Journal of the Korea Industrial Information Systems Research Vol.26 No.2, Apr. 2021 :27-41
http://dx.doi.org/10.9723/jksiis.2021.26.2.027 ISSN:1229-3741

개인의 대처 유형과 조직문화가 조직원의 정보보안에 미치는 영향+

(The Influence of Individual's Coping Style and Organizational Culture on Information Security of Employee)

황 인 호[1)*]
(Inho Hwang)

요 약 연구 목적은 개인의 행동 유형과 조직문화 구조에 따라 조직원의 정보보안 행동에 미치는 영향 관계를 검증하는 것이다. 연구는 개인적 특성을 업무중심 대처와 정서중심 대처로, 조직문화를 집단주의와 개인주의로 구분하여 교차설계를 실시한다. 정보보안 요인은 정보보안 인식, 인지된 취약성, 대처 효능감, 그리고 준수 행동으로 제시하였다.

연구 결과, 대처와 조직문화는 모두 정보보안 인지 요인에 영향을 미치는 것을 확인하였다. 특히, 정서중심 대처가 업무중심 대처보다 인지 평균이 높은 것으로 나타났으며, 집단주의가 개인주의보다 인지 평균이 높은 것으로 나타났다. 또한, 정보보안 인식은 인지된 취약성, 대처 효능감을 매개로 하여 준수 행동에 영향을 주는 것으로 나타났다. 연구의 시사점은 개인 대처유형과 조직문화에 따라 정보보안 행동에 미치는 영향의 차이를 확인하였고, 준수 행동 향상을 위한 선행 요인을 제시하였다. 즉, 연구는 개인-조직 차원별 조직의 정보보안 전략 방향을 제시한다.

핵심주제어: 대처, 조직문화, 정보보안인식, 인지된 취약성, 대처 효능감, 정보보안 행동

Abstract The purpose of this study is to prove the relationship of the influence of individual behavior style and organizational culture structure on the information security cognitive factors of employees. The study conducts cross-design by dividing individual characteristics into task coping and emotion coping, and organizational culture into collectivism and individualism. Information security factors consisted of information security awareness, perceived vulnerability, response efficacy, and compliance behavior.

As a result of the study, it was confirmed that both personal coping style and organizational culture had an influence on the all cognitive factors of information security. In addition, information security awareness was found to influence compliance behavior through perceived vulnerability and response efficacy. The implications of the study were to confirm the difference in the impact on the compliance behavior according to the individual coping style and organizational culture, and to present the precedent factors for improving the compliance behavior. In other words, the research suggests the information security strategy direction for each individual-organizational dimension.

Keywords: Coping, Organizational Culture, Security Awareness, Perceived Vulnerability, Response Efficacy, Compliance Behavior

* Corresponding Author: hwanginho@kookmin.ac.kr
+ 이 논문은 2020년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2020S1A5A8040463)

Manuscript received December 04, 2020 / revised December 31, 2020 / accepted March 16, 2021
1) 국민대학교 교양대학, 제1저자, 교신저자

1. 서 론

정보가 조직의 중요 자산으로 인식되면서, 조직들의 정보보안에 대한 관심과 투자가 증가하고 있다. 실제 전 세계 정보보안은 솔루션 시장을 중심으로 연평균 10%이상으로 증가하고 있으며(Grand View Resarch, 2020), 많은 조직들은 정보 가치 확대를 위해 정보보안 관련 ISO 국제표준을 확보하는 등의 다각적인 노력을 하고 있다. 그럼에도 불구하고, 노출된 정보보안 사고는 지속적으로 증가하고 있는 상황이다(Verizon, 2020). 정보보안 사고를 유형별 살펴보면, 매년 해킹, 멀웨어, 바이러스 등과 같은 외부의 침입에 의한 보안 사고가 전체 사고의 60-70%를 차지하고 있으며, 내부자의 악의적 또는 비악의적인 정보 오·남용으로 인한 정보 노출 사고가 매년 전체 사고의 20-30%를 차지하고 있다(Verizon, 2020). Loch et al.(1992)은 외부 침입으로 인한 정보보안 위협에 대한 해결은 정보보안 관련 신기술 및 엄격한 규정 도입 등을 통해 해결할 수 있으나, 내부자에 의한 정보보안 노출 사고 방지는 구성원들의 개별적인 보안 행동에 의지할 수 밖에 없다고 하였다. 그래서, 그들은 내부자들의 정보보안 수준 향상을 위해서는 사전 보안 억제 및 예방에 대한 동기적 관점의 개선을 위한 다각적 지원을 해야 한다고 보았다(Loch et al., 1992).

조직원의 정보보안 준수 관련 선행연구들은 범죄학, 심리학, 사회학 등에서 적용되던 개인의 행동이론을 정보보안 분야에 적용하여 내부자의 정보보안 준수 방안을 논의해왔다. 첫째, 특정 환경에 대한 위협에 대한 대처 유형 및 절차를 제시한 보호동기이론(protection motivation theory) 기반의 연구(Vance et al., 2012; Boss et al., 2015), 둘째, 조직의 정보보안 정책 인식을 통해 정보보안 관련 혜택과 비용을 종합적으로 고려하여 정보보안 준수행동으로 이어진다는 합리적 선택이론(rational choice theory) 기반의 연구(Bulgurcu et al., 2010), 셋째, 조직 차원의 정보보안 미준수에 대한 명확한 제재가 개인의 준수행동으로 이어진다는 일반제재이론(general deterrence theory) 기반의 연구(Guo et al., 2011; Merhi and Ahluwalia, 2019), 넷째, 개인의 반대적 행동은 개인이 처한 환경과 위험에 대한 인식, 그리고, 기회발견에 따라 결정된다고 보는 상황적 범죄 예방 이론(situational crime prevention theory)을 정보보안에 적용한 연구(Safa et al., 2019), 다섯째, 정보보안 관련된 자기효능감, 태도, 사회적 영향 등 계획된행동이론(theory of planned behavior)과 타 이론과 통합을 통해 동기를 형성하는 선행 요인을 제시한 연구(Sommestad et al., 2015; Ahmad et al., 2019), 마지막으로, 조직의 정보보안 정책이 개인의 행동으로 이어지는 통합적인 프레임워크를 제시함으로서 통합적 고려요인을 제시한 연구(De Veiga and Martins, 2017) 등이 제시되었다. 선행연구들은 정보보안 준수 행동은 개인과 조직 환경간의 관계에서 형성된 개인의 심리적 동기에 의해서 결정된다는 것을 확인하고, 정보보안 준수 행동을 높이기 위한 선행 요인을 제시해왔다는 측면에서 시사점을 가진다. 즉, 선행연구는 조직에서 구축한 정보보안 관련 기술적 매커니즘 & 보안 환경관점의 정책 및 규범적 매커니즘을 제시함으로써, 조직 기술적, 문화적 환경이 개인의 동기 형성에 영향을 준다는 것을 증명하였을 뿐 아니라, 개인은 주위 환경적 특성을 받아들이되, 자신의 의사결정 특성 및 성향 등에 따라 정보보안 준수 행동을 결정한다는 것을 증명하였다.

하지만, 조직원의 정보보안 행동이 조직 보안 환경적 구조와 개인의 의사결정 특성에 기반함에도 불구하고, 조직 구조적 특성별, 개인의 행동적 특성별 집단화 및 집단별 보안 행동의 차이에 대한 연구는 부재한 상황이다. 즉, 조직의 문화가 정보보안 준수에 영향을 주는 것은 확인하였음에도 불구하고, 어떠한 문화적 구조가 개인의 정보보안 인식 및 행동에 높은 영향을 주는가에 대한 답변을 하지 못하고 있다. 또한, 개인이 의사결정의 특성이 조직 구조 유형과 연계하여 정보보안 인식 및 행동에 어떠한 영향을 미치는가에 대한 답변을 하지 못하고 있다.

