Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 5 pp. 538-547, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.5.538
ISSN 1975-4701 / eISSN 2288-4688

정보윤리 활동에서 개인의 낙관적 편견과 정보보안 인식 및 정보보안 행위와의 관련성에 관한 실증 연구

최종근[1], 채명신[2*]
[1]서울벤쳐정보대학원대학원 정보경영학부, [2]서울벤쳐정보대학원대학원 융합산업학부

An empirical study on the relationship of personal optimistic bias and information security awareness and behavior in the activity of information ethics

Jong-Geun Choi[1], Myung-Shin Che[2*]
[1]Division of Management Information, Seoul Venture University
[2]Division of Fusion Industry, Seoul Venture University

요 약 정보보안 인식 및 행위에 미치는 요소와 관련하여 심리학에서 사용되는 개념인 낙관적 편견과의 연관성에 대한 연구가 활발하다. 즉, 개인이 가진 낙관적 편견이 정보윤리 활동에 얼마나 어느 분야에 영향을 미치는 가를 알아보는 것이다. 이러한 점에서 본 연구는 개인의 낙관적 편견과 정보보안 인식 및 정보보안 행위와의 관련성을 실증해 보았다. 국내 민간기업 종사하는 111명을 대상으로 설문조사한 결과, 개인의 보안관련 경험적 요인으로 인해 개인별 낙관적 편견이 존재하며, 낙관적 편견은 정보보안 인식에 영향을 미치며, 낙관적 편견이 많을수록 정보보안에 대한 인식은 부(-)의 영향을 미침으로서 정보보안 인식이 낮아진다는 것을 확인하였다. 즉, 낙관적 편견이 정보보안 인식에 영향을 미치며, 낙관적 편견을 줄이는 활동을 함으로써 정보유출 등 정보보안 사고를 줄이는데 기여할 것으로 판단된다. 그러나, 정보보안 인식을 제고시키는데 낙관적 편견이 조절효과를 보여줄 것으로 판단되었어나 그 조절효과를 보여주지 못하였다. 그 이유는 낙관적 편견관련 건강분야 연구와 달리 IT분야는 선행연구가 부족하여 구체적인 조절 요인을 제시하는데 어려움이 있는 등의 한계점이 제시되었다.

Abstract With respect to the factors affecting information security awareness and behavior, the study of the relevance of the concept of optimistic bias is actively used in psychology. In other words, this study examines whether the optimistic bias of individuals affects information security in the field. In this sense, this study attempted to demonstrate the relevance of optimistic bias in information security behavior and awareness. A questionnaire survey was conducted targeting 111 people engaged in domestic private enterprises. The survey results showed that this personalized optimistic bias exists because of empirical factors related to personal security. Optimistic bias affects the security awareness information. The greater the optimistic bias, the lower the awareness and recognition of information security. In other words, optimistic bias affects information security awareness. Reducing the effects of optimistic bias is expected to reduce information security incidents, such as information leakages. However, the variety of information related ethical activities of a company did not have any effect on the information security awareness. Most previous studies have only examined the effect optimistic bias in the field of health. Therefore, this study fills an important gap in research in IT.

Keywords : Information Ethics, Information Security, nformation Security Activisity, Information Security Awareness, Optimistic Bias

*Corresponding Author : Myungsin Chae(SVU)
Tel: +82-2-3470-52667 email: mlee31@anver.com
Received April 6, 2016 Revised (1st April 25, 2016, 2nd May 11, 2016)
Accepted May 12, 2016 Published May 31, 2016

1. 서론

정보화 사회는 정보의 공유를 원활하게 보장하여 업무의 효율화와 생산성 향상에 많은 기여를 하고 있으나, 또 다른 한편으로는 정보를 취급하는 과정에서 부정조작이나 파괴, 변조, 오용,불법복제, 음해 및 신상정보 유출과 같은 역기능으로 인한 피해가 급격하게 증가하고 있다.

2014년 1월 카드사에서 1억 건이 넘는 고객의 개인정보가 유출되어 사회적인 문제로 번졌음에도 불구하고 아직도 같은 문제가 되풀이 되고 있다는 점에서 정보보안에 대한 우려는 더욱 증폭되고 있다.

하지만 아직도 기업에서의 정보보안에 필요한 솔루션 도입수준은 상승되고 있지만 여전히 낮은 편이다. 이에 대해 정보보안에 대한 인식의 부족이 가장 큰 문제점이라고 지적이 많이 보인다. 일반적으로 사람들은 자신이 정보보안에 대한 위협을 처할 가능성이 적다고 인식한다. [1]은 이렇게 사람들이 자신들이 부정적인 상황에 처할 가능성에 대하여 다른 사람에 비해 낮다고 믿는 경향을 보이는 것을 낙관적 편견(optimistic bias)이라 칭하였다. 정보보안에 대한 낙관적 편견은 정보보안에 대한 불감증의 주원인이 된다고 할 수 있다. 이미 오래전에, [2]은 보안 관리자들조차도 외부 네트워크들의 확대가 그들의 정보시스템에 큰 위협이 된다고 확신하였지만 자신들이 그것을 자신의 일로서는 큰 관심을 보이지는 않는 낙관적 편견의 문제점을 지적하였다.

이에 본 연구는 기업의 정보 및 개인정보 유출 등 각종 침해사고를 발생시키는 문제를 해결하기 위해서는 기업차원의 정보보호활동이 전개함과 아울러 개인차원의 정보보호 관련 낙관적 편견을 줄이는 활동도 병행되어야 한다는 전제하에 다음과 같은 목적으로 연구를 하고자 한다.

첫째, 기업의 정보윤리 활동에서 개인이 소유한 낙관적 편견이 정보보안 인식에 영향을 미치는지 검증한다. 둘째, 기업의 정보윤리 활동들이 기업의 정보보안인식 제고 및 정보보안 행동에 영향을 미치는지를 검증하고자 한다. 셋째, 정보윤리 활동이 정보보안 인식에 영향을 미치는데 있어서 낙관적 편견이 이를 조절하는지를 검증하고자 한다.

