Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.2, Apr. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.2.355

정보보안문화와 경영진 리더십이 조직 구성원의 정보보안 행동에 미치는 영향

박 성 환,[1†] 김 범 수,[2] 박 재 영[3‡]
[1]한국거래소 (차장), [2,3]연세대학교 정보대학원 (교수, 박사후 연구원)

Impacts of Information Security Culture and Management Leadership Styles on Information Security Behaviors

Sunghwan Park,[1†] Beomsoo Kim,[2] Jaeyoung Park[3‡]
[1]Korea Exchange(Deputy General Manager),
[2,3]Graduate School of Information, Yonsei University (Professor, Postdoctoral Researcher)

요 약

본 연구는 개인적 요인에 초점을 맞춘 기존 연구를 확장하여, 조직의 환경적 요인(정보보안문화, 경영진 리더십)이 조직 구성원의 정보보안 행동(정보보안정책 준수 의도, 정보보안 참여 의도)에 미치는 영향을 살펴본다. 본 연구는 금융기관 구성원 236명으로부터 데이터를 수집하였으며, 본 연구에서 개발한 모형을 구조방정식모형으로 분석하였다. 분석 결과, 정보보안문화는 정보보안정책 준수 의도와 정보보안 참여 의도에 모두 긍정적인 영향을 주었다. 거래적 리더십은 정보보안정책 준수 의도와 정보보안 참여 의도에 모두 긍정적인 영향을 주었지만, 변혁적 리더십은 정보보안 참여 의도에만 긍정적인 영향을 주었다.

ABSTRACT

This research investigates the impacts of information security (IS) culture and management leadership styles on employee's security behaviors (IS policies compliance, IS participation) in financial institutions. This study use the survey data collected from 236 employees of financial institutions. This research shows that IS culture has a positive effect on both behavioral intentions to comply with IS policies and the intentions to actively participate in information security activities. Transactional leadership has a positive impact on the IS policies compliance intentions and to participate in information security activities. In contrast, transformational leadership has a positive impact on the intentions to participate in information security activities, but not on the IS policies compliance intentions.

Keywords: Information Security Culture, Transactional Leadership, Transformational Leadership, Information Security Policy

I. 서 론

Ernst & Young이 실시한 설문 조사에 따르면, 전 세계 기업의 93%가 사이버 공격의 위협에 대응하기 위해 사이버 보안에 대한 투자를 유지하거나 늘리고 있다[1]. 국내 기업 역시, IT 예산 중 정보보호 예산이 차지하는 비중이 매년 증가하고 있다[2]. 하지만, 기업들의 노력에도 불구하고, 전세계적으로 2018년 상반기에만 개인정보 유출 사고가 945건 발생했으며, 유출된 개인정보는 약 45억 건을 기록하였다[3].

정보보안 사고의 주요 원인으로 산업계 전문가들

Received(02. 09. 2022), Modified(03. 22. 2022), Accepted(03. 22. 2022)
† 주저자, suloji1014@naver.com
‡ 교신저자, inyourface33@gmail.com(Corresponding author)

과 정보보안 연구자들은 조직 구성원을 지목한다[4,5]. 즉, 조직의 정보보안관리 측면에서 직원이 가장 취약한 지점이다[6]. 직원들은 정보보안을 생산성을 저해하고 불편한 것으로 인식하고, 이러한 인식은 정보보안정책 위반 요인 중 하나로 작용한다[7]. 기존 연구는 억제이론[8,9], 보호동기이론[10], 합리적 선택 이론[7]에 기반하여 조직 구성원의 태도를 변화시키는 것에 초점을 맞추었다[11]. 하지만, 조직 구성원의 정보보안 행동은 개별적 태도 변화뿐 아니라, 조직이 보유한 특성에 의해서도 영향을 받게 된다[12].

이에 본 연구는 조직 구성원의 정보보안 행동을 촉진하는 주요 동인으로써 조직의 환경적 요인에 주목한다. 그 이유는 조직은 개개인으로 구성된 하나의 집합이며, 하나의 사회성을 보여주는 집단이기 때문이다[13]. 정보보안에 있어 조직과 조직 구성원은 상호 교환관계가 성립되는데[14], 조직은 조직의 요구 수준에 맞는 정보보안 행동을 조직 구성원이 수행하길 기대하고, 조직 구성원은 제한된 정보를 기반으로 정보보안과 관련된 의사결정을 하게 된다[15]. 그리고 이것은 궁극적으로 조직의 전반적인 정보보안 수준을 결정한다[13]. 따라서, 조직의 정보보안 수준 향상을 위한 조직 구성원의 정보보안 행동을 설명하는데 있어서 조직의 환경적 요인을 고려할 필요가 있다.

본 연구는 정보보안 행동을 역할 내 행동인 정보보안정책 준수와 역할 외 행동인 정보보안 참여로 구분한다. 전자는 다수 연구에서 다루어졌으나[7,8,9,10], 후자를 살펴본 연구는 그 중요성에도 불구하고 아직 부족한 실정이다. 정보보안 참여는 조직의 정보보안을 적극적으로 촉진하는 능동적인 행동(예를 들어, 정보보안과 관련하여 다른 사람을 도와주는 행동, 정보보안 수준 향상을 위한 아이디어 제시)으로 조직의 정보보안 수준을 강화하는데 있어서 중요한 요소로 고려된다[16]. 따라서, 조직의 정보보안을 연구하는데 있어서 정보보안정책 준수와 더불어 정보보안 참여 행동을 살펴보는 것이 필요하다.

본 연구는 조직 구성원의 정보보안 행동에 영향을 주는 환경적 요인으로, 정보보안문화와 경영진 리더십을 고려한다. 먼저, 정보보안문화는 다양하게 정의되는데, 황인호 등[11]은 정보보안문화를 "조직원의 활동과 의식에 조직이 요구하는 보안 수준이 내재하여 올바르게 이루어지는 정도"라고 하였다. 다수의 연구에서 조직 관점에서 정보보안 문화를 형성하는 것이 중요한 것으로 밝혀졌다[11,19]. 정보보안 문화는 하나의 차원이 아닌 다수의 차원으로 구성되는 복합적인 개념이다. 본 연구는 Schein[18]이 제시한 조직문화 개념과 Van Niekerk and Solms[19]의 정보보안문화 프레임워크를 토대로 정보보안문화의 구성요인(정보보안 정책, 교육 및 훈련, 경영진 지원, 정보보안 지식)을 도출한다. 그리고 4가지 하위 차원으로 구성된 정보보안문화가 조직 구성원의 정보보안 행동에 미치는 영향을 살펴본다. 다음으로, 리더는 직원들이 조직의 정보보안 정책을 인지하고 이를 준수하도록 장려하는 중요한 역할을 가지고 있다[20]. 이에 본 연구는 Bass and Avolio[21]가 제시한 Full-range 리더십에서 거래적 리더십과 변혁적 리더십을 가져와 이러한 리더십이 조직 구성원의 정보보안 행동에 각각 어떠한 영향을 주는지 살펴본다.

정리하면, 본 연구는 조직문화와 리더십 이론을 바탕으로 조직의 환경적 요인이 조직 구성원의 정보보안 행동에 미치는 영향을 살펴봄으로써, 특히, 이전 연구에서 거의 다루지 않던 정보보안 참여 행동을 고려함으로써, 정보보안정책 문헌에 학술적으로 공헌한다. 또한, 본 연구결과는 정보보안 문화와 리더십의 중요성을 강조함으로써, 실무자에게 조직의 정보보안 수준 강화를 위한 시사점을 제시한다.

