The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 6, pp.243-253, Dec. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2016.16.6.243
JIIBC 2016-6-32

통제수용자에 의해 인지된 정보보안정책 특성요인이 보안스트레스와 보안준수의도에 미치는 영향에 대한 연구

A Study on Influence of Information Security Stress and Behavioral Intention for Characteristic factors of Information Security Policy Perceived by Employee

임광수*, 권헌영**

Kwang-su Im*, Hun Yeong Kwon**

요 약 기업들은 중요한 지적 자산을 보호하고, 개인정보 유출과 같은 보안 사고를 예방을 위하여, 사내 보안 활동을 강화 하고 있다. 하지만, 이로 인한 구성원들의 보안스트레스는 점점 증가하고 있으며, 내부자에 의한 보안사고도 지속적으로 발생하고 있는 현실이다. 그리고 기업 내 다양한 정보보안 상황과 활동에 따라 통제수용자가 실제 인지하는 보안 스트레스 강도에도 차이가 있을 것으로 예상된다. 따라서 본 연구에서는 다양한 분야에서 인간의 행동결정을 설명하는데 많이 이용되고 있는 합리적 행동이론, 계획된 행동이론, 일반 억제이론 등을 정보보안 분야에 접목한 기존 연구의 이론적 고찰을 통해, 기업에서 시행되고 있는 다양한 보안정책 및 보안활동으로부터 인지된 조직 구성원의 보안정책 특성요인을 탐색적 연구를 통해 분석하고, 이러한 특성요인을 독립변수로 하여, 이들 변수들과 조직 구성원이 체감하는 보안스트레스와의 인과관계를 다중 회귀분석을 통해 설명하고, 궁극적으로는 통제수용자의 인지된 보안스트레스가 통제수용자의 보안준수행동의도에 미치는 영향에 대한 인과관계를 설명하고자 금융회사 조직 구성원을 대상으로 실증분석을 하고자 한다.

Abstract Company strengthen various information security policy and activity in order to protect important information assets that the company has been dealing with and prevents information security accidents such as personal information spill. However, some study said these policy and activity increase employee's information security stress and still information security accidents by employees have happened so far.
Therefore, this study will review preceding theories and studies used in many various fields including Information Security areas needed to explain human's behavioral intention and determinants and summarize characteristic factors that have influence on control of human's behavioral intention in the results of the above theories and studies. Secondly, this study will implement exploratory analysis on characteristic factors perceived by employees that has been stemmed from various company's information security policy and activity in order to increase employee/'s information security compliance intention under the its surrounding security circumstance.
Thirdly, this study will fulfil multiple-regression analysis in order to identify cause-effect relationship between employee's perceived information security stress and employee's perceived characteristic factor. Finally, this study will explain casual relationship with same analysis methods between information security stress and information security compliance intention based on results of the survey conducted on the financial firm's employees with same analysis methods

Key Words : Information Security Policy, Security Stress, Information Security Compliance Intent

*정회원, 고려대학교 금융보안학과 금융보안정책전공
**정회원, 고려대학교 정보보호대학원
접수일자: 2016년 10월 5일, 수정완료: 2016년 11월 15일
게재확정일자: 2016년 12월 9일

Received: 5 October, 2016 / Revised: 15 November, 2016
Accepted: 9 December, 2016
*Corresponding Author: hopaut@naver.com
Center for Information Security Technologies(CIST), Korea University, Korea

Ⅰ. 서 론

1. 내부자에 의한 보안사고의 증가

기업은 고객에게 더 나은 서비스를 제공하고자 고객으로부터 더 많은 정보를 법적 허용 범위 내에서 수집, 활용하고 있다. 기업은 기업이 보유하고 있는 정보자산으로부터 더 많은 비즈니스 기회와 이익 등 많은 혜택을 누리고 있지만 그 역기능으로 사이버테러, 개인정보 유출 등 새로운 보안 위협에 노출되어 있다. 이러한 기업의 보안위협은 다양한 원인과 동기로 발생될 수 있으며, 연구자 Loch는 보안위협을 아래 표 1과 같이 4가지 범주로 구분하였다.(Loch et al.1992)

표 1. 보안위협의 구분
Table 1. Category of Information Security Threats

Source	Perpetrator	
	Human	Non-Human
Internal Threats	· Acts by employees · Administrative Procedures	· Mechanical & Electrical Failures · Program Problems
External Threats	· Competitors · Hackers	· Natural Disasters · Computer Viruses

이러한 보안위협으로부터 기업은 기술적, 관리적, 물리적 보호조치를 위해 막대한 비용을 투자하였지만, 이러한 노력에도 불구하고, 아래 표 2에서 보듯이 최근국내 기업에서도 많은 보안사고가 발생되고 있으며, 주목할 만한 특징은 대다수 보안사고가 주로 기업 내부의 조직구성원에 의해 발생되었다는 것이다.

표 2. 내부자에 의한 금융회사 개인정보 유출 사고
Table 2. Scales of Customer Personal Information Leakage Accidents at Domestic Financial company

금융회사	발생시기	규모
KB카드	2012년 ~ 2013년 12월	5300만 건
롯데카드		2600만 건
NH카드		2500만 건
씨티은행	2013년 4월	3만 4000여 건
SC제일은행	2012년 2월	10만 3000여 건
IBK캐피탈	2011년 12월	5796 건
삼성카드	2011년 8월	47만 건
하나SK카드	2011년 7월	9만 7000여 건
현대캐피탈	2011년 4월	175만 건

출처 : 금융감독원 창원지점

연구자 Bulgurcu는 그의 연구에서 정보보안 사고는 특히 외부요인보다 내부요인에 따른 발생빈도가 높게 나타나고 이에 대한 내부위협이 조직에게 보다 치명적인 것으로 평가되고 있다.(Bulgurcu et al., 2010)고 하였으며, 연구자 Shaul은 내부자의 의도적이고 악의적인 위협은 탐지하기 어렵고 발생 시 막대한 손실을 발생시킬 수 있다고 하였다 (Shaul 2011). 또한 연구자 Thompson은 내부자에 의한 악의적인 공격은 외부자의 공격에 비해 그 피해가 50배가 크며 정보보안 사고의 80% 이상이 내부자의 위협으로 추정하고 있다(Power 2002; Thompsonet al. 2004). [1]