이에, 본 연구는 탐색적 연구 차원에서 조직문화적 구조의 차이와 개인 의사결정 대처의 차이에 따라 정보보안 인지 및 보안 행동에 차이가

발생하는지를 확인하고자 한다. 연구는 세부적으로, 문화 구조를 가장 대표적인 집단 구조적 차이인 개인주의와 집단주의로 구분하고, 개인 의사결정 차이를 대처 유형인 업무중심 대처와 정서중심 대처로 구분하여, 정보보안 인지 요인(정보보안 인식, 인지된 취약성, 그리고 대처효능감)과 정보보안 행동에 미치는 영향의 차이를 확인하고자 한다. 즉, 탐색적 관점에서 조직문화, 대처 유형으로 구성된 4개의 집단별 정보보안 인지 및 행동 차이를 확인하는 것을 목표로 다음과 같은 연구 질문을 제시하고, 설계 및 검증하고자 한다.

RQ 1. 조직문화 형태와 개인 대처 유형별 차이에 따라 형성된 집단은 정보보안 인지 및 준수 행동에 어떤 차이가 있는가?

또한, 연구는 제시한 정보보안 요인들에 대한 인과관계를 확인하고자 한다. 즉, 정보보안 인식과 정보보안 준수 행동간의 관계를 인지된 취약성, 대처 효능감 요인이 매개 효과를 가질 것으로 판단하고 복수 매개모델을 제시 및 관련성을 검증하고자 한다. 즉, 연구는 정보보안 준수 행동에 영향을 주는 선행요인들의 관계성을 확인하기 위하여 다음과 같은 연구 질문을 제시하고, 설계 및 검증하고자 한다.

RQ 2. 정보보안 인식은 정보보안 준수 행동에 어떻게 영향을 미치는가?

연구는 탐색적 관점에서 조직의 문화적 차이와 개인의 대처 유형에 따른 정보보안 인지 및 행동의 차이를 찾고 요인별 영향 관계를 증명함으로써, 조직원의 정보보안 준수 행동 향상을 위한 개인 성향 및 조직문화 차원의 고려요인을 다각적으로 제시함으로써, 조직 내부 정보보안 준수 수준 향상을 위한 전략적 시사점을 제시할 수 있을 것으로 판단한다.

2. 이론적 배경

2.1 대처

대처 이론(coping theory)은 개인이 보유한 자원을 초과하는 특정한 형태로 요구하는 상황을 극복하고자, 변화를 추구하는 인지적 및 행동적 노력을 설명하는 이론으로서, 특정 상황에서 발생한 스트레스를 해결하기 위한 방식을 잘 설명하는 이론이다(Endler and Parker, 1994).

대처는 개인이 외부 또는 내부의 특정한 요구를 관리하기 위해 지속적으로 변화하는 인지 및 행동 수준으로서(Higgins and Endler, 1995), 개인을 둘러싼 환경적 측면의 문제에 대처하는 개인의 인지된 행동 개념이다(Endler and Parker, 1994).

외부 환경에 대한 개인의 대처 유형은 업무중심 대처(task coping)와 정서중심 대처(emotion coping)이 있다. 업무중심 대처는 개인이 문제의 원인을 해결하기 위해 결정을 내리거나 직접적인 조치를 취하고자 하는 행동 유형을 의미하며, 정서중심대처는 경험하는 정서를 조정하여 자신과 조직 환경과의 관계 변화를 추구하는 유형을 의미한다(Folkman and Lazarus, 1985). 즉, 업무중심 대처를 보유한 개인은 조직 내 특정한 문제가 발생하거나 해결해야 할 이슈가 존재할 때, 관련 문제에 집중하는 경향이 있기 때문에, 보다 기술 습득, 행동 기준 마련 등 보다 이성적 관점에서 접근한다. 반면, 정서중심 대처를 보유한 개인은 대상 문제에 대한 접근을 경험 등 감성적으로 접근이기 때문에 심리적 관점에서 문제를 대처하려는 경향을 보인다(Jung and Yoon, 2014).

정보보안 분야에서 대처유형은 개인의 정보보안 준수 의도에 절차적 영향을 주는 조절 조건이다. 정보보안 정책 및 기술의 적용은 개인에게 적용의 어려움을 가지게 되며, 개인의 대처 유형별 접근 방식에 따라 부정적 행동을 완화하는 효과를 가진다(Galluch et al., 2015). 본 연구는 개인 의사결정 요인으로 업무중심 대처-정서중심 대처를 적용하여, 개인의 대처 유형 차이에 따른 개인의 정보보안 인식 및 행동의 차이를 확인하고자 한다.

2.2 조직문화

조직문화(organizational culture)는 특정 집단의 역사, 언어, 분위기 등의 조건을 공유한 사람들의 신념, 평가, 지각 등을 공통적으로 보유하는 특성 개념으로서(Markus and Kitayama, 1991), 조직의 분위기 등 특성화된 구조를 만들고, 구성원이 따르도록 하는 개념이기 때문에 조직과 개인간의 관계를 설명하기 위한 중요한 요인이다(Flores and Ekstedt, 2016).

정보보안 분야에서도 조직문화는 개인의 준수행동을 설명하기 위한 선행 조건으로 활용되고 있다. Hu et al.(2012)은 개인의 정보보안 정책 준수행동은 조직이 부여한 정책의 방향과 목적에 대한 개인의 믿음으로서 형성될 수 있는데, 개인을 둘러싼 보안 관련 문화의 형성이 중요한 선행조건이 된다고 보았다.

심리학, 사회학 등에서는 대조적 관점의 조직문화에 대한 구분을 다양하게 제시하고 있는데, 공정성 측면에서 형평(equity)과 평등(equality)관점의 차이를 제시한 연구(Mannix et al. 1995), 조직의 행동 중심이 개인 관점 또는 집단 관점인지 차이에 따라 행동적 차이가 발생한다는 연구(Triandis, 1995) 등이 있다.

이중, Triandis의 개인주의적(individualistic)-집합주의적(collectivist) 차이 개념은 기업 및 구성원들의 행동의 차이가 문화적 차이에 의해 명백하게 발생함을 제시하였다. 개인주의 문화는 집단보다 자기(self)를 우선순위로 두며, 자기(self)를 집단과 독립적인 관점으로 고려하는 경향이 있다. 집단주의 문화는 자기(self)와 집단간의 상호 연계되는 목표를 가지려고 하며, 갈등 발생 시 집단을 우선시한다. 또한, 자기(self)의 개념을 집단과 상호의존적인 관계로 판단하는 경향이 있다(Medvene et al., 2000). 본 연구는 우선적으로 개인주의-집합주의 문화적 차이가 정보보안 관련 인지 및 행동에도 영향을 다르게 줄 것으로 판단하며, 문화적 차이 요인으로 활용하고자 한다.

2.3 정보보안 준수행동

정보보안 준수 행동(compliance behavior)은 개인에게 형성된 정보보안 인지 및 의도를 통해서 실제 조직이 요구하는 정보보안 관련 행동을 실행하는 수준을 의미한다(Kim and Kim, 2017). 조직은 정보보안과 관련된 개인의 행동 내역을 쉽게 알 수 없고, 항상 개인이 조직보다 행동 정보를 더 많이 가지고 있기 때문에, 조직과 개인간에는 대리인 문제가 발생한다(West, 2008). 즉, 개인의 보안 행동이 적절한지를 판단하기 위해서는 드러난 결과만을 가지고 확인하기 때문에, 개인의 준수 행동에 대한 정확한 평가가 어렵다. 따라서, 개인의 정보보안 준수 행동은 자발적인 개인의 노력을 요구할 수밖에 없기 때문에, 개인의 정보보안 동기 형성을 위한 지원이 필요하다(Kim et al., 2018; Park et al., 2019; Safa et al., 2019). 즉, 조직 내부자들의 보안 수준을 높이기 위해서는 구성원들의 자발적인 준수 행동이 많아져야 하며, 조직은 구성원들의 준수 동기 형성을 위한 교육, 훈련, 캠페인 등 다각적 활동이 필요하다.

