

전사적 보안협업을 위한 핵심성공요인에 관한 연구

도정민*, 김정덕**

중앙대학교 경영학과 석사과정*, 중앙대학교 산업보안학과 교수**

A Study on Critical Success Factors for Enterprise Security Collaboration

Jung-Min Do*, Jungduk Kim**

Dept. of Business Administration, The Graduate School of Chung-Ang Univ.*

Dept. of Industrial Security, The College of Business & Economics of Chung Ang Univ.**

요약 전사적 보안을 위한 요구사항은 점차 커지고 있는 반면, 이를 구현하기 위한 수단 중 하나인 보안협업에 대한 연구는 매우 미흡하다. 따라서 본 논문은 보안협업에 대한 개념 정립을 통해 보안협업의 유형을 분석하고, 효과적인 보안협업 수행을 위한 핵심 성공요인들을 파악하고자 한다. 이를 위해 조직관리 분야에서의 기존 연구를 조사 분석하여 보안협업 모델을 정립하였고, 협업에 영향을 미치는 요인 및 보안특성을 반영하여 협업 인력, 협업 프로세스, 협업 환경 등 세 영역에서 여덟 개의 변수를 도출하였다. 본 연구는 경력 3년 이상 보안 및 IT 전문가 106명의 데이터를 수집, PLS-SEM를 사용하여 검증을 하였다. 본 연구의 결과로는 협업 구성원의 신뢰성, 전문성, 참여 동기와 협업 성과기준, 최고경영자의 의지, 협업지원도구 등이 보안협업에 영향을 미치는 요인으로 나타났다.

주제어 : 정보보호, 정보보호 조직, 정보보호 관리, 정보보호 협업 핵심성공요인, 전사적 보안 협업

Abstract Although the requirement of enterprise security implementation has been raised, a few research on security collaboration, which is one of the methods for enterprise security has been performed. This paper approached information security from the collaboration-centric perspective and propose critical success factors for security collaboration. In this study, a model of security collaboration, which includes coordination and cooperation activities was devised. Based on the previous research on organizational collaboration literature, the eight success factors for collaboration were deduced and examined the significance of the eight factors using the PLS-SEM statistical method with data of 106 samples who are security and IT professionals who have worked for more than 7 years. The result of the hypothesis test supported that trust, expertise motivation, collaboration performance criteria, top manager support and collaboration tools are the prominent factors of security collaboration.

Key Words : security, security organization, security management, security collaboration, CSF

* 본 논문은 2014년도 중앙대학교 연구장학기금 지원에 의해 수행되었습니다.

Received 4 August 2014, Revised 6 September 2014

Accepted 20 October 2014

Corresponding Author: Jungduk Kim

(Dept. of Industrial Security, The College of Business & Economics of Chung Ang Univ.)

Email: jdkimsac@cau.ac.kr

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0>), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. 서론

정보보호의 패러다임은 기술적 관점에서 비즈니스적 관점으로 변화되고 있으며, 이에 따라 정보보호 거버넌스에 대한 중요성이 증대되고 있다. 즉, 보안활동을 통한 조직 내 유기적인 상호작용이 중요해짐으로 인해 정보보호는 더 이상 단일 부서의 이슈가 아닌 전사적 이슈로 확대되고 있다[20]. 이에 따라 기존 정보보호 조직 관련 연구에선 정보보호 거버넌스를 성공적으로 이끌기 위해 문화정착, 행동양식, 업무의 효율성 제고, 기술과 관리의 정합성 등을 주장하기도 했다[25,26,27]. 그러나 전사적인 정보보호 문화 도입 및 전략적 연계 실패, 부적절한 권한과 책임의 할당, 조직의 보안 인식 미흡 등의 이유로 전사적 정보보안 활동에 어려움이 존재하고 있다[21]. 이러한 문제는 정보보호 전담조직 뿐만 아니라 관련 사업 부서들과의 협업(collaboration)을 통해 해결할 수 있다[28, 31].

