J. Korea Saf. Manag. Sci. Vol. 17 No. 3 September 2015
http://dx.doi.org/10.12812/ksms.2015.17.3.205

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

정보보호 활동이 정보경영성과에 미치는 영향에 관한 실증분석

손 태 현* · 박 정 선*
*명지대학교 산업경영공학과

Empirical analysis on Information Management Performance Impact of Information Security activities

Son Tae Hyun* · Park Jung Sun*
*Dept. of Industrial and Management Engineering, MyongJi University

Abstract

This study aims to verify the structural correlation empirically between information security performance and information management performance. To verify the correlation, three factors such as managerial controlled activity, technical controlled activity, and physical controlled activity are divided for the information security activities variable. the security performance are divided into accident prevention and accident response variables. As a result, security organization activity is a unique factor being positively significant to information security and management performance. And three activities such as human security, security training, development security do not affect at all on both information security and management performance.

keywords : Information Security, Information Protection, Security Performance

1. 서 론

인터넷의 생활화와 사회의 정보화 혁명은 새로운 산업을 창출하고 생산의 부가가치를 높이는 긍정적 효과를 가져 오기도 했으나 개인정보의 침해로 인한 재산상의 피해와 인권 침해 사례들은 정보보호의 중요성을 더욱 강조하고 있다. 기업의 정보화 기반이 대량화, 고도화 될수록 다양한 데이터와 정보가 증가하고 있으며 이를 안전하고 효율적으로 관리하는 것이 경영 목적을 달성하기 위한 핵심 역량으로 부상하고 있다. 정보시스템의 보안위험이 기업의 대외 이미지 하락, 브랜드 가치 하락, 신뢰성 추락, 매출 감소 등 유무형의 손실을 초래할 가능성이 상존하고 있기 때문에 정보보호에 관한 관심이 고조되고 있고 정보보호에 대한 투자가 크게 증가하는 추세를 보이고 있다. 정보의 위험은 기업과 조직의 생사를 결정하는 중요한 경쟁력이 되었고 기업의 정보보호는 매우 중요한 성공 요소가 되었다.

온라인 및 모바일 환경에서 개인정보의 주체인 이용자들은 자신의 개인정보가 노출되거나 유출되어 오·남용되는 것은 아닌지 하는 불안감을 느끼고 있으며 기업의 경우도 과거에 비해 개인정보보호가 중요하다는 것을 심각하게 인식해가고 있다. 하지만 이용자와 기업 모두 개인정보보호의 중요성에 공감하면서도 구체적으로 어떤 조치를 취하여야 하고 어떻게 개인정보를 보호해야 하는지에 대해서는 충분한 지식을 갖지 못하는 경우가 많다. 정보 유출은 개인정보의 수집, 이용, 제공, 파기 등 개인정보 생명주기에 걸쳐 전 방위적으로 발생하고 있어 종합적인 예방, 점검 체계가 시급하다고 할 수 있다.

†Corresponding Author: Park Jung Sun,
Dept. of Industrial and Management Engineering, Myongji University,
E-mail: jspark@mju.ac.kr
Received April 17, 2015; Revision Received September 23, 2015; Accepted September 23, 2015.

개인정보 침해사고가 대형화, 지능화 되고 있을 뿐만 아니라 개인 이용자의 불안감도 날로 증폭되고 있는 상황에서 개인정보의 안전 조치는 정보주체의 기대에 미치지 못하고 있어서 정부 및 기업에 의한 정보보호 장치 마련의 필요성이 어느 때보다 크다고 할 수 있겠다.

기업의 비즈니스는 ICT 기술혁명으로 환경 변화를 겪게 되었고 새로운 비즈니스 기회제공으로 매출과 이익을 극대화하고 있으며 정보자산과 정보 전략은 비즈니스 성공의 핵심으로써 사업의 성패를 좌우하고 있다.

이에 대하여 기업은 보유한 정보에 대하여 다양한 통제수단을 통해 보호활동을 하고 있으나 보안수준의 강도를 높게 할수록 업무 불편함과 효율성 및 생산성이 단기적으로 감소하는 현상이 발생하고 있다. 따라서 기업에서는 정보보호 관리를 체계화하고 보호할 정보 대상과 범위, 방법과 수준을 정의하여 체계적이고 효율적인 정보보호 관리체계가 되도록 균형을 맞춰야 한다.

그리고 보유하고 운영하는 정보자산을 식별하고 중요도에 따라 기밀성, 무결성, 가용성을 평가하고 내재되어 있는 취약점과 외부의 위협요인을 파악하여 적절한 보호대책을 수립하는 등 일련의 정보보호 활동이 필요한 시점이다. 그러나 많은 기업들이 정보보호활동을 일시적이고 소극적인 사업으로 인식하고 있으며 이러한 인식부족이 정보보호활동을 조직적이고 체계적으로 수행하는데 장애물이 되고 있으며 정보보호 프로세스의 정립을 방해하고 단지 단편적인 통제활동 중심으로 실행되고 있는 것이 현실이다.