2.4 인지된 취약성

조직 내부자들의 정보보안 준수행동 원인과 대처 방안을 동기적 관점에서 제시한 대표적인 이론이 보호동기이론(protection motivation theory)이다(Vance et al., 2012). 보호동기 이론은 개인의 행동은 개인을 둘러싼 위협에 대한 평가 및 대처 방안에 대한 통합적 고려를 통해서 실현된다는 관점이다(Boss et al., 2015; Posey et al., 2015). 정보보안분야에서 개인의 행동에 영향을 주는 위협에 대한 평가를 결정하는 요인으로서 인지된 취약성이 있다. 인지된 취약성(perceived vulnerability)은 정보보안 문제에 대응하기 위한 조치를 취하지 않을 경우 부정적인 사건이 발생할 것이라 개인이 느끼는 수준을 의미한다(Siponen et al., 2014).

정보보안에 대한 개인이 인지한 취약성은 개인에게 보안 미준수 시 발생가능한 위협 요인 및 위치를 인식시켜주는 요인이기 때문에, 스스로가 어떻게 보안 관련 행동을 해야하는지를 이해하도록 돕는 선행 동기요인이다. 인지된 취약성을 높이기 위해서는 조직의 정보보안 수준에 대한 지식 형성이 선행되어야 한다. Boss et al.(2015)은 보안 취약성을 인지하기 위해서는 정보보안 관련 조직의 정책, 기술 등 관련 정보를 사전에 인지

하도록 지원하는 것이 필요함을 제시하였다.

인지된 취약성은 정보보안 행동에 긍정적 영향을 주는 요인이다. Posey et al.(2015)은 조직이 제공한 정보보안 정보 원천을 받아들인 개인은 보안 위협 또는 불확실성에 대한 문제점을 인지할 뿐 아니라, 미준수 시 발생하는 개인의 피해까지 함께 고려하기 때문에, 준수행동을 높이는 요인이라고 하였다. 즉, 인지된 취약성은 개인의 목표 달성을 위해 행동을 하도록 하는 선행 조건이며, 정보보안 준수행동을 높이고, 미준수행동을 낮추도록 돕는 요인이다(Siponen et al., 2014). 따라서, 인지된 취약성은 정보보안 준수행동에 영향을 줄 것으로 판단하고, 다음의 연구가설을 제시한다.

H1 : 인지된 취약성이 높을수록 정보보안 준수행동이 높을 것이다.

2.5 대처효능감

보호동기이론은 외부 위협에 대한 공포 소구(fear appeal)을 인지하고 어떻게 대처할 것인가를 판단하는 이론이기 때문에, 외부 위협 요인에 대한 종합적 평가 및 대처하기 위한 개인 본인의 평가 조건을 요구 한다(Posey et al. 2015). 이중 대처효능감은 조직차원의 위협 대처 방식에 관한 요인으로, 개인이 외부 문제에 대한 대응 방식을 결정할 수 있도록 돕는다(Sommestad et al., 2015).

대처효능감(response efficacy)은 특정 행동에 대한 조직 차원의 대처 방안이 효과적일 것이라고 생각하는 개인의 믿음 수준이다(Ifinedo, 2012). 다시말해, 정보보안 분야에서 대처 효능감은 개인의 정보보안 미준수 결과로 인한 예상되는 취약성, 심각성 등에 대한 대처를 어떻게 할 것인가에 대한 관점으로서, 조직 차원의 정보보안 대처 방식 및 규정 등이 효과적이라고 판단할 때, 개인은 조직의 요구사항에 따르는 경향을 가진다고 본다(Sommestad et al., 2015).

정보보안 관련 대처 효능감은 정보보안 관련 자기 효능감과 함께, 개인의 행동의도에 영향을 주고, 실제 행동으로 이어지도록 돕는 선행 동기적 요인이다(Chou and Chou, 2017). 자기효능감은 자신이 가지고 있는 역량과 능력이 적합한 행동으로 이어지도록 돕는 개념이며, 대처효능감은 조직의 특정 역량이 적정 행동으로 이어지도록 돕는 역할을 한다는 개념이기 때문에, 정보보안의 긍정적 동기 요인이다. 따라서, 조직에서 구축한 보안 정책 및 규범, 기술 등 보안 문제 대처가 높게 인지될 때 개인은 조직의 요구사항에 맞게 보안 행동을 실행하는 경향을 가진다(Siponen et al., 2014).

대처 효능감이 형성된 개인은 조직이 요구하는 보안 활동에 대한 믿음이 발생하여 긍정적 보안 행동을 할 가능성이 높다(Sommestad et al., 2015). Vance et al.(2012)은 정보보안에 대한 습관이 대처효능감과 자기효능감을 높이고, 형성된 효능감은 정보보안 정책 준수의도에 긍정적 영향을 주는 것을 확인하였다. 따라서, 정보보안 대처 효능감은 준수행동에 긍정적인 영향을 줄 것으로 판단하고, 다음의 연구가설을 제시한다.

H2 : 대처효능감이 높을수록 정보보안 준수행동이 높을 것이다.

2.6 정보보안 인식

정보보안 인식(information security awareness)은 정보보안에 대한 일반적인 지식으로서, 조직원이 조직의 정보보안 수준 및 관련 영향과 관련된 지식과 이해의 수준을 의미한다(Bulgurcu et al., 2010). 즉, 정보보안 인식은 조직의 정보보안 관련 규범, 활동 요구수준 등의 정보를 알고 있는 것을 의미한다.

개인의 정보보안 관련 정보 취득은 조직에서 제공하는 정보보안 워크숍, 세미나 등 교육을 통해서 확립하거나, 전문 저널이나 조직의 보안 가이드라인, 문서 등을 통해서도 확보할 수 있다(Park et al., 2017; Soh and Kim, 2017).

정보보안 인식은 조직 내 정보보안 규칙을 알고 있는 수준이기 때문에, 정보보안 준수 행동 수준을 이해하고, 관련된 보안 지식을 확보할 수 있도록 도움을 준다. Mamonov and Benbunan-Fich(2018)는 정보보안 위협에 대한 인식은 개인의 정보보안 행동에 직접적인 영향을 주는 선행요인임을 증명하였으며, Park et al.(2017)은 병원 조직 내 환자 정보에 대한 조직원들의 정보보안 인식 형성이 정보 노출을 방지할 수 있다고 하였다. 즉, 정보보안

인식은 조직에서 요구하는 정보보안 관련 행동을 수준을 파악하고 지식화할 수 있는 기반 요인이다.

정보보안 인식은 정보보안에 대한 개인의 지식 또는 이해 수준으로서, 지식 및 이해 수준이 형성되어야 정보보안 관련 태도 또는 행동의 전환이 이루어진다(Bulgurcu et al., 2010).

첫째, 정보보안 인식은 정보보안 준수 행동의도에 긍정적인 영향을 미친다. Park et al.(2017)은 병원의 개인 건강정보 보호 의도는 건강 정보보안 인식이 사전에 형성되는 것이 중요하다고 보았으며, 보안 인식이 개인적 규범과 자기통제의 완전 매개효과를 통해 준수의도에 영향을 미치는 것을 확인하였다. 또한, yazdanmehr and Wang(2016)은 정보보안 정책 인식이 개인의 규범과 준수행동 사이를 조절하는 것을 확인하였다. 따라서, 정보보안 인식이 정보보안 행동에 긍정적인 영향을 줄 것으로 판단하고, 다음의 연구 가설을 제시한다.