2. 이론적 배경

2.1 정보윤리 활동과 정보보안 인식

정보윤리는 기업의 정보를 운영함에 있어 각종 정보가 부당하게 유출, 변조되는 것을 방지하고 정보시스템을 정상적으로 운영되는 것을 방해하는 요인들을 차단하기 위한 기업 차원의 조직적, 기술적 활동"이라 정의할 수 있다[3,4].

정보보호 분야 국제 표준인 ISO 27001는 정보보호 관리체계를 전반적인 경영시스템의 일부로 검토, 유지 및 개선하기 위한 시스템으로 정보보호 조직, 정책, 계획 활동, 책임, 실무 절차, 프로세스 및 자원을 포함하여 총 11개 분야의 통제 항목을 제시하고 있다. 국내의 정보보호 표준인 KISA ISMS의 정보보호 관리체계는 조직의 적절한 정보보호를 위해 정보보호 관리과정을 통해 구현된 여러 정보보호대책들이 유기적으로 통합된 시스템으로 정의하며, 활동 항목으로 정책, 교육 및 훈련, 물리적 보안 등 15개 통제 항목을 제시하고 있다.

이처럼 정보 보안 제고를 위한 정보 윤리 활동의 영역/요인들에 대하여 학자들 사이에 활발한 논의가 있었다. 정보보안 관련 연구들은 대개 초기에는 주로 기술적 차원에서 집중적으로 연구가 되었다 정보기술을 활용함에 있어 발생하는 윤리적 의사결정으로 정보보안 시스템을 구축하여 기술적으로 안전한 환경을 만들어 주는 것이 조직에서 정보윤리를 지키기 위한 중요한 활동으로 인식되었다[5].

그러니 정보보안 기술자체가 조직의 정보자원을 보호해 줄 수 없으며 조직의 정보자원을 보호하기 위해서는 정보보안 기술 개발에 많은 투자를 하더라도 조직 구성원의 정보보안에 대한 충분한 인식과 인지를 하지 않고 있다면 효과적인 정보보안은 달성될 수 없다는 인식이 점차 대두되기 시작하면서 조직적/ 관리적 차원의 활동의 중요성이 강조되었다[6].

조직적 요인 대하여는 조직의 정보보안 정책수립, 교육훈련, 조직구성, 평가 및 통제의 요소를 정보보안 관리요소의 중요성이 강조되었다 [7,4]. 특히 많은 학자들이 보안 담당자와 조직원의 보안에 대한 인식 수준 향상의 중요성을 강조하였으며, 정보 보안 교육과 그 교육담당자들의 인식수준 향상을 위한 교육의 중요성 또한 강조되었다[5,8].

하지만 같은 교육 프로그램을 받더라도 개인마다 인

식의 차이가 나게 된다. 기본적으로 본인은 정보 보안 관련 문제가 생기지 않을 것이라는 낙관적 편견이 만연한 가운데 정보보안관련 사고를 직간접으로 경험한 사람은 좀 더 보안에 대한 인식이 높은 것으로 나타났다. [9]는 기업내의 정보보안은 보안정책을 잘 준수하고 이에 따른 개인적 특성과 보안의식 수준이 향상되었을 때 안전한 보안효과를 거둘 수 있다는 것이다. 위와 같이 기업의 정보보안활동과 위에서 살펴 본 윤리경영활동과 정보보안 관리에 과한 선행 연구 고찰을 바탕으로 기업(조직)의 정보보안 활동요소를 Table 1 과 같이 도출하였다.

Table 1. Factor of Information Ethics Activity

variables	Operational definition	References
Org-factor	**Information ethics policy :** Establishment of information ethics policy in accordance with the objectives of information ethics in organization	[10]
	The education system of information ethics : Continuing education and training system on information ethics	[11]
	Information ethics control : Official surveillance, compensation and process of disciplinary punishment for the correct information ethics activities	[3]
	Information ethical commitment of the CEO : Recognition of the importance, care and support for the activities of information ethics of the Chief Executive Officer	[12]
Technical factor	**Information leakage prevention system:** Security measures and systems for internal information leakage prevention	[3]
	Data Backup system: The system of backup and control to database	
Ind- factor	**The past experiences of individuals :** An experience in the past related to information security	[13]

이상의 연구들을 살펴보면 조직의 정보윤리에 관련된 활동이 조직구성원의 정보보안 인지에 영향을 준다는 것을 알 수 있으며 다음과 같이 연구가설 H1, H2을 설정하였다.

가설 H1: 정보윤리 활동의 조직적 요인은 정보보안 인식에 정(+)의 관계에 있다.

가설 H2: 정보윤리 활동의 기술적 요인은 정보보안 인식에 정(+)의 관계에 있다.

2.2 낙관적 편견

정보보안의 행동에 미치는 중요한 심리적 성향으로서 이 연구에서 주목하고자 하는 것은 바로 '낙관적 편견(optimistic bias)'이다.

어떤 상황이 일어날 개연성에 대한 확신의 정도는 인지적인 요인 보다는 동기유발적인 요인들, 즉 방어적인 태도나 낙관적인 관측, 평가자의 선호도에 의해 결정된다. 그 중 하나의 유력한 동기부여 요인은 일어날 상황에 대한 바람 정도이다. 사람들은 본인에게 불리한 결과가 일어날 확률을 낮게 책정하는 반면 자신들에게 유리한 결과가 일어날 사건에 대해 그 확률을 높게 보는 경향이 있다. 이런 현상을 비현실적인 낙관, 낙관적 편견[14], 또는 자기선호적인 편견(self-favoring bias: [15])이라 정의한다. 사람들은 이러한 구조적 편견을 지니고 모호한 정보나 불확실한 상황을 자기에게 유리한 방향으로 해석한다.

낙관적 편견은 학교폭력에 관한 문제[16,17]. 기업위기에 관한 인식조사[18]나 탄저균 테러를 주제로 한 기업체 연구[19]와 같은 현상을 설명하는 등 다양하게 적용되었다.

