기업의 정보보안 활동이 구성원의 정보보안 준수의도에 미치는 영향 연구

정재원* 이정훈** 김채리***

요 약

기업의 정보시스템에 대한 내·외부의 위협이 증가되고 있으며 이를 감소시키기 위해 많은 돈과 인력을 투자하고 있다. 하지만 이러한 투자에도 불구하고 보안위협과 사고는 지속적으로 발생하고 있다. 본 연구는 기업의 사고 방지를 위한 다양한 정보보호 활동을 예방 지향적과 억제 지향적으로 구분하고 건강신념모델을 이용하여 기업의 정보보안 활동이 구성원들에게 어떤 영향을 미치고 정보보안 정책을 준수하도록 하는지 연구하였다. 연구결과 예방 지향적 활동은 심각성에, 억제 지향적 활동은 유익성에 유의미한 영향을 주고, 심각성과 유익성은 각각 준수의도에 영향을 주었다. 이러한 결과로 미루어보아, 기업에서 교육, 홍보, 모니터링 등 사전적인 활동을 시행할 경우 미 준수로 발생할 수 있는 부정적인 결과에 대해 강조하여야 하며, 감사, 처벌 등 사후적인 활동을 통해 보안을 유지하고자 할 경우 기업의 의지를 보임으로써 보안 정책을 준수하는 것이 유익할 것이라는 판단을 구성원 스스로 하도록 하는 것이 더욱 효과적인 정보보안 활동이 될 것이다.

A Study on the influence of firm's Information Security Activities on the Information Security Compliance Intention of Employees

Jaewon Jung* Jung-hoon Lee** Chae-ri Kim***

ABSTRACT

An internal and external threat against an information system has increased, and to reduce it, organization has spent a great deal of money and manpower. However, in spite of such investment, security threat and trouble have happened continuously. Organization has conducted information security activity through various policies. The study classified such activities into prevention-oriented activity and control-oriented activity, and researched how information security activity of organization affects members of an organization and obeys information security policy by using health belief model. As a result of the study, prevention-oriented activity has a meaningful impact on seriousness, and this seriousness affects compliance intention for information security. Control-oriented activity has a meaningful impact on benefits, and the benefits have an effect on compliance intention. When an organization conducts prior activities such as education, PR, and monitoring, this organization should emphasize negative results that can happened because of deviation. In addition, in case of exposure and punishment through post activities such as inspection and punishment, if the organization emphasizes the positive effects of exposure and punishment rather than emphasis of negative parts, information security activity will be more effective.

Key words : information security activity, information security policy, health belief model, compliance intention for information security

접수일(2016년 11월 17일), 게재확정일(2016년 12월 20일)

* 본 논문은 정재원의 학위논문을 요약 발제하였습니다.

* 연세대학교 일반대학원 기술경영협동과정
** 연세대학교 정보대학원 교수(교신저자)
*** 연세대학교 정보대학원

1. 서 론

정보시스템이 발전할수록 정보시스템에 대한 기업의 의존도는 올라갔다. 이에 따라 정보시스템에 대한 내·외부의 위협이 증가되고 있으며 이를 감소시키기 위해 기업은 많은 돈과 인력을 투자하고 있지만 보안위협과 사고는 지속적으로 발생하고 있다. 2013년 국내에서 발생한 카드회사 개인정보 대량 유출 사고에서는 내부 직원의 보안통제 실패로 인하여 대량의 개인정보가 유출되었다. 이 사건은 용역업체 직원이 정보를 유출한 사건으로, 신원미상의 해커나 불가항력적인 자연재해와 같은 위협도 중요한 통제 대상이지만 내부자의 무지에서 비롯된 단순 실수, 시스템 오류로 인한 위협 또한 매우 중요한 통제 대상이라는 것을 인지시키는 사건이었다. 정보시스템에 가해지는 위협을 줄이기 위하여 기업에서는 기술 기반의 통제 방법에 많은 비용을 투자를 하고 있지만 정보보안관련 사고 수는 증가하고 있으며[1], 내부자에 의한 악의적인 공격은 외부자의 공격에 비해 그 피해가 50배가 크며 정보보안 사고의 80% 이상이 내부자의 위협으로 인한 사고로 추정되고 있다[2]. 즉 급격한 IT 환경의 변화와 외부 위협의 증가로 인하여 기존의 기술 기반의 정보보호 대책으로는 그 한계가 이 있으며 사람 중심의 정보보호 전략이 필요하다[3].