II. 이론적 배경

2.1 정보보안문화

정보보안문화는 다양하게 정의된다. 우선 해외 문헌을 살펴보면, Mcllwraith[17]은 정보보안문화를 "정보보안 표준 및 정책 준수의 가치에 대한 개별 직원의 신념"으로 정의한다. Karlsson et al.[22]은 정보보안문화에는 "정보보안에 영향을 미치면서 조직 구성원들 간에 거래되는 가치, 정신 모델 및 활동의 공유 패턴으로 구성됨"에 대한 공통된 이해가 있다고 말한다. Alhogail and Mirza[23]는 정보보안문화를 "직원의 행동에 영향을 미치기 위해 조직의 정보자산과 인간의 상호 작용을 안내하는 인식, 태도, 가치, 가정 및 지식의 수집"이라고 하였다. 국내에서도 정보보안문화의 중요성을 인식하고 관련 개념을 수립하기 시작했다. 김혜정과 안중호[24]는 정보보안문화를 "조직 환경의 객관적 특성(규정, 정책, 절차 등)을 구성원들에게 인식될 수 있도록 하는 조직의

정보보안 상황"으로 보았다. 황인호 등[11]은 정보보안문화를 "조직원의 활동과 의식에 조직이 요구하는 보안 수준이 내재하여 올바르게 이루어지는 정도"로 정의하고, 정보보안문화의 선행요인으로 경영층 지원, 보안 규정, 보안 가시성, 교육 및 훈련을 제시했으며, 정보보안 문화가 정보보안 정책 준수 의도에 긍정적으로 영향을 준다는 사실을 밝혔다. 하지만, 정보보안 문화와 정보보안 참여 행동 간의 관계를 살펴보지 않았다.

한편, Schlienger and Teufel[25]은 정보보안문화를 다양한 측면에서 묘사된 조직문화의 일부라고 했다. 즉, 정보보안문화는 조직에서 일이 이루어지는 방식과 관련이 있다[26]. 기존 연구에서 제시한 정보보안문화는 Schein[18]의 조직문화 개념을 토대로 개발되었다. 즉, 조직문화는 인공물(artifacts), 지지된 가치(expoused Value) 및 공유된 암묵적 가정(basic assumptions & belief)으로 구성된다. Van Niekerk and Solms[19]는 Schein[18]이 제시한 조직문화 세 가지 구성요소에 정보보안 지식을 추가하여, 정보보안문화를 개념화했다.

본 연구는 정보보안문화 프레임워크[19]와 이전 연구를 참고하여 정보보안문화를 개념화한다. 선행연구를 살펴보면, 경영진 관심 및 지원, 정보보안 정책, 보안 프로그램 관리, 교육 및 훈련, 정보자산 관리, 변화 관리 등이 정보보안문화의 구성요인으로 제시되었다[27,28]. 또한, 본 연구는 10년 이상의 정보보안 실무 경력을 가진 전문가 4명을 대상으로 인터뷰를 실시했다. 그들은 바람직한 정보보안문화를 수립하기 위해서 경영진 지원 및 노력, 정보보안 중요성 강조, 지속적인 교육 및 실제적인 가상훈련, 보안 규정 마련, 최소한의 정보보안 지식 등이 필요하다고 제언했다.

본 연구는 위와 같은 선행연구와 전문가 의견을 근거로 정보보안문화를 조직원의 활동과 의식에 조직이 요구하는 보안 수준이 내재하여 올바르게 이루어지는 정도로 정의하고[11], 그 구성요소를 경영진 지원, 정보보안 정책, 교육 및 훈련 그리고 정보보안 지식으로 도출했다.

2.2 리더십

본 연구는 Bass and Avolio[21]가 제시한 Full-range 리더십에서 거래적 리더십과 변혁적 리더십을 가져온다. 거래적 리더십(transactional leadership)은 구성원이 달성한 성과에 대하여 리더가 보상을 실시한다는 개인 간 이해관계에 기초한 리더와 구성원간의 상호 교환관계를 말한다. 반면에, 변혁적 리더십(transformational leadership)은 리더가 구성원에게 보다 높은 비전과 도덕적 가치 및 신념에 호소하여 구성원들에게 동기를 부여하는 것을 의미한다[29].

변혁적 리더십은 사람들로 하여금 개인으로서 일하기보다는 협력하는 것을 장려한다[29]. 변혁적 리더들은 카리스마가 넘치고 사람들이 조직의 이익에 자신의 이익을 두도록 동기를 부여함으로써 가치와 기준에 적응하도록 권장한다[30]. Bass[31]는 변혁적 리더십에는 이상화된 영향력(idealized influence), 지적 자극(intellectual stimulation) 및 개별적 배려(individual consideration)와 같은 3가지 구성 요소가 있다고 제안했고, 이 후 Bass and Avolio[21]는 수정된 이론에서 영감적 동기(inspirational motivation)를 변혁적 리더십 구성 요소에 추가했다.

이상화된 영향력은 경영진들이 직원들에게 모범을 보여주고 구성원들이 그들과 동일시하도록 동기를 부여한다[32,33]. 영감을 주는 리더는 직원들에게 열정과 긍정적 마음 그리고 에너지를 부여한다[34,35,36]. 또한, 지적 자극을 주는 리더는 직원이 기존 방법에 도전하고 표준을 개선하기 위한 혁신적인 전략을 개발하도록 권장한다[33,37,38]. 그리고 경영자들은 개별화된 배려를 통해 지지하는 분위기를 조성하고 직원들이 자신의 능력과 잠재력을 키울 수 있도록 한다[36,39]. 이 네 가지 특징은 변혁적 리더가 조직 구성원의 현재 요구를 충족시킬 뿐만 아니라 그들의 성격 개발을 촉진함으로써 자신과 자신이 속한 집단에 대한 더 높은 요구를 고려하도록 해줄 수 있다[38].

Bass[31]는 변혁적 리더십이 어떠한 상황이나 문화적 차이에 상관없이 효과적으로 인정된다고 주장하였다. 또한, 변혁적 리더십이 더 강한 효과를 보일 수 있는 상황도 제시하였는데, 사회적으로 변화가 일어나는 시기, 위기 상황, 정형화된 조직보다는 유기적인 조직에서 보다 효과적일 수 있다고 하였다[31]. 따라서 명확한 규범이나 제도를 가지고 있는 구조화된 환경에서는 변혁적 리더십의 효과가 제약될 수 있다. 그럼에도 불구하고, 변혁적 리더십을 가지고 있는 리더는 그러한 상황을 변화시킴으로써 효과

를 발휘할 수 있다.

반면, 거래적 리더십은 조직 구성원이 자신의 이익을 실현하도록 동기를 부여하는 것을 목표로 한다[40]. 경영진은 이전에 정의된 성과 목표를 달성하는 대가로 보상과 처벌을 제공한다[30,35]. 경영진과 조직 구성원 사이의 관계는 더 높은 성과를 달성하기 위해 상호 보강이라는 내재적 계약에 기반을 두고 있다[30,41]. Burns[29]는 한 사람이 가치 있는 어떤 것을 교환할 목적으로 다른 사람과 계약을 하면서 주도권을 행사할 때 거래적 리더십이 발생한다고 하였다. 즉 리더가 자신이 가지고 있는 가치 있는 것을 조직 구성원이 가지고 있는 가치 있는 것과 교환하여 거래의 이익을 취하고자 하는 리더십이라는 것이다[42].