H3 : 정보보안 인식이 높을수록 정보보안 준수 행동이 향상될 것이다.

둘째, 정보보안 인식의 형성은 정보보안 관련 위협 또는 취약점을 이해하도록 돕는 선행 조건이다. Yazdanmehr and Wang(2016)은 정보보안 정책 관련 결과에 대한 인지의 형성은 정보보안 관련 개인의 행동 규정에 영향을 주며, 행동규정은 미준수 시 발생할 위협 및 조직의 제재를 포함한다고 보았다. 또한, Bulgurcu et al.(2010)은 개인은 정보보안 인식이후, 준수를 통한 혜택과 미준수를 통한 비용을 합리적으로 고민한다고 보았는데, 미준수 행동 요인으로 인지된 취약성을 제시하였다. 즉, 정보보안에 대한 전체적인 이해 및 지식을 보유할 경우, 조직의 정보보안 중 취약성을 이해하고 미준수 시 발생하는 위협 및 비용을 계산할 수 있다. 선행연구를 기반으로 정보보안 인식은 인지된 취약성에 긍정적인 영향을 줄 것으로 판단하고 연구가설을 제시한다.

H4 : 정보보안 인식이 높을수록 인지된 취약성이 높을 것이다.

마지막으로, 정보보안 인식의 형성은 조직에서 자신이 정보보안을 지킬 수 있다는 개념인 효능감에 긍정적인 영향을 준다. Flores and Ekstedt(2016)는 정보보안 인식이 개인이 정보보안을 지켰을 때 받을 수 있는 혜택과 수행할 수 있다고 판단하는 내적 믿음에 영향을 주는 선행요인으로 보았다. 특히, 그들은 내적 동기 요인인 믿음의 구성항목으로 자기효능감, 태도, 그리고 사회적 믿음을 제시하였으며, 이중 정보보안 인식은 자기효능감에 높은 영향을 미치는 것을 확인하였다. 또한, 대처효능감은 조직의 보안 활동이 보안 준수에 효과적이라는 믿음으로서, 정보보안 정보가 개인에게 지속적으로 제공되면 대처효능감을 높인다(Posey et al. 2015). 따라서, 정보보안 인식이 대처효능감에 긍정적인 영향을 줄 것으로 판단하고, 다음의 연구가설을 제시한다.

H5 : 정보보안 인식이 높을수록 대처 효능감이 높을 것이다.

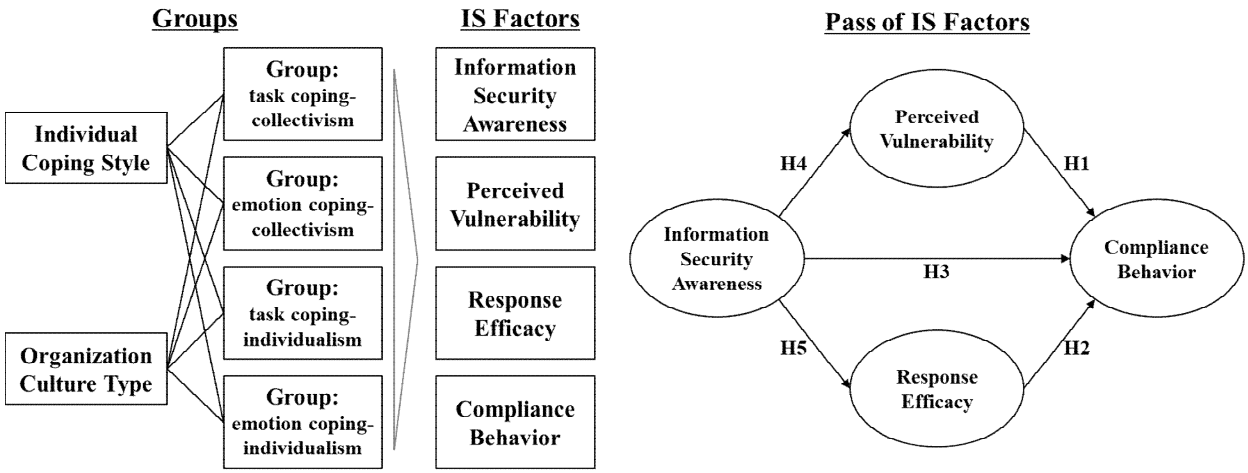

Fig. 1 Research Framework

3. 연구 방법

3.1 연구 설계

본 연구는 조직문화 유형과 개인 대처 유형 집단에 따른, 정보보안 인지 및 행동에 미치는 영향의 차이 분석과 정보보안 인지 요인들의 준수 행동에 미치는 영향 분석을 실시한다. 즉, 다음 Fig. 1과 같은 연구 설계에 기반하여 2개의 연구 질문에 대한 결과를 확인하고자 한다.

3.2 연구 대상

본 연구는 특정 문제에 대한 개인의 대처 방식 관점과 조직의 문화 관점에 따라, 조직원의 정보보안 인식과 준수 행동에 미치는 영향의 차이를 확인하는 것을 목적으로 한다. 이에 따라, 연구 대상은 정보보안 정책 및 기술을 도입한 조직에서, 보안 목표 및 절차에 따라 정보보안 준수 행동을 수행해야 하는 직장인들을 대상자로 하였다. 특히, 정보보안 관련 업무가 자신의 직접적인 업무 목표가 아닌 일반 근로자들을 대상으로 하였으며, 전산팀 또는 보안 부서에서 근무하는 사람들은 제외하였는데, 보안 부서 근로자들은 업무 목표가 정보보안 수준 확립에 있기 때문에, 일반인과는 차이가 있다고 판단하였기 때문이다.

설문은 직장인을 대상으로 운영하는 학과에 다니는 학생들에게 실시하였으며, 대면과 비대면을 함께 진행하였다. 사전 설문 목적 및 데이터 사용 방법을 공지하였으며, 설문을 허락한 사람들만 설문에 응답하도록 하였다.

3.3 측정도구

조직 내부자의 정보보안 준수 행동 향상이 개인의 특정 문제에 대한 의사결정 방식과 조직의 문화적 특성이 상호연관적인 관계에 있음을 확인하기 위하여, 본 연구는 조직문화 유형(개인주의, 집단주의)과 대처 유형(업무중심 대처, 정서중심 대처)으로 구분하여 정보보안 인지 요인(정보보안 인식, 인지된 취약성, 대처 효능감)과 정보보안 준수 행동에 미치는 영향 관계를 제시하고자 하며, 다음의 측정 도구를 적용하였다.

3.3.1 대처차원과 조직문화 차원

대처는 개인의 특정 문제를 해결하는 방식을 의미하며, “업무중심 대처(task coping)”, “정서중심 대처(emotion coping)”으로 구분하였으며(Endler and Paker, 1994), 응답자에게 자신의 대처 방식을 선택하도록 하였다. 조직문화는 집단 내 공통된 신념, 평가, 가치 등을 의미하며, 응답자가 소속된 조직의 “개인주의(individualism)”와 “집단주의(collectivism)” 성향을 선택하도록 하였다(Triandis, 1995).

3.3.2 정보보안 인식

정보보안 인식(information security awareness)은 조직의 정보보안 관련 정보를 알고 있는 수준으로서(Bulgurcu et al., 2010), 정보보안 관련 선행연구에서 적용한 개념을 적용하여, 다음과 같은 “나는 전반적으로 잠재적인 보안위협과 부정적 결과를 알고 있음”, “잠재적인 보안 문제와 비용에 대한 지식을 보유”, “정보보안 우려와 일반적인 위험을 이해”의 3개 요인으로 측정도구를 구성하였다.