IT에 관련하여 낙관적 편견은 e-File 시스템의 수용 및 e-Commerce에서의 프라이버시 보호 문제와 관련하여 논의 된 바 있다[20]. 정보보호와 관련하여 [21]은 정보보호 분야에 처음으로 낙관적 편견과 적용시켜 이 영역에 있어 사용자들의 낮은 보안의식을 논의하였다. 그들은 보안 인식에 있어 동료 및 모르는 일반인 그룹을 비교 대상으로 하여 설문 대상자들이 자신들의 보안 위험 가능성을 비교 대상 그룹들보다 낮게 평가함을 실증하였다.

2.2.1 개인의 경험과 낙관적 편견

한편 개인별 낙관적 편견의 차이에는 개인의 경험이 주 요인으로 밝혀져 있다. [22]는 홍수나 범죄 등의 위험을 경험한 적이 없는 사람들은 위험 경험이 있는 사람들에 비해 낙관적 경향을 보인다고 하였다. 또 이러한 경험을 했던 사람들은 그렇지 않은 사람들에 비해 위험이 더 자주 일어난다고 생각하는 것으로 나타났다. 즉 어떤 위험에 대해 과거의 경험이 있는 경우 어떠한 상황에서는 과거의 경험이 위험인식을 낮춰주고, 어떠한 상황에서는 위험인식을 높여준다는 것이다. 사람들마다 위험인식에 다르게 보는 이유는 위험인식에 다른 낙관주의 경향이다. 이상의 연구들을 살펴보면 개인이 과거의 경험에 따라 낙관적 편견이 있다는 것을 알 수 있으며 다음과 같이 가설을 설정하였다.

가설 H3: 정보윤리 활동관련 개인 경험은 낙관적 편견에 부(-)의 관계에 있다.

2.2.2 낙관적 편견과 정보보안인식

정보보안인식은 단순히 다양한 정보보안에 위협이 되는 요소를 이해하는 데서 결정되는 것이 아니라 이 위협적 요소에 대하여 얼마나 개인이 민감하게 반응을 하는지에 따라 결정된다고 할 수 있다. 이는 마치 흡연이 암을 유발한다는 것을 누구나 다 아는 사실이지만 개개인이 금연을 하는 등 미리 방지 활동을 하도록 동기화시키는 것은 그러한 부정적인 사건 (암에 걸리는 것)이 자신에게 일어날 수도 있다는 것을 얼마나 높게 인식하는가에 달려 있다. 현재 정보보안 관련 연구에서 사용자의 보안 불감증이 정보보안 사고의 가장 큰 문제점이 된다고 지적 되어 왔다. 이 불감증의 주 원인은 자신들이 부정적인 상황에 처할 가능성에 대하여 다른 사람에 비해 낮다고 믿는 경향을 보이는 낙관적 편견(optimistic bias)이에 있다고 할 수 있다.

예전부터 위험 (건강, 안전 등)을 인식하는데 있어 낙관적 편견의 영향은 충분히 입증이 되어 있다. 아직 정보보안과 낙관적 편견의 직접적인 영향에 대한 연구는 충분하지 않다고 할 수 있지만 낙관적 편견과 IT 위험(risk)과 인식 관계에 대하여 꾸준히 연구되고 있다고 할 수 있다.

[23]는 일반인 대상의 설문 조사를 통해서 사람들이 IT사용에 있어 위험스러운 상황이 자신보다는 친구에게 또는 다른 사람들에게 일어날 확률을 훨씬 더 높을 것으로 인식하고 있음을 보고하였다. [24의 정보 관리 부서의 메니저들을 인터뷰한 결과, 관리자들은 정보보안에 대한 인식의 부족이 가장 큰 문제점이라고 지적을 스스로 하였으면서도 그 중에 사용자들의 정보보호의식을 높이고 그에 대한 교육과 실습을 제공하는 것을 최우선 아젠다로 설정한 사람들은 28%에 불과하였다고 보고하고 있다. 이는 그들이 자신이 정보보안에 대한 위협을 처할 가능성이 적다고 인식하는 것을 의미한다.

[25]의 설문결과 또한 유사하게 정보보안의 위험에 대하여 사람들은 실제보다 작게 평가하는 경향이 있음을 보여준다. 먼저 저자들은 응답자들의 정보보안에 대한 인식과 지식에 대하여 인터뷰를 한 후 그들이 사용하는 컴퓨터에서 정보보안 장치- 방화벽(Firewall) 세팅이나, 바이러스 백신 등 - 들을 제대로 사용하고 있나 조사하였다. 이 연구 결과는 사람들이 그 자신의 컴퓨터가 바이러스에 감염될 수 있는 가능성에 대하여 매우 낮게 평가하고 있음을 알 수 있다. 나아가 [26]은 e-filing 시스템을 사용하려는 의도에 개인적인 요인으로 시스템 위험에 대한 낙관적 편견이 영향을 미침을 실증하였다. 이처럼 정보보안 인식에 낙관적 편견이 영향요인이 될 수 있는 개연성은 충분하다고 할 수 있다. 따라서 다음과 같은 가설을 설정한다.

가설 H4:조직원 개인의 낙관적 편견은 조직원들의 정보보안 인식에 부(-)의 관계에 있다.

2.3 정보보안 인식과 정보보안 행동

조직구성원이 책임감 있는 정보보안 행위를 할 수 있는 정보보안 교육 및 훈련이 되기 위해서는 실제 행동에 영향을 미치는 행동의도, 그리고 태도의 변화까지 고려되어야 한다. 인지가 인간의 정서와 행동을 좌우한다는 인지행동이론과 사회학 관점의 의도기반모형을 적용하여 정보보안 행동과 정보보안 인식과의 관계가 많이 증명되었다[4]. 나아가 정보보안에 대한 구성원의 인지적인 차원과 행태적인 차원에서 차이가 있다는 규명하였으며[7]은, 인간의 인지적 차원과 행태적 차원의 격차를 통해 정보보안과 관련된 조직 내 구성원의 정보보안 실천 정도를 파악하였다[29].