거래적 리더십은 주로 조건적인 보상(contingent reward)과 적극적 예외 관리(management by exception-active)의 2차원적 행동으로 구성된다[33,36,37]. 조건적인 보상은 정의된 성과 기준에 부합하는 대가로 조직원이 보상받는 정도 (예를 들어, 임금)를 포함하고[33,38], 적극적 예외 관리를 하는 경영진은 실수에 대한 직원들의 행동을 감독하여 위반 사항을 규명하고 오류 및 문제가 심각해지기 전에 이를 수정하려고 한다[40].

2.3 정보보안 행동

직원의 정보보안 행동은 2가지 행동, 즉 역할 내 행동(in-role behaviour)과 역할 외 행동(extra-role behaviour)으로 구분할 수 있다[16]. 하지만, 기존 연구는 정보보안 행동으로 대부분 역할 내 행동이라고 할 수 있는 정보보안 정책 준수(또는 정보보안 정책 위반)만을 다루었다[7,8,9,10]. 역할 내 행동은 일상적이고 지속적인 직무수행 평가에 기초를 두고 보상과 처벌이 연계되는 조직 활동이다[43]. 정보보안 맥락에서는 역할 내 행동을 정보보안 정책 준수 행동이라고 할 수 있으며, 조직의 정보 자산을 보호하기 위해 관리자는 적절한 정보보안 정책을 수립하고 구성원이 해당 정보보안 정책을 따르도록 동기를 부여하는 데 주의를 기울여야한다[7,44,45,46].

역할 외 행동은 조직 성과를 높여줄 수 있는 행동으로 누군가의 강제에 의한 행동이 아닌 조직 구성원 자신이 자발적으로 조직의 발전에 도움이 되는 행동을 하는 것을 말한다[47]. 정보보안 맥락에서 역할 외 행동은 조직의 정보보안을 적극적으로 촉진하는 능동적인 행동으로 본 연구에서는 이를 정보보안 참여 행동이라고 한다[16]. 정보보안 참여 행동의 대표적인 예로 동료를 돕는 것이 있다. 다른 직원(특히 신입 직원)에게 정보보안 정책과 관련된 지침을 알려주거나, 다른 직원의 부적절한 행동을 식별하고 정보보안 정책을 인지할 수 있도록 도움을 제공 할 수 있다. 정보보안 참여 행동의 또 다른 예로 현재 상태를 개선하기 위한 의견 제시가 있다. 역할 외 행동은 조직의 공식적인 보상 시스템에 의해 직접적으로 인식되지는 않지만 조직의 효율성과 운영 효율성을 향상시킬 수 있다[43]. 마찬가지로, 정보보안 수준 향상을 위해서는 조직 구성원의 정보보안 관련 역할 외 행동(즉, 정보보안 참여 행동)이 중요하다[16]. 따라서 본 연구는 기존 연구를 확장하여, 조직 구성원의 정보보안 행동으로 정보보안 정책 준수 행동과 정보보안 참여 행동을 모두 고려한다.

III. 연구 가설

3.1 정보보안문화와 정보보안 행동

정보보안문화는 정보기술 보안에 대한 개인, 그룹 및 전체 조직의 태도와 행동에 영향을 미치는 일련의 원칙이다[48]. 정보보안문화는 조직 구성원의 정보보안 행동에 영향을 줄 수 있다. 먼저, 정보보안문화가 잘 구축된 조직에서는 구성원들이 정보보안 규정을 잘 준수할 것이라고 예상할 수 있다. D'Arcy and Greene[49]는 정보보안문화 수준이 높을수록 조직 구성원의 정보보안 정책 준수 의도가 높다고 하였다. 즉 조직 차원의 압력이 조직 구성원의 정보보안 정책 준수 의도를 높이는 요인이다[9].

또한, 정보보안문화가 잘 구축된 조직에서는 조직 구성원들이 정보보안 규정에 있지 않지만 조직의 정보보안 수준을 높일 수 있는 정보보안 행동을 스스로 할 것이라고 예상할 수 있다. 조직행동 문헌에 따르면, 조직문화가 (역할 외 행동 중 하나로 볼 수 있는) 직원의 혁신행동에 긍정적인 영향을 준다[50]. 또한, 회사와 같은 공동작업 환경에서 (정보보안문화 구성요인 중 하나인) 정보보안 지식은 조직 구성원의 능동적 보안 활동과 긍정적인 관련이 있다[51,52]. 즉 정보보안을 강조하는 조직에서는 조직 구성원이 누가 시키지 않아도 혹은 규정에 있지 않더라도 조직의 정보보안 수준을 향상시키는 행동을 스스로 할 것

이다[53]. 따라서, 다음과 같은 가설을 설정한다.

H1a: 조직의 정보보안문화는 조직 구성원의 정보보안 정책 준수 의도에 긍정적으로 영향을 미칠 것이다.

H1b: 조직의 정보보안문화는 조직 구성원의 정보보안 참여 의도에 긍정적으로 영향을 미칠 것이다.

3.2 리더십과 정보보안 행동

리더십은 앞서 말한바와 같이, 거래적 리더십과 변혁적 리더십이 있으며, 이것은 직원의 행동에 영향을 준다. 먼저, 거래적 리더십을 살펴보면, 거래적 리더십은 조직 구성원의 정보보안 정책 준수 행동에 긍정적인 영향을 줄 수 있다. 거래적 리더십을 가진 리더는 직원의 행동에 대해 보상과 처벌을 명확히 한다. 정보보안 정책 준수에 대한 공식적인 조치(즉, 보상 및 처벌)는 직원의 정보보안 정책 준수 의도를 높인다[54]. Humaidi and Balakrishnan[20]은 직원들에게 순응적 행동을 유도하는 데 있어서 거래적 리더십이 효과적이라고 하였다. 본 연구는 정보보안에 대한 감시와 규제가 엄격한 국내 금융기관 직원을 대상으로 한다. 구성원들의 정보보안 규정 준수를 모니터링하고 그 결과를 근무 평가에 반영하는 금융기관의 환경을 고려하면, 거래적 리더십이 직원의 정보보안 정책 준수 의도를 높일 것이라고 예상할 수 있다. 또한, 거래적 리더십은 조직 구성원의 정보보안 참여 의도 역시 높일 수 있다. 조직행동 연구를 보면, 거래적 리더십과 직원의 역할 외 행동(즉, 조직시민행동) 간에 긍정적인 연관성이 있는 것으로 나타났다[55]. 즉, 직원에 대한 관리자의 긍정적인 피드백은 직원들이 스스로 조직에 이익이 되는 행동을 하게 만들 수 있다. 따라서, 아래와 같이 가설을 설정한다.

H2a : 거래적 리더십은 조직 구성원의 정보보안 정책 준수 의도에 긍정적으로 영향을 미칠 것이다.

H2b : 거래적 리더십은 조직 구성원의 정보보안 참여 의도에 긍정적으로 영향을 미칠 것이다.

다음으로 변혁적 리더십을 살펴보면, 변혁적 리더는 직원들에게 정보보안 정책 준수 행동의 가치와 중요성을 전달하므로 직원들이 조직의 이익을 위해 보안 조치의 불편함을 감수하도록 자극하고, 이것은 직원들의 정보보안 준수 의도에 긍정적인 영향을 줄 수 있다. Guhr et al.[56]은 변혁적 리더십이 조직 구성원의 정보보안 정책 준수 의도를 높일 수 있음을 보였다. 또한, 변혁적 리더십은 조직 구성원이 조직의 정보보안 수준을 높이는 행동을 하게 만들 수 있다. 변혁적 리더는 공식적인 직무 사항을 넘어 목표를 달성하고[55], 최소 직무 요구 사항을 초과하도록 목표 수준에 따라 직원에게 동기 부여를 할 수 있기 때문이다[31]. 최근 연구는 변혁적 리더십이 조직 구성원의 정보보안 관련 역할 외 행동을 증가시킬 수 있음을 보였다[56]. 따라서, 아래와 같이 가설을 설정한다.