3.3.3 인지된 취약성

인지된 취약성(perceived vulnerability)은 정보보안에 대한 미비한 대처 시 부정적인 사건이 발생할 것이라 느끼는 수준으로서(Siponen et al., 2014), 정보보안 관련 선행연구에서 적용한 개념을 적용하여, 다음과 같은 “보안 정책의 미준수 시 보안 침해에 취약해질 수 있음”, “보안 정책을 준수하지 않으면 악의적 공격을 받을 수 있음”, “정보보안은 불법 엑세스를 감소시킬 수 있음”, “정보보안에 대한 미주의는 조직 데이터와 리소스 손상을 일으킬 수 있음”의 4개의 요인으로 측정도구를 구성하였다.

3.3.4 대처 효능감

대처 효능감(response efficacy)은 정보보안 위협에 대한 조직의 대처가 효과적이라고 인식하는 수준으로서(Ifinedo, 2012), 정보보안 관련 선행연구에서 적용한 개념을 적용하여, 다음과 같은 "업무용 컴퓨터에서 보안조치 활성화가 해커의 공격을 막을 수 있음", "조직의 보안조치가 외부 엑세스를 방지할 수 있음", "조직의 정보 위협을 막기 위해 사용할 수 있는 예방조치는 적절"의 3개의 요인으로 측정도구를 구성하였다.

3.3.5 정보보안 준수 행동

정보보안 준수 행동(compliance behavior)은 조직이 요구하는 정보보안 수준에 대한 개인의 행동으로서(Siponen et al., 2014), 정보보안 관련 선행연구에서 적용한 개념을 적용하여, 다음과 같은 "정보보안 정책을 준수", "정보보안 정책 준수를 추천", "다른 구성원들이 정보보안 정책을 준수하도록 도움"의 3개의 요인으로 측정도구를 구성하였다.

4. 연구 결과

4.1 기초 통계

연구 목적에 적합한 정보보안 조직에 근무하는 직장인을 대상으로 한 설문 결과, 총 376명의 설문 응답 중 무성의하거나 답변이 없는 응답을 제외하고 324개의 응답을 표본으로 활용하였다.

연구에 적용된 표본에 대하여 적용하고자 하는 집단(대처 차원, 조직문화 차원)간 성별(남성, 여성)과 직위(대리이하, 과장 이상)에 따른 차이를 제시하였다. 즉, 업무중심 대처, 정서중심 대처 집단과 개인주의, 집단주의 집단 내 성별 및 직위에 따른 응답 결과를 살펴보면 Table 1과 같다. 집단별 비율이 비슷한 수준으로 나타나 교차분석과 요인간의 연관관계 분석에 문제가 없는 것으로 파악되었다.

Table 1 Demographic Characteristics

Coping	Culture	Sex		Position		Total
		Male	Female	Assistant	Manager	
Task	In	36 (47%)	40 (53%)	28 (37%)	48 (63%)	76 (100%)
	Co	55 (63%)	33 (37%)	28 (32%)	60 (68%)	88 (100%)
	Total	91 (55%)	73 (45%)	56 (34%)	108 (64%)	164 (100%)
Emotion	In	41 (50%)	41 (50%)	66 (80%)	16 (20%)	82 (100%)
	Co	35 (45%)	43 (55%)	71 (91%)	7 (9%)	78 (100%)
	Total	76 (48%)	34 (52%)	137 (86%)	23 (14%)	160 (100%)
Total	In	77 (49%)	31 (51%)	94 (59%)	64 (41%)	158 (100%)
	Co	90 (54%)	76 (46%)	99 (60%)	67 (40%)	166 (100%)
	Total	167 (52%)	157 (48%)	193 (60%)	131 (40%)	324 (100%)

In(Individualism), Co(Collectivism)

4.2 교차 분석

개인의 의사결정 행동 유형인 업무중심 대처와 정서중심 대처 집단과 조직의 문화적 구성 유형인 개인주의 집단과 집단주의 집단에 대한 분석을 위하여, 교차분석설계(cross-over design)를 실시한다. 즉, 개인-조직 특성 집단별 개인의 정보보안 인지(정보보안 인식, 인지된 취약성, 대처 효능감)와 정보보안 준수 행동의 영향 차이를 확인한다.

교차분석을 실시하기 전, 적용 요인(정보보안 인식, 인지된 취약성, 대처 효능감, 정보보안 준수행동)에 대하여 탐색적 요인분석과 신뢰성 분석을 실시하였다(Table 2). SPSS 21.0을 활용하여 cormbach's α를 분석한 결과 신뢰성 요구사항인 0.7을 넘은 것으로 나타나(Nunnally, 1978), 교차분석을 실시한다.

Table 2 Exploratory Factor Analysis

	1	2	3	4	Cronbach's α
ISA1	0.103	0.052	0.094	**0.788**	
ISA2	-0.023	0.157	-0.042	**0.758**	0.763
ISA3	0.183	-0.070	0.250	**0.727**	
PV1	**0.845**	0.088	0.116	0.151	
PV2	**0.812**	0.041	0.239	0.124	0.816
PV3	**0.828**	0.168	0.121	-0.011	
RE1	0.090	0.214	**0.802**	0.118	
RE2	0.166	0.105	**0.790**	0.122	0.785
RE3	0.220	0.167	**0.793**	0.035	
CB1	0.063	**0.823**	0.217	-0.096	
CB2	0.093	**0.829**	0.205	0.085	0.807
CB3	0.146	**0.819**	0.059	0.192	

* ISA(Information Security Awareness), PV(Perceived Vulnerability), RE(Response Efficacy) CB(Compliance Behavior)

첫째, 대처유형과 조직문화 변인의 정보보안 인식(information security awareness)에 미치는 영향에 대한 검증을 실시하였다(Table 3). 대처 유형은 정서중심 대처 집단(M = 6.12)이 업무중심 대처 집단(M = 5.80)보다 정보보안 인식 평균이 높은 것으로 나타났으며, 대처 유형 변인이 정보보안 인식에 미치는 영향은 유의한 것으로 나타났다(F(1, 320) = 13.34, p < 0.01). 조직문화 유형은 집단주의 집단(M = 6.07)이 개인주의 집단(M = 5.84)보다 정보보안 인식 평균이 높은 것으로 나타났으며, 조직문화 변인이 정보보안 인식에 미치는 영향은 유의한 것으로 나타났다(F(1, 320) = 59.32, p < 0.01). 대처와 조직문화간의 상호작용효과는 유의하지 않은 것으로 나타났다(F(1, 320) = 0.34, n.s.).

Table 3 ANOVA of Information Security Awareness

Variables	SS	df	MS	F
Coping	8.85	1.00	8.85	13.34**
Culture	5.02	1.00	5.02	7.57**
Coping X Culture	0.23	1.00	0.23	0.34

**: p < 0.01, *: p < 0.05

둘째, 대처유형과 조직문화 변인의 인지된 취약성(perceived vulnerability)에 미치는 영향에 대한 검증을 실시하였다(Table 4. 대처 유형은 정서중심 대처 집단(M = 5.43)이 업무중심 대처 집단(M = 5.11)보다 인지된 취약성이 높은 것으로 나타났으며, 대처 유형 변인이 인지된 취약성에 미치는 영향은 유의한 것으로 나타났다(F(1, 320) = 10.49, p < 0.01). 조직문화 유형은 집단주의 집단(M = 5.69)이 개인주의 집단(M = 4.83)보다 인지된 취약성이 높은 것으로 나타났으며, 조직문화 변인이 인지된 취약성에 미치는 영향은 유의한 것으로 나타났다(F(1, 320) = 59.32, p < 0.01). 대처와 조직문화간의 상호작용효과는 유의하지 않은 것으로 나타났다(F(1, 320) = 1.19, n.s.).