이를 위해 많은 연구자들이 다양한 분야의 이론을 통해 정보보안 정책 준수 요인에 대한 연구를 하였지만 기업의 정보보안 정책이 구성원의 준수 및 준수의도에 영향을 미치는 과정에서 어떤 요인으로 인해 준수를 하게 되는지 통합된 연구가 부족한 현실이다. 본 연구를 통해 기업의 정보보안 정책을 예방적 및 억제적 활동 개념으로 재구성하여 기업의 활동과 구성원의 준수의도와의 관계를 파악하고자 한다. 또한, 이를 통해 기업의 효과적인 정책 수립과 방향에 대하여 이론적 근거를 제시하고자 한다.

2. 이론적 논의

2.1 정보보안 문헌연구

2.1.1 정보보안 준수의도

여러 연구에서 정보보안정책 준수의도의 요인들을 확인할 수 있었는데, 보안정책 준수의도, 태도, 행동에 영향을 미치는 요인들로는 준수함으로써 받는 혜택, 준수하지 않음으로써 받는 불이익, 이런 불이익을 제도화 시켜 놓은 규정과 규범, 마지막으로 주변 이해관계자들의 사회적 압박 등 기업이 구성원을 통제하는 수단이 주요 요인으로 연구되었다. 구성원에 대한 다양한 규정과 통제에도 불구하고 80%의 사고가 내부자로 추정된다[4]. 즉 다양한 규정과 통제는 내부자가 정보보안을 준수하는 요인이라고 설명하는데 부족하다고 할 수 있으며 인간의 내적 요인에 대한 더 자세한 연구가 필요하다고 할 수 있다.

연구자 박종원은 정보보안 준수에 대한 선행연구를 예방지향성과 억제지향성으로 구분하여 연구하였으며 그 구분에 따른 선행연구의 변수를 다음 표와 같이 구분하였다[5].

<표 1> 정보보안의 예방 및 억제

구분	변수명	연구자
예방 지향성	보안정책	[6], [7], [8], [9], [10]
	보안/시스템 교육	[8], [11]
	접근제어	[9]
	모니터링	[8]. [9]
억제 지향성	처벌의 확실성	[6], [7], [8], [9], [10], [12]
	처벌의 엄격성	[6], [7], [8], [9], [10], [12]
	처벌의 파급효과	[7], [12]
	감사	[8], [10]

다양한 연구에서 정보보안은 전략적으로 접근해서 해결해야 한다고 말하고 있다. 이에 따라 본 연구는 정보보안 전략을 선행연구에서 제안한 정보보안 구분을 채용하여 기업의 정보보안 예방 지향적 활동과 억제 지향적 활동으로 구분하여 정보보안 준수의도에 미치는 영향에 대해 연구하고자 한다.

2.1.2 정보보안 예방 지향적 활동

예방지향성은 상황적 범죄예방이론에 근거하고 있다. 상황적 범죄예방이론은 '제도의 개선에 의존하는 것이 아니고 범죄기회에 의존하는 예방적인 접근 방법'을 말하며 범죄학에서 주목할 만한 중요 이론으로 등장하였다. 연구자 Cornish는 상황적 범죄이론을 적용할 때 고려해야 하는 전략을 '노력증가', '위험증가', '보상감소', '자극감소', '변명제거' 총 5가지로 정의하였다[13].

노력증가는 범죄를 저지르는데 필요한 노력을 증가시

키는 방법이며, 위험증가는 범죄행위를 함으로서 범죄자가 받는 위험 증가, 셋째는 범죄로 얻을 수 있는 보상을 감소, 넷째는 범죄를 도발 할 수 있는 자극을 감소 마지막 다섯째는 범죄에 대한 변명을 제거하는 방법을 말한다. 즉, 규정과 제도를 통한 적발과 처벌이 아닌 사전에 범죄자가 받는 위협을 증가시키고 인지하게 하는 활동을 예방 지향적 활동이라 할 수 있다.

2.1.3 정보보안 억제 지향적 활동

Lebow와 Stein은 억제란 '올바르지 않은 행동을 하려는 자에게 이익보다 비용이 많다는 것을 알림으로써 행위를 예방하는 것'이라고 정의하였다[14]. 인간은 합리적이고 경제적인 존재이기 때문에 예상되는 이익을 계산하여 얻는 불이익이 크다면 범죄의 동기가 줄어든다는 억제이론(Deterrence Theory)을 바탕으로 하고 있으며 이는 처벌과 이득과의 합리적인 계산을 통해 범죄의 동기가 결정된다는 결과와 같다[15].

연구자 Workman은 억제이론(Deterrence Theory)과 계획된 행동이론(the theory of planned behavior)을 사용하여 연구하였는데 사람의 두려움을 이용한 제재적 억제방법인 처벌(Punishment)과 양심과 자기통제를 기초로 하는 발전적 억제방법인 윤리교육(Ethics Training)이 부적절한 행위를 방지하는데 영향을 미치는 요인임을 확인하였다[16].