2. 보안스트레스 증가

보안 사고를 방지하기 위하여, 기업은 삼엄한 사내 보안활동을 강화 하고 있다. 그리고, 클라우드 컴퓨팅과 모바일, 웹2.0, 파일공유 애플리케이션의 확산, 모바일 오피스, IOT, 스마트워크 환경, 모바일 오피스 및 BOYD (Bring Your Own Device) 등과 같은 새로운 정보기술과 제도를 조직 내에 적극적으로 도입함으로써 직원들이 준수해야 하는 보안정책은 지속적으로 증가하고 있고, 이로 인해 보안스트레스를 받는 부작용이 발생하고 있는 것이 현실이다. 마크로밀엠브레인이 2014년 4월 직장인 517명을 대상으로 설문조사한 결과에 따르면 직장인들 중 64%가 사내 보안으로 인해 스트레스를 받았으며, 43%는 업무에 차질을 빚은 경험이 있다고 하였다. 그리고 기업 내 조직구성원이 가장 불만을 갖는 사내 보안은 ▲외부 USB 반입·반출 금지(25.3%) ▲개인 이메일 사용 금지(22.1%) 등이 뒤를 이었다.[9] 또한, 직장인 절반가량은 소속된 회사의 정보보안이 심한 편이라고 생각하였다.(강유현, 2010). [2] 따라서 정보보안은 기업이 기업의 문화, 환경 등과 같은 상황적 요인에 대한 중요성을 인식하는 것에서부터 시작되어야만 하며, 기업이 효과적인 보안정책을 세우고 이를 조직 구성원들이 실행할 수 있도록 동기 부여를 하는 것이 중요하다. 조직 구성원은 왜 이러한 보안정책이 필요한지 이해가 안 되면 정책을 무시하는 경향이 있고, 때로는 반발하기도 하며 이것으로 인해 스트레스를 받기도 한다. 이렇듯 사용자 편의성을 무시한 기업의 정보보안 활동은 조직원들에게 부담으로 다가올 수 있으며, 결국 사람들의 피로도를 증가시켜, 지키지 않는 보안 규정만 생기는 상황으로 정보보호에 대한 사용자 인식에 부정적 영향만 주게 된다.[3]

3. 연구목적 및 필요성

국내외를 막론하고, 기업에 있어서의 정보보호는 조직의 존망을 결정하는 가장 핵심적인 경쟁력이 되었다. 정보보안의 중요성은 당연히 인정되어야 하지만, 기업은 가시적 보안성과에만 치중한 나머지 조직 구성원들이 업무에서 느끼는 불편함과 업무 생산성 저하는 간과되었다. 이에 대해, 그간의 보안스트레스 관련 연구는 직접적인 스트레스 유발요인(업무과부하, 개인프라이버시 침해 등)을 규명하고, 테크노스트레스분야에 치중하여 왔다. 하지만 본 연구는 목적은 기존 연구과는 달리, 정보화의 편리성 이면에 산재되어있는 기업 마다 상이한 보안정책의 어떠한 성격적 특성 요인으로부터 통제수용자에 의해 인지된 보안스트레스가 실제 통제수용자 보안행동의도(준수 및 위반)에 어떤 영향을 미치는 지에 대해 연구하고자 하며, 그 실증 분석 결과를 바탕으로 기업 차원의 스트레스 관리에 도움이 되고자 한다.

II. 이론적 배경 및 선행연구

1. 정보보안정책의 개념적 정의

보안정책은 기업의 정보와 기술 자원을 지키기 위한 직원들의 역할과 책임에 대해 기술한 것(Bulgurcu et al. 2010)으로 조직의 목표와 신념, 현재의 통제규정, 그리고 조직의 정보시스템 자원에 대한 허용된 접근과 관련된 세부적인 가인드라인을 제공해 준다. 보안정책은 다음의 세가지 내용으로 포괄적으로 인식될 수 있다. 첫째, 보안전략(Strategy)이다. 보안전략은 상위수준의 보안 총괄 계획을 나타내며, 경영목표, 이해관계자, 정책의 범위, 정책의 목적 등이 포함된다. 다음으로 정책(Policy)이다. 정책은 중간레벨의 정보보안 방법을 포함한다. 또한 정책에서는 정책 근거, 가이드라인, 보안행위 강화 메커니즘 등이 결합된 상황 특화적(Issue-specific) 정책을 제공한다. 마지막으로 운영절차(Operating Procedures)가 있다. 운영절차에는 하위 수준에서 다양한 시스템에서의 보안정책을 구현할 수 있는 구체적인 실행활동들이 기술되어 있다. [4]

2. 보안정책의 현실적 한계 특성

내부 보안위협을 방지하기 위해 기업이 수행하고 있는 보안정책은 불행하게도 통상적으로 조직의 모든 수준에서 비효과적이며, 불필요하고 심지어는 강제성이 결여되어 있다는 비판받아 오고 있으며(Goel & Chengalur-Smith, 2010) 실제 기업 내 조직원들은 아래 언급되고 있는 보안정책에 대한 현실적 한계 특성으로 인해 불편함을 느끼거나, 자신의 업무의 생산성을 저해하고 있음을 알 수 있다. 따라서 여전히 조직 구성원들로 하여금 보안정책을 준수하도록 독려하는 것은 아직도 많은 기업들이 직면한 도전과제라 할 수 있다.[7]

가. 보안정책 수립의 불완전성

일반적으로 보안정책은 다양한 보안관련 경험과 경력이 있는 책임자에 의해 수립되는 경우가 많지 않다.다수의 기업 보안정책은 다른 조직의 보안정책을 참고하거나, 국제표준협회 IOS가 제공하는 표준안을 기반으로 하거나, 심지어는 인터넷에서 공유되는 자료를 참조하여, 작성하는 경우도 있다. 하지만 이러한 자료의 경우, 필수적인 권장사항(Best Practices)만을 포함하고 있기에 이를 그대로 수용하는 것은 적절치 못하다고 볼 수 있다. [4] 또한, 보안정책은 내부 전문가나 의사결정자에 의해서 수립되더라도 보안정책을 따라야 하는 구성원들의 목소리가 반영되기는 쉽지 않으며, 정책 수립자와 수용자가 동일한 위치에 있지 않기 때문에 상호이해가 전제되지 않은 상태에서 정책 수용자의 입장에서 보안정책의 효과성을 기대하기란 쉽지 않다는 것이다. [7]

나. 보안기술의 간접적 효익 한계

보안기술(Security Technology)은 DoS(Denial of Service)나 맬웨어(Malicious Software)등과 같은 보안을 위협하는 부정적 요소들에 대처키 위한 기술로서 그 사용자에게 단순히 보안위협을 막아주는 간접적인 효익만을 제공한다. 합리적 행동이론, 계획된 행동이론 등 선행연구들을 보면, 그 대상은 모두 긍정적 기술(Positive Technology)이었다는 공통점이 있다. 긍정적 기술이란 사용자들에게 생산성, 효율성, 경쟁력, 오락성의 혜택을 가져다주는 등 직접적 효익을 위해 만들어진 기술을 의미한다. 하지만 보안기술의 태생적인 간접적 효익 한계로 조직 구성원들로 하여금 일반적인 업무에 추가된 귀찮은 짐으로 느끼게 하거나, 짜증나는 일로 인지되는 경향이 있다. [8]