기업 정보보호활동 평가 항목 및 세부 지표에 대한 범용성 및 적용성의 결여로 인해 기업 정보보호활동의 가운데 어느 요인이 더 중요한지에 대한 중요도 혹은 가중치 부여가 의사결정자의 주관 혹은 이해관계 당사자 기업 및 기관에 따라 유동적일 수 있으므로 객관화된 기업 정보보호활동 핵심 요인의 도출을 위해서는 기업의 정보보호성과에 실제로 영향을 미칠 수 있는 기업 정보보호활동을 실증분석을 통해 통계적으로 검증함으로써 그 요인들을 도출하고 아울러 상대적 중요성을 검증할 필요가 있다.

기업의 정보 및 개인정보 유출 등 각종 침해사고를 발생시키는 문제를 해결하기 위해서는 정보보호 관리체계 구축 및 운용 등과 같은 기업차원의 정보보호활동이 수반되어야 한다. 국내에도 여러 가지 정보보호 관리체계에 대한 제도를 운용하고 있지만(장상수, 2011), 관리체계 프레임워크에 대한 연구가 부재하고 기업에서 실제 관리체계를 운용하면서 이러한 정보보호활동이 정보보호 성과에 미치는 영향에 관한 연구는 매우 제한적이며, 특히 구체적으로 어떠한 정보보호활동 요인이 어떠한 경영 성과와 투자 효과에 영향을 미치는지에 대한 구체적인 실증적 연구와 개별 정보보호 활동에 대한 효율성 진단과 비용 효과성 분석도 더욱 많은 연구가 필요한 실정이다. 따라서 기업의 정보보호 활동 유형에 따라 정보보호성과의 어떤 측면에 어느 정도 영향을 미치는지를 실증적으로 검증하는 것은 매우 가치 있는 일이 될 것이다.

이에 본 연구는 기업의 정보보호활동 유형에 따라 실제 정보보호성과 및 기업의 정보경영성과 간의 구조적 인과관계를 실증적으로 검증하는 것을 목적으로 하며 구체적인 검증목표를 다음과 같이 설정하였다.

첫째, 기업의 정보보호활동 유형이 기업의 정보보호성과에 미치는 영향을 검증한다.

둘째, 기업의 정보보호성과가 기업의 정보경영성과에 미치는 영향을 검증한다.

셋째, 기업의 정보보호활동 유형이 기업의 정보경영성과에 미치는 영향을 검증한다.

넷째, 기업의 정보보호활동 유형이 기업의 정보경영성과에 미치는 영향에 있어서 기업의 정보보호성과가 어떠한 영향을 미치는지 검증한다.

이와 같은 검증을 통하여 기업은 정보보호활동을 통한 통제의 성과와 실효성을 평가하고 경영성과 달성을 위한 정보보호 활동의 합리적 운영방향을 수립한다면, 정보보호활동이 경영 목적에 일치하는 성과를 거둘 수 있을 것이다.

2. 관련 연구

정보보호 성과와 관련한 선행 연구동향을 살펴보면 정보보호활동에 따른 기업 혹은 조직의 투자효과를 분석하기 위한 정보보호성과 척도가 매우 다양하고 정보보호 비용에 해당하는 투자대상이 명확하지 않아서 투자 의사결정 및 정보보호 개선 방향 도출에 어려움이 있고 정확한 정보보호성과에 대한 효과성 분석이 주요 이슈가 되어왔다. 개인정보보호에 대한 투자의 비용과 효과를 측정하기 위해서 적절한 척도의 도출은 매우 중요하다.

선한길(2005)의 연구에서는 국내 기업의 정보보호 정책 및 조직 요인이 정보보호 성과에 미치는 영향을 실증적으로 검증하였는데, 정보보호 투자에 대한 성과를 정보보호 사고의 감소, 자산의 손실건수 감소, 비즈니스 기회손실 감소, 타사 경쟁 시 손해 감소, 이미지 실추건수 감소, 사고발생시 신속한 처리 등으로 구분하고 성과측정을 하위요인화 하였다[1].

이종선(2007)의 연구에서는 조직차원에서 체계적인 정보보호 활동을 유지하며, 목표수준에 적합한 투자비

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

용을 위해서는 위험분석이 선행되어야 한다고 하며, 보호대상으로서의 자산, 위협, 취약성에 대한 분석과정으로 위험규모의 평가를 실시하고 위험분석 결과를 토대로 위험 규모를 평가 방법을 제안하였다[2].

홍기향(2003)의 연구에서는 정보보호 통제와 활동이 정보보호 성과에 미치는 영향을 실증적으로 검증하였는데, 정보보호 성과는 정보보호 사고를 예방하는 소극적 성과로부터 정보보호와 관련된 대내외적인 변화를 감지하여 능동적으로 대처하도록 하는 조직의 정보보호 체질강화와 같은 적극적 성과에 이르기까지 정보보호 성과를 정보보호사고, 최고경영자, 정보보호조직, 직원, 공급자/협력자, 고객, 공공 총 7개의 변수로 하위요인화 하였다[3].