즉 억제 지향적 활동은 정해놓은 규정을 위반했을 경우 처벌과 같은 사후 조치에 대한 두려움 또는 양심에 대한 부담으로 자기통제 능력을 근간으로 위반을 억제하기 위한 것으로 말할 수 있다[5].

2.2 건강신념모델(Health Belief Model)

건강신념모델은 1950년대에 사회 심리학자 Hochbaum, Rosenstock과 Kegels에 의해 미국의 공중보건사업에서 시민들이 질병예방 프로그램에 참여하지 않는 원인을 이해하고자 개발되었다[17].

건강신념모델은 지각된 심각성(perceived severity), 지각된 취약성(perceived susceptibility), 지각된 이익(perceived benefit), 지각된 장애(perceived barriers), 행동계기(cues to action)로 구성되어 있다.

연구자 Ng의 연구에 의하면 인간이 질병을 예방하기 위해 취하는 행동, 즉 건강행동을 하는데 설명되는 요인들이 직원이 정보보안을 지키고자 하는 보안 행동을 결정하는 프로세스와 유사하다고 하였다[18]. 따라서 본 연구는 건강신념모델을 통해 기업의 다양한 정보보안 정책과 기업의 정보보안 활동이 구성원의 어떠한 주관적인 지각에 영향을 미쳐 최종적으로 정보보안 준수 및 행동을 하는지 알아보고자 한다.

3. 연구방법

3.1 연구가설

3.1.1 예방 지향적 활동

본 연구의 예방 지향적 활동은 사전에 정보보안 사고가 일어나지 않도록 조치하는 활동으로 보안정책, 보안/시스템의 교육, 시스템에 대한 접근제어, 모니터링, 정보보안 인식 등이 예방지향적인 보안활동이라고 정의하였다.

연구자 임채호는 정보보안 인식제고는 정보보안의 가장 중요한 구성요소라 하였으며[9] 연구자 임명선은 정보보안 인식교육이 정보보안 위반에 대한 적발 가능성에 영향을 미치고 이는 보안정책 준수의도에 영향을 준다고 확인하였다[20].

즉, 예방 지향적 활동은 건강신념모델의 요인들에 영향을 미치게 되며 그에 따라 정보보안 정책을 준수하는 의도에 영향을 미칠 것이다. 이러한 내용을 근거로 다음과 같은 가설을 설정하였다.

H1 예방 지향적 활동은 인지된 민감성에 양(+)의 영향을 미칠 것이다.

H2 예방 지향적 활동은 인지된 심각성에 양(+)의 영향을 미칠 것이다.

H3 예방 지향적 활동은 인지된 유익성에 양(+)의 영향을 미칠 것이다.

H4 예방 지향적 활동은 인지된 장애성에 양(+)의 영향을 미칠 것이다.

3.1.2 억제 지향적 활동

본 연구의 억제 지향적 활동은 감사, 엄격하고 확실한 처벌 등의 사후적 보안 정책이라 할 수 있다.

연구자 Workman은 억제이론과 계획된 행동이론을

사용하여 연구하였는데 사람의 두려움을 이용한 제재적 억제방법인 처벌(Punishment)이 부적절한 행위를 방지하는데 영향을 주는 요인임을 확인하였다[16]. 연구자 김상현의 연구에 의하면 페널티의 강도, 보안위반 적발도가 보안정책 준수의도에 유의한 영향을 미친다고 연구하였다[21].

즉, 억제 지향적 활동은 정해놓은 규정을 위반했을 경우 처벌과 같은 억압적이고 강압적인 사후 조치에 대한 두려움 또는 양심에 대한 부담감을 통해 위반을 억제하는 것으로 말할 수 있다[5]. 이러한 내용을 근거로 다음과 같은 가설을 설정하였다.

H5 억제 지향적 활동은 인지된 민감성에 양(+)의 영향을 미칠 것이다.

H6 억제 지향적 활동은 인지된 심각성에 양(+)의 영향을 미칠 것이다.

H7 억제 지향적 활동은 인지된 유익성에 양(+)의 영향을 미칠 것이다.

H8 억제 지향적 활동은 인지된 장애성에 양(+)의 영향을 미칠 것이다.

3.1.3 인지된 민감성

건강신념모델에서의 인지된 민감성은 언제든지 질병에 감염될 수 있다고 인식하는 정도이다. 이 개념을 정보보안에 적용해 보면 개인의 일상생활에서 인지하지 못한 보안위반을 할 수도 있다고 인식하는 정도라고 할 수 있다. 따라서 개인이 민감성을 크게 가질 때 정보보안 행동은 높아 질 것이고 위반을 회피하기 위해 정보보안 규정을 준수하고자 할 것이다[18]. 따라서 이러한 인식은 정보보안을 준수하고자 하는 의도에 긍정적인 영향을 미칠 것 이라고 가설을 설정하였다.