다. 새로운 보안환경의 복잡성 대두

빠르게 변하는 사용자 보안 환경의 변화로 인한 보안

정책의 모호성, 복잡성은 증대 된다. 보안 복잡성은 최근 기업들이 직면하고 있는 최우선의 장애물인 것으로 나타났다.[5] 이러한 복잡성을 가중시키는 가장 큰 이유 중 하나는 그동안 많은 기업들은 정보보안을 위해 기술적 대안으로 자신의 기업에 맞는 보안 기술이 아니라 가격효율성을 고려하여 상용화 패키지를 구입하는 경우가 많았다는 것이다. 이 경우 조직의 환경 및 조직이 지금까지 사용하고 있는 시스템과의 이질성으로 인해 조직원들이 느끼는 기술적 이질감은 더욱더 높아질 수밖에 없다. 이로 인해 조직원들은 정보보안에 대해 불편함을 느끼거나, 자신의 업무의 생산성을 저해 한다고 느끼게 된다. 이러한 복잡성을 야기하는 또 다른 이유로는 사용자에게는 생소한 클라우드 컴퓨팅과 모바일, 웹2.0, 파일공유 애플리케이션의 확산, 모바일 오피스, IOT, 스마트워크 환경, BYOD (Bring your own device)등 새로운 기술의 채택으로 인해 기업들은 알맞은 보안수준을 적용하기 위해 노력하고 있으며, 이를 위해 조직 구성원으로부터 보다 엄격한 컴플라이언스 준수를 요구하고 있다. [6]

3. 정보보안 행동동기 선행 이론 고찰

가. 합리적 행동이론 (Theory of Reasoned Action)

본 이론은 Fishbein의 기대-가치 (Expectancy -Value) 이론을 확장하여 정립된 이론으로 인간의 행동은 신념 → 태도 → 의도→ 행동으로 영향을 주는 것으로 나타난다[Ajzen, 1991]. 결국 인간의 행동을 결정하는 요소는 행동의도이며, 행동의도는 다시 선행요인인 태도(Attitude)와 주관적 규범(Subjective Norm)에 의해 결정된다는 것이다. 태도란 '행위를 수행하는 것에 대한 개인의 긍정적 또는 부정적인 느낌'이며, 만약 행위의 결과가 긍정적이라고 인식될 경우, 개인은 긍정적 태도를 형성하게 된다. 주관적 규범은 개인이 특정한 행위를 수행하거나, 하지 않는데 영향을 미치는 사회적 압력에 대한 영향을 말하며, 본인의 행위가 다른 사람들에게 중요한 것인지에 대한 개인의 인식'으로 보고 있다.[9] 따라서, 본 연구에서는 태도와 주관적 규범을 통제 수용자 보안준수의도와 보안스트레스에 영향을 미치는 보안정책의 주요 특성요인으로 제시한다.

나. 계획된 행동이론(Theory of Planned Action)

계획된 행동이론은 주어진 행위를 수행할 수 있는 능력 수준에 대한 개인의 기대, 필요 자원을 가지고 있는지 여부, 직면한 장벽을 극복할 수 있는 능력 등을 말한다. 즉, 앞으로 있을 행동에 대해 편의성, 용이성 또는 반대로 난해성, 복잡성 등의 개인의 인지 정도를 말하는 것으로 인지수준은 과거의 경험이나 그 행동을 실행하는데 기대되는 장애물, 난관 등에 의해 반영된다. 이렇게 행동에 제약을 주는 장애물이나 난관은 실제 기업에서 시스템이나 인증절차와 같은 물리적, 기술적 환경을 말한다.(Triandis, 1979) 즉, 개인이 자원이나 기회를 충분히 가지고 있다고 생각 할수록, 그리고 행동하는데 있어서 장애물이 덜 예상된다고 생각 할수록 행동에 대한 인지된 행동통제 수준이 증가하게 된다는 것이다.(Ajzen 1985, 1991) 따라서, 태도와 주관적 규범과 더불어 인지된 행동통제(Perceived Behavioral Control)가 통제수용자의 행동의도를 결정하게 된다는 것이다. 다시 말하면, 행동의도를 갖고 있더라도 인지된 행동통제가 낮다면 실제로 행동을 하지 않는다는 것이다. (Doll& Ajzen, 1992)[10] 따라서, 본 연구에서는 본 이론에 근거하여, 인지된 통제요인으로 언급되고 있는 인지된 복잡성, 인지된 자기효능감을 통제 수용자 보안준수의도와 보안스트레스에 영향을 미치는 보안정책의 주요 특성요인으로 제시한다.

다. 억제이론 (Deterrence Theory)

억제이론은 범죄학에서 주로 통용되는 이론으로 바람직하지 않거나 정당하지 못한 범죄적 행동을 하려는 행위자로 하여금 행동의 손해가 이익보다 많다는 것을 제시한 이론이다. 즉, 범죄로 얻는 이익보다 범죄를 저지른 후에 입는 손해가 더 크다는 것을 인식시키는 이다. (Lebow & Stein 1990)[10] 보안정책의 억제성과 관련하여, 보안정책이 정보시스템의 오용을 억제 할 수 있는 중요한 요소라고 주장한 연구가 있는 반면, 다른 연구는 보안정책이 제한적 효과만 발휘한 다고 주장하였다. Lee and Lee(2002)는 보안정책 미준수를 발생할 수 있는 처벌에 대해 기술하며, 처벌에 대한 위협을 증가시켰음에도 불구하고 여전히 많은 미국기업에서 보안사고가 발생하고 있다고 주장하였다. 반면, Foltz et al.(2008)은 보안정책이 업무환경에서 부적합한 자원의 접근을 억제시킴과 동시에 해당 정책의 침해는 강력한 처벌이 수반됨을 구성원들에게 인지시킴으로써, 조직 내에서 매우 중요한 역할을 한다고 주장한다.[4]이러한 불일치의 원인중 하나는 같은 보안정책이라도 사용자들의 인식 (USER's Perceptions)에 따라 다르게 작용하기 때문이며, 억제 메

커니즘으로써 보안 정책의 성공여부는 결국 조직 구성원들의 행위 (Actions)와 인지(Awareness)에 달려 있기 때문이다. 따라서, 본 연구에서는 억제이론에 근거하여, 처벌의 심각성, 처벌의 확실성을 통제 수용자 보안준수의도와 보안스트레스에 영향을 미치는 보안정책의 주요 특성요인으로 제시한다.