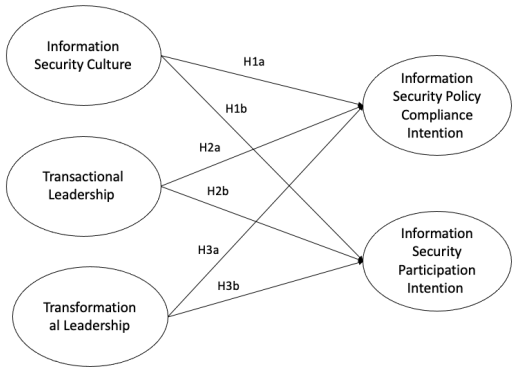

Fig. 1. Research model

H3a : 변혁적 리더십은 조직 구성원의 정보보안 정책 준수 의도에 긍정적으로 영향을 미칠 것이다.

H3b : 변혁적 리더십은 조직 구성원의 정보보안 참여 의도에 긍정적으로 영향을 미칠 것이다.

조직문화와 리더십 이론 그리고 이전 연구를 바탕으로, 본 연구는 Fig.1.과 같이 조직의 환경적 요인과 조직 구성원의 정보보안 행동 간 관계를 설명하는 연구모형을 제시한다.

IV. 연구방법

4.1 데이터 수집 및 표본 특성

본 연구는 금융업종에 종사하는 직장인을 연구 대상으로 선정했다. 금전과 신용 거래를 주된 업무로

하는 금융업은 정보보안 사고에 가장 민감하고, 사고 발생 시 피해 규모가 큰 분야 중 하나이다. 이러한 이유로 금융업에 속하는 조직은 정보보안을 매우 중요하게 생각한다. 따라서, 금융 분야는 정보보안에 관한 연구를 수행하기에 적합한 분야라고 할 수 있다.

데이터 수집을 위해 국내 리서치 전문 기업을 통해 온라인 설문조사를 실시하였다. 연구목적에 맞게 정보보안 정책이 내부적으로 존재하지 않는 기업의 직원은 설문조사 대상에서 제외되었다. 총 250명이 설문조사에 참여하였으며, 이 중에서 결측값 존재 또는 불성실 응답자 14명을 제외한 236명의 데이터를 분석에 사용하였다. 유효한 설문 응답자의 인구통계학적 특성은 Table 1과 같다. 응답자 중 남성이 107명(45.3%), 여성이 129명(54.7%)이다. 연령의 경우에는 20대가 47명(19.9%), 30대가 99명(41.9%), 40대가 56명(24.6%), 50대, 60대가 각각 28명(11.9%), 4명(1.7%)이다. 직급을 보면 사원이 99명(40.3%), 대리가 57명(24.2%), 과장이 37명(15.7%), 차장/부장이 40명(16.9%), 기타 7명(3%)이다.

Table 1. Demographic characteristics

		Frequency	Percentage (%)
Gender	Male	107	45.3
	Female	129	54.7
Age	20s	47	19.9
	30s	99	41.9
	40s	56	24.6
	50s	28	11.9
	60s	4	1.7
Position	Staff	99	40.3
	Assistant manager	57	24.2
	Manager	37	15.7
	General manager	40	16.9
	etc	7	3.0
Total		236	100

4.2 측정항목

본 연구의 측정항목은 총 37개로 3개의 독립변수와 2개의 종속변수로 구성되어 있다(부록 참고). 독립변수로 조직 환경 요인 중 하나인 정보보안문화는 다차원 2차적 구성(second-order construct)으로 4개의 하위 차원, 즉 경영진 지원, 정보보안 정책, 교육 및 훈련, 정보보안 지식을 포함하고 있다. 또 다른 조직 환경인 경영진의 리더십은 거래적 리더십과 변혁적 리더십으로 구성되어 있다. 그리고 종속변수는 조직 구성원의 정보보안 행동 의도를 파악하기 위한 정보보안 정책 준수 의도와 정보보안 참여 의도가 있다. 모든 항목은 리커트(Likert) 7점 척도로 측정되었다.

V. 분석 및 결과

5.1 측정모형 검정

본 연구에서 제시한 가설을 검정하기에 앞서, SPSS 25.0과 SmartPLS 3.2.8을 이용하여 측정문항에 대한 신뢰성 및 타당성 검정을 실시하였다. Table 2에서 보는 바와 같이, 측정문항의 cronbach's α 와 개념 신뢰도(composite reliability) 값이 모두 0.7이상으로 나왔으므로 측정문항은 신뢰성이 있다고 볼 수 있다[57]. 또한, 요인 적재량(factor loading) 값이 모두 0.7 이상이고 AVE 값이 모두 0.5 이상으로 나왔으므로 모든 측정문항에 대한 수

Table 2. Reliability and Validity of Variables

Variable	Factor Loding	t-value	Cronbach's α	Composite Reliability	AVE
Top Management Support	0.892	53.115	0.933	0.952	0.833
	0.933	93.803			
	0.916	59.295			
	0.909	61.411			
Information Security Policy	0.884	52.832	0.915	0.940	0.798
	0.906	64.757			
	0.888	51.824			
	0.895	48.469			

Variable	Factor Loding	t-value	Cronbach's α	Composite Reliability	AVE
Security Education & Training	0.915	84.801	0.938	0.956	0.843
	0.932	83.253			
	0.917	67.303			
	0.908	57.111			
Information Security Knowledge	0.896	56.327	0.912	0.938	0.791
	0.866	37.353			
	0.910	75.654			
	0.885	50.547			
Transactional Leadership	0.897	61.417	0.920	0.940	0.758
	0.881	45.364			
	0.821	26.485			
	0.865	38.565			
	0.887	49.474			
Transformational Leadership	0.821	35.707	0.938	0.949	0.726
	0.883	53.370			
	0.868	42.111			
	0.892	58.168			
	0.849	36.114			
	0.831	28.214			
	0.816	28.333			
Information Security Policy Compliance	0.942	104.642	0.965	0.975	0.906
	0.952	123.800			
	0.960	168.958			
	0.953	127.754			
Information Security Participation	0.887	48.741	0.941	0.955	0.809
	0.923	78.375			
	0.911	64.563			
	0.883	41.930			
	0.891	55.745			

Table 3. Discriminant Validity of Latent Variables

Variable	M(SD)	1	2	3	4	5	6	7	8
1.Information Security Policy	5.06(0.99)	**.890**							
2.Information Security Knowledge	5.45(1.05)	.446	**.893**						
3.Information Security Policy Compliance	5.64(1.03)	.455	.516	**.952**					
4.Security Education & Training	5.18(1.12)	.427	.556	.505	**.918**				
5.Information Security Participation	5.25(1.05)	.497	.386	.540	.380	**.899**			
6.Transactional Leadership	4.99(1.05)	.481	.364	.526	.452	.503	**.870**		
7.Transformational Leadership	4.88(1.14)	.460	.426	.436	.530	.533	.586	**.852**	
8.Top Management Support	4.94(1.09)	.427	.427	.477	.509	.417	.391	.476	**.913**

Note: Diagonal elements (bold) are the square root of average variance extracted (AVE) between the constructs and their measures.

렴타당성을 확보하였다[57]. 마지막으로, 각 변수의 AVE 값의 제곱근이 다른 변수들의 관계에서 가장 높은 상관계수 값보다 커야하고 수치가 모두 0.7 이상이어야 판별 타당성이 있다[57]. Table 3에서 보는 바와 같이, 상관계수 중 어떠한 수치도 AVE의 제곱근 값보다 높지 않고 AVE 값의 제곱근이 모두 0.852 이상이다. 따라서, 본 연구에서 사용된 변수들은 판별 타당성을 만족한다.