연구결과, 조직구성원의 정보보안행동을 유도하는 중요한 요인은 정보보안에 대한 인식이고 이 인식은 개인의 정보보안에 대한 태도, 동기부여, 도덕, 믿음, 윤리, 개인적 특성 등이 서로 영향을 주고받기는 하지만 정보보안인식과 정보보안실천 사이의 관계가 직접적으로 유의하다는 것은 충분히 증명되었다[30]. 따라서 본 연구는 다음과 같은 가설 H5를 설정하였다.

가설 H5: 정보보안 인식은 정보보안 행위에 정(+)의 관계에 있다.

2.4 정보윤리 활동과 낙관적 편견의 조절효과

정보보안을 인식하고 행동을 결정하는 과정에서 여러 가지 요인들이 복합적으로 작용 한다.

[1]은 비현실적 낙관주의 그룹은 위험요소에 대한 사전지식을 적게 가지고 있다는 것을 밝혔다. 뿐만 아니라 그들은 자신들이 그 정보에 대한 지식이 적다는 사실을 믿으려 하지 않으려는 모습을 보였다. 조직적인 정보 윤리 활동을 개인적인 차원에서 흡수하는 정도는 다를 수

있다. 위의 연구 결과를 적용하여 볼 때, 조직의 정보보안 정책이나 교육 그리고 기술적 시스템을 구비하여 보안을 강화시키더라도 그로 인한 보안에 미치는 인식은 낙관적 편견이 높은 직원과 편견이 낮은 직원사이에 차이가 날 수 밖에 없다.

따라서 이상의 논의에 기반하여 본 연구에서는 개인의 낙관적 편견이 정보윤리 활동의 조직적, 기술적 요인 정도에 따라 정보보안 인식을 조절하는 효과와 관련해서 다음과 같은 가설 H6, H7을 설정하였다.

가설 H6 : 조직구성원의 정보보안에 대한 낙관적 편견은 정보윤리 활동의 조직적 요인이 정보보안 인식에 미치는 영향을 조절할 것이다. 즉 조직구성원들의 낙관적 편견 정도가 높을수록 조직적 요인이 정보보안 인식에 미치는 영향은 적을 것이다.

가설 H7 : 조직구성원의 정보보안에 대한 낙관적 편견은 정보윤리 활동의 기술적 요인이 정보보안 인식에 미치는 영향을 조절할 것이다. 즉 조직구성원들의 낙관적 편견 정도가 높을수록 기술적 요인이 정보보안 인식에 미치는 영향은 적을 것이다.

위의 가설들을 정리하면 Fig 1과 같이 모형화할 수 있다.

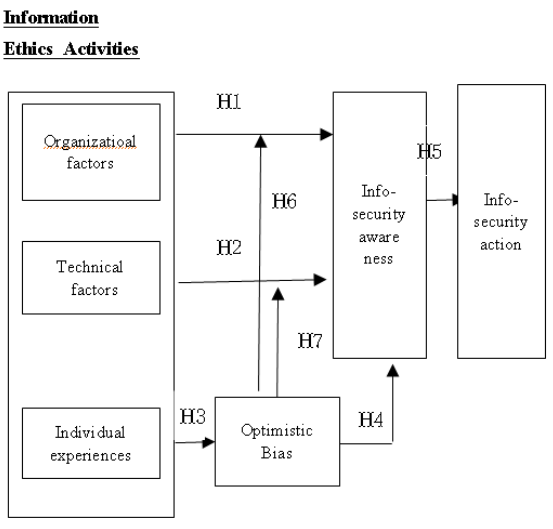

Fig. 1. Research Model

3. 연구 설계 및 방법론

3.1 주요 변인의 조작적 정의 및 측정도구

본 연구에서 정보윤리 활동은 기업에서의 정보를 보호하기 위한 제반 활동으로 영향요인은 측정방법에 따라 많은 요인이 있지만 선행연구에서 다루어졌던 변수들과 기업 구성원의 특성을 고려하여 크게 조직적 요인, 기술적 요인, 개인적 요인으로 선정하였으며 그 구체적인 조작적 정의와 관련 문헌은 Table 1과 같으며 총 22문항을 개발하였다.

추가적으로 낙관적 편견은 자신이 속한 기업체가 정보보안위험에 처할 확률이 같은 산업의 다른 업체보다 낮게 측정하는 것을 의미한다. 대부분의 낙관적 편견에 대한 선행연구에서는 타인이 부정적인 상황을 경험할 개연성에 대한 추정치를 뺀 값으로 계량화되며 그 값이 0보다 크면 낙관적 편견이 있다고 보았다. [18]이 사용한 낙관적 편견 측정문항에서 6문항을 개발하였다.

정보보안 인식은 정보보안에 대한 중요한 자각 및 정보보안활동에 대한 관심정도로 조작적 정의 하였으며, [6]연구에서 제시하고 있는 항목들을 참고하여 정보보안의 필요성, 정보보안의지, 정보의 가치, 정보보안의 실행의지, 정보보안의 이해정도 등을 평가하는 개념으로 총 10문항을 개발하였다.

정보보안행동은 정보보안에 대한 기술적, 관리적, 제도적 행태로 정의하였으며, [6]의 설문과 [4]의 설문을 일부 수정하여 총 11항목으로 개발하였다.

3.2 자료수집

본 연구는 2014년 8 월에 6주일에 걸쳐 중견기업 30개 업체에 종사하는 구성원 200명을 대상으로 문서 또는 E-mail로 설문을 실시하였다. 설문결과 121부가 회수되었으며, 이 중 응답이 비논리적이거나 지나치게 불성실한 10부를 제외한 111부가 분석에 사용되었다.

4. 가설 검증 및 논의

4.1. 표본의 특성

설문조사결과 기업의 업종은 정보통신업(83%)의 비율이 가장 높았으며, 공공기관이 4%로 나타났다. 기업규모는 500명 미만의 기업이 전체 85%를 차지하고 있으

며, 5,000명 이상의 규모는 12%로 나타났다. 근무 년 수는 10년 이상(29%)이 가장 많았으며 직위는 과장급(38%), 대리급(24%), 부장급(18%) 등의 순서로 나타났다. 마지막으로 정보시스템이나 IT 업무와의 관련성에 대해 질문을 하였는데 관련성이 있다는 대답이 68%, 관련이 없다는 대답이 32%로 나타났다.