이희명·임종인(2008)의 연구에서는 기업의 정보보호 수준 측정 모델 및 개발에 관한 연구를 수행하였는데, 측정지표를 통제항목 중심으로 균형성과 지표 방법론(Balanced Scorecard, BSC) 기반의 3가지 지표 영역별로 구분하여 기반지표 9개, 이행지표 9개, 결과지표 9개 총 27개의 측정 지표를 제안하였다. 기반지표는 기업의 정보보호 체계를 각 영역별로 측정하기 위한 원칙과 기준을 중심으로 지표를 선정하고, 이행지표는 실제 업무 수행과정에서 정보보호 규정이나 프로세스를 실천하는 정도를 측정할 수 있는 지표를 선정하였으며, 마지막으로 결과지표는 기반지표와 이행지표의 최종결과로서 나타나는 보안수준을 정량적으로 측정할 수 있는 지표를 선정하였다[4].

또한, ISA 인터넷 & 시큐리티 이슈에서는 ISMS 인증이 기업의 성과에 미치는 영향을 정형화된 업무처리를 위한 효율성 개선, 글로벌 비즈니스 기회 증대, 침해사고 피해비용 절감의 3가지 주요 지표별로 정보보호성과를 측정하였다.

3. 연구 방법

3.1 조사 대상

본 조사에서는 수도권 소재 기업 정보보호 실무자 180명을 대상으로 직접 방문 또는 e-메일 설문을 통해 전체 180부의 설문지를 배포하였다. 이들 기업 정보보호 실무자를 표본 집단으로 하여 2014년 6월 첫째 주부터 6주 동안 설문을 실시하였으며, 총 설문지 180부 가운데 불성실한 응답을 제외하고 유효한 자료 172부만 최종 분석에 활용하였다[Table 1]. 설문조사의 경우 응답에 협조한 조사대상자들에게 충분한 설명과 양해를 구한 후 자기기입법에 의하여 설문지를 작성하도록 하였다.

3.2 모형 및 가설

3.2.1 연구 모형

본 연구에서는 독립변인으로 기업의 정보보호활동 변인을, 종속변인으로는 기업의 정보경영성과 변인을 설계하였으며, 아울러 이들 변인들 간의 인과관계에 있어서 매개변인으로 기업의 정보보호성과 변인을 투입하였다. 기업의 정보보호활동 변인의 하위 요인으로는 관리적 통제활동 요인, 기술적 통제활동 요인, 물리적 통제활동 요인 등 3개의 요인으로 하위 요인화하였다. 또한 각 하위 요인은 각각 세분화하여 요인화하였다, 기업의 정보보호성과 변인의 경우 사고예방 요인과 사고대응 요인 등 2개의 하위요인으로 요인화하였고, 마지막으로 기업의 정보경영성과 변인의 경우 경영목표 달성, 비용절감, 이미지 향상 등으로 측정하고자 하였다[5].

<Table 1> Survey Content

Survey Period	June 1st, 2014 ~ July 15th, 2014
Population	Nationwide Enterprise Security Staffs
Sampling	metropolitan Enterprise Security Staffs (172 persons)
Questionnaire number	172 significant answer from 180 questionnaires
Survey Method	Personal visit or e-mail survey

3.2.2 연구 가설

[Figure 1]과 같은 연구 모형을 기초로 하여 다음과 같은 가설을 도출하였다.

가설 1. 조직의 정보보호활동은 정보보호성과에 영향을 미칠 것이다.

가설1-1 : 조직의 정보보호활동은 사고예방성과에 영향을 미칠 것이다.