H9: 인지된 민감성은 정보보안 준수의도에 양(+)의 영향을 미칠 것이다.

3.1.4 인지된 심각성

건강신념모델에서의 인지된 심각성은 질병이 자신에게 심각한 영향을 가지고 올 것이라고 인식하는 정도로, 정보보안에서는 개인의 보안문제로 인하여 기업의 정보시스템에 심각한 영향을 줄 수 있다고 믿는 인식이라고 할 수 있다[18]. 따라서 이러한 인식은 정보보안을 준수하고자 하는 의도에 긍정적인 영향을 미칠 것 이라고 가설을 설정하였다.

H10: 인지된 심각성은 정보보안 준수의도에 양(+)의 영향을 미칠 것이다.

3.1.5 인지된 유익성

건강신념모델에서의 인지된 유익성은 건강행위를 함으로 질병감염이 줄어들고 건강에 이로울 것이라고 인식하는 정도로, 정보보안에서는 규정을 준수함으로 기대할 수 있는 긍정적인 이득의 정도라고 할 수 있다[18]. 따라서 인지된 유익성이 크면 정보보안을 준수하고자 하는 의도에 긍정적인 영향을 미칠 것 이라고 가설을 설정하였다.

H11: 인지된 유익성은 정보보안 준수의도에 양(+)의 영향을 미칠 것이다.

3.1.6 인지된 장애성

인지된 장애성은 위협을 감소시키기 위해 하는 행위의 부정적인 측면을 말한다[18]. 정보보안의 위협을 감소시키기 위한 행위로 간단한 암호 인증 대신 이중 인증, 복잡한 암호, 주기적인 암호 변경 등을 요구하여 사용자의 불편을 야기하는 것을 예로 들 수 있다. 연구자 Bulgurcu의 연구에 의하면 정보보안 준수에 대한 비용이 크면 클수록 정보보안에 대한 태도에 음의 영향을 미치는 것으로 연구가 되었다[7].

따라서 본 연구에서는 인지된 장애성이 클수록 정보보안을 준수하고자 하는 의도에는 부정적인 영향을 미칠 것이라고 가설을 설정하였다.

H12: 인지된 장애성은 정보보안 준수의도에 음(-)의 영향을 미칠 것이다.

3.2 표본 추출과 자료 수집

본 연구의 표본은 정보보안 정책이 있는 기업의 정보보안 담당자와 일반직원을 분석단위로 설정하여 이메일을 통해 설문을 실시하였다. 조사기간은 2015년 5월 7일~5월 22일 동안 수집되었으며 설문결과는 총 172명에게 응답을 받았고 불성실한 답변 8건을 제외한 164명의 응답 데이터가 사용되었다. 수집된 데이터는 SPSS 18을 이용하여 요인 및 신뢰도 분석을 실시하였으며, 본 연구에의 가설을 검증하기 위하여 SmartPLS

2.0을 이용하여 분석을 하였다. 설문결과 대한 인구통계학적 특징은 다음 표와 같다.

<표 2> 인구통계학적 특성

Demographic	Category	담당자	일반직원
성별	남	138(84.1%)	119(72.6%)
	여	26(26%)	45(27.4%)
연령	20 대	17(10.4%)	34(20.7%)
	30 대	105(64.0%)	112(68.3%)
	40 대	38(23.2%)	14(8.5%)
	50 대 이상	4(2.4%)	4(2.4%)
최종학력	고졸	9(5.5%)	15(9.1%)
	학사(전문학사 포함)	131(79.9%)	126(76.8%)
	석사	23(14.0%)	22(13.4%)
	박사	1(0.6%)	1(0.6%)
직급	사원(주임 포함)	32(19.5%)	29(17.7%)
	대리	44(26.8%)	60(36.6%)
	과장	48(29.3%)	44(26.8(%)
	차장	22(13.4%)	18(11.0%)
	부장	11(6.7%)	13(7.9%)
	임원	7(4.3%)	-
회사 규모	대기업	42(25.6%)	
	중견기업	41(25%)	
	중소기업	77(47%)	
	기타	4(2.4%)	

4. 연구 분석 및 결과

4.1 주성분 분석

수집된 설문 데이터의 타당성 및 신뢰성 검증을 위하여 각 변수에 대한 요인분석을 실시하였다. 요인분석은 VARIMAX를 사용하였으며 첫 번째 요인분석 시 예방5, 6 항목이 요인 적재치 0.6미만으로 분석되어 해당 측정항목을 제외 하여 다시 요인분석을 실시하였다. 그 결과 다음 표와 같이 7개의 요인, 적재치 0.6 이상으로 명확히 구분되었다. 요인분석을 통해 구분된 각 요인에 대한 신뢰성 분석을 실시한 결과 Cronbach's alpha값이 0.7 이상의 값을 확인하였다. 따라서 본 연구의 각 요인들의 신뢰성이 검증되었다.