4.2 측정도구의 신뢰성과 타당성 검증

신뢰성은 측정변인에 대한 문항들의 내적일관성을 측정하는 Cronbach α로 검증하였다. Table 2에서 보듯이 변인들은 와 같이 모두 0.7이상으로 신뢰성을 인정받았다.

Table 2. Exploratorry Factor Analysis Result

Q	factors					α
	1	2	3	4	5	
org-1	.128	**.771**	.042	.262	.089	.965
org-2	.108	**.788**	-.060	.154	.107	
org-3	.051	**.862**	.089	-.015	.084	
org-4	.097	**.844**	.090	.125	.055	
org-5	.290	**.741**	.204	.059	.088	
org-6	.083	**.829**	.194	.052	-.032	
org-7	.018	**.882**	.115	.077	.096	
org-8	.077	**.836**	.126	.159	-.103	
org-9	.104	**.727**	.094	.179	-.083	
org-10	.067	**.761**	.231	.108	-.047	
org-12	.178	**.785**	.079	.224	-.054	
org-13	.140	**.784**	.023	.348	-.034	
tec-1	.237	.511	-.044	**.683**	.048	.913
tec-2	.151	.590	-.049	**.597**	.113	
tec-3	.236	.453	-.014	**.618**	-.030	
tec-4	.089	.356	.085	**.753**	-.109	
tec-5	.097	.351	.160	**.757**	.133	
exp-1	.084	.195	**.823**	.015	-.022	.919
exp-2	.023	.116	**.922**	.008	-.020	
exp-3	.002	.204	**.884**	.013	.028	
exp-4	.026	.185	**.857**	.110	.027	
awa-1	**.873**	.189	.048	.020	-.184	.985
awa-2	**.918**	.170	.000	.011	-.110	
awa-3	**.921**	.124	-.006	.032	-.162	
awa-4	**.935**	.134	.031	.009	-.107	
awa-5	**.931**	.107	.027	-.004	-.109	
awa-6	**.893**	.185	.074	.001	-.089	
awa-7	**.957**	.048	-.047	.025	-.027	
awa-8	**.946**	.033	-.008	.010	-.111	
awa-9	**.928**	.099	.013	-.008	-.130	
awa-10	**.928**	.099	.035	.014	-.113	
action1	.459	.145	.001	-.142	**.759**	.971
action2	.448	.043	-.079	.060	**.773**	
action3	.270	.040	.038	.272	**.819**	
action4	.344	.112	.015	.212	**.807**	
action5	.260	.269	.083	.193	**.795**	
action6	.149	.094	.013	.178	**.871**	
action7	.321	.088	-.015	.195	**.823**	
action8	.181	.068	.041	.260	**.857**	
action9	.350	.149	.114	.320	**.705**	
action10	.306	.234	.200	.241	**.725**	
action11	.102	.027	.033	.122	**.867**	

Table 3. Exploratorry Factor Analysis Result of Optimistic Bias

Measurement Items	factors		α
	1	2	
Bias_Self1	.276	**.883**	.814
Bias_Self2	.230	**.880**	
Bias_Self3	.467	**.640**	
Bias_Others1	**.880**	.238	.891
Bias_Others2	**.911**	.262	
Bias_Others3	**.843**	.218	

연구에서는 낙관적 편견 변인은 따로 신뢰성과 타당성 검증을 하였다. 이는 그 변인이 다른 변인들과는 달리 같은 내용인데 본인에 대한 인식과 타인에 대한 인식으로 구분되는 형식이라 일반적으로 연속적인 성격을 띤 다른 측정항목들과는 그 측정항목의 속성이 다르기 때문이다. 낙관적 편견을 제외한 다른 변인들의 타당성 검증 결과는 Table 2 와 같다.

한편, 낙관적 편견의 항목들의 집중타당성은 본인에 대한 인식 문항과 타인에 대한 인식문항이 서로 구분되어 묶이는지 확인하였으며 그 결과는 Table3과 같다 본인에 대한 인식은 요인 2에 모두 0.6 이상이며, 타인에 대한 인식은 요인 1에 0.8 이상으로 두 변인이 서로 구분됨을 보여주었다.

4.3 상관관계 분석

독립변수와 종속변수의 상관관계는 높은 상관관계를 보이면서 유의함으로 두 변인 사이에 설정한 가설에서와 같이 인과관계가 성립할 가능성이 높다. 아래의 Table 4에서 보듯이 조직적 요인, 기술적 요인, 개인적 요인의 상관관계는 유의하면서 0.4 이하로 높지 않다고 할 수 있다. 한편 이들 변수들과 인식과의 관계는 모두 유의하지만 조직적 요인만이 높은 상관관계를 보여주고 있다. 한편 인식과 행동과의 상관관계는 매우 높다고 할 수 있다.

Table 4. Correlations

	Org	Tech	Exp	Awa
Org				
Tech	.258**			
Exp	.310**	.190*		
Awa	.502**	.266**	.305**	
Actions	.320**	.424**	320**	.855**

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

4.4 가설 검증

본 연구의 개념적 모형에서 매개 역할을 하는 낙관적 편견이 명목척도 (있다= 1 없다 =0) 인 관계로 구조방정식 모형을 적용하는 것 보다, 각 경로를 따로 검증하는 것이 데이터 분석에 왜곡이 막기에는 더 적당하다고 판단되어 연구의 가설검증은 세단계로 진행된다.

첫번째는 개인적 경험이 낙관적 편견의 선행요인이 되고(가설 3) 낙관적 경험은 조직적, 기술적 정보윤리활동과 같이 정보보안 인식에 영향을 주는 것으로 가설이 설정됨에 따라 (가설 1, 2, 4) 가설 검증 순서는 H3을 제일 먼저 하게 된다. H3 검증은 종속변수가 이분형이므로 (낙관적 편견 낮음=0, 낙관적 편견 높음=1)이므로 로지스틱 회귀분석을 사용하여 검증한다.