라. 기술수용모델 (Technology Acceptance Model)

Davis는 합리적 행동이론을 발전시켜 기술수용모형을 제시하였는데, 이 이론적 모형을 통하여 사용자의 정보기술 수용과정을 잘 설명할 것으로 기대하였다. 기술수용모형에서 중요한 변수는 두 가지로, 인지된 유용성(Perceived Usefulness)과 인지된 사용 용이성(Perceived Ease of Use)이 있다. 인지된 유용성은 '조직 환경에서 해당 정보시스템의 사용으로 직무성과를 증대시킬 수 있다고 믿는 사용자의 주관적 평가정도'로, 인지된 용이성(Perceived Ease of Use)은 '사용자가 목표한 시스템을 많은 노력을 기울이지 않고도 이용할 수 있다고 기대하는 정도'로 정의된다. 따라서, 본 연구에서는 인지된 유용성과 인지된 복잡성을 통제 수용자 보안준수의도와 보안스트레스에 영향을 미치는 보안정책의 주요 특성요인으로 제시한다.[8]

마. 공포소구이론 (Fear Appeal Theory)

보안위협 심각성(Threat Severity) 개념은 Rogers에 의하여 처음 사용된 개념으로서 개인의 반응에 영향을 미치는 공포소구에 있어서 우선되는 개념인데 위협의 중대성에 대하여 공포소구 청자가 가지게 되는 신념수준을 의미한다. Witte는 위협(Threat)에 대하여 '개인에 의하여 인지되든지 아니든지 존재하는 외부의 자극(External Stimulus)'이라고 정의하고 있으며, '위협 심각성'에 대해서 '보안위협의 발생이 미칠 부정적 영향을 인식한 정도'라고 정의 하였다.[8] 예를 들면, 개인이 컴퓨터 바이러스 백신을 사용하지 않아, 내부의 중요자료가 외부로 유출 된다면, 본인과 조직에 미칠 부정적 영향에 대한 인식수전이고, 이러한 인식 강할수록 통제수용자 보안 준수 의도에 긍정적 영향 미친다는 연구가 있다.[1] 따라서, 본 연구에서는 공포소구이론에 기반하여, 인지된 보안위협을 통제 수용자 보안준수의도와 보안스트레스에 영향을 미치는 보안정책의 주요 특성요인으로 제시한다.

바. 보안스트레스 (Information Security Stress)

일반적인 스트레스의 정의는 '특정 시점에 평가한 개인의 수요(demand)가 가용할 수 있는 자원을 초과할 때 생기며 이는 건강을 위협하고 이와 같은 불균형을 회복하기 위한 개인의 기능적 변화를 필요'로 한다(Lazarus 1991).[2] 즉 환경의 규정이 개인의 능력과 재원을 초월하거나 직무 환경에 의해 개인의 욕구가 공급되어지지 않았을 때 스트레스를 유발하게 된다는 것이다[14]. 보안스트레스 직접적인 유발 요인으로써, 업무과부하(work overload)는 개인이 업무나 역할을 수행하는데 기대되는 정도가 개인의 능력을 초과하거나, 어떤 일을 급하게 실행해야 하거나 주의를 기울이지 못하게끔 강요당하는 상황을 말한다(이종목, 1989) 그리고, 또 다른 직접적 보안스트레스 유발 요인으로는 프라이버시 침해(Invasion of Privacy)가 있다.[11] 기업은 재정적, 법적 책임의 잠재적 리스크 때문에 조직 구성원의 기업의 보안 정책 상 있을 수 있는 이메일 검열 등이 있다. 기업의 정보 보안활동 노력으로는 정보보안정책 수립, 기업 내 보안 감사, 보안교육, 비밀번호 관리, 안티바이러스 백신 설치 및 업데이트, 중요한 정보 백업, 소프트웨어 정품 사용, 이메일 및 메신저 모니터링 등이 있는데, 이러한 모든 정보보안 활동으로부터 조직구성원에 의해 인지된 감내할 수 없는 통제의 적정 수준을 넘는 경우, 이는 곧 보안스트레스의 요인이 될 수 있는 것이다.

Ⅲ. 연구모형 및 가설

1. 연구모형

본 연구에서는 다양한 분야에서 특정행동을 설명하는데 많이 이용되고 있고, 정보보안정책 준수에 영향을 주는 정책적 특성 요인을 분석하기 위한 선행연구 에서 제시하고 있는 통제수용자 행동동기요인에 대해 탐색적 요인분석을 실시하여, 개념적 중복가능성이 높은 요인들을 제외하고, 조작적 정의를 통해 통제 수용자에 의해 인지된 보안정책 특성요인을 아래 표 3과 같이 4개의 독립변수로 단순화하였으며, 각각의 독립변수가 통제수용자의 인지된 보안스트레스에 어떠한 영향을 미치는 지에 대해 회귀분석을 수행하였다. 그리고 궁극적으로 인지된 보안스트레스가 통제수용자 보안준수의도에는 어떠한 영향을 미치는 지에 대한 상관관계를 설명하기 위하여, 아래 Figure 1의 연구모델을 제시하고, 실증 분석을 하고자 한다.

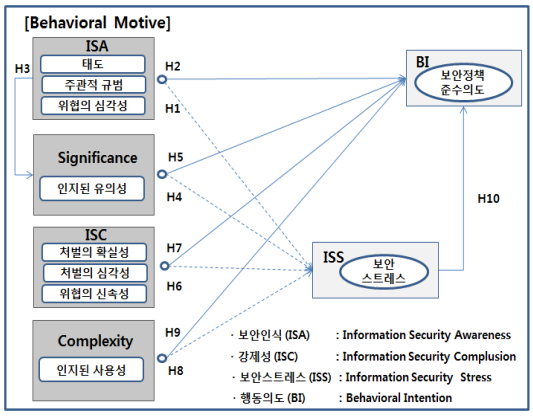

그림 1. 연구모델
Fig. 1. Study Model

표 3. 통제수용자의 인지된 정보보안정책 특성 요인
Table 3. Information Security Policy Characteristic factors Perceived by Employee

독립변수	행동동기요인	개념 / 정의
보안인식	태도	행위를 수행하는 것에 대한 개인의 긍정적 또는 부정적인 느낌
	주관적 규범	행위를 수행하는 것이 다른 사람들에게 중요한 것인지에 대한 개인의 인식
	인지된 위협의 심각성	보안 사건의 결과의 심각성 개인이 평가하는 위협적인 사건들의 확률로 정의
인지된 강제성	인지된 처벌의 심각성	보안 미준수에 따른 처벌의 확실성, 처벌의 엄격성에 대한 인식의 정도
인지된 유의성	대응효능감	권고되는 행동이 효과적으로 위협을 피하도록 해줄 것이라는 것에 대한 개인적 신념의 정도
	인지된 유용성	개인의 업무생산성 및 효율성의 측면에서 특정기술을 선택하고, 사용하는 것이 업무수행을 향상시킬 것이라는 신념수준
	인지된 유의성	보안준수로 인한 긍정적인 결과에 대한 믿음의 정도 ☞ 해당 보안 정책이 꼭 필요하다고 느끼는 정도
	상대적 이점	사용자에 의하여 기존의 것보다 혁신의 결과물이 더 낫다고 지각하는 정도
인지된 복잡성	인지된 자기효능감	행동을 취하는데 요구되는 기술, 능력에 대한 자신감
	복잡성	사용자에 의하여 혁신의 이용하기가 어렵다고 지각되는 정도
	불안정성	정보시스템으로 인한 불안감과 불확실성으로 프라이버시 유출에 대한 우려, 기술적 장애로 인한 업무 목적 미달성 등
	인지된 통제성	행동 결정에 수반되는 자원과 기회의 가용성 및 중요성에 대한 판단

2. 연구가설

상기 Figure 1.에 제시된 연구모형에 포함되어 있는 변수들 간의 관계에 관한 가설을 도출한 구체적인 논리적 추론과정(Logical Reasoning)을 각 가설별로 기술하면 아래와 같다.

