 이처럼 보안의 중요성에도 정보보안을 위한 대안 중 하나인 SBOM의 도입이 활성화되지 않고 있다. 이 SBOM은 소프트웨어 프로그램의 모든 구성요소를 파악하고 구조를 투명하게 관리하여 보안성과 종속성 그리고 투명성을 높이는 목적으로 도입되었으며 미국에서는 2021년 정보보안관련 행정명령(EO 14028)에 의해 정식으로 도입되기도 하였다[23][24]. 본 연구는 이러한 SBOM의 국내도입에 기여하고자 직접 시스템을 관리하는 기업의 협업시스템 담당자로 하여금 SBOM의 도입 의도에 미치는 영향을 연구하였다.

본 연구 결과의 첫 번째로 계획된 행동이론의 행동예측요인인 정보보안에 대한 행동 태도, 주관적 규범, 인지된 행동 통제는 SBOM 도입으로 기대하는 성과에 긍정적인 영향을 미쳤다. 이를 바탕으로 정보보안에 관련하여 쉽게 지킬 수 있는 규정을 제시하고 긍정적 태도와 사회적 분위기를 조성한다면 SBOM의 성과기대에 긍정적 효과를 볼 수 있을것이다.

두 번째로 본 연구는 SBOM을 기업의 협업시스템에 도입하고자 연구된 만큼 기업이라는 배경이 가지는 특징을 가진다. 따라서 궁극적 목적인 도입 의도에 성과기대는 높은 경로계수로 유의미한 결과를 나타났지만 사용 용이성은 유의하지 않았다. 이러한 결과로 보안을 위한 SBOM이 기업의 생산적 활동에 도움을 주는 것이 아닌 정보보안을 위한 목적이기에 용이성보다 성과가 중요한 요인인 것으로 판단할 수 있다.

세 번째로 행동 예측요인과 도입 의도 간 관계에서 성과기대와 노력기대가 매개역할을 보는 연구 결과는 행동 태도와 주관적 규범 채택되었다. 특히 행동 태도는 도입 의도에 직접적 영향을 미치지 않았지만, 성과기대와 노력기대를 매개할 때 유의미한 결과를 나타내었다. 이를 미루어 볼 때 보안에 대한 긍정적인 태도는 SBOM의 도입으로 기대되는 성과를 매개하여 도입 의도에 유의미한 영향을 미친다는 것을 알 수 있다.

본 연구는 실무적으로 기술의 발전에 따라 기업이 널리 활용하는 다양한 협업시스템의 보안 문제를 제기하며 이에 대응책으로 SBOM을 제안하였다. 그리고 SBOM의 도입 확산을 위해 실무자들을 대상으로 연구된 부분에서 실무적 시사점을 가진다. 학문적으로는 기존의 국내에서 정보보안의 연구는 보안시스템의 발전이나 블록체인 등 신기술에 초점을 맞추고 있으며 현재 시스템을 보완하고 관리하는 부분에서 상당히 미흡하다[12][49][50]. 이에 국내의 SBOM 연구에 대한 기반으로 본 연구가 학문적 시사점을 가지고 있다.

SBOM은 미국에서도 2021년 본격적으로 도입되었고, 세계적으로는 물론 국내에서 SBOM에 관련한 연구의 초기 단계이다. 이에 본 연구가 가지는 한계점으로 다양한 국내 도입사례 및 SBOM으로 달라진 성과 등을 제시하기 어렵다는 부분이다. 다른 한계점으로 SBOM은 하나의 기업이 도입하는 것이 아닌 협업하는 모든 기업들이 함께 도입되어야 하며 표준화된 규정도 필요하다. 미국 정부는 NTIA(National Telecommunications and Information Administration)를 통해 표준화 작업을 시도하였으나[21] 국내는 아직 그 움직임이 나타나고

있지 않다. 이에 본 연구에서는 이러한 환경적 부분을 제외하였기에 그 한계점을 가지고 있다. 그러나 아직 SBOM 연구에 초기 단계인 만큼 본 연구가 향후 SBOM에 관련한 더 의미 있는 연구에 기여될 수 있을 것으로 기대한다.