두 번째 단계는 H1, 2, 4에서 설정된 관계에서 낙관적 편견의 조절효과를 검증하는 것이 H 6, 7 이므로 H 1, 2, 4, 6, 7이 동시에 검증된다. 이를 위하여 위계적 회귀분석이 적용된다. 이 경우 낙관적 편견은 더미변수로 처리된다.

마지막으로 H5가 검증되며 단순회귀분석이 사용된다. Table 5는 가설검증단계를 요약하여 보여준다

4.4.1 개인의 보안관련 경험과 낙관적 편견과의 관계 검증 (H3 검증)

앞에서 설명하였듯이 종속변수인 낙관적 편견의 유.무 (있다 =1 없다=0)로 이분항이었으므로 로지스틱회귀분석을 사용하여 검증하였다.

Table 4 에서 보듯이 모형적합도 측정을 chi-square와 Hosmer와 Lemeshow 검정을 하였다. chi-square는 상수항만으로 구성된 모형과 독립변수들이 포함된 모형의 적합도 차이의 유의성을 검증한 결과이다. 즉 독립변수들이 포함되었을 때의 로지스틱 회귀모형의 유용성을 보여준다. 이 표에서 모형은 포함된 모든 독립변수들의 계수가 0이라는 (즉 본 연구의 모형이 종속변수를 설명 예측하는데 유용하지 않다는 것을 의미) 영가설을 검증한 결과이다. 모형의 유의확률은 .000으로서 영가설이 기각된다. 따라서 모형에 포함된 독립변수들의 영향력은 0이라고 할 수 없으며, 모형은 유용하다고 할 수 있다.

Hosmer와 Lemeshow 검정의 카이제곱 값은 로지스틱 회귀모형의 전체적인 적합도를 나타내는 값이다. 즉 이 값은 종속변수의 실제치와 모형에 의한 예측치 간의 일치정도를 나타내는데, 그 값이 작을수록 모형의 적합도는 높다. 본 연구 모형의 경우 카이제곱 값이 1.732이고 유의확률은 .943으로 비유의적으로 나타났다. 여기서 그 값이 비유의적으로 나타났음은 종속변수의 실제치와 예측치간의 차이가 작으며 모형의 적합도가 수용할 만한 수준임을 나타낸다.

한편 아래의 Table 4 에 나타난 로지스틱회귀분석의 결과를 보면 경험의 부호가 (-)를 보여준다. 로지스틱 회귀분석에서는 변수의 계수의 부호가 (+)이면 그 변수의 값이 클 수로 내부 값이 1인 집단 (낙관적 편견이 있는 집단)에 속하고 (-)이면 내부 값이 0인 집단 (낙관적 편견이 없는 집단)에 분류될 가능성이 커진다. 그리고 계수의 유의성은 Wald로 판명한다. 회귀분석에서 t-값에 상응한다고 할 수 있다. 본 연구에서 경험은 낙관적 편견과 유의한 부의 관계를 가진다고 할 수 있다. 즉 보안 사고에 경험이 클수록 낙관적 편견이 적어진다고 할 수 있다. 따라서 가설 H3은 채택되었다.

Table 5. Logistic Regression Result

	B	S.E.	Wald	df	Sig.	Exp (B)
Experience	-.851	.274	9.621**	1	.002	.427
constant	1.361	.625	4.735*	1	.030	3.899
Model Fit		Chi-square		12.331(1) **		
		Hosmer and Lemeshow Test		Chi-square = 1.732 (1)		

*: p<.05, **: p<0.01

4.4.2 정보윤리 활동의 조직적 요인, 기술적 요인, 낙관적 편견이 정보보안 인식에 미치는 영향 (가설 H1, 가설 H2, 가설 H4 검증) 과 낙관적 편견의 조절효과 (가설 H6과 H7 검증)

낙관적 편견은 이분형 척도 (0과 1)를 사용하고 있었으므로 더미변수로 처리한 후 .위계적 회귀분석을 실시하였다. 모형1은 독립변인들 (조직적 요인과 기술적 요인)과 종속변인 (정보보안 인식)만을 투입하였으며, 모형 2에는 모형 1의 조절변수인 낙관적 편견이 더 투입되었다. 모형 3에는 모형 2에 각 독립변인과 조절변인의 상호작용 변인이 더 투입되었다. 그 결과는 Tabel 6에 정리 및 요약되어 있다.

F-검증한 결과 모든 모형은 회귀모형으로서 적합함을 알 수 있다.

Table 6. Hierarchial Regression Analysis

	Info- Security Awareness		
	model1	model 2	model3
(Constant)	1.357*** (3.108)	2.265*** (4.429)	1.070 (1.841)
Organization	.526.*** (3.188)	439*** (2.874)	.597*** (2.856)
Technology	057 (.386)	.240 (1.294)	.163 (.696)
Optimistic Bias		-.524.*** (-3.517)	-.667*** (-2.802).
Organization*Bias			-.026 (-.084)
Technology*Bias			-.153 (-.457)
R^2	.176	.177	.181
Adj-R^2	.161	.154	.141
F	11.337***	7.532***	4.550**
ΔR^2	.176	.001	.004

: p< 0.1, **: p<0.05, ***: p<0.01

검증결과 조직적 요인(β=.597 t=2.856)과 낙관적 편견이 (β=-.-.667 t=-2.802) 정보보안 인식과의 관계가 유의하나 기술적 요인은 그렇지 못함을 알 수 있다. 낙관적 편견은 계수의 부호가 (-)이므로 부의 관계를 이루고 있음을 알 수 있다. 즉 조직적 요인이 높을수록 정보보안에 대한 인식이 높아지고 낙관적 편견이 많을수록 정보보안에 대한 인식은 낮아진다는 것을 알 수 있다. 이로서 가설 H1과 H4는 채택되었고 가설 H2은 기각되었다.

낙관적 편견의 조절효과는 모형 2와 모형 3사이의 변화 정도가 유의하면 조절효과가 있다고 본다. 위의 Table 6 에서 보면 모형 2와 모형 3의 R^2 변화량은 .004로서 (p= .778) 변화량이 유의하지 않다. 따라서 낙관적 편견의 조절효과는 없다고 할 수 있다(가설 H6과 H7은 기각).