가. 보안인식 (Information Security Awareness)

조직 구성원의 보안인식은 정보보호경영의 중요한 부분이고 [Bulgurcu et a], 조직의 정보보안 목적을 달성하기 위한 직원의 상태이며 [Siponen, 2000], 정보보안에 대한 조직원의 일반적인 이해와 조직의 정보보안정책에 대한 이해로 정의된다.[9] 보안인식은 정보보안 관련 잠재된 이슈와 파급효과에 대한 전반적인 지식과 이해이다. 따라서, 합리적 행동이론과 계획된 행동이론에서 보안준수 선행 요인으로 언급하고 있는 태도, 인지된 보안위협, 주관적 규범은 보안인식과 매우 관련이 높은 속성 요인으로 분류 될 수 있다[12]고 볼 수 있으며, 통제수용자의 보안인식이 높을수록 보안준수의도가 높아지고, 보안정책에 대한 긍정적 인식으로 보안스트레스를 덜 인지할 것이라는 추론을 바탕으로 아래와 같이 가설을 검증하고자 한다.

H1. 통제수용자 보안인식은 보안스트레스에 부(-)의 영향을 미칠 것이다.

H2. 통제수용자 보안인식은 보안준수의도에 정(+)의 영향을 미칠 것이다.

나. 인지된 유의성 (Perceived Usefulness)

인지된 유의성은 '조직 환경에서 해당 정보시스템의 사용으로 직무성과를 증대시킬 수 있다고 믿는 사용자의 주관적 평가정도'와 특정 시스템을 사용함으로써, 자신의 업무성과를 향상시킬 것이라고 믿는 정도로 정의될 수 있다. 뱅킹서비스에 대한 연구에서 뱅킹서비스의 지각된 유용성이 높을수록 지각된 위험 및 제품의 기능적 복잡성과 피로 등 부정적 요인에 부(-)의 영향을 미칠 것이라고 하였다 이국용(2005).[13]결국 통제수용자의 지각된 유의성은 정보보안정책에 대한 가치를 높이고, 만족도를 높여 통제수용자로부터 보안스트레스를 낮게 지각하게 만들 것이며, 보안준수의도를 향상시킬 것으로 가정할 수 있을 것이다. 따라서 다음의 가설을 설정하였다.

H3. 보안정책의 유의성은 보안스트레스에 부(-)의 영향을 미칠 것이다.

H4. 보안정책의 유의성은 보안준수의도에 정(+)의 영향을 미칠 것이다.

다. 인지된 강제성 (Perceived Complusion)

억제이론에 입각한 처벌과 같은 보안통제의 강제성은 통제가 과도하거나 처벌이 심하다고 인지하는 통제수용자에게 비용 낭비, 업무 처리시간 증가 등의 비효율성이 발생토록 하여, 조직 구성원이 느끼는 보안 스트레스는 증가할 것이고, 과소 통제하게 되면 실질적 효과가 없는 통제로 인해 보안스트레스는 감소할지라도 정보보안의 목적을 달성할 가능성이 희박하기 때문에 정보보안 통제에 대한 통제수용자의 인지수준은 향후 정보보안 성과 및 보안 스트레스에 큰 영향을 미칠 수 있다.[9] 따라서, 본 연구에서는 처벌 수위 등 강제성에 대해 사용자가 인지하는 정도가 높을수록 보안정책 준수에 더 신경을 쓰거나 더한 스트레스를 받을 것을 전제로 아래와 같은 가설을 설정 하였다.

H5. 처벌에 의한 통제수용자의 인지된 강제성은 보안 스트레스에 (+)의 영향을 미칠 것이다.

H6. 처벌에 의한 통제수용자의 인지된 강제성은 보안 준수의도에 정의(+)의 영향을 미칠 것이다.

라. 인지된 복잡성 (Perceived Complexity)

정보기술이 발전해 감에 따라, 앞서 언급한 보안정책의 현실적 한계 등으로 업무의 편리성이 증대되는 반면 복잡성 또한 증가하게 된다.[11] (Ragu-Nathan et al., 2008) Herath and Rao(2009)는 구성원들이 보안정책을 준수하지 않는 이유 중 하나는 불편함을 초래하기 때문이라고 주장하였다. 또한 제품 수용저항 요인으로써 복잡성은 스마트폰 제품을 구매하는 소비자들에게 긍정적인 영향을 줄 수도 있는 반면, 적지 않은 부정적인 영향을 미치기도 한다.(Brown and Capenter 2000). 너무 많은 속성은 소비자들로 하여금 은 그들이 구매한 제품의 속성을 모두 사용하지 않으며, 이러한 제품의 복잡성은 너무 많은 기능들을 익혀야 하는 걱정과 스트레스와 같은 부정적 감정을 경험하게 될지도 모른다고 한다. (Mick and Fournier 1998). 따라서 본 연구에서는 보안정책의 복잡성이 조직 보안스트레스와 보안준수의도에 다음의 영향을 미칠 것으로 가설을 설정하였다. [13]

H7. 통제수용자가 인식하는 보안정책의 복잡성은 보안 스트레스에 정(+)의 영향을 미칠 것이다.

H8. 통제수용자가 인지하는 보안정책의 복잡성은 보안 준수의도에 부(-)의 영향을 미칠 것이다.

마. 인지된 보안스트레스 (Perceived Information Security Stress)

기존에 많은 연구들이 보안성과를 높이기 위한 통제수용자의 정보보안정책준수에 영향을 주는 행동동기 요인을 분석하는 것을 강조하고 있지만, 이로 인해 직간접적으로 유발 될 수 있는 조직구성원의 보안스트레스가 통제수용자의 정보보호행동 동기 의도에 어떠한 영향을 미치는 지에 대한 연구는 많지 않다. 따라서, 본 연구에서는 기업 내 정보보안 통제에 따른 스트레스가 통제수용자의 정보보안정책 준수 또는 위반 의도에 실제 영향을 미치는 지를 규명하기 하기 위하여, 다음과 같은 가설을 설정하였다.