5.2 가설 검정

SmartPLS 3.2.8을 이용한 구조방정식모형 분석 결과는 Fig.2와 같다. 먼저, 정보보안문화와 정보보안 행동을 살펴보면, 가설 1a '조직의 정보보안문화는 조직 구성원의 정보보안 정책 준수 의도에 긍정적으로 영향을 미칠 것이다.'는 유의수준 0.1% 수준에서 채택되었다. 가설 1b '조직의 정보보안문화는 조직 구성원의 정보보안 참여 의도에 긍정적으로 영향을 미칠 것이다.' 역시 유의수준 0.1% 수준에서 채택되었다. 이와 같은 결과는 조직 구성원의 정보보안 행동에 있어서 정보보안문화가 중요한 역할을 한다는 것을 말해준다.

다음으로, 리더십과 정보보안 행동을 살펴보면, 가설 2a '거래적 리더십은 조직 구성원의 정보보안 정책 준수 의도에 긍정적으로 영향을 미칠 것이다.'는 유의수준 0.1% 수준에서 채택되었다. 가설 2b '거래적 리더십은 조직 구성원의 정보보안 참여 의도에 긍정적으로 영향을 미칠 것이다.' 역시 유의수준 1% 수준에서 채택되었다.

가설3a '변혁적 리더십은 조직 구성원의 정보보안 정책 준수 의도에 긍정적으로 영향을 미칠 것이다.'는 기각되었으며, 가설3b '변혁적 리더십은 조직 구성원의 정보보안 참여 의도에 긍정적으로 영향을 미칠 것이다.'는 유의수준 1% 수준에서 채택되었다.

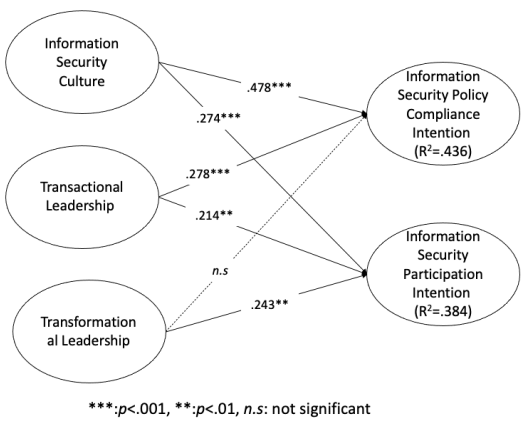

Fig. 2. Results of PLS Structural Model Analysis

VI. 결 론

6.1 연구결과 논의

본 연구는 조직문화 문헌과 리더십 이론에 기반하여 금융업종 종사자를 대상으로 조직의 환경적 요인(정보보안문화, 리더십)이 조직 구성원의 정보보안 행동(정보보안정책 준수, 정보보안 참여)에 어떻게 영향을 미치는지를 살펴보았다.

연구 결과를 살펴보면, 첫째, 4가지 하위 차원(경영진 지원, 정보보안 정책, 교육 및 훈련, 정보보안 지식)으로 구성된 정보보안문화는 조직 구성원의 정보정책 준수 의도와 정보보안 참여 의도에 모두 긍정적인 영향을 주었다. 이것은 정보보안문화와 보안 준수 및 직원의 행동 역할 사이에는 강한 상관관계가 있다는 이전 연구결과와 일치한다[58]. 그리고 정보보안문화와 정보보안 정책 준수 의도를 연구한 최근의 연구[11,28]와도 동일한 결과를 보여준다. 즉, 정보보안문화의 수준이 높을수록 조직 구성원의 수동적 및 능동적 보안 행동 의도가 증가한다는 것이다. 특히, 정보보안문화가 정보보안 참여 의도를 높여준다는 결과는 조직의 정보보안 전략 수립에 새로운 방향을 제시한다.

둘째, 거래적 리더십은 조직 구성원의 정보보안정책 준수 의도 및 정보보안 참여 의도에 모두 긍정적인 영향을 주었다. 이러한 결과는 이전 연구결과와 다르다는 점에서 주목할 만하다. 이전 연구에서는 거래적 리더십이 정보보안 정책 준수 의도와 정보보안 참여 의도에 영향이 있음을 검증하지 못했다[56]. 본 연구는 이전 연구와 다르게 정보보안에 가장 민감한 업종이라고 할 수 있는 금융업에 종사하는 직원을 대상으로 하였다. 금융기관 구성원들의 대부분이 규정 준수 여부를 모니터링 받고, 정기적으로 그 결과가 평가되고 있다. 따라서 이러한 금융업의 조직 환경에서는 조건적 보상이나 적극적인 예외 관리를 특징으로 하는 거래적 리더십이 조직의 정보보안 수준을 향상하는데 도움이 될 수 있다. 향후 연구에서 정보보안이 민감한 업종(예를 들어, 금융업)과 덜 민감한 업종(예를 들어, 제조업)에 종사하는 직원을 대상

으로 거래적 리더십의 영향력 차이를 살펴보는 것은 의미가 있을 것이다.

마지막으로, 거래적 리더십과 다르게, 변혁적 리더십은 조직 구성원의 정보보안 참여 의도에만 긍정적인 영향을 주었다. 이러한 연구 결과는 변혁적 리더십이 조직 구성원의 능동적 보안행동, 즉 정보보안 참여를 촉구하는데 도움이 되지만, 수동적 보안행동, 즉 정보보안 정책을 준수하게 만드는데 있어서 큰 역할을 하지 못한다는 것을 말한다.

6.2 한계점

본 연구의 한계점으로, 본 연구는 금융업을 대상으로 하였는데, 본 연구 결과가 다른 업종에서도 동일하게 나타난다고 보장할 수 없다. 특히, 리더십의 영향에 있어서 다른 결과가 나올 수 있는데, 예를 들어, 변혁적 리더십이 수동적 보안 행동에 긍정적인 영향을 줄 수 있다. 향후 연구에서 이를 살펴보는 것은 의미가 있을 것이다. 또한, 본 연구는 거래적 리더십과 변혁적 리더십을 다루었는데, 정보보안 맥락에 알맞은 또 다른 리더십(예를 들어, 윤리적 리더십)이 존재할 수 있다. 향후 연구에서 정보보안 맥락에서 윤리적 리더십이 어떤 역할을 하는지 살펴볼 필요가 있다. 마지막으로, 본 연구는 다른 설문조사 연구와 마찬가지로, 실제 행동이 아닌 의도를 측정하였다. 향후 연구에서는 실제 행동을 측정할 필요가 있다.

6.3 시사점

본 연구는 정보보안 정책 문헌에 학술적으로 공헌하며, 정보보안 정책 연구자에게 시사점을 제공한다. 첫째, 본 연구는 정보보안문화의 4가지 하위 차원을 도출하였으며, 정보보안문화가 조직 구성원의 정보보안 행동에 긍정적인 영향을 준다는 것을 밝혔다. 특히 이전 연구와 다르게, 정보보안문화가 정보보안 참여 행동을 증진시킬 수 있음을 보였다. 이처럼 조직의 정보보안 성과에 있어서 정보보안문화가 중요한 역할을 할 수 있음에도 불구하고, 정보보안문화 개념에 대한 포괄적인 합의가 아직 제대로 이루어지지 않았다. 본 연구는 정보보안문화의 개념을 확립하기 위한 향후 연구에 도움이 될 수 있다.