<표 3> 요인 분석 및 신뢰도 분석

구분		성분							신뢰도
변수명	측정항목	1	2	3	4	5	6	7	Cronbach's alpha
정보보안억제활동	억제5	.889							0.94
	억제4	.880							
	억제3	.824							
	억제6	.808							
	억제1	.800							
	억제2	.800							
준수의도	준수의도1		.915						0.95
	준수의도2		.902						
	준수의도3		.894						
	준수의도4		.837						
유익성	유익성3			.908					0.89
	유익성4			.888					
	유익성1			.775					
	유익성5			.752					
	유익성2			.726					
심각성	심각성2				.892				0.89
	심각성3				.890				
	심각성1				.811				
	심각성4				.778				
민감성	민감성2					.922			0.89
	민감성1					.883			
	민감성3					.870			
장애성	장애성1						.864		0.81
	장애성2						.836		
	장애성3						.825		
정보보안예방활동	예방1							.707	0.83
	예방2							.698	
	예방4							.658	
	예방3							.621	

4.2 측정모형

연구모형의 타당성은 수렴타당성(Convergent Validity)과 판별타당성(Discriminant Validity)을 통해 확인할 수 있다[22]. 본 연구에서는 수렴타당성은 구성요인의 조합신뢰성(Composite Reliability) 및 추출된 평균분산(Average Variance Extracted) 에 의해

평가하고, 판별타당성은 구성요인 간의 상관관계를 추출된 평균분산(Average Variance Extracted)과 비교하여 평가한다[23].

일반적으로 조합신뢰성(Composite Reliability)은 0.8 이상, 추출된 평균분산(Average Variance Extracted)은 0.5이상이면 수렴타당성이 있는 것으로 본다[22], [24]. 다음 표와 같이 요인별 분석결과를 보면 조합신뢰성(Composite Reliability) 과 추출된 평균분산(Average Variance Extracted)이 각각 0.8, 0.5 이상이 확인되어 본 연구의 연구모형은 수렴타당성이 확인되었다. 또한 표의 Communality값은 측정모형에 대한 통계량으로써 측정변수가 잠재요인에 의해 설명되는 비율로, 측정모형의 적합성(Quality)을 나타내며 기준값은 최소 0.5 이상이어야 한다. 본 연구에서 조사된 Communality 값은 모두 0.5 이상으로써 측정모형의 적합성을 만족시키고 있다.

<표 4> 확인적 요인분석

	AVE	Composite Reliability	R Square	Cronbach's Alpha	Communality
민감성	0.81	0.93	0.04	0.89	0.81
심각성	0.76	0.93	0.12	0.89	0.76
억제	0.77	0.95		0.94	0.77
예방	0.66	0.89		0.83	0.66
유익성	0.70	0.92	0.14	0.89	0.70
장애성	0.66	0.85	0.03	0.81	0.66
준수의도	0.87	0.96	0.22	0.95	0.87

PLS에서 연구모형의 판별타당성 확인은 추출된 평균분산(Average Variance Extracted)의 제곱근 값에 의해 평가되는데 각 요인의 추출된 평균분산(Average Variance Extracted)의 제곱근 값이 해당 요인과 다른 상관계수보다 크면 판별타당성이 존재한다고 할 수 있다. 표와 같이 추출된 평균분산(Average Variance Extracted)의 제곱근 값이 다른 요인간 상관계수보다 높음으로써 판별타당성을 확인할 수 있다.

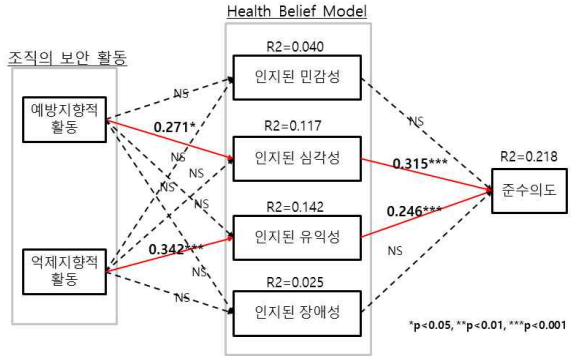
<표 5> 변수간의 상관계수와의 제곱근 값

	민감성	심각성	억제	예방	유익성	장애성	준수의도
민감성	0.9						
심각성	-0.01	0.87					
억제	-0.18	0.27	0.88				
예방	-0.06	0.33	0.64	0.81			
유익성	-0.01	0.20	0.37	0.27	0.84		
장애성	-0.07	0.12	0.10	0.16	-0.13	0.81	
준수의도	-0.16	0.37	0.33	0.40	0.30	0.07	0.93

4.3 구조모형 분석 및 결과

4.3.1 가설검증

본 연구에 대한 가설을 검증하기 위해 PLS(Partial Least Square)를 사용하였으며 분석 도구로 SmartPLS 2.0을 사용하였다. 구조모형 분석을 통하여 경로계수와 내생변수에 대한 결정계수를 도출 하였고 총 164개의 설문 결과를 500으로 부트스트랩(bootstrap)하여 가설의 유의성을 검증하였다. 구조모형의 검증 결과는 다음과 같다.