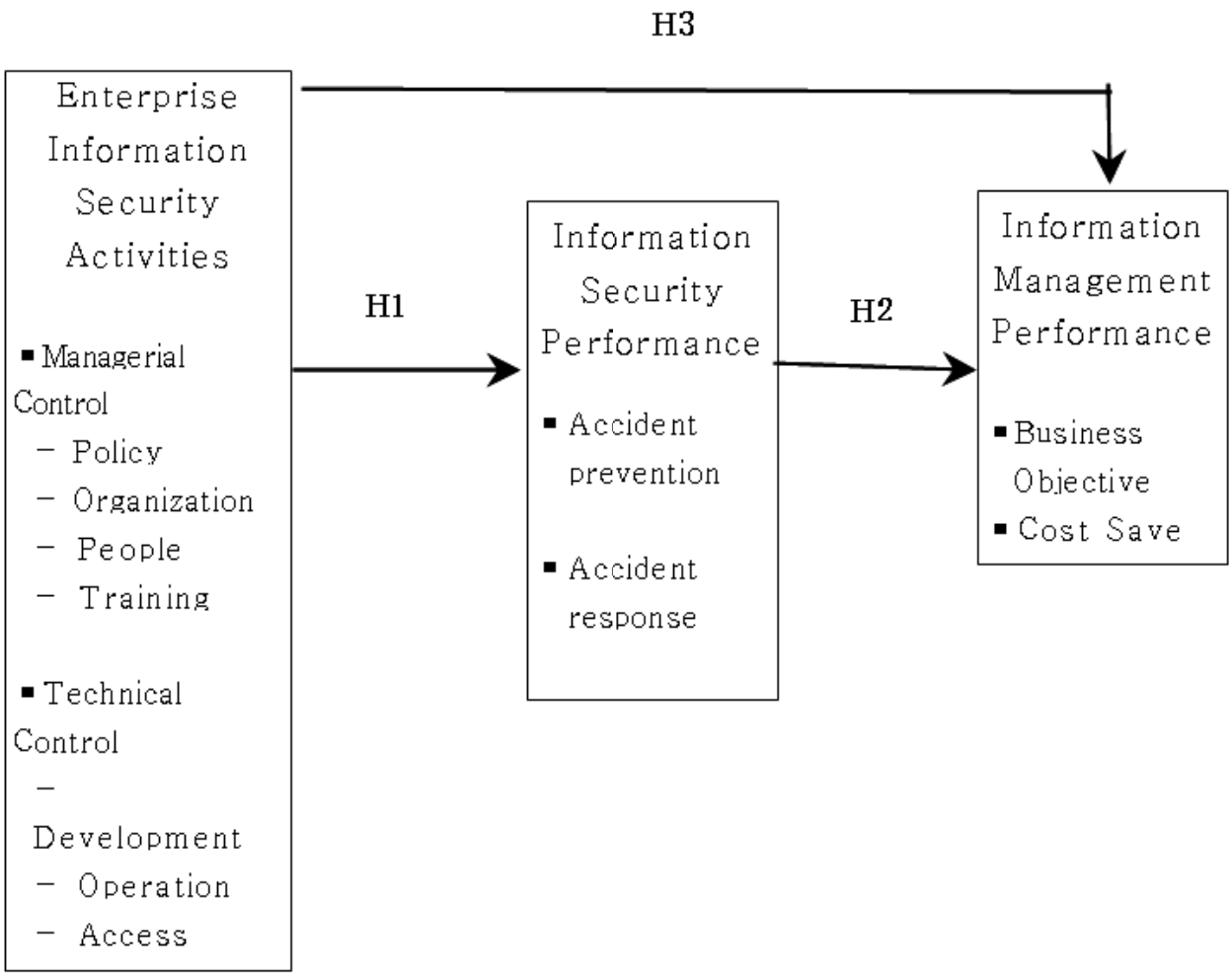
가설1-1-1 : 조직의 관리적 통제는 사고예방성과에 영향을 미칠 것이다.

가설1-1-1-1 : 조직의 보안정책은 사고예방성과에 영향을 미칠 것이다.

가설1-1-1-2 : 조직의 보안조직은 사고예방성과에 영향을 미칠 것이다.

가설1-1-1-3 : 조직의 인적보안은 사고예방성과에 영향을 미칠 것이다.

가설1-1-1-4 : 조직의 보안교육은 사고예방성과에 영향을 미칠 것이다.
가설1-1-2 : 조직의 기술적 통제는 사고예방성과에 영향을 미칠 것이다.
가설1-1-2-1 : 조직의 개발보안은 사고예방성과에 영향을 미칠 것이다.
가설1-1-2-2 : 조직의 운영보안은 사고예방성과에 영향을 미칠 것이다.
가설1-1-2-3 : 조직의 접근통제는 사고예방성과에 영향을 미칠 것이다.
가설1-1-3 : 조직의 물리적 통제는 사고예방성과에 영향을 미칠 것이다.
가설1-1-3-1 : 조직의 문서보안은 사고예방성과에 영향을 미칠 것이다.
가설1-1-3-2 : 조직의 출입보안은 사고예방성과에 영향을 미칠 것이다.
가설1-2 : 조직의 정보보호활동은 사고대응성과에 영향을 미칠 것이다.
가설1-2-1 : 조직의 관리적 통제는 사고대응성과에 영향을 미칠 것이다.
가설1-2-1-1 : 조직의 보안정책은 사고대응성과에 영향을 미칠 것이다.
가설1-2-1-2 : 조직의 보안조직은 사고대응성과에 영향을 미칠 것이다.
가설1-2-1-3 : 조직의 인적보안은 사고대응성과에 영향을 미칠 것이다.
가설1-2-1-4 : 조직의 보안교육은 사고대응성과에 영향을 미칠 것이다.
가설1-2-2 : 조직의 기술적 통제는 사고대응성과에 영향을 미칠 것이다.
가설1-2-2-1 : 조직의 개발보안은 사고대응성과에 영향을 미칠 것이다.
가설1-2-2-2 : 조직의 운영보안은 사고대응성과에 영향을 미칠 것이다.
가설1-2-2-3 : 조직의 접근통제는 사고대응성과에 영향을 미칠 것이다.



[Figure 1] Research Model

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

가설1-2-3 : 조직의 물리적 통제는 사고대응성과에 영향을 미칠 것이다.
가설1-2-3-1 : 조직의 문서보안은 사고대응성과에 영향을 미칠 것이다.
가설1-2-3-2 : 조직의 출입보안은 사고대응성과에 영향을 미칠 것이다.