Table 4 ANOVA of Perceived Vulnerability

Variables	SS	df	MS	F
Coping	10.76	1.00	10.76	10.49**
Culture	60.82	1.00	60.82	59.32**
Coping X Culture	1.22	1.00	1.22	1.19

**: p < 0.01, *: p < 0.05

셋째, 대처유형과 조직문화 변인의 대처 효능감(response efficacy)에 미치는 영향에 대한 검증을 실시하였다(Table 5). 대처 유형은 정서중심 대처 집단(M = 5.34)이 업무중심 대처 집단(M = 4.99)보다 대처 효능감이 높은 것으로 나타났으며, 대처 유형 변인이 대처 효능감에 미치는 영향은 유의한 것으로 나타났다(F(1, 320) = 13.42, p < 0.01). 조직문화 유형은 집단주의 집단(M = 5.57)이 개인주의 집단(M = 4.73)보다 대처 효능감이 높은 것으로 나타났으며, 조직문화 변인이 대처 효능감에 미치는 영향은 유의한 것으로 나타났다(F(1, 320) = 63.91, p < 0.01). 대처와 조직문화간의 상호작용효과는 유의하지 않은 것으로 나타났다(F(1, 320) = 1.78, n.s.).

Table 5 ANOVA of Response Efficacy

Variables	SS	df	MS	F
Coping	12.58	1.00	12.58	13.42**
Culture	59.94	1.00	59.94	63.91**
Coping X Culture	1.67	1.00	1.67	1.73

**: $p < 0.01$, *: $p < 0.05$

넷째, 대처유형과 조직문화 변인의 준수 행동(compliance beahavior)에 미치는 영향에 대한 검증을 실시하였다(Table 6). 대처 유형은 정서중심 대처 집단(M = 5.73)이 업무중심 대처 집단(M = 5.35)보다 준수 행동이 높은 것으로 나타났으며, 대처 유형 변인이 준수 행동에 미치는 영향은 유의한 것으로 나타났다($F(1, 320) = 13.42$, $p < 0.01$). 조직문화 유형은 집단주의 집단(M = 5.62)이 개인주의 집단(M = 5.45)보다 준수 행동이 높은 것으로 나타났으며, 조직문화 변인이 준수 행동에 미치는 영향은 유의한 것으로 나타났다($F(1, 320) = 63.91$, $p < 0.05$). 대처와 조직문화간의 준수 행동에 대한 상호작용효과는 유의한 것으로 나타났다($F(1, 320) = 6.16$, $p < 0.01$.).

Table 6 ANOVA of Compliance Behavior

Variables	SS	df	MS	F
Coping	11.96	1.00	11.96	12.98**
Culture	2.90	1.00	2.90	3.15*
Coping X Culture	5.67	1.00	5.67	6.16**

**: $p < 0.01$, *: $p < 0.05$

정보보안 준수 행동에 대한 대처유형과 조직문화간의 상호작용효과를 확인한 결과(Fig. 2), 개인주의 집단에서 업무중심 대처와 정서중심 대처간의 행동에 미치는 영향 차이는 크지 않았으나, 집단주의 집단의 경우 정보보안 준수 행동에 정서중심 집단이 업무중심 집단보다 높은 영향을 미치는 것으로 나타났다.

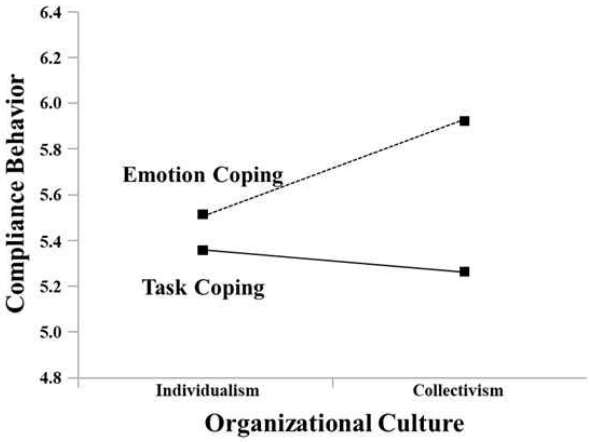

Fig. 2 Moderation Effect of Compliance Behavior

개인과 조직의 특성간 교차설계를 통한 개인인지를 확인한 결과, 정보보안 분야에서는 개인 대처 유형은 업무 중심 대처 집단에서 정보보안 인식 및 행동을 높게 인지하고 있는 것으로 나타났는데, 이러한 결과는 정보보안 분야에 대한 대처가 위험 회피 성향을 띄고 있기 때문인 것으로 판단된다. 또한, 조직문화 관점에서 집단주의의 성향을 가진 조직이 개인주의보다 높게 정보보안 인식 및 행동에 대하여 인식하는 것으로 나타났는데, 조직과 일치하려는 성향이 집단주의에 높게 나타나기 때문인것으로 판단된다.

특히, 보안 행동에 대하여 각 집단간 상호작용효과가 있음을 확인하였는데, 집단주의 중 감성대처 유형 집단에서 정보보안 행동이 높은 것으로 나타났다. 즉, 집단주의는 개인의 이성적 접근보다는 집단의 감정에 충실하려는 성향이 있고, 정보보안 분야에서도 적용됨을 확인하였다.

4.3 연구모델 분석

연구에서 제시하는 이중매개모형 검증은 SPSS 21.0의 위계적 회귀분석과 소벨테스트(sobel test)를 통해 확인하였다.

Table 7 Hierarchical Regression Analysis of Mediation Model

Step		Path	Beta
0 step	H3	ISA → CB	0.19**
1-1 step	H4	ISA → PV	0.24**
	H5	ISA → RE	0.25**
1-2 step	H1	PV → CB	0.14*
	H2	RE → CB	0.47**
2 step	H3	ISA → CB	0.06

* ISA(Information Security Awareness), PV(Perceived Vulnerability), RE(Response Efficacy) CB(Compliance Behavior)
**: $p < 0.01$, *: $p < 0.05$

첫째, 정보보안 인식이 인지된 취약성을 통해 준수 행동으로 이어지는 매개효과를 검증하였다. 첫째, 정보보안 인식이 준수 행동에 미치는 개별 영향력은 통계적으로 유의하였으며(H3; β = 0.19, $p < 0.01$), 정보보안 인식이 인지된 취약성에 미치는 영향력(H4; β = 0.24, $p < 0.01$)과 인지된 취약성이 준수 행동에 미치는 개별 영향력(H1; β = 0.14, $p < 0.05$)은 모두 통계적으로 유의한 것으로 나타났다. 그리고 정보보안 인식이 준수 행동에 미치는 영향력은 통계적으로 유의하지 않은 것으로 나타났다(H3'; β = 0.06, n.s.).

둘째, 정보보안 인식이 대처 효능감을 통해 준수 행동으로 이어지는 매개효과를 검증하였다. 첫째, 정보보안 인식이 준수 행동에 미치는 개별 영향력은 통계적으로 유의하였으며(H3; β = 0.19, $p < 0.01$), 정보보안 인식이 대처 효능감에 미치는 영향력(H5; β = 0.25, $p < 0.01$)과 대처 효능감이 준수 행동에 미치는 개별 영향력(H2; β = 0.47, $p < 0.01$)은 모두 통계적으로 유의한 것으로 나타났다. 그리고 정보보안 인식이 준수 행동에 미치는 영향력은 통계적으로 유의하지 않은 것으로 나타났다(H3′; β = 0.06, n.s.).