<그림 4> 분석결과

통계 분석결과 12개의 가설 중 4개의 가설이 채택되고 8개의 가설은 기각되었다.

5. 연구결과 및 의의

5.1 연구결과

본 연구는 건강신념모델 관점으로 기업의 정보보안의 활동(예방지향, 억제지향)이 어떠한 매개 요인들을 통해 정보보안 준수의도에 영향을 미치는가에 관하여 실증분석을 하였다. 연구결과 예방 지향적 활동은 인지된 심각성에, 억제 지향적 활동은 인지된 유익성에 각각 유의미한 영향을 주는 것으로 확인되었으며 인지된 심각성, 인지된 장애성이 정보보안 준수의도에 영향을 주는 것으로 확인되었다. 본 연구에서 설정한 가설 중 채택된 가설은 총 4개이며 각 채택된 가설이 의미하는 바는 다음과 같다.

첫째, 예방 지향적 활동은 인지된 심각성에 정(+)의 영향을 주는 것으로 나타났다. 기업은 구성원의 보안 의식을 높이고자 교육 활동 등의 예방 지향적 활동을 수행한다. 교육은 정보보안 실패로 인한 부정적인 결과를 강조하여 구성원이 정보보안의 중요성과 실패 시 발생할 수 있는 심각성을 인식하도록 하기 때문에 예방 지향적 활동은 구성원이 심각성을 인지할 수 있도록 한다. 본 가설의 채택으로 현업에서는 구성원이 정보보안에 대하여 인식할 수 있도록 계획적인 정보보안 인식 강화 프로그램을 수행하여야 한다.

둘째, 억제 지향적인 활동은 인지된 유익성에 정(+)의 영향을 미친다고 분석되었다. 기업의 정보보안 감사와 적발을 통한 강력한 처벌 등의 강제적인 활동은 기업이 정보보안에 대해 강력한 의지를 가지고 있다는 것을 인식하게 한다. 강력한 처벌 및 감사 등의 억제 지향적 활동을 통해 구성원은 규정을 지키고 보안 정책을 준수하는 것이 유익할 것이라는 인식을 하게 될 것이다.

셋째, 인지된 심각성, 인지된 유익성은 각각 정보보안 정책 준수의도에 정(+)의 영향을 주는 것으로 분석되었다. 이 결과는 Bulgurcu의 연구결과를 통해 설명할 수 있다. 연구자 Bulgurcu는 합리적 선택이론을 통해 정보보안 정책 준수 혜택과 미 준수 시 발생하는 비용이 정보보안에 대한 태도에 영향을 미친다고 연구하였는데 정보보안을 지키지 않았을 때 발생될 수 있는 부정적인 결과(인지된 심각성)를 미 준수 비용으로 생각할 수 있으며 정보보안을 지킴으로써 얻을 수 있는 긍정적인 유익함(인지된 유익성)을 준수 혜택으로 해석할 수 있다. 그러므로 Bulgurcu의 연구와 유사한 결과가 도출 되었다고 할 수 있다.

본 연구에서 기각된 가설을 언급하면 다음과 같다.

첫째, 예방 지향적 활동과 억제 지향적 활동은 인지된 민감성에 유의미한 영향을 미치지 못하는 것으로 분석되었다. 인지된 민감성의 조작적 정의는 '자신이 의도치 않게 보안사고가 일어날 가능성이 있다고 믿는 정도'이다. 기업에서 예방 지향적 또는 억제 지향적인 정보보안 활동을 통해 구성원의 '나는 아니겠지' 라는 인식의 변화를 시키지 못하기 때문에 기업의 정보보안 활동이 인지된 민감성에 유의미한 영향을 미치지 못한 것으로 생각된다.

둘째, 억제 지향적 활동은 인지된 심각성에 유의미한 영향을 미치지 못하는 것으로 분석되었다. 예방 지향적 활동은 보안 사고에 따른 실패 사례 등을 통해 구성원의 심각성을 높이지만 주기적인 감사 등의 억제 지향적 활동은 수행해야 하는 일련의 업무라 인식하기 때문에 인지된 심각성에 유의미한 영향을 미치지 못한 것으로 생각된다.