가설 2. 조직의 정보보호성과는 정보경영성과에 영향을 미칠 것이다.

가설2-1 : 조직의 사고예방성과는 정보경영성과에 영향을 미칠 것이다.
가설2-2 : 조직의 사고대응성과는 정보경영성과에 영향을 미칠 것이다.

가설 3. 조직의 정보보호활동은 정보경영성과에 영향을 미칠 것이다.

가설3-1 : 조직의 관리적 통제는 정보경영성과에 영향을 미칠 것이다.
가설3-1-1 : 조직의 보안정책은 정보경영성과에 영향을 미칠 것이다.
가설3-1-2 : 조직의 보안조직은 정보경영성과에 영향을 미칠 것이다.
가설3-1-3 : 조직의 인적보안은 정보경영성과에 영향을 미칠 것이다.
가설3-1-4 : 조직의 보안교육은 정보경영성과에 영향을 미칠 것이다.

가설3-2 : 조직의 기술적 통제는 정보경영성과에 영향을 미칠 것이다.
가설3-2-1 : 조직의 개발보안은 정보경영성과에 영향을 미칠 것이다.
가설3-2-2 : 조직의 운영보안은 정보경영성과에 영향을 미칠 것이다.
가설3-2-3 : 조직의 접근통제는 정보경영성과에 영향을 미칠 것이다.

가설3-3 : 조직의 물리적 통제는 정보경영성과에 영향을 미칠 것이다.
가설3-3-1 : 조직의 문서보안은 정보경영성과에 영향을 미칠 것이다.
가설3-3-2 : 조직의 출입보안은 정보경영성과에 영향을 미칠 것이다.

3.2.3 측정도구 정의

(1) 기업 정보보호활동

본 연구의 독립변수인 기업 정보보호활동 변인은 Ariss(2002), Kevin(2002)이 제시한 관리적 요인, 기술적 요인, 시스템적 요인을 토대로 이정환(2013)의 연구에서 사용한 측정도구를 본 연구의 목적에 맞게 수정 보완하여 사용하였다. 본 연구에서는 기업 정보보호활동의 하위요인은 관리적 통제, 기술적 통제, 물리적 통제 요인으로 하위 요인화하였으며, 관리적 통제 요인의 경우 보안정책, 보안조직, 인적보안, 보안교육 요인으로 측정하였으며, 기술적 통제 요인의 경우 개발보안, 운영보안, 접근통제 요인으로 측정하였고, 물리적 통제 요인의 경우 문서보안, 업무보안, 출입보안 요인으로 측정하였다. 본 변수는 Likert 5점 척도로 설문을 구성하였으며, 점수가 높을수록 기업 정보보호활동 수준이 높음을 의미한다[5].

(2) 기업 정보보호성과

본 연구의 매개변수인 기업의 정보보호성과 변인은 장상수(2012)의 연구에서 사용한 측정도구를 본 연구의 목적에 맞게 수정 보완하여 사용하였다. 본 연구에서는 기업 정보보호성과의 하위요인은 사고예방, 사고대응 요인으로 하위 요인화하였으며, 사고예방 요인의 경우 유출차단, 보안인식 요인으로 측정하였으며, 사고대응 요인의 경우 대응력 향상, 피해감소 요인으로 측정하였다. 본 변수는 Likert 5점 척도로 설문을 구성하였으며, 점수가 높을수록 기업 정보보호성과 수준이 높음을 의미한다[6].

(3) 기업 정보경영성과

본 연구의 종속변수인 기업의 정보경영성과 변인은 장상수(2012)의 연구에서 사용한 측정도구를 본 연구의 목적에 맞게 수정 보완하여 사용하였다. 본 연구에서는 기업 정보경영성과의 하위요인은 경영목표 달성, 비용 절감, 이미지 향상 요인으로 하위 요인화하여 측정하였다. 본 변수는 Likert 5점 척도로 설문을 구성하였으며, 점수가 높을수록 기업 정보경영성과 수준이 높음을 의미한다[6].

3.3 분석 방법

본 연구를 위해 수집된 자료의 통계 처리는 SPSS

18.0 프로그램과 AMOS 18.0 프로그램을 이용하여 분석하였다.
첫째, 조사대상 기업과 기관의 특성을 알아보기 위해 빈도와 백분율을 산출하였다.
둘째, 연구변인 구성항목들의 신뢰도를 검증하기 위하여 Cronbach's α 계수를 산출하였고, 타당성 검증을 위해 확인적 요인분석(CFA)을 실시하였다.
셋째, 조사대상 공기업과 사기업의 주요 특성에 따라 연구변인들의 차이를 알아보기 위해 t 검정과 일원변량 분석(One-way ANOVA)을 실시하였다.

이상의 통계적 분석과 가설 검증의 유의수준은 α =.05, α =.01, α =.001에서 검증하였다.