H9. 인지된 보안스트레스는 통제수용자 보안준수 행위 의도에 부(-)의 영향을 미칠 것이다

Ⅳ. 실험 및 결과

본 연구는 실증적 연구로써 정보보안 정책에 영향을 받는 금융회사 직장인들을 대상으로 설문을 통해 데이터를 수집하였다. 국내 대형 금융회사 한곳을 대상으로 2016년 7월 21일부터 8월 5일 간 전자설문을 통해 전체 설문대상 329명 중 253명으로부터 설문 결과를 회신 (응답율 59.5%)을 받았으며, 이중 일관된 응답으로 분석에 사용하기에 부적합하다고 판단되는 20부를 제외하고 총 233부를 최종분석에 사용하였다. 본 연구에서 사용된 측정 항목들은 신뢰성과 타당성이 검증된 선행연구에서 가져왔고, 기존 항목들을 정보보안 정책 및 활동이라는 문맥에 맞게 수정하였으며, 모든 변수들은 Likert 7점 척도를 사용하여 전혀 그렇지 않다(1)는 것에서 매우 그렇다(7) 산정하였다. 수집된 설문자료들은 신뢰도 검증을 위한 탐색적 요인분석을 실시하여 일부 항목을 제거하였다. 총35문항 중 5문항이 이론 구조에 맞지 않게 적재되어 제거하였고 최종적으로 30개 문항을 분석에 이용하였다.

1. 측정지표의 타당성 및 신뢰성 요인 분석

가. 탐색적 요인분석

실증연구를 수행함에 있어 구조적 관계에 대한 잘 못

된 해석을 피하기 위하여 가설검증 전에 측정모형에 대한 추정을 먼저 수행하여야 한다. 이를 위해 설문 원천 데이터가 요인분석에서 사용되는 것이 적합 한지를 KMO(Kasier-Meyer-Olkin)의 표본 적합성 검증을 통해 확인하였다. 일반적으로 본 값이 0.5 이상 혹은 0.7이상이 될 경우 요인 분석을 위한 상관관계의 적합성이 존재 한다고 볼 수 있는데, 본 연구의 경우 KMO 값이 0.887로 나타나 매우 높은 수준의 적합성을 보유하고 있다고 볼 수 있다. 다음으로 탐색적 요인 분석을 수행하였다. 탐색적 요인 분석은 해석의 용이함을 위해 관측변수의 수를 줄이고, 테이터 내에 존재하는 숨겨진 구조를 발견하는 것을 목적으로 한다. 탐색적 요인분석은 Varimax회전을 통한 Kaiser정규화법을 활용하였으며, 연구모델에서 독립변수와 종속변수를 분리하여 수행하였다. 분석결과 고유치(eigenvalue)가 1 이상이고 요인 적재치(Factor Loading)가 0.5이상인 값을 갖는 총 6개의 요인이 도출되었다. 추출된 6개의 요인의 분산 설명력은 68% 이상로 나타나 일반적 기준인 60% 이상을 훨씬 상회했으며, 각각의 적재 항목의 공통성(Communality)도 최소값이 .570로 모든 항목이 50% 이상의 설명력을 가지고 있는 것으로 나타났다. 신뢰성 검증은 Cronbach's alpha 계수를 사용하여 각 개념들의 측정 항목들의 내적 일관성(Internal Consistency)을 평가함으로 확인하였다. 분석결과 Cronbach's alpha값은 0.7이상의 값을 갖는 것으로 나타나 신뢰성도 높은 수준을 나타냈다.

표 4. 회전 주성분행렬 분석 결과 (독립/종속변수)
Table 4. The results of factor analysis

회전된 성분행렬a						
변수	설문문항	성분				신뢰도 통계량
		1	2	3	4	Cronbach'α
A 보안의식	q1_1	0.797	0.263	-0.125	-0.01	0.86
	q1_2	0.783	0.256	-0.125	-0.037	
	q3_1	0.755	0.069	-0.172	0.096	
	q2_3	0.744	0.014	-0.148	0.225	
	q2_1	0.743	0.152	-0.148	0.183	
	q3_3	0.723	0.284	-0.099	0.053	
	q3_2	0.67	0.298	-0.024	0.083	
	q2_2	0.635	-0.105	-0.061	0.343	
	q1_3	0.531	0.516	-0.117	0.103	
B 인지된 유용성	q4_2	0.285	0.772	-0.118	0.038	0.784
	q4_3	-0.049	0.769	-0.179	0.146	
	q1_4	0.499	0.611	-0.235	0.047	
	q4_1	0.488	0.543	-0.195	0.11	
C 인지된 복잡성	q6_1	-0.164	-0.137	0.917	-0.045	0.873
	q6_3	-0.194	-0.086	0.896	-0.039	
	q6_2	-0.128	-0.3	0.762	0.025	
D 인지된 강제성	q5_3	0.126	0.103	-0.044	0.919	0.879
	q5_2	0.222	0.16	0.011	0.886	
표본 적절성의 Kaiser-Meyer-Olkin 측도.						0.887
Bartlett의 구형성 검정		근사 카이제곱				2528.12
		자유도				153
		유의확률				0
YE 보안스트레스	Yq9_5	0.874	-0.096			0.938
	Yq9_4	0.865	-0.194			
	Yq9_3	0.823	-0.214			
	Yq7_1	0.807	-0.089			
	Yq9_2	0.796	-0.086			
	Yq7_2	0.787	-0.196			
	Yq8_2	0.755	-0.291			
	Yq7_3	0.742	-0.217			
	Yq9_1	0.738	-0.222			
YF 보안준수의도	Yq10_2	-0.099	0.868			0.833
	Yq10_3	-0.187	0.841			
	Yq10_1	-0.252	0.83			
표본 적절성의 Kaiser-Meyer-Olkin 측도.						0.915
Bartlett의 구형성 검정		근사 카이제곱				2528.12
		자유도				153
		유의확률				0

추출방법 : 주성분 분석.
회전방법 : Kaiser 정규화가 있는 베리멕스.
a. 5 반복계산에서 요인회전이 수렴되었습니다.

2. 연구 모형 분석 결과

다음으로 본 연구에서는 SPSS v2.2을 활용하여 다중회귀분석 실시하였다. 다중회귀분석은 한 개 또는 그 이상의 독립변수들과 한 개의 종속변수의 관계를 파악하기 위한 분석기법이다. 결과 분석 시 R^2 값을 통하여 독립변수 요인이 종속변수를 어느 정도 설명하는지 알아보고, 변수별 표준화 계수와 유의확률을 중심으로 중속변수와 독립변수 간의 인과관계를 분석하였다.

가. 독립변수에 의한 보안스트레스 회귀분석 결과

4개의 독립변수가 각각 보안스트레스에 어느 정도 인과관계가 있는 지 아래의 결론이 도출되었다.