4.4.3 정보보안 인식이 정보보안행동에 미치는 영향 검증 (가설 H5 검증)

정보보안 인식과 정보보안 행동과의 관계를 단순회귀분석으로 검증하였다. 먼저 모형의 적합도를 검증한 결과 Table 7과 같이 r^2 =0.732로 상당히 높았다. 이는 전체 분산의 78%를 독립과 종속변인과의 회귀선이 설명하고 있다는 것으로 그 회귀선의 설명력이 상당히 높음을 알 수 있다. F-검증(F= 297.516, p= .000) 결과 유의한 것으로 분석되어 정보보안 인식과 정보보안 행동과의 관계는 선형회귀모형으로 적합하다고 할 수 있다.

한편 정보보안 인식은 정보보안과 유의한 정의 관계를 (β=-.808, t=-17.249) 가짐을 보여준다. 즉 정보보안 인식이 높을수록 정보보안 행동이 많아진다고 할 수 있다.

Table 7. Regression Analysis Results

Model	unstandardized		Standarized	t	Sig.
	B	S.E	Beta		
Constant	.222	.190		1.169	.245
Awar	.808***	.047	.855	17.249	.000
Model Fit	F=297.516 *** , R = .855, R^2 = .732, Adj R^2 = .729				

*: p< 0.1, **: p<0.05, ***: p<0.01

4.5 연구결과 요약

본 연구결과를 통해 조직의 정보윤리 활동이 정보보안에 영향을 미치는 것으로 확인되었다. 정보보안 분야에도 낙관적 편견이 존재하며 낙관적 편견이 정보보안 인식에 영향을 미치는 것으로 검증되었다.

첫째, 낙관적 편견의 조직원 개인의 정보보안 인식에 있어 역할이다. 가설 H3 과 H4에서검증결과에서 보듯이 개인의 경험은 바로 정보보안인식에 영향을 주지 않고 낙관적 편견의 매개를 통해 정보보안 인식에 영향을 주는 것으로 드러났다. 이는 개인적 요인을 다른 선행연구가 있기는 하였지만 낙관적 편견에 대한 언급은 드물었다. 통상 정보보안 분야에 근무를 많이 하는 경우에는 자신이 정보보안에 대한 통제감이 향상되어 낙관적 편견이 증가되지만 이들 중 정보보안 유출 사고를 경험한 개인은 낙관적 편견이 줄어들어서 정보보안 활동을 적극적으로 수행함을 알 수 있다.

둘째, 하지만 가설 H6, H7의 연구결과 정보윤리 활동의 조직적, 기술적 요인이 정보보안 인식에 영향을 미치는데 낙관적 편견의 조절효과는 유의하지 않았다. 이는 개인적인 요인보다는 조직적 관리 통제와 교육으로 조직 전체의 정보보안에 대한 인식을 충분히 제고 할 수 있음을 보여준다고 할 수 있다. 따라서 조직적인 노력은 개인적인 요인과 상관없이 조직 전체의 보안인식을 제고하는데 중요하다고 할 수 있다.

셋째, 가설 H2, H3의 검증결과에서 보듯이 정보윤리 활동의 조직적 요인은 정보보안 인식에 유의한 것으로 나타났다. 이는 기존의 연구와 동일한 결과로 정보보안유출을 예방하기 위해서는 CEO의 정책의지는 물론 보안유출을 막기 위한 교육 등 조직적인 다양한 활동을 전개해야 될 것이다. 기술적인 요인이 정보보안 인식에 정(+)의 영향을 미치는 것은 유의하지 않는 것으로 나타

났다. 이는 기업의 정책적인 측면과 달리 기술적인 측면은 기업 구성원들의 인식에 영향을 덜 주는 일반적인 통념의 일환으로 사료된다. 그리고 기술적인 면을 강화하다 보면 사용자들에게는 불편이 더해지는 경우도 많다. 조직에서 보안관련 시스템을 구축시 통제와 편리함 사이에 균형을 이루는 것이 큰 문제로 대두된 점은 기존의 연구에서 많이 연구되었으며 본 연구 결과 같은 맥락에서 이해될 수 있다.

5. 결론

본 연구의 결과는 기업이 정보를 효과적으로 관리하기 위해서는 조직 구성원들의 정보보안인식의 제고와 개인들이 소유한 낙관적 편견을 줄이는 것이 매우 중요하다는 것을 알 수 있다. 정보보안 분야에도 낙관적 편견이 존재하고, 낙관적 편견으로 인해 정보보안인식에 영향을 미치는 것으로 나타남에 따라 기업차원에서 개인의 심리적 차원인 낙관적 편견을 줄이는 활동을 병행한다면 보다 높은 정보보안 수준을 유지할 수 있음을 기대할 수 있다

낙관적 편견의 연구가 주로 건강분야에 수행되어온 반면 IT분야에 대한 선행연구가 미흡한 상태로 인해 본 연구는 다음과 같은 제한점이 있다.

첫째, 본 연구에서 필요한 자료를 기업 종사자 중 IT 분야 근무하는 사람을 대상으로 수집하여 분석함으로 인해 그 결과에 대한 일반화에 다소 제한적일 수 있다. 향후 업종별, 전 분야별 등으로 폭넓게 표본을 선정하면 더 의미 있는 연구가 될 수 있을 것이다.

둘째, 낙관적 편견의 연구가 주로 건강분야에 수행되어온 반면 IT분야에 대한 선행연구가 미흡한 상태로 인해 기업의 구성원들에게 낙관적 편견이 존재하고 이것이 정보보안 인식에 영향을 미치는지 여부를 확인하는 제한적인 연구가 되었다. 따라서 연구의 깊이를 더하기 위해 전문가 인터뷰나, 집중 관찰 그룹을 선정하여 그 행태적인 요인을 관찰하는 정성적 분석을 가미하는 후속 연구가 필요하다고 사료된다.

셋째, 낙관적 편견 존재 유무에 따른 기업 구성원들의 직능별, 직책별 등 분류 통한 그 낙관적 편견이 어떤 요원들에게 주로 생기는지에 관한 후속 연구를 진행하면 정보 분야의 보안성과를 제고하고 보안행위를 저해하는 또 다른 차원의 원인을 규명할 수 있을 것으로 판단이 된다.