셋째, 예방 지향적 활동은 인지된 유익성에 유의미한 영향을 미치지 못하는 것으로 분석되었다. 예방 지향적 활동은 교육, 모니터링 등을 통한 보안 사고의 부정적 결과를 전달하기 때문에 정책 준수를 통해 얻을 수 있는 유익성이 낮을 것이라고 인식하기 때문이라고 예상된다.

넷째, 인지된 민감성은 정보보안 준수의도에 유의미한 영향을 미치지 못하는 것으로 분석되었다. 기업에서 보안을 민감하게 인식하는 사람이 적기 때문에 인지된 민감성은 정보보안 준수의도에 영향을 미치지 못한 것으로 판단된다.

다섯째, 예방 지향적, 억제 지향적 활동은 인지된 장애성에 영향을 유의미한 영향을 미치지 못하였으며 인지된 장애성 또한 정보보안 준수의도에 유의미한 영향을 미치지 못한 것으로 분석됐다. 정보시스템에서 강제적으로 발생시키는 불편함(패스워드 길이 및 변경 주기 등) 즉, 인지된 장애성은 무조건 받아 들여야 하는 필수사항이 되었고 회피 할 수 없는 업무필수 조건이 되었다. 인지된 장애성은 Bulgurcu 연구에서는 준수비용(Cost of Compliance)로 연구되었으며 다른 선

행 연구에서도 유사한 의미로 연구되었다. 과거에는 정보보안 준수에 부정적인 영향을 미치는 중요한 변수였으나 정보보안을 위해 발생되는 불편함은 업무를 위해 당연히 받아들여야 하는 필수적인 요소가 되었기에 기업의 정보보안 활동과 정보보안 준수의도의 매개효과가 낮아졌고 이로 인하여 기각된 것으로 생각된다.

본 연구 결과를 종합해 보면 기업의 정보보안 활동이 지향해야 할 방향을 단적으로 나타낸다고 할 수 있다. 즉 기업에서 정보보안 정책을 결정하고 시행 할 때 정보보안 정책 위반에 대한 부정적인 인식과 준수했을 때의 긍정적인 결과를 인지하게 하는 정책을 포괄적으로 적용해서 시행해야 한다고 할 수 있다. 처벌(penalty)과 보상(benefit)만을 강조하는 것이 아니라 복합적이고 통합적인 정책이 정보보안 준수를 강화하는데 적합하다고 할 수 있다. 또한 본 연구를 통해 기업의 정보보안 활동이 구성원들에게 어떻게 작용되고 정보보안 준수에 영향을 주는지 확인 할 수 있었으며 연구 결과를 통해 기업에서 정책을 수립하고 적용하는데 이론적 근거로 사용될 수 있을 것이다.

5.2 시사점

본 연구의 시사점은 다음과 같다.

첫째, 정보보안 활동에 대한 개념을 상황적 범죄이론과 억제이론으로 통해 예방 지향적 활동과 억제 지향적 활동으로 구분하였다. 기업의 정보보안 활동을 개념화, 체계화 하고 이를 통해 정보보안 준수, 준수의도와 통합적으로 연구함으로써 기업의 정보보안 활동 전략 수립에 이론적 근거를 제시하였다.

둘째, 본 연구에서 제시한 연구 틀을 토대로 정보보안 활동과 정보보안 준수, 준수의도와의 관계를 분석할 수 있는 연구 모델을 새롭게 개발 하였다. 보건 분야의 이론인 건강신념모델을 도입하여 정보보안 정책이 구성원의 내적 요인인 민감성, 심각성, 유익성, 장애성에 어떠한 영향을 미치고 결과적으로 정보보안 정책 준수 의도에 어떤 영향을 미치는지를 실증적으로 분석하는 연구모델을 개발 하였다. 정보보안의 활동을 예방지향과 억제지향으로 구분하여 기업의 정책 방향 및 우선순위를 결정하고 수립하는데 중요한 근거로 사용할 수 있도록 하였으며, 기존 연구에서 주로 사용된 이론이 아닌 새로운 이론을 통한 연구로 정보보안 분야 연구의 이론적 기반 확장에 기여하였다.

5.2 연구 한계점 및 향후 연구 방안

본 연구과정에서 나타난 몇 가지의 한계점으로 결과를 분석하고 제안하는데 신중하여야 한다.

첫째, 다양한 산업분야, 구성원의 경력, 직급, 업무 등으로 다양한 변수들을 통한 연구가 필요하다. 일반적인 제조업과 고도의 기술적 수준이 필요한 분야는 관리가 필요한 정보와 자산도 다를 것이기에 다양한 산업 분야에 대해 세분화된 연구가 필요하다.