표 5. 독립변수와 보안스트레스간 회귀분석 결과표
Table 5. The Result of Regression Analysis between security stress and independent variables

ye ~a + b + c + d

R	R 제곱	수정된 R제곱	추정된값의 표준오차	Durbin-Watson
.850a	0.723	0.718	0.671310209	2.218

독립변수	비표준화 계수		표준화 계수		유의확률
	B	표준오차	베타	t	
(상수)	2.946	0.57		5.168	0
보안의식	-0.061	0.093	-0.03	-0.652	0.515
인지된 유의성	-0.321	0.058	-0.259	-5.587	0
인지된 강제성	0.034	0.048	0.026	0.699	0.485
인지된 복잡성	0.667	0.037	0.691	17.858	0

1) 보안스트레스에 대한 인지된 유의성(B)와 인지된 복잡성(D)의 표준화 계수는 각각 (- 0.259)와 (+ 0.691)

으로 유의확률이 0.05 이하인 '0'으로 유의하다.

2) 인지된 유의성(B)는 보안스트레스(YE)에 유의하게 부(-)의 영향을 미친다.
3) 인지된 복잡성(D)는 보안스트레스(YE)에 유의하게 양적(+)인 영향을 미친다.
4) D(+0.691) >B (-0.259) 순으로 표준화 계수가 크므로, 상대적으로 인지된 유의성(B) 보다 인지된 복잡성(D)이 보안스트레스에 더 큰 영향을 미친다.
5) 보안인식 (A)와 인지된 강제성(C)는 보안스트레스(YE)와의 인과관계는 유의하지 않다

나. 독립변수에 의한 보안준수의도 회귀분석 결과

각각의 독립변수가 보안스트레스와 어느 정도 인과관계가 있는 지 아래의 결론이 도출되었다.

표 6. 독립변수와 보안행동의도간 회귀분석 결과표
Table 6. The Result of Regression Analysis between security policy compliance intent and independent variables

yf ~ a + b + c + d

R	R 제곱	수정된 R제곱	추정된 값의 표준오차	Durbin-Watson
.771a	0.594	0.587	0.435013474	1.934

독립변수	비표준화 계수		표준화 계수		유의확률
	B	표준오차	베타	t	
(상수)	1.488	0.369		4.03	0
보안의식	0.666	0.06	0.615	11.063	0
인지된 유의성	0.063	0.037	0.094	1.679	0.095
인지된 강제성	0.089	0.031	0.126	2.842	0.005
인지된 복잡성	-0.045	0.024	-0.088	-1.869	0.063

1) 보안행동의도에 대한 보안인식(A) 와 인지된 강제성(C)의 표준화 계수는 각각 (+ 0.615)와 (+ 0.126)으로 유의확률 0.005 이하인 '0' 으로 유의하다.
2) 보안의식 (A)는 보안준수의도에 유의하게 양적(+)인 영향을 미친다.
3) 인지된 강제성 (C)는 보안행동의도(YF)에 유의하게 양적(+)인 영향을 미친다.
4) A(0.615) >C(0.126) 순으로 표준화 계수가 크므로, 상대적으로 인지된 강제성(C) 보다 보안인식(A)가 통제수용자 보안행동의도(YF)에 더 큰 영향을 미친다.
5) 인지된 유의성(B)와 인지된 복잡성(D)는 보안행동의도(YF)와 인과관계가 유의하지 않다

다. 스트레스에 의한 보안준수의도 회귀분석 결과

표 7. 보안스트레스와 보안행동의도간 회귀분석 결과표
Table 7. The Result of Regression Analysis between security stress and security policy compliance intent

R	R 제곱	수정된 R제곱	추정된값의 표준오차	Durbin-Watson
0.409a	0.167	0.164	0.619281798	1.818

비표준화 계수		표준화 계수		유의확률
B	표준오차	베타	t	
7.244	0.149		48.477	0
-0.219	0.032	-0.409	-6.927	0

1) 보안준수행동의도에 대한 보안스트레스의 표준화 계수(-0.409)는 유의확률 0.05 이하로 유의
2) 보안스트레스는 통제수용자 보안준수 행동의도에 유의하게 부(-)의 영향을 미친다.

라. 보안인식과 인지된 유의성간 회귀분석 결과

표 8. 보안인식과 인지된 유의성간 회귀분석 결과표
Table 8. The Result of Regression Analysis between security awareness and perceived usefulness of security policy

R	R 제곱	수정된 R제곱	추정된값의 표준오차	Durbin-Watson
.630a	0.397	0.395	0.7932	2.049

비표준화 계수		표준화 계수		유의확률
B	표준오차	베타	t	
7.244	0.149		48.477	0
-0.219	0.032	-0.409	-6.927	0

비표준화 계수		표준화 계수		유의확률
B	표준오차	베타	t	
-1.591	0.515		-3.087	0.002
1.028	0.082	0.63	12.547	0

1) 인지된 유의성 변수에 대한 보안인식 변수의 표준화 계수(+ 0.63)는 유의확률 0.005이하로 유의
2) 보안인식은 통제수용자 인지된 유용성에 유의하게 부(+)의 영향을 미친다.

마. 보안인식과 인지된 유의성간 다중 회귀분석 결과

상기 회귀분석결과에 따라 연구가설이 아래와 같이 검증 되었다.

표 9. 가설검증 결과 요약
Table 9. The summary of hypothesis testing

변수	가설	분석 결과	표준화 계수
보안 인식	보안인식은 보안스트레스에 부(-)의 영향을 미칠 것이다.	기각	-0.03
	보안인식은 보안준수의도에 정(+)의영향을 미칠 것이다.	채택	0.615
	보안인식은 인지된 유의성에 정(+)의영향을 미칠 것이다.	채택	0.63
인지된 유의성	인지된 유의성은 보안스트레스에 부(-)의 영향을 미칠 것이다.	채택	-0.258
	인지된 유의성은 보안준수의도에 정(+)의 영향을 미칠 것이다.	기각	0/094
인지된 강제성	인지된 강제성은 보안스트레스에 정(+)의 영향을 미칠 것이다.	기각	0.026
	인지된 강제성은 보안준수의도에 정(+)의 영향을 미칠 것이다.	채택	0.126
인지된 복잡성	인지된 복잡성은 보안스트레스에 정(+)의 영향을 미칠 것이다.	채택	0.691
	인지된 복잡성은 보안준순의도에 부(-)의 영향을 미칠 것이다.	기각	-0.088
인지된 스트레스	인지된 스트레스는 보안준수의도에 부(-)의 영향을 미칠 것이다.	채택	-0.409

V. 결 론

본 연구 결과에 따르면, 조직 구성원의 보안스트레스를 낮추기 위해서는 기업의 보안정책과 활동에 대해 인지된 유의성을 높이고, 인지된 복잡성 낮춤으로써, 보안정책/활동 자체에 대한 조직 구성원의 정책적 보안인식 수준을 높이는 것이 중요하다고 볼 수 있다. 보안스트레스와는 무관하게 조직 구성원의 보안준수의도를 높이기 위해서는 인지된 처벌 강제성을 높이고, 보안 인식을 강화하는 것이 중요하다고 볼 수 있다. 보안인식을 강화하기 위해서는 기업의 정보보안활동이나 정책 등 전반에 대한 긍정적 태도와 인지된 보안위협, 주관적 규범을 조직 구성원 개인 스스로가 자각할 수 있도록 기업 차원에서의 통제수용자 보안교육과 인센티브 등 다양한 방식으로의 지원과 심리적 행동 통제가 필요할 것으로 사료된다. 결국, 조직구성원의 보안스트레스와 보안준수의도에 영향을 미치는 요인은 서로 다른 요인에 의한 영향을 받는 것으로 파악되었기에 조직구성원에 의해 인지된 처벌 강제성이 높거나, 또는 일반 보안인식이 낮은 경우, 해당 기업의 조직 구성원은 더 많은 보안스트레스를 체감할 것이라는 가설은 기각 되었다.