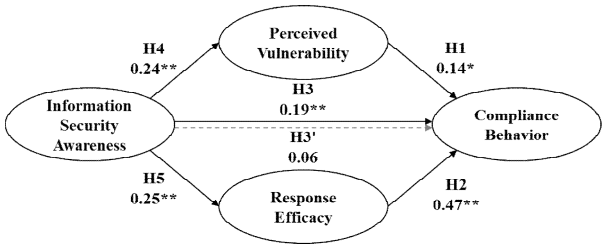

Fig. 3 Result of Multiple Pass Mediation Model

마지막으로, 제시한 두 개의 매개모형 모두 유의미하였기 때문에, 복수 매개모형(multiple mediator)의 유효성 검증을 실시하였다. 소벨 테스트 결과 통계적으로 유의한 것으로 나타나, 복수 매개효과가 있음을 확인하였다($Z = 1.85$, $p < 0.05$).

본 연구에서 제시한 정보보안 인지 요인(정보보안 인식, 인지된 취약성, 대처효능감)과 정보보안 준수 행동간의 관계를 구조적으로 살펴본 결과(Fig. 3), 연구 모델에서 제시한 요인간에는 복수매개모형의 영향을 가지는 것을 확인하였다. 즉, 개인의 정보보안 행동은 조직에서 제공한 정보보안 정보 등을 통해서 형성된 정보보안 인식을 통해서 발현되는데, 정보보안 인식을 통해서 개인은 조직 내 정보보안 준수의 필요성 측면인 취약성의 문제점을 확인하고, 조직의 대처 방식의 효과를 인지하게 됨으로써, 행동으로 이어진다는 결과를 확인하였다.

5. 결 론

5.1 연구의 시사점

연구는 조직구성원들의 정보보안 준수 인지 요인과 준수 행동에 미치는 개인의 의사결정 요인 및 조직의 문화적 특성을 제시하고 인지 요인과 준수 행동간의 영향 관계를 확인하고자 하였다. 이에, 개인 요인과 조직 요인에 대한 교차 분석을 실시하여 집단 간 차이 분석을 실시하였으며, 회귀분석을 통해 매개 모델에 대한 검증을 하였다. 이에 연구 결과는 다음과 같은 학술적, 실무적 시사점을 가진다.

첫째, 조직의 정보보안이 조직과 개인의 상호 관계에 의해 결정되고 개인의 행동으로 이어진다고 판단하고, 개인의 문제에 대한 해결 유형과 조직의 문화를 구분하여 집단별 개인의 정보보안 인지에 미치는 영향 분석을 실시하였다. 세부적으로 개인의 문제 해결 유형을 대처이론을 적용하여, 업무중심 대처와 정서중심 대처로 구분하였으며, 조직문화는 개인주의 집단과 집단주의 집단으로 구분하여 4개의 집단에 대한 구성원의 보안 인지 및 행동을 확인하였다. 이러한 결과는 학술적으로 정보보안 준수 행동이 개인을 둘러싼 조직적 환경과 개인의 의사결정 방식에 따라 다르게 결정될 수 있음을 제시하였다는 측면에서 시사점을 가진다. 또한, 실무적 관점에서 조직원의 정보보안 수준을 향상시키기 위한 지원체계가 단순히 정책, 규범 등을 제시함으로써 해결할 수 있는 문제가 아님을 제시하였다. 즉, 조직문화적 특성과 개인의 의사결정 방식에 대한 특성 등을 함께 고려하여 맞춤형 지원체계를 갖추는 것이 필요함을 제시한 측면에서 실무적 시사점을 가진다.

둘째, 연구는 문제에 대한 의사결정 관점인 대처 유형에 따른 집단 차이 분석을 실시하였다. 즉, 개인이 특정 문제에 대한 행동의지는 유형별 발현될 수 있는데, 대표적으로 업무중심 대처와 정서중심 대처가 존재한다. 학술적 관점에서 연구는 업무중심과 정서중심에 따른 집단간 차이 분석을 통해 정보보안 분야에서 영향을 확인하였다. 분석 결과 정보보안 인지요인(정보보안 인식, 인지된 취약성, 대처 효능감)과 준수 행동에 정서중심 집단이 업무중심 집단보다 각각의 평균이 높으며, 대처 집단이 각 요인에 영향을 미치는 것을 확인하였다. 실무적 관점에서 이러한 결과는 정보보안에 대한 조직의 노력이 이성적인 접근보다는 정서적인 접근을 통해 보안 준수를 요구해야함을 제시한다.

셋째, 연구는 조직문화 관점 중 개인주의 집단과 집단주의 집단 유형별 차이 분석을 실시하였다. 즉, 조직의 환경이 개인에 미치는 영향의 차이를 확인하고자 하였다. 학술적 관점에서 연구는 개인에게 높은 영향을 미치는 문화적 관점의 차이가 실제 정보보안 분야의 개인 보안 인지 및 행동에 영향력의 차이가 발생함을 확인하였다. 집단주의 조직이 개인주의 조직보다 개인의 정보보안 인지(정보보안 인식, 인지된 취약성, 대처 효능감)과 준수 행동에 더 높은 영향을 미치는 것을 확인하였으며, 조직문화 집단이 각 요인에 영향을 미치는 것을 확인하였다. 실무적 관점에서 이러한 결과는 정보보안 준수에 대한 조직문화 형성은 개인주의보다 집단주의가 구성원의 정보보안 행동에 영향을 줄수 있음을 제시하였다는 측면에서 시사점을 가진다.

마지막으로, 연구는 집단 분석에 활용한 정보보안 인지 요인과 행동 요인간의 영향 관계를 확인함으로써, 개인의 정보보안 준수 행동 향상을 위하여 조직에서 지원해야 할 방향을 제시하고자 하였다. 학술적으로 연구는 각 요인간의 복수 매개모형을 제시하고 통계적으로 확인하였다. 즉, 개인의 정보보안에 대한 인식이 인지된 취약성과 대처 효능감을 통해 준수 행동으로 이어지는 완전 복수 매개효과가 있음을 확인하였다. 실무적으로, 조직이 개인들의 정보보안 준수 행동을 높이기 위해서는 정보보안 관련 정보를 지속적으로 제공함으로써, 구성원들이 정보보안 인식을 통해서, 정보보안 준수의 필요성을 위협관점에서 인지하고, 조직의 보안 대처를 따른다면, 충분히 정보보안을 지킬 수 있다고 믿도록 하는 것이 필요함을 제시하였다.

5.2 연구의 한계점

연구는 개인 의사결정 요인과 조직문화적 요인이 개인의 정보보안에 미치는 영향을 확인하였다는 측면에서 학술적, 실무적 시사점을 가지지만, 다음과 같은 연구적 한계로 인한 추가 연구가 필요하다. 첫째, 연구는 집단간 차이 분석을 위하여 설문 당시의 응답자 생각을 중심으로 집단의 특성을 확인하였다. 집단의 특성을 보다 명확하게 파악할 수 있는 분류 기준을 활용함으로써, 집단별 정보보안 준수에 대한 영향의 차이를 명확하게 제시하는 것이 필요하다. 둘째, 조직 특성요인을 문화적 관점에서 집단주의와 개인주의로 구분하여 접근하였다. 최근 조직문화에 따른 집단 차이는 다양한 측면에서 제시되고 있는데, 업무 중

심 조직-인간관계 중심 조직 등 보다 다양한 조직 차원을 구분하여 분석한다면 유의미한 결과를 제시할 수 있을 것으로 판단된다. 셋째, 개인 특성 관점에서 대처유형이외에도 조절초점이론 등 다양한 관점에서 의사결정에 영향을 미치는 요인들이 있다. 개인의 특성과 조직의 특성을 다양한 관점에서 비교하고 의미를 제시한다면, 보다 심도 있는 정보보안 준수 방향을 제시할 수 있을 것으로 판단한다.