둘째, 본 연구는 정보보안 맥락에서 거의 다루어지지 않았던 리더십 개념을 고려하였다. 구체적으로, 거래적 리더십과 변혁적 리더십이 직원의 보안행동에 어떻게 영향을 주는지 살펴봄으로써, 기존 연구를 확장하였다. 특히, 거래적 리더십과 변혁적 리더십이 조직 구성원의 정보보안 행동에 차별적으로 영향을 준다는 결과는 향후 연구에 유용한 시사점을 제공한다.

마지막으로, 본 연구는 조직 구성원의 보안행동으로 역할 내 행동인 정보보안 정책 준수 의도와 역할 외 행동인 정보보안 참여 의도를 모두 고려함으로써, 정보보안정책 준수에만 초점을 맞춘 기존 연구를 확장하였다. 역할 외 행동은 조직의 공식적인 보상 시스템에 의해 직접적으로 인식되지는 않지만 조직의 효율성과 운영 효율성을 향상시킬 수 있다[43]. 마찬가지로, 조직의 정보보안 수준을 향상시키기 위해서는 조직 구성원의 정보보안 관련 역할 외 행동(즉, 정보보안 참여 행동)에 관심을 가져야 한다[16]. 향후 연구에서 이것의 선행요인을 살펴보는 연구가 진행된다면 의미가 있을 것이다.

본 연구결과는 또한 실무자에게도 유용한 시사점을 제공한다. 첫째, 본 연구는 정보보안문화의 구성요인으로 경영진 지원, 정보보안 정책, 교육 및 훈련, 정보보안 지식을 제안하였으며, 이것이 금융업종 구성원의 정보보안 행동을 촉진할 수 있다는 것을 밝혔다. 이를 통해 기업에게 바람직한 정보보안문화 수립 방안을 제시한다. 우선, 정보보안 향상을 위한 경영진의 지원이 조직의 정보보안 수준 향상을 위한 중요한 요소임을 강조한다. 경영진의 지원과 관심이 높아지면 정보보안 예산과 타 부서의 업무 협조가 수월해지고, 무엇보다 조직 구성원 전체의 정보보안에 대한 관심과 참여가 늘어날 수 있다. 이것은 조직 전체의 공유 가치인 정보보안문화 수립에 필수적이다. 따라서, 조직은 경영진의 정보보안에 대한 관심을 높일 수 있는 방안을 고민해야 한다. 예를 들어, 경영진 보고 시 전사적 보안의 중요성을 강조하고, 궁극적으로 비용 절감 효과로 이어질 수 있음을 설득해야 한다. 이를 위해 관련 뉴스레터 등 임원 전용 자료를 준비하는 것이 하나의 방법이 될 수 있다.

다음으로, 조직이 수립하는 정보보안 정책이나 규정은 조직 구성원들의 신뢰를 얻을 수 있어야 한다. 그러기 위해서는 조직의 현실에 맞게 잘 정의되고, 외부환경 변화에 따라 변경관리가 이루어져야 한다. 그리고 교육 및 훈련은 조직 구성원에게 정보보안 목적을 인식시키고, 정보보안 협력 분위기를 정립할 수 있다. 그러기 위해서는 구성원의 참여가 필수적이다. 이를 위해 불참에 대한 처벌 및 비난보다 참여에 대

한 인센티브 제공이 효과적일 수 있다. 끝으로, 직원의 정보보안 정책 위반은 관련 지식이 부족해서 발생하는 경우가 많다[4,5]. 따라서, 조직은 보안 절차 및 행동 방법 등을 조직 구성원에게 체계적으로 전달함으로써, 조직 구성원의 정보보안 지식을 높이는 것이 중요하다.

둘째, 본 연구는 리더십 유형과 정보보안 행동 간의 관계를 실증적으로 검증하였다. 조직의 정보보안 수준을 향상하는데 있어서 조직 구성원이 수립된 정보보안 정책을 얼마나 잘 준수하는지도 중요하지만, 능동적으로 정보보안 관련 행동을 하는 것 역시 중요하다. 본 연구결과는 적어도 금융기관에서는 거래적 리더십이 변혁적 리더십보다 더 효과적이라고 말한다. 따라서 금융기관 리더들은 조직 구성원들이 정보보안 정책을 잘 준수할 수 있도록 거래적 리더십을 적극적으로 발휘할 필요가 있다. 하지만, 변혁적 리더십 역시 조직 구성원의 정보보안 참여를 증가시킬 수 있는 만큼 금융기관에 소속된 리더는 두 가지 유형의 리더십을 모두 보유하는 것이 중요하다.

마지막으로, 본 연구는 조직 구성원의 보안 행동을 결정하는데 있어서 조직적 환경(정보보안 문화, 리더십)이 중요한 역할을 한다는 것을 밝혀냈다. 하지만, 조직 내에 정보보안을 위한 문화를 조성하고, 리더가 적절한 리더십을 발휘하는 것은 특정 부서에서 단독으로 할 수 있는 것은 아니다. 본 연구는 기업이 자사의 정보보안 전략을 수립하고 실행을 추진할 때 전사적 관점으로 대응할 필요가 있음을 강조한다.

References

[1] van Kessel, P., & Allan, K. Under cyber attack. EY's Global Information Security Survey 2013. Ernst & Young, 2013.

[2] Korea Internet & Security Agency. Survey on Information Security-Business, 2020.

[3] https://www.businesswire.com/news/home/20181008005322/en/Data-Breaches-Compromised-4.5-Billion-Records-in-First-Half-of-2018, 2022.3.30.

[4] Kreicberge, L., "Internal threat to information security-countermeasures and human factor with SME," Ph.D. Thesis, Luleå University of Technology, Dec. 2020.

[5] Siponen, M. and Vance, A., "Neutralization: new insights into the problem of employee information systems security policy violations," MIS quarterly, vol. 34, no. 3, pp. 487-502, Sep. 2010.

[6] Padayachee, K., "Taxonomy of compliant information security behavior," Computers & Security, vol. 31, no. 5, pp. 673-680, July 2012.

[7] Bulgurcu, B. H., Cavusoglu, H. and Benbasat, I., "Information security policy compliance: An empirical study of rationality based beliefs and information security awareness," MIS Quarterly, vol. 34, no. 3, pp. 523-548. Sep. 2010.

[8] D'Arcy, J., Hovav, A. and Galletta, D. "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," Information Systems Research, vol. 20, no. 1, pp. 79-98, Mar. 2009.

[9] Herath, T. and Rao, H. R. "Protection motivation and deterrence: a framework for security policy compliance in organisations," European Journal of Information Systems, vol. 18, no. 2, pp. 106-125, April 2009.

[10] Ifinedo, P. "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," Computers & Security, vol. 31, no.1, pp. 83-95, Feb. 2012.