4. 연구가설 검증

(1) 가설 1 검증: 정보보호활동과 정보보호성과와의 관계

조직의 정보보호활동이 사고예방과 사고대응성과 등의 정보보호성과에 유의한 영향을 미칠 것으로 예측한 가설 1을 검증한 결과는 다음과 같다.

먼저 정보보호활동이 사고예방성과에 미치는 영향을 살펴보면, 관리적 통제활동 변인 중에서는 보안조직 변인만이 사고예방성과에 유의한 정(+)의 영향(표준화 경로계수=0.202, t=3.155, p<0.01)을 미치는 것으로 나타났고, 보안정책과 인적보안, 보안교육은 사고예방성과에 유의한 영향은 미치지 않았다. 따라서 적절하게 구성된 보안조직은 사고예방에 긍정적인 영향을 미치고 있음을 알 수 있어 가설 1-1-1-2는 지지되었으나, 가설 1-1-1-1, 1-1-1-3, 1-1-1-3은 기각되었다.

기술적 통제활동 변인 중에서는 운영보안(표준화 경로계수=0.173, t=2.091, p<0.05)과 접근통제(표준화 경로계수=0.192, t=2.710, p<0.01) 변인이 사고예방성과에 유의한 정(+)의 영향을 미치는 것으로 나타나 운영보안과 접근통제가 잘 이루어질수록 사고예방성과는 높아지는 것으로 나타나 가설 1-1-2-2와 1-1-2-3은 지지되었으나, 가설 1-1-2-1은 기각되었다. 물리적 통제활동 변인인 문서보안(표준화 경로계수=0.148, t=2.297, p<0.05)과 출입보안(표준화 경로계수=0.242, t=3.333, p<0.001) 변인은 모두 사고예방성과에 유의한 정(+)의 영향을 미치는 것으로 나타나 문서보안과 출입보안이 잘 이루어질수록 사고예방성과가 높아지는 것으로 예측되어 가설 1-1-3-1과 1-1-3-2는 모두 지지되었다.

다음으로 정보보호활동이 정보보호성과 중 사고대응성과에 미치는 영향을 살펴보면, 관리적 통제활동 변인 중에서는 보안정책(표준화 경로계수=0.160, t=2.260, p<0.05)과 보안조직(표준화 경로계수=0.189, t=3.065, p<0.01) 변인이 사고대응성과에 유의한 정(+)의 영향을 미치는 것으로 나타났고, 인적보안과 보안교육은 사고대응성과에 유의한 영향은 미치지 않았다. 따라서 조직의 보안정책이 잘 수립되고 보안조직이 잘 구성되어 있을수록 사고대응성과는 높아지는 것으로 예측되어 가설 1-2-1-1과 1-2-1-2는 지지되었으나, 가설 1-2-1-3과 1-2-1-3은 기각되었다. 기술적 통제활동 변인 중에서는 접근통제 변인만이 사고대응성과에 유의한 정(+)의 영향(표준화 경로계수=0.197, t=2.878, p<0.01)을 미치는 것으로 나타나 접근통제가 잘 이루어질수록 사고대응성과는 높아지는 것으로 예측되어 가설 1-2-2-3은 지지되었으나, 가설 1-2-2-1과 1-2-2-2는 기각되었다.

물리적 통제활동 변인 중에서는 문서보안 변인이 사고대응성과에 유의한 정(+)의 영향(표준화 경로계수=0.250, t=4.020, p<0.001)을 미치는 것으로 나타나 문서보안이 잘 이루어질수록 사고대응성과가 높아지는 것으로 예측되어 가설 1-2-3-1은 지지되었으나 1-2-3-2는 기각되었다.

(2) 연구가설 2의 검증: 정보보호성과와 정보경영성과와의 관계

조직의 정보보호성과는 정보경영성과에 유의한 영향을 미칠 것으로 예측한 가설 2를 검증한 결과, 사고예방(표준화 경로계수=0.285, t=3.127, p<0.01)과 사고대응(표준화 경로계수=0.458, t=4.842, p<0.001) 성과 변인은 정보경영성과에 모두 유의한 정(+)의 영향을 미치는 것으로 나타났다. 따라서 조직의 사고예방과 사고대응 성과가 높을수록 정보경영성과는 높아지는 것으로 예측되어 가설 2-1과 2-2는 모두 지지되었다.

(3) 연구가설 3의 검증: 정보보호활동과 정보경영성과와의 관계

조직의 정보보호활동이 정보경영성과에 유의한 영향을 미칠 것으로 예측한 가설 3을 검증한 결과는 다음과 같다.