둘째, 본 연구에서 사용한 독립변수의 예방지향과 억제지향을 더욱 세분화하여 구분할 수 있을 것이다. 사전, 사후 개념이 아닌 새로운 개념을 통해 변수들에 대한 세분화 및 구체화 하는 연구가 필요하다.

참고문헌

[1] Fossi, M., Turner, D., Johnson, E., Mack, T., Adams, T., Blackbird, J., Entwisle, S., Graveland, B., McKinney, D., and Mulcahy, J., "Symantec global internet security threat report," White Paper, Symantec Enterprise Security (1), 2009.

[2] Power, R. 2002 CSI/FBI computer crime and security survey, Computer Security Institute, 2002.

[3] 김정덕, "정보보호관리 패러다임 변화에 따른 주요 이슈와 미래 전략," 정보보호학회지, 제23권, 제5호, pp. 5-8. 2013.

[4] Thompson, H. H., Whittaker, J. A., and Andrews, M. "Intrusion detection: Perspectives on the insider threat," Computer Fraud & Security:1), pp 13-15, 2004.

[5] 박종원, "Impact of information security strategy on information security compliance intention,"공주대학교, 2013.

[6] Boss, S., and Kirsch, L, "The last line of defense: motivating employees to follow corporate security guidelines," Proceedings of the 28th International Conference on Information Systems), pp 9-12, 2007.

[7] Bulgurcu, B., 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, 2010.

[8] D'Arcy, J., D'Arcy, A., Hovav, D., and Galletta, "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, 2009.

[9] Straub, D. W., and Welke, R. J., "Coping with Systems Risk: Security Planning Models for Management Decision Making," MIS Quarterly, Vol.22, No.4, pp. 441-469, 1998.
[10] Straub Jr, D. W., "Effective IS security: An empirical study," Information Systems Research, Vol. 1, No. 3, pp. 255-276, 1990.
[11] Piccoli, G., Ahmad, R., and Ives, B., "Web-based virtual learning environments: A research framework and a preliminary assessment of effectiveness in basic IT skills training," MIS quarterly, Vol. 25, No. 4, pp. 401-426, 2001.
[12] 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, 2010.
[13] Cornish, D. B., and Clarke, R. V., "Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention," Crime prevention studies, Vol.16, pp. 41-96, 2003.
[14] Lebow, R. N., and Stein, J. G., "Deterrence: The elusive dependent variable," World Politics, Vol. 42, No. 3, pp. 336-369, 1990.
[15] Scholz, J. T., "Enforcement Policy and Corporate Misconduct: The Changing Perspective of Deterrence Theory," Law and Contemporary Problems, Vol. 60, No. 3, pp. 253-268, 1997.
[16] Workman, M., and Gathegi, J., "Punishment and ethics deterrents: A study of insider security contravention," Journal of the American Society for Information Science & Technology, Vol.58, No. 2, pp. 212-222, 2007.
[17] Becker, M. H., "The health belief model and personal health behavior," Slack, Vol. 2, No. 4, 1974.
[18] Ng, B.-Y., Kankanhalli, A., and Xu, Y. C., "Studying users' computer security behavior: A health belief perspective," Decision Support Systems, Vol. 46, No.4, pp. 815-825, 2009.
[19] 임채호, "효과적인 정보보호인식제고 방안," 정보보호학회지, 제16권, 제2호, pp. 30-36, 2006.
[20] 임명성, "조직 구성원들의 정보보안 정책 준수행위 의도에 관한 연구," 디지털융복합연구, 제10권, 제10호, pp. 119-128, 2012.
[21] 김상현, 송영미, "조직 구성원들의 정보보안 정책 준수 동기요인에 관한 연구," e-비즈니스연구, 제12권, 제3호, pp. 327-349, 2011.
[22] Hair, J. F., Multivariate data analysis, 2009.
[23] Fornell, C., and Larcker, D., "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," Journal of Marketing Research, pp. 39-50, 1981.
[24] NUNNALLY, Jum. C.(1978). Psychometric theory. 1978.

[著者紹介]

정 재 원 (Jaewon Jung)

2009년 2월 세명대학교
정보통신학 학사
2015년 8월 연세대학교 정보대학원
정보시스템학 석사
2016년~현재 연세대학교 일반대학원
박사과정

email : jwjung0307@gmail.com

이 정 훈 (Jung-hoon Lee)

1995년 University of Manchester
전자공학 학사
1996년 University of Manchester
시스템공학 석사
1998년 London School of Economics
경영정보학 석사
2003년 University of Cambridge
생산/정보 시스템 공학 및 경영 박사

email : jhoonlee@yonsei.ac.kr

김 채 리 (Chae-ri Kim)

2015년 8월 서울여자대학교
정보보호학 학사
2016년~현재 연세대학교 정보대학원
석사과정

email : cofl921107@naver.com