References

[1] W.S. Kang, and H.J. Pang, "Researching technology trends and suggesting future developments for software supply chain security management", *Journal of The Korea Institute of Information Security and Cryptology (JKIISC)*, Vol. 32, No. 5, pp. 21-25, October 2022

[2] H. Cavusoglu, S. Raghunathan, and H. Cavusoglu, "Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems", *Information Systems Research*, Vol. 20, No. 2, pp. 198-217, February 2009. DOI:10.1287/isre.1080.0180

[3] J.M. Kim, D.H. Kwon, S.H. Joo, and S.H. Joo, "A Study on the Improvement of the National Cyber Security Policy Against the Spread of Ransomware Damage", *The Journal Of Korean Institute Of Communications And Information Sciences (J-Kics)*, Vol. 47, No. 11, pp. 1932-1948, November 2022. DOI:10.7840/kics.2022.47.11.1932

[4] S. Ahmad, and R.G. Schroeder, "The impact of electronic data interchange on delivery performance", *Production and operations management*, Vol. 10, No. 1, pp. 16-30, January 2001. DOI:10.1111/j.1937-5956.2001.tb00065.x

[5] R. Croson, and K. Donohue, "Impact of POS data sharing on supply chain management: An experimental study", *Production and Operations Management*, Vol. 12, No. 1, pp. 1-11, January 2003. DOI:10.1111/j.1937-5956.2003.tb00194.x

[6] D. Delen, and B.C. Hardgrave, "RFID for better supplychain management through enhanced information visibility", *Production and Operations Management*, Vol. 16, No. 5, pp. 613-624, January 2007. DOI:10.1111/j.1937-5956.2007.tb00284.x

[7] J. Whitaker, S. Mithas, and M.S. Krishnan, "A field study of RFID deployment and return expectations", *Production and Operations Management*, Vol. 16, No. 5, pp. 599-612, January 2007. DOI:10.1111/j.1937-5956.2007.tb00283.x

[8] G.P. Cachon, and M. Fisher, "Supply chain inventory management and the value of shared information", *Management science*, Vol. 46, No. 8, pp. 1032-1048, August 2000. DOI:10.1287/mnsc.46.8.1032.12029

[9] S. Gavirneni, R. Kapuscinski, and S. Tayur, "Value of information in capacitated supply chains", *Management Science,* Vol. 45, No. 1, pp. 16-24, January 1999. DOI:10.1287/mnsc.45.1.16

[10]L.H. Newman, Apple's ransomware mess is the future of online extortion, Available from https://www.wired.com/story/apple-mac-lockbit-ransomware-samples/ (accessed May 1, 2023)

[11]S. Kumar, and R.R. Mallipeddi, "Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions", *Production and Operations Management*, Vol. 31, No. 12, pp. 4488-4500, September 2022. DOI:10.1111/poms.13859

[12]Y. Sheffi, "Supply chain management under the threat of international terrorism", *The International Journal of Logistics Management*, Vol. 12, No. 2, pp. 1-11, July 2001. DOI:10.1108/09574090110806262

[13]N.R. Joglekar, J. Davies, and E.G. Anderson, "The role of industry studies and public policies in production and operations management", *Production and Operations Management*, Vol. 25, No. 12, pp. 1977-2001, September 2016. DOI:10.1111/poms.12640

[14]M.J. Baek, and S.H. Sohn , "A Study on the Effect of Information Ethics on the Information Security Awareness and Behavior in Organization", *Koreanische Zeitschrift fuer Wirtschaftswissenschaften*, Vol. 28, No. 4, pp. 119-145, December 2010

[15]S.J. Lee, and M.J. Lee, "An Exploratory Study on the Information Security Culture Indicator", *Informatization Policy*, Vol. 15, No. 3, pp. 100-119, October 2008

[16]J.T. Kim, "Analyses of Security Issues and Vulnerability for Healthcare System For Under Internet of Things", *The journal of Convergence on Culture Technology (JCCT)*, Vol. 9, No. 4, pp. 699-706, July 2023. DOI:10.17703/JCCT.2023.9.4.639

[17]S.H. Kim, and S.Y. Park, "Influencing Factors for Compliance Intention of Information Security Policy", *The Journal of Society for e-Business Studies*, Vol. 16, No. 4, pp. 33-51, November 2011. DOI:10.7838/jsebs.2011.16.4.033

[18]J.E. YOO, "A Study on the Application of Cybersecurity by Design of Critical Infrastructure", *The journal of Convergence on Culture Technology*