[11] Hwang, I., Kim, D., Kim, T. and Kim, J. "Effect of security culture on security compliance and knowledge of employees," Information Systems

Review, 18(1), pp. 1-23, Mar. 2016.
[12] Knapp, K. J., Marshall, T. E., Kelly Rainer, R. and Nelson Ford, F. "Information security: management's effect on culture and policy," Information Management & Computer Security, vol. 14, no.1, pp. 24-36, Jan. 2006.
[13] Ernest Chang, S., and Lin, C. S. "Exploring organizational culture for information security management," Industrial Management & Data Systems, vol. 107, no.3, pp. 438-458, April 2007.
[14] Molm, L. D. "Structure, action, and outcomes: The dynamics of power in social exchange," American Sociological Review, vol. 55, no. 3, pp. 427-447. June 1990.
[15] Hu, Q., Xu, Z., Dinev, T. and Ling, H. "Does deterrence work in reducing information security policy abuse by employees?," Communications of the ACM, vol. 54, no.6, pp. 54-60, June 2011.
[16] Hsu, J. S. C., Shih, S. P., Hung, Y. W. and Lowry, P. B. "The role of extra-role behaviors and social controls in information security policy effectiveness," Information Systems Research, vol. 26, no.2, pp. 282-300, June 2015.
[17] McIlwraith, A. Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education. Training and Awareness, 2nd Ed., Routledge, Aug. 2021.
[18] Schein, E. H. and Schein, P. A. The corporate culture survival guide, 3rd Ed., John Wiley & Sons, June 2019.
[19] Niekerk, J. A., and Solms, R. V. "Understanding information security culture: A conceptual framework," Proceedings of the ISSA 2006 from Insights to Foresight Conference, pp. 21-30, July 2006.
[20] Humaidi, N. and Balakrishnan, V. "Leadership styles and information security compliance behavior: The mediator effect of information security awareness," International Journal of Information and Education Technology, vol. 5, no.4, pp. 311-318, April 2015.
[21] Bass, B. M. and Avolio, B. J. Improving organizational effectiveness through transformational leadership, Sage, Nov. 1993.
[22] Karlsson, F., Åström, J. and Karlsson, M. "Information security culture- state-of-the-art review between 2000 and 2013," Information & Computer Security, vol. 23, no.3, pp. 246-285, July 2015.
[23] Alhogail, A. and Mirza, A. "Information security culture: a definition and a literature review," In 2014 World Congress on Computer Applications and Information Systems (WCCAIS), pp. 1-7, Jan. 2014.
[24] Kim, H. J. and Ahn, J. H. "An Empirical Study of Employee's Deviant Behavior for Improving Efficiency of Information Security Governance," Journal of Society for e-Business Studies, 18(1), Feb. 2013.
[25] Schlienger, T. and Teufel, S. "Information security culture-from analysis to change," South African Computer Journal, vol. 2003, no.31, pp. 46-52, Dec. 2003.
[26] Martins, A. and Elofe, J. Information security culture. Security in the information society, Springer, Boston, MA, May 2002.
[27] Alnatheer, M., Chan, T. and Nelson, K. "Understanding and measuring information security culture,"

Proceedings of the 16th Pacific Asia Conference on Information Systems (PACIS), 144. July 2012.

[28] Nasir, A., Abdullah Arshah, R. and Ab Hamid, M. R. "A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions," Information Security Journal: A Global Perspective, vol. 28, no.3, pp. 55-80, July 2019.

[29] Burns, J. M. Leadership. Open Road Media, April 2012.

[30] Jung, D. I. and Sosik, J. J. "Transformational leadership in work groups: The role of empowerment, cohesiveness, and collective-efficacy on perceived group performance," Small group research, vol. 33, no.3, pp. 313-336, June 2002.

[31] Bass, B. M. Leadership and performance beyond expectations, Free Press, May 1985.

[32] Bass, B. M., Avolio, B. J., Jung, D. I. and Bergson, Y. "Predicting unit performance by assessing transformational and transactional leadership," Journal of Applied Psychology, vol. 88, no.2, pp. 207-218, April 2003.

[33] Bono, J. E. and Judge, T. A. "Personality and transformational and transactional leadership: A meta analysis," Journal of Applied Psychology, vol. 89, no.5, pp. 901-910, Oct. 2004.

[34] Liu, J., Siu, O. L. and Shi, K. "Transformational leadership and employee well being: The mediating role of trust in the leader and self efficacy," Applied Psychology, vol. 59, no.3, pp. 454-479, July 2010.

[35] Rafferty, A. E. and Griffin, M. A. "Dimensions of transformational leadership: Conceptual and empirical extensions," The leadership quarterly, vol. 15, no.3, pp. 329-354, June 2004.

[36] Stewart, J. "Transformational leadership: An evolving concept examined through the works of Burns, Bass, Avolio, and Leithwood," Canadian Journal of Educational Administration and Policy, 54, pp. 1-29, June 2006.

[37] Avolio, B. J., Bass, B. M. and Jung, D. I. "Re examining the components of transformational and transactional leadership using the Multifactor Leadership," Journal of occupational and organizational psychology, vol. 72, no.4, pp. 441-462, Dec. 1999.

[38] Bass, B. M., Waldman, D. A., Avolio, B. J. and Bebb, M. "Transformational leadership and the falling dominoes effect," Group & Organization Studies, vol. 12. no.1, pp. 73-87, Mar. 1987.

[39] Geijsel, F., Sleegers, P., Leithwood, K. and Jantzi, D. "Transformational leadership effects on teachers' commitment and effort toward school reform," Journal of educational administration, vol. 41, no.3, pp. 228-256. June 2003.

[40] Sadeghi, A. and Pihie, Z. A. L. "Transformational leadership and its predictive effects on leadership effectiveness," International Journal of Business and Social Science, vol. 3, no.7, pp. 186-197, April 2012.

[41] Kim, Woo-Jin and Seo, Won-Seok. "The Effects of Transformational and Transactional Leadershipon Organizational Citizenship Behavior of Hotel Employees: Focused on the Moderating Role of Empowerment," Korean Journal of Hospitality & Tourism, 19(3), pp. 173-198. June

2010.
[42] Ko, S. S. and Lee, C. W. "A study on the effectiveness of leadership styles for each rank in Korea's national defense organization," korean Journal of association for policy sciences, 15(2), pp. 111-139, June 2011.
[43] Zhu, Y. "Individual behavior: In-role and extra-role," International Journal of Business Administration, vol. 4, no.1, pp. 23-27, Jan. 2013.
[44] Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A. and Boss, R. W. "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security," European Journal of Information Systems, vol. 18, no.2, pp. 151-164, April 2009.
[45] Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J. and Courtney, J. F. "Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors," MIS Quarterly, pp. 1189-1210, Dec. 2013.
[46] Wall, J. D., Palvia, P. and Lowry, P. B. "Control-related motivations and information security policy compliance: The role of autonomy and efficacy," Journal of Information Privacy and Security, vol. 9, no.4, pp. 52-79, 2013.
[47] Van Dyne, L. and LePine, J. A. "Helping and voice extra-role behaviors: Evidence of construct and predictive validity," Academy of Management Journal, vol. 41, no.1, pp. 108-119, Feb. 1998.
[48] Ngo, L., Zhou, W., Chonka, A. and Singh, J. "Assessing the level of IT security culture improvement: Results from three Australian SMEs," In 2009 35th Annual Conference of IEEE Industrial Electronics, pp. 3189-3195, Nov. 2009.
[49] D'Arcy, J. and Greene, G. "Security culture and the employment relationship as drivers of employees' security compliance," Information Management & Computer Security, vol. 22, no.5, pp. 474-489, Nov. 2014.
[50] Kwon, J. S. "The influence of innovative organization culture to human resource innovation and organizational commitment," Journal of Business Research, vol. 26, no.1, pp. 153-182, 2011.
[51] Jaeger, L. and Eckhardt, A. "When Colleagues Fail: Examining the Role of Information Security Awareness on Extra-Role Security Behaviors," Proceedings of the Twenty-Sixth European Conference on Information Systems (ECIS), 124, June 2018.
[52] Park, J. and Kim, B. "The Impact of Organizational Information Security Climate on Employees' Information Security Participation Behavior," The Journal of Information Systems, 29(4), pp. 57-76, Dec. 2020.
[53] Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A. and Spector, P. E. "Information security climate and the assessment of information security risk among healthcare employees," Health informatics journal, vol. 26, no.1, pp. 461-473, Mar. 2020.
[54] Lebek, B., Guhr, N. and Breitner, M. "Transformational Leadership and Employees' Information Security Performance: The Mediating Role of Motivation and Climate," Proceedings of the 35th International Conference on Information Systems (ICIS), Dec. 2014.