조직 구성원의 인지된 보안스트레스가 보안준수의도에 미치는 인과관계 분석결과를 보면, 보안스트레스는 조직 구성원의 보안준수행동의도에 - 0.409의 영향을 미치는 것으로 확인 되었다. 따라서, 기업이 정보보호 활동 및 정책을 통해 조직 구성원의 보안인식과 인지된 처벌 강제성을 강화하여, 해당 기업 조직 구성원의 보안정책 준수행동의도를 대폭 향상시킬 수는 있으나, 만약, 해당 기업의 보안활동 및 정책 운영 절차 또는 프로세스 상에서 조직 구성원이 수행해야 하는 업무절차가 부담스럽거나, 까다로워 진다면, 낮은 수준의 인지된 유의성과 높은 수준의 인지된 복잡성을 유발하게 될 것이다. 이로 인해 기업의 보안정책 수립 의도와는 달리 입장에서 최초 보안정책 및 활동 기획 의도와는 달리 보안스트레스에 의한 조직구성원의 보안준수의도가 상당수 상쇄될 수 있음을 확인할 수 있었다. 상기 결론을 토대로 기업 내 정보보안 담당자가 정보보호정책, 제도, 규정, 관리적/기술적/물리적 정보보안활동 업무 기획 시, 보다 효과적인 조직 구성원 보안통제를 위하여 조직 구성원에게 미치는 보안준수행동 동기와 보안스트레스의 영향도를 함께 고려해야 할 것이다. 독립변수 간 인과관계 분석결과를 토대로 보안인식은 인지된 유의성(+0.64)의 영향이 있는 것으로 확인된 바, 조직 구성원의 보안인식 강화를 통해 기업 내 정보보호활동 및 보안정책에 대한 조직 구성원의 인지된 유의성을 함께 높일 수 있다면, 인지된 보안스트레스도 낮추고, 보안준수행동의도를 강화할 수 있다는 유의미한 결과를 도출할 수 있을 것이다. 본 연구는 사내 정보보안 교육 커리큘럼을 구성할 때나 정보보안 활동을 개진할 때 조직원들의 스트레스를 최소화할 수 있는 지원 방안을 도출해내는 데 기여할 수 있을 것이라고 본다. 정보보안 정책 준수활동에 대한 효과를 높이기 위해서는 정보보안 정책 수립 및 변경 시, 조직원들의 의견을 수렴하고, 정보보안 활동에 대한 보안인식과 인지된 유의성를 높이기 위한 효과적인 보안 컨텐츠를 만들어서 종사자들에게 배포함으로써 정보보안 활동에 지속적으로 관심과 긍정적인 시각을 가지도록 권장하는 것이 매우 중요하다.

References

[1] Jung, Jae Won (2015). A Study for the Effect on Members' Compliance Intention for Information Security of Information Security Activity of

Organization : From the Perspective of Health Belief Model pp.8 ~9.

[2] Kim, Su Hyun (2013), A Research on Information Security Policy Compliance Activity's Effect on Stress: Centered on Compliance Activity Type pp. 2

[3] Seoung-Ju Kim, the security system, and practical measures required. Security measures that are in reality to admit to that people are not perfect, The Digital Times, the April 12, 2016

[4] Myung-Seong Yim (2013), The effect of Characteristics of Information Security Policy on Security Policy Compliance Intent. The Korea Society of Digital Policy & Management Vol.9, No. 1

[5] http://www.ddaily.co.kr/news/article.html?no=75678, 2011.03.17, digital daily Internet news article

[6] http://www.zdnet.co.kr/news/news_view.asp?artice_id=20141127123339&type=det&re=,zdnet korea article, KISA (SNC 2015) Jung, Kyoung-Ho, (2014.11.27)

[7] Shin, So-Young · Kim, Chang-Ho (2015) A Study on the Influence of Industrial Security Policies and Input for Compliance on the Industrial Security Supervisors' Compliance Motivations towards Security Policies, Journal of the Korean Society of Private Security Vol. 14, Issue 14 No.4

[8] Sang-Hoon Kim (2016) An Empirical Study on Influencing Factors of Using Information Security Technology. Journal of Society for e-Business Studies 20(4). 151-175

[9] Jeong-Ha Lee (2015). A Study on the Factors for Violation of Information Security Policy in Financial Companies : Moderating Effects of Perceived Customer Information Sensitivity. Journal of Information Technology Applications & Management, 22(4), 225-251.

[10] Jung,WooJin (2012), The study on the behavioral attitude of employees toward the customer information security in financial firms. pp.27

[11] Haejung Yun, Guiyoung Choi, Choong C. Lee(2011) The Influence of Mobile Office Systems on Users' Job Stress and Work Overload, Journal of Management Information Systems, Vol.20, Issue. 20, No.2, June. 2011, pp.155-176

[12] Kim, Moon-Tae (2013)A Study of Influence Factors that effect on Consumer Fatigue in the Adoption of Convergence Products. Management and Information Systems Review, Vol. 32, No.2

[13] Sung Min Ryu (2013), Study on information security stress in Public Enterprise

[14] Hae-Sool Yang(2007) A Study on the Influential Relationship of Job Stress in R&D Personnel on their Organizational Effectiveness, Journal of the Korea Academia-Industrial cooperation Society, Vol. 8, No. 6, pp. 1695-1705.

저자 소개

임 광 수(정회원)

- 2002년 : The University of Memphis, Graduate Schooll
- 2006년 ~ 현재 : 신한카드 재직
- 2015년 ~ 현재 : 고려대학교 정보 보호대학원 석사과정

권 헌 영(정회원)

- 2005년 : 연세대학교 법학과 법학 박사
- 2008년 : 광운대학교 법학과 교수
- 2015년 ~ : 고려대학교 정보보호대학원 교수
- *정부3.0추진위원회 법제도 특별 위원회 위원장, 공공데이터 법 제도전문위원회 위원장, 개인정보분쟁조정위원회 위원, (사)한국블로거협회 협회장 등 활동 중

<주 관심 분야 : 정보보호, 개인정보보호, 정보통신정책, 법제도>