References

Ahmad, Z., Ong, T. S., Liew, T. H. and Norhashim, M. (2019). Security Monitoring and Information Security Assurance Behaviour among Employees, *Information & Computer Security*. 27(2), 165-188. DOI : 10.1108/ICS-10-2017-0073

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D. and Polak, P. (2015). What Do Systems Users have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors, *MIS Quarterly*, 39(4), 837-864.

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

Chou, H. L. and Chou, C. (2016). An Analysis of Multiple Factors Relating to Teachers' Problematic Information Security Behavior, *Computers in Human Behavior*, 65, 334-345. DOI : 10.1016/j.chb.2016.08.034.

Da Veiga, A. and Martins, N. (2017). Defining and Identifying Dominant Information Security Cultures and Subcultures, *Computers & Security*, 70, 72-94. DOI : 10.1016/j.cose.2017.05.002.

Endler, N. S. and Parker, J. D. (1994). Assessment of Multidimensional Coping: Task, Emotion, and Avoidance Strategies, *Psychological Assessment*, 6(1), 50-60.

Flores, W. R. and Ekstedt, M. (2016). Shaping Intention to Resist Social Engineering through Transformational Leadership, Information Security Culture and Awareness, *Computers & Security*, 59, 26-44. DOI : 10.1016/j.cose.2016.01.004.

Folkman, S. and Lazarus, R. S. (1985). If It Changes It Must Be a Process: Study of Emotion and Coping during Three Stages of a College Examination, *Journal of Personality and Social Psychology*, 48(1), 150-170.

Galluch, P. S., Grover, V. and Thatcher, J. B. (2015). Interrupting the Workplace: Examining Stressors in an Information Technology Context, *Journal of the Association for Information Systems*, 16(1), 1-47. DOI : 10.17705/1jais.00387.

Grand View Research. (2020). Cyber Security Market Size, Share & Trends Analysis Report By Component, By Security Type, By Solution, By Service, By Deployment, By Organization, By Application, By Region, And Segment Forecasts, 2020 - 2027.

Guo, K. H., Yuan, Y., Archer, N. P. and Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model, *Journal of Management Information Systems*, 28(2), 203-236. DOI : 10.2753/MIS0742-1222280208.

Higgins, J. E. and Endler, N. S. (1995). Coping, Life Stress, and Psychological and Somatic Distress, *European Journal of Personality*, 9(4), 253-270.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational

Culture, *Decision Sciences*, 43(4), 615-660. DOI : 10.1111/j.1540-5915.2012.00361.x.

Ifinedo, P. (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.

Jung, H. S. and Yoon, H. H. (2015). Understanding Regulatory Focuses: The Role of Employees' Regulatory Focus in Stress Coping Styles, and Turnover Intent to a Five-star Hotel, *International Journal of Contemporary Hospitality Management*, 27(2), 283-307. DOI : 10.1108/IJCHM-07-2013-0288.

Kim, J., Kim. K. and Park, H. (2018). The Impact of Family-Friendly Corporate Culture on Employees' Behavior, *Journal of the Korea Industrial Information Systems Research*. 23(2), 75-92. DOI : 10.9723/jksiis.2018.23.2.075.

Kim, S. S. and Kim, Y. J. (2017). The Effect of Compliance Knowledge and Compliance Support Systems on Information Security Compliance Behavior, *Journal of Knowledge Management*. 21(4), 986-1010. DOI : 10.1108/JKM-08-2016-0353.

Loch, K. D., Carr, H. H. and Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding, *MIS Quarterly*, 16(2), 173-186. DOI : 10.2307/249574.

Mamonov, S. and Benbunan-Fich, R. (2018). The Impact of Information Security Threat Awareness on Privacy-Protective Behaviors, *Computers in Human Behavior*, 83, 32-44. DOI : 10.1016/j.chb.2018.01.028.

Mannix, E. A., Neale, M. A. and Northcraft, G. B. (1995). Equity, Equality, or Need? The Effects of Organizational Culture on the Allocation of Benefits and Burdens, *Organizational Behavior and Human Decision Processes*, 63(3), 276-286. DOI : 10.1006/obhd.1995.1079.

Markus, H. R. and Kitayama, S. (1991). Culture and the Self: Implications for Cognition, Emotion, and Motivation, *Psychological Review*, 98(2), 224 - 253. DOI : 10.1037/0033-295X.98.2.224.

Medvene, L. J., Teal, C. R. and Slavich, S. (2000). Including the Other in Self: Implications for Judgments of Equity and Satisfaction in Close Relationships, *Journal of Social and Clinical Psychology*, 19(3), 396-419. DOI : 10.1521/jscp.2000.19.3.396.

Merhi, M. I. and Ahluwalia, P. (2019). Examining the Impact of Deterrence Factors and Norms on Resistance to Information Systems Security, *Computers in Human Behavior*, 92, 37-46. DOI : 10.1016/j.chb.2018.10.031.

Nunnally. J. C. (1978). *Psychometric Theory* (2nd ed.). New York: McGraw-Hill.

Park, E. H., Kim, J. and Park, Y. S. (2017). The Role of Information Security Learning and Individual Factors in Disclosing Patients' Health Information, *Computers & Security*, 65, 64-76. DOI :10.1016/j.cose.2016.10.011.

Park, K. (2019). A Study on the Influence of the Perception of Personal Information Security of Youth on Security Attitude and Security Behavior, *Journal of the Korea Industrial Information Systems Research*, 24(4), 79-98. DOI : 10.9723/jksiis.2019.24.4.079.

Posey, C., Roberts, T. L. and Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems*, 32(4), 179-214. DOI : 10.1080/07421222.2015.1138374

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and Prevention-based Model to Mitigate Information Security

Insider Threats in Organisations, *Future Generation Computer Systems*, 97, 587-597. DOI : 10.1016/j.future.2019.03.024.

Siponen, M., Mahmood, M. A. and Pahnila, S. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study, *Information & Management*, 51(2), 217-224. DOI : 10.1016/j.im.2013.08.006.

Soh, H. and Kim, J. (2017). Influence of Information Security Activities of Financial Companies on Information Security Awareness and Information Security Self Confidence : Focusing on the Mediating Effect of Information Security Awareness, *Journal of the Korea Industrial Information Systems Research*, 22(4), 45-64. DOI : 10.9723/jksiis.2017.22.4.045

Sommestad, T., Karlzén, H. and Hallberg, J. (2015). The Sufficiency of the Theory of Planned Behavior for Explaining Information Security Policy Compliance, *Information & Computer Security*. 23(2), 200-217. DOI : 10.1108/ICS-04-2014-0025.

Triandis, H. C. (1995). *Individualism and Collectivism*, Boulder, CO: Westview Press.

Vance, A., Siponen, M. and Pahnila, S. (2012). Motivating IS Security compliance: Insights from Habit and Protection Motivation Theory, *Information & Management*, 49(3-4), 190-198. DOI : 10.1016/j.im.2012.04.002.

Verizon. (2020). Data Breach Investigations Report.

West, R. (2008). The Psychology of Security, *Communications of the ACM*, 51(4), 34-40. DOI : 10.1145/1330311.1330320.

Yazdanmehr, A. and Wang, J. (2016). Employees' Information Security Policy Compliance: A Norm Activation Perspective, *Decision Support Systems*, 92, 36-46. DOI : 10.1016/j.dss.2016.09.009.

황 인 호 (Inho Hwang)

- 정회원
- 건국대학교 경영학과 경영학사
- 중앙대학교 경영학과 경영학석사
- 중앙대학교 경영학과 경영학박사
- 국민대학교 교양대학 조교수
- 관심분야: IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야 등