이러한 제한점이 있지만 본 연구의 결과는 기업체의 정보보안을 위한 정보윤리 활동 계획을 구상하고 추진하는데 있어 효과적인 정보보안 관련 의사결정에 기여할 것으로 보인다.

References

[1] N. D. T. Weinstein and Klein, D. J.“Effects of Mood on High Elaboration Attitude Change: The Mediating Role of Likelihood Judgments. *European Journal of Social Psychology*, Vol. 24, No. 2, pp. 25-43, 1994.

[2] K. D. Loch, H. C. Houston and E. W. Merrill. "Threats to Information Systems: Today's Reality, Yesterday's Understanding." *Mis Quarterly*, Vol. 16, No. 2, pp. 173-186, 1992.

[3] The Federation of Korean Information Industries. Information Ethics andDigital Socity, 2005

[4] M. J. Back, “A Study on the Effect of Information Ethics on the Performance of Information Security in Organization”, *2010 Information Policy,* 2010

[5] M. Kabay, "Psychosocial Factors in the Implementation of Information Security Policy." *EDPACS: The EDP Audit, Control, and Security Newsletter,* Vol. 21. No. 10, pp. 1-10, 1994.

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

[7] N. Choi, D. Kim, and A. Whitmore, Knowing Is Doing, *Information Management & Computer Security*, Vol. 16, No. 5, pp. 484-501, 2008.

[8] E. Berkman, "How to Staff Up for Security." *CIO Magazine,* Vol. 15, 2002.

[9] J. G. Kim and D. Y. Kang, “The Effects of Security Policies, Security Awareness and Indivisual Characterics on Password Security Effctiveness.” *Institute of Security & Cryptolog*, Vol. 18, No. 4, pp.123-133. 2008.

[10] M. A. Pierce and J. W. Henry. "Computer ethics: The Role of Personal, Informal, and Formal Codes." *Journal of Business Ethics,* Vol. 15, No. 4, pp. 425-437, 1996.

[11] E. Cohen and L. Cornwell. "College Students Believe Piracy Is Acceptable." *CIS Educator Forum.* Vol. 1. No. 3. 1989.

[12] K. H. Hong and J. D. Kim. "National Standard on Information Security in ISO." *Institute of Security & Cryptolog* Vol. 14.No. 2 pp. 1-5, 2004

[13] J. Park, B. Kim and S. Joo, “Primary factors affecting corporate employees' attitudes toward information security,” The Studies of Management Vol. 40, No. 4, pp. 955-985, 2011년.

[14] N. D. T. Weinstein, “Unrealistic Optimism about Future Life Events,” *Journal of Personality and Social Psychology*, Vol. 39, No. 5, pp. 806-820, 1980.

[15] V. Hoorens "Self-favoring Biases for Positive and Negative Characteristics: Independent Phenomena?." *Journal of Social and Clinical Psychology* Vol. 15, No. 1 pp. 53, 1996.

[16] B.C.Kim and D.G. Lee. "Optimistic Bias in Crisis of Company," Core Association for AD & PR, Vol. 8, No. 2, pp. 82-105. 2006.

[17] J. R. Chapin, Optimistic Bias Regarding Campus Violence, *Current Research in Social Psychology*, Vol. 6, No. 16, pp. 237-251, 2000.

[18] M.J. Han "Optimistic Bias on the Crisis of Smoking healthy," Korean Association for Broadcasting & Telecommunication Studies, 1999.

[19] C. T. Salmon, H. S. Park, and B. J. Wrigley. "Optimistic Bias and Perceptions of Bioterrorism in Michigan Corporate Spokespersons, Fall 2001." *Journal of Health Communication,* Vol. 8. No. 1, pp. 130-143, 2003.

[20] A. Acquisti "Privacy in Electronic Commerce and the Economics of Immediate Gratification," *Proceedings of the 5th ACM conference on Electronic commerce*, New York, NY. pp. 21 – 29. 2004.

[21] H. S. Rhee, Y. Ryu, and C. T. Kim. "I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security." I*CIS 2005 Proceedings,* 2005.

[22] L. S. Perloff, Social Comparison and Illusion of Invulnerability to Negative Life Events, In Snyder. C. R. and Ford, C., *Coping with Negative Life Effects: Clinical and Social Psychological Perspectves on Negative Life Event.* Plenum Press. 1987

[23] L. Sjöberg, and J. Fromm, "Information Technology Risks as Seen by the Public" *Risk Analysis. Vol. 21*. No. 3, pp. 427 - 441, 2001.

[24] Ernst & Young "Global Information Security Service," White Paper, Ernst & Young, 2004

[25] AOL/NCSA. "AOL/NCSA Online Safe Study" Research Report, American Online and the National Cyber Security Alliance, October, 2004

[26] L. C. Schaupp and L. Carter " The impact of trust, risk and optimism bias on E-file adoption" Informatio" *Information Systems Frontiers*, Volume 12, Issue 3, pp299-309, 2010,

[27] C. H. Lim. "The method of Effective Information Security Awarness," *Institute of Security & Cryptolog*, Vol. 16, No. 2, pp. 30-35. 2006.

[28] T. Layton, *Information Security Awareness: the Psychology Behind the Technology,* Author House, 2005.

최 종 근(Jong-Geun Choi) **[정회원]**

- 2001년 2월 : 국방대학교 국방경영학과 (경영학석사)
- 2015년 8월 : 서울벤처대학원대학교 정보경영학과 (정보경영학박사)
- 2015년 1월 ~ 현재 : 육군 군수사령부 군수혁신TF장

<관심분야>
정보경영, 물류, e-Biz

채 명 신(Myungsin Chae) **[정회원]**

- 1994년 12월 : U of Texas at Austin, Instructional Technology (석사)
- 2003년 7월 : U of Illinois at Chicago, Management Information System (박사)
- 2004년 3월 ~ 현재 : 서울벤처 대학원 대학교 교수

<관심분야>
e-Biz, 모바일 비즈니스, FinTech