먼저 정보보호활동이 정보경영성과에 미치는 영향을 살펴보면, 관리적 통제활동 변인 중에서는 보안조직 변인만이 정보경영성과에 유의한 정(+)의 영향(표준화 경로계수=0.265, t=3.290, p<0.01)을 미치는 것으로 나타났고, 보안정책과 인적보안, 보안교육은 정보경영

성과에 유의한 영향은 미치지 않았다. 따라서 보안조직이 잘 구성되어 있을수록 정보경영성과는 높아지는 것으로 나타나 보안조직은 직접적으로 정보경영성과에 영향을 미치는 예측되어 가설 3-1-1은 지지되었으나, 가설 3-1-2, 3-1-3, 3-1-4는 기각되었다. 한편, 기술적 통제활동 변인인 개발보안, 운영보안, 접근통계 변인은 정보경영성과에 직접적으로 유의한 영향을 미치지 않은 것으로 나타나 가설 3-2-1, 3-2-2, 3-2-3은 모두 기각되었고, 물리적 통제활동 변인인 문서보안과 출입보안 변인 역시 정보경영성과에 직접적으로 유의한 영향을 미치지 않은 것으로 나타나 가설 3-3-1과 3-3-2는 모두 기각되었다.

<Table 2> Results on hypothesis testing

Hypothesis					Non-STD Coefficient	STD Coefficient	STD Error	t-value	p	Results
Managerial Control	1-1-1-1	Policy	→	Prevent Effect	.054	.067	.059	.911	.362	Reject
	1-1-1-2	Organization	→	Prevent Effect	.170	.202	.054	3.155	.002	Accept
	1-1-1-3	People	→	Prevent Effect	-.022	-.025	.064	-.347	.728	Reject
	1-1-1-4	Training	→	Prevent Effect	.037	.044	.052	.710	.478	Reject
Technical Control	1-1-2-1	Development	→	Prevent Effect	-.058	-.069	.059	-.985	.325	Reject
	1-1-2-2	Operation	→	Prevent Effect	.157	.173	.072	2.091	.037	Accept
	1-1-2-3	Access Control	→	Prevent Effect	.156	.192	.058	2.710	.007	Accept
Physical Control	1-1-3-1	Document	→	Prevent Effect	.157	.148	.060	2.297	.022	Accept
	1-1-3-2	Entrance	→	Prevent Effect	.195	.242	.058	3.333	.000	Accept
Managerial Control	1-2-1-1	Policy	→	Prevent Effect	.124	.160	.055	2.260	.024	Accept
	1-2-1-2	Organization	→	Prevent Effect	.155	.189	.051	3.065	.002	Accept
	1-2-1-3	People	→	Response Effect	-.107	-.123	.060	-1.781	.075	Reject
	1-2-1-4	Training	→	Response Effect	.022	.027	.049	.460	.645	Reject
Technical Control	1-2-2-1	Development	→	Response Effect	.089	.109	.055	1.615	.106	Reject
	1-2-2-2	Operation	→	Response Effect	.058	.069	.067	.865	.387	Reject
	1-2-2-3	Access Control	→	Response Effect	.155	.197	.054	2.878	.004	Accept
Physical Control	1-2-3-1	Document	→	Response Effect	.257	.250	.064	4.020	.000	Accept
	1-2-3-2	Entrance	→	Response Effect	.097	.124	.055	1.769	.077	Reject
	2-1	Prevention	→	Management Effect	.254	.285	.081	3.127	.002	Accept
	2-2	Response	→	Management Effect	.420	.458	.087	4.842	.000	Accept
Managerial Control	3-1-1	Policy	→	Manegement Effect	-.071	-.100	.063	-1.120	.263	Reject
	3-1-2	Organization	→	Management Effect	.199	.265	.060	3.290	.001	Accept
	3-1-3	People	→	Manegement Effect	-.081	-.101	.069	-1.174	.240	Reject
	3-1-4	Training	→	Manegement Effect	.008	.010	.055	.138	.890	Reject
Technical Control	3-2-1	Development	→	Manegement Effect	-.049	-.065	.063	-.773	.439	Reject
	3-2-2	Operation	→	Manegement Effect	-.064	-.083	.078	-.824	.410	Reject
	3-2-3	Access Control	→	Manegement Effect	.039	.053	.064	.605	.545	Reject
Physical Control	3-3-1	Document	→	Manegement Effect	.034	.036	.077	.444	.657	Reject
	3-3-2	Entrance	→	Manegement Effect	-.073	-.102	.064	-1.132	.258	Reject

$^{*}p<0.05$, $^{**}p<0.01$, $^{***}p<0.001$

5. 결론

본 연구에서 얻어진 결과[Table 2]를 통해 정보보호활동이 정보보호 성과에 미치는 영향에 관한 실증분석을 통하여 얻은 결론은 아래와 같다.

첫째, 정보보호활동의 하위변인 정보보호성과와 정보경영성과에 유의하게 영향을 미치고 있는 하위변인은 보안조직 활동이 유일한 요인이라는 점이다. 특히 보안조직은 정보경영성과에 영향을 미칠 것이라는 가설을 수용하여 정보보호활동 중 성과에 기여하는 가장 강력하고 중요한 변인이라는 것을 입증하였다.