[55] Podsakoff, P. M., MacKenzie, S. B., Moorman, R. H. and Fetter, R. "Transformational leader behaviors and their effects on followers' trust in leader, satisfaction, and organizational citizenship behaviors," The leadership quarterly, vol. 1, no.2, pp. 107-142, 1990.

[56] Guhr, N., Lebek, B. and Breitner, M. H. "The impact of leadership on employees' intended information security behaviour: An examination of the full range leadership theory," Information Systems Journal, vol. 29, no.2, pp. 340-362, Mar. 2019.

[57] Fornell, C. and Larcker, D. F. "Evaluating structural equation models with unobservable variables and measurement error," Journal of marketing research, vol. 18, no.1, pp. 39-50, Feb. 1981.

[58] D'Arcy, J. and Greene, G. "The multifaceted nature of security culture and its influence on end user behavior," In Proceedings of IFIP TC8 International Workshop on Information Systems Security Research, pp. 145-157, 2009.

부록. 설문문항

Variables	Items	Reference
Top Management Support (경영진 지원)	1) 우리 회사 경영진은 정보보안 회의에 참석한다. 2) 우리 회사 경영진은 정보보안 의사결정에 참여한다. 3) 우리 회사 경영진은 정보보안 활동에 참여한다. 4) 우리 회사 경영진은 정보보안 시스템 활성화를 위한 기능적 지원을 제공한다.	Kankahalli et al. (2003)
Information Security Policy (정보보안 정책)	1) 우리 회사는 직원들이 사용이 허가되지 않은 정보시스템에 접근 하는 것을 금지하는 정책을 가지고 있다. 2) 우리 회사는 정보시스템 자원 사용을 위한 행동규칙을 정하고 있다. (예: 패스워드 복잡도 기준 등) 3) 우리 회사는 정보보안과 관련한 조직원들의 역할과 책임을 규정하고 있다. 4) 우리 회사는 개인의 업무환경에 대한 정보보안 정책을 가지고 있다. (예: 개인용 PC 보호설정, 중요문서 파기 등)	D'Arcy and Greene (2009); Hovav and D'Arcy (2012); Chen et al. (2015)
Security Education and Training (교육 및 훈련)	1) 우리 회사는 직원들에게 정보보안의 중요성과 위험성에 대해 교육을 제공하고 있다. 2) 우리 회사는 직원들에게 정보보안과 관련된 법과 보안정책에 대한 교육을 제공하고 있다. 3) 우리 회사는 직원들에게 정보보안 책임에 대해 교육을 하고 있다. 4) 우리 회사는 침해사고 대응절차 등 정보보안 관련 내부규정에 대한 교육 및 훈련을 실시하고 있다.	D'Arcy et al. (2009)
Information Security Knowledge (정보보안 지식)	1) 나는 우리 회사가 정보보안 프로그램 및 캠페인을 실행하는데 적절한 보안지식을 사용했다고 믿는다. 2) 우리 회사의 정보보안 통제는 정보자산을 확보하기 위한 적절한 가이드라인과 일치한다고 생각한다. 3) 회사의 정보보안 프로그램은 나의 정보보안 지식을 향상시키는데 도움이 된다. 4) 회사의 정보보안 프로그램은 나의 보안능력을 향상시키는데 도움이 된다.	Veiga (2008); Niekerk and Solms (2006)

Transformational Leadership (변혁적 리더십)	1) 우리 회사 경영진은 정보보안을 회사의 사업과 정보자산을 지원하는 기능이라고 설명한다. 2) 우리 회사 경영진은 정보보안에 대한 합리적인 수준의 지식과 이해를 가지고 있다. 3) 우리 회사 경영진은 회사의 정보보안을 집단적 노력이라고 생각한다. 4) 우리 회사 경영진은 효과적인 정보보안을 달성하고 유지하기 위한 수단으로 공통의 이해, 소통, 협력을 촉진한다. 5) 우리 회사 경영진은 문제를 해결할 때 직원으로 부터 상이한 관점/의견을 구한다. 6) 우리 회사 경영진은 직원들이 타인과는 다른 필요성, 능력 및 영감을 가지고 있다고 여긴다. 7) 우리 회사 경영진은 직원들이 자신의 강점을 개발하도록 돕는다.	Bass and Riggio (2006); Dvir et al. (2002); Li et al. (2012)
Transactional Leadership (거래적 리더십)	1) 우리 회사 경영진은 정보보안 정책을 준수하지 않는 사람들에 대해 해당하는 조치를 취한다. 2) 우리 회사 경영진은 목표달성을 위해 직원들에게 보상과 처벌을 적절하게 사용한다. 3) 우리 회사 경영진은 사전에 합의한 대로 노력하는 직원들에게 보상을 해준다. 4) 우리 회사 경영진은 회사에서 제시하는 정보보안 기준에 직원이 벗어나지 않는 데에 주로 관심을 둔다. 5) 우리 회사 경영진은 정보보안 위반사항을 점검하고 사항이 심각해지기 전에 수정조치를 취한다.	Bass and Riggio (2006); Li et al. (2012)
Information Security Policy Compliance Intention (정보보안정책 준수 의도)	1) 나는 조직의 정보보안 정책요건을 준수할 생각이다. 2) 나는 조직의 정보보안 정책요건에 따라 정보 및 기술자원을 보호하고자 한다. 3) 나는 정보와 정보기술을 활용할 때 조직의 정보보안 정책에 규정된 책임을 수용할 것이다. 4) 나는 조직의 정보보안 정책을 따를 것이다.	Neal and Griffin (2007); Clarke et al. (2006)
Information Security Participation Intention (정보보안 참여 의도)	1) 나는 회사의 정보보안을 위해 동료들을 도울 수 있다. 2) 나는 직장에서 정보보안을 향상시키기 위해 규정 준수 이외에 추가적인 노력을 기울일 수 있다. 3) 나는 정보보안을 개선하는 데 도움이 되는 활동을 자발적으로 실시할 수 있다 4) 나는 정보보안 효과에 대해 논의하는데 참여할 수 있다. 5) 나는 새로운 직원이 회사의 정보보안 정책을 따를 수 있도록 도울 수 있다.	Bulgurcu et al. (2010); Herath and Rao (2009); Warkentin et al. (2009)

〈저자소개〉

박 성 환 (Sunghwan Park) 정회원
2020년 2월: 연세대학교 정보대학원 정보시스템 석사
2001년 8월~현재: 한국거래소 차세대시스템구축TF
〈관심분야〉 정보보호, 프라이버시, 정보보안 정책

김 범 수 (Beomsoo Kim) 종신회원
1990년 2월: 서울대학교 경영학 학사
1992년 2월: 서울대학교 경영학 석사
1999년 2월: University of Texas at Austin 경영학 박사
1999년~2002년: University of Illinois at Chicago 조교수
2002년~현재: 연세대학교 정보대학원 교수
〈관심분야〉 ICT의 효과적 활용, 데이터 거버넌스, 프라이버시, 개인정보보호

박 재 영 (Jaeyoung Park) 정회원
2012년 8월: 숭실대학교 정보통신전자공학부
2017년 2월: 연세대학교 정보대학원 정보시스템 석사
2021년 8월: 연세대학교 정보대학원 정보시스템 박사
2021년 9월~현재: 연세대학교 정보대학원 박사후 연구원
〈관심분야〉 정보보호, 프라이버시, 정보보안 정책, 디지털 기술 영향