(JCCT), Vol. 7, No. 1, pp. 674-681, February 2021. DOI:10.17703/JCCT.2021.7.1.397

[19]N. Choi, D. Kim, J. Goo, and J. Goo, "Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action", *Information Management & Computer Security*, Vol. 16, No. 5, pp. 484-501, November 2008. DOI:10.1108/09685220810920558

[20]T. Dinev, and Q. Hu, "The centrality of awareness in the formation of user behavioral intention toward protective information technologies", *Journal of the Association for Information Systems*, Vol. 8, No. 7, pp. 23, July 2007. DOI:10.17705/1jais.00133

[21]A. Arora, V. Wright, and C. Garman, "Strengthening the Security of Operational Technology: Understanding Contemporary Bill of Materials", *JCIP The Journal of Critical Infrastructure Policy*, Vol. 3, No. 1, pp. 111, Spring/Summer 2022. DOI:10.18278/jcip.3.1.8

[22]R. Anderson, *Why information security is hard - an economic perspective*, Seventeenth Annual Computer Security Applications Conference, New Orleans, LA, USA, pp. 358-365, December 2001. DOI:10.1109/ACSAC.2001.991552

[23]R. Schmidt and T. Duffy, *Non-interfering software distribution*, Paris: Data Systems in Aerospace-DASIA, Vol. 97, No. 409, PP. 351 - 358, May 1997.

[24]P.M. Fangman, L.H. Gerhardstein and B.J. Homer, *Federal Emergency Management Information System (FEMIS): Bill of Materials (BOM) for FEMIS (version 1.4.5. No. PNL10689-Ver. 1.4.5.)*, Richland, WA: Pacific Northwest National Laboratory, June 1998. DOI:10.2172/663230

[25]N. Zahan, E. Lin, M. Tamanna, and M. Tamanna, "Software Bills of Materials Are Required. Are We There Yet?", *IEEE Security & Privacy*, Vol. 21, No. 2, pp. 81-88, April 2023. DOI:10.1109/MSEC.2023.3237100

[26]M. Fishbein and I. Ajzen, *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*, Reading, MA: Addison-Wesley, May 1975.

[27]S.H. Yoo, Y.J. Park, H.M. Kang, and H.M. Kang, "The Effect of Motivation for Emoticon Use on Behavior of Purchasing Paid Emoticon: Focused on Theory of Planned Behavior", *The journal of Convergence on Culture Technology (JCCT)*, Vol. 7, No. 2, pp. 395-404, May 2021. DOI:10.17703/JCCT.2021.7.2.39

[28]J.J. Chun, "A Study on Manufacturing Innovation in the Jewelry Industry through Automated Systems", *The journal of Convergence on Culture Technology (JCCT)*, Vol. 6, No. 4, pp. 123-130, November 2020. DOI:10.17703/JCCT.2020.6.4.12

[29]B. Sparks, "Planning a wine tourism vacation? Factors that help to predict tourist behavioural intentions", *Tourism management*, Vol. 28, No. 5, pp. 1180-1192, October 2007. DOI:10.1016/j.tourman.2006.11.003

[30]I. Ajzen, and M. Fishbein, "Attitudes and the attitude-behavior relation: Reasoned and automatic processes", *European review of social psychology*, Vol. 11, No. 1, pp. 1-33, April 2001. DOI:10.1080/14792779943000116

[31]J.C. Oh, "A Study on the Impulsive Buying of Digital Contents Using Theory of Planned Behavior :Focused on Sensation Seeking Tendency", *Journal of The Korean Academic Association of Business Administration Presentation Conference*, pp. 477-504, November 2007

[32]I. Ajzen, "The theory of planned behavior", *Organizational behavior and human decision processes*, Vol. 50, No. 2, pp. 179-211, December 1991. DOI:10.1016/0749-5978(91)90020-T

[33]A. Bandura, "Self-efficacy: toward a unifying theory of behavioral change", *Psychological review*, Vol. 84, No. 2, pp. 191, 1977. DOI:10.1037/0033-295X.84.2.191

[34]D.W. Hahn, and M.K. Rhee, "Explaining Drinking and Driving : An Application of Theory of Planned Behavior", *Korean Journal of Social and Personality Psychology*, Vol. 15, No. 2, pp. 141-158, August 2001