둘째, 정보보호활동 변인 중 사고예방성과, 대응성과,

정보경영성과 모두에 전혀 영향을 미치지 못하는 활동이 인적보안, 보안교육, 개발보안 3개 활동으로 분석된 것은 이들 정보보호활동이 실행단계에서 정보보호 목표 및 경영목표와 부합하지 않는 단편적이고 단발적인 활동으로 이루어지고 있음을 추정할 수 있다. 특히 관리적 통제의 인적보안 활동은 관행적이고 형식적인 방법으로 수행되어 실질적인 성과를 기대하기 어려운 것으로 판단되며, 보안교육 활동은 법적 의무사항을 준수하기 위한 요식행위로 인식되어 참여자의 자발성과 교육내용의 내실화가 미진한 것이 성과를 거두지 못하는 요인으로 분석되고 있다. 기술적 통제의 개발보안 활동은 어플리케이션 개발자들의 오래된 개발관행이 고착화되어 보안요구사항 등이 반영되지 못하고 있으며 개발조직의 폐쇄성으로 인해 보안관리가 체계적으로 실효성 있게 운영되지 못하고 있으며 그 결과가 정보보호성과로 이어지지 않고 있음을 보여주고 있다.

셋째, 정보보호활동이 성과를 거두기 위해서는 특정 분야에 집중하여 일부 영역에 대해서만 전문성을 확보하는 것 보다는 전사적인 보안조직 구성, 정보보호 기반환경 전반에 대한 접근통제 정책 수립, 사무환경의 문서보안 철저 등 일상 업무환경에서 부터 민감 정보관리에 이르기까지 전반 과정의 보안 평균 수준이 일정 수준을 유지할 수 있도록 정보보호 관리체계를 구축하는 것이 필요할 것으로 판단된다. 정보보호활동과 정보보호 및 정보경영 성과와의 연계성을 높이기 위하여 정보보호 투자를 결정하는 단계에서 보호 대상과 범위, 기대 목표를 설정하고 검증하여 정보경영성과에 기여하도록 비용 효과성과 투자 타당성을 확보하는 노력을 기울일 필요가 있다.

넷째, 연구 가설 중 정보보호활동이 정보보호성과에 영향을 미치는 가설의 채택율이 50%이며 정보경영성과에 영향을 미치는 가설의 채택률이 10%이하로 나타난 것은 정보보호활동의 실효성이 저조하여 정보보호의 목적 달성에 미흡한 현실을 반영하고 있는 것이다. 특히 정보보호활동과 성과 변인들 간의 불일치성은 기업들이 정보보호를 위하여 운영하고 투자하는 리소스 투입을 소비성 비용으로만 인식하고 있으며 조직목표와 경영목표 달성을 위한 생산적 투자라는 인식이 부족한 것으로 해석된다.

이상에서 본 바와 같이 현행의 정보보호활동의 결과가 적절히 성과로 이어지는 활동이 있는 반면에 성과에 기여하지 못하는 활동도 여전히 있는 것을 확인할 수 있었다. 또한 정보보호활동에 대한 우선순위와 중요도에 따른 가중치를 반영한 전략적 투자가 필요한 것으로 판단된다. 이러한 상황을 개선하고 진일보된 정보보호활동을 추진하기 위해서는 정보자산에 대한 위험평가를 정기적으로 수행하고 이에 따른 정보보호대책을 수립하여 정보보호 거버넌스를 달성하는 것이 기업의 정보 경쟁력을 확보하는 중요한 과제라고 할 수 있다.

6. References

[1] Sun, Han-gil(2005), "Impacts of Information Security Policies and Organizations on the Information Security Performance in Korean Enterprises", Korean society of management information systems, Vol.2005 No.1, 1087-1095

[2] Lee, Jong-Sun(2007), "Evaluating Information Security Investment using TCO based Security ROI", Graduate School, Korea University, Ph.D. thesis

[3] Hong, Kihyang(2003), "A study on the effect of Information Security Control and Processes on the Performance of Information Security", Graduate School, Kookmin University, Ph.D. thesis

[4] Lee, Hee-Myung•Lim, Jong-In(2008), "A study on the Development of Corporate Information Security Level Assessment Models", Korea institute of Information Security and Cryptology, 18(5), 162-170

[5] Lee, Jeong Hwan(2013), "The Impact on security accomplishment according to Interaction effect of Firm Security Types", Graduate School Hankuk University of Foreign Studies, Master's thesis

[6] Jang, Sangsoo(2012), "The effects of the operation of an information security management system on the performance of information security", Graduate School, Chonnam National University, Ph.D. thesis

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

저 자 소 개

손 태 현

연세대학교 수학과에서 이학사, 서울대학교 대학원 계산통계학과에서 이학석사 취득. 명지대학교 대학원 산업경영공학과 공학박사 취득. 현재 정보보호 컨설팅 Primus 대표

관심분야 : 개인정보보호, 산업정보보안, 위험관리

박 정 선

서울대학교에서 학사, 한국과학기술원에서 석사학위를 취득하였고, 미국 텍사스주립대학교 경영학박사를 취득하였으며, 현재는 명지대학교 산업경영공학과 교수로 재직중이다. 연구분야는 BSC-IT, Green IT, 정보 보안 등