[35]F.D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS quarterly*, Vol. 13, No. 3, pp. 319-340, September 1989. DOI:10.2307/249008

[36]V. Venkatesh, M.G. Morris, G.B. Davis, and G.B. Davis, "User acceptance of information technology: Toward a unified view", *MIS quarterly*, Vol. 27, No. 3, pp. 425-478, August 2003

[37]Y.S. Choi, "US Software Supply Chain Security Policy Trends: Focusing on SBOM Case", *Review Of Kiisc*, Vol. 32, No. 5, pp. 7-14, October 2022

[38]B.S. Suh, G.H. Hwang, and S.K. Kim, "A Study on the Factors Affecting the Intention to Adapt PMO in Public Sectors", *Journal of Digital Convergence*, Vol. 12, No. 5, pp. 159-169, May 2014. DOI:10.14400/JDC.2014.12.5.159

[39]M.H. Ahn, and C.M. Heo, "The Effect of Technical Characteristics of Smart Farm on Acceptance

Intention by Mediating Effect of Effort Expectation", *Journal of Digital Convergence*, Vol. 17, No. 6, pp. 145-157, June 2019. DOI:10.14400/JDC.2019.17.6.145

[40]K.A. Park, "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, Vol. 24, No. 4, pp. 79-98, August 2019. DOI:10.9723/jksiis.2019.24.4.079

[41]D.H. Jun, S.h. Jang, J.J. Lee, and J.J. Lee, "A Study of IT Maintenance Outsourcing Service Factors of Local Governments: Based on AHP Analysis Method", *Journal of Information Technology Services (JITS)*, Vol. 21, No. 3, pp. 43-61, June 2022. DOI:10.9716/KITS.2022.21.3.043

[42]K.S. Kang, and H.Y. Kwon, "A Study on Influence of Information Security Stress and Behavioral Intention for Characteristic factors of Information Security Policy Perceived by Employee", *The Journal of The Institute of Internet, Broadcasting and Communication (JIIBC)*, Vol. 16, No. 6, pp. 243-253, December 2016. DOI:10.7236/JIIBC.2016.16.6.243

[43]M.J. Baek, and S.H. Sohn , "A Study on the Effect of Information Security Awareness and Behavior on the Information Security Performance in Small and Medium Sized Organization", *The Korea Association of Small Business Studies*, Vol. 33, No. 2, pp. 113-132, June 2011

[44]D.H. Kim, S.D. Park, S.J. Kim, and S.J. Kim, "A Study on Establishment of Cyber Threat Information Sharing System Focusing on U.S. Cases", *Journal of convergence security*, Vol. 17, No. 2, pp. 53-68, june 2017

[45]D.Y. Chang, and C.K. Lee, "A Study of Use Intention of Chatbot Using the Extended Theory of Planned Behavior: Focusing on the Role of Interaction", *Journal of Tourism and Leisure Research*, Vol. 31, No. 8, pp. 433-454, August 2019

[46]M.R. Hamid, W. Sami, and M.M. Sidek, "Discriminant Validity Assessment: Use of Fornell & Larcker criterion versus HTMT Criterion", *Journal of Physics: Conference Series*, Vol. 890, No. 1, pp. 8-10, August 2017. DOI:10.1088/1742-6596/890/1/012163

[47]J. Hulland, "Use of partial least squares (PLS) in strategic management research: A review of four recent studies", *Strategic management journal*, Vol. 20, No. 2, pp. 195-204, February 1999. DOI:10.1002/(SICI)1097-0266(199902)20:2<195::AID-SMJ13>3.0.CO;2-7

[48]C. Fornell, and D.F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error", *Journal of marketing research*, Vol. 18, No. 1, pp. 39-50, February 1981. DOI:10.1177/002224378101800104

[49]M.S. Sodhi, B. Son, and C.S. Tang, "Researchers' perspectives on supply chain risk management", *Production and Operations Management*, Vol. 21, No. 1, pp. 1-13, June 2012. DOI:10.1111/ j.1937-5956.2011.01251.x

[50]Z. Liu, Q. Wang, and Y. Tang, "Design of a cosimulation platform with hardware-in-the-loop for cyber-attacks on cyber-physical power systems", *IEEE Access*, Vol. 8, pp. 95997 - 96005, May 2020. DOI:10.1109/ACCESS.2020.2995743