따라서 본 연구는 전사적 보안활동을 원활하게 진행하기 위한 주요 수단인 협업에 대한 개념 정립과 협업에 영향을 미치는 요인을 분석하여 핵심성공요인을 제시하고자 한다. 이를 위해 선행연구를 통해 일반적인 조직협업에 영향을 미치는 요인들을 도출하고 보안특성을 반영한 요인을 적용하여 보안협업 성공요인 모형을 설계한다. 마지막으로 실증연구를 통해 연구요인 간 상관관계 및 중요요인을 분석하고 궁극적으로 전사적 정보보호활동을 위한 보안협업 성공요인들을 제시하고자 한다.

2. 관련 연구

2.1 협업의 개념

협업과 유사한 의미로 협동(cooperation), 조정(coordination) 등의 개념이 있으며 협업과 혼용해서 사용되고 있다. 협동은 “조직간 공헌과 성과에 대한 이해를 일치시키는 방식으로 합치된 목적(goal)을 달성시키기 위한 공동의 활동”이라 할 수 있다[8]. Mattessich[14]은 “협동은 상호간 이익과 공통의 목적을 달성하기 위한 정보 교환, 활동/역할 변경, 자원 공유”로 정의하고 있다.

Horwath[11]은 조정이란 “공동의 작업을 좀 더 형식화하지만 비 준수에 따른 제제가 없는 일종의 작업유형”

이라 말한다. 다른 연구에서는 조정을 “내부 조직간 함께 결정한 목적을 달성하기 위해 정보교환, 조직간 커뮤니케이션 등을 활용한 연계(alignment) 혹은 조율(adjustment)하는 일련의 활동”이라 말한다[8,19].

협업은 조직간 다른 비즈니스 영역에서 공동의 작업을 촉진시키는 프로세스이다[4]. Gulati[8]는 협업을 조정과 협동간의 균형을 맞추는 활동을 말하며 조직간 협업은 조정과 협동을 포함하는 말로써 정의한다. 협업은 일련의 프로세스로서 조직 간의 공유된 목표, 자원 활용을 위한 공동의 책임 등 단순 정보 교환에서 의사결정을 위한 공동의 업무까지 조직간 관계가 긴밀해 질수록 단계가 높아진다고 할 수 있다[11].

위 연구를 통해 협업은 공동의 작업의 가장 큰 문맥으로 그 하위 개념으로 협동 및 조정으로 분류할 수 있다.

2.2 협업에 영향을 주는 요인

이웅찬[29]는 사슬관리 관점의 공동업무를 바라보았다. 정보기술, 활성화지원, 파트너쉽, 계획과 운영, 성과관리 등 5개의 카테고리로 협업 성공을 이끌 수 있는 요인을 나누었으며 조직 내의 관점보다 조직 간의 관점으로 연구를 접근하였다.

Forest[7]은 소규모 개인 구성원간의 협업을 대상으로 파트너쉽, 협업 정당성, 의사소통, 목적설정, 책임/계획, 멤버 역량(skills), 학습과 수행(learns and practices)이 성공적인 협업을 위해 고려해야할 이슈라고 정의하고 있다.

Meng[15]은 제조, 구매, 소매, 공급 등의 활동을 영위하는 산업을 대상으로 파트너간의 관계에 영향을 주는 요인을 전문가 인터뷰를 통해 도출하였다. Meng[15]이 제시한 요인은 총 여덟 가지로 상호목적, 자원공유, 신뢰, 문화, 공동업무, 의사소통, 문제해결, 위험할당, 성과측정, 지속적 개선을 포함하고 있다.

Dean[5]은 기업 내 협업을 촉진시키는 요인을 양적연구를 통해 도출, 그 요인이 서비스 기업의 성과에 어떤 영향을 미치는지 조사하였다. Dean[5]은 협업을 촉진시키는 요인으로 신뢰, 리더십, 문화, 갈등관리 등 네 개로 도출하였고 이 요인들은 서비스기업 협업의 성공을 결정짓는 잣대가 될 수 있다고 말한다.

Winer[22]은 목적을 달성하기 위해 사람간의 관계설정 및 협업에 관한 설계, 역할 결정, 평가, 성공요소 등의

내용을 다루고 있다. Winer[22]는 협업의 성공요소를 환경, 멤버 특징, 프로세스/구조, 의사소통, 목적, 자원 등 5가지를 제시하고 있다.

Amabile[1]은 질적/양적 연구를 거쳐 의료연구 분야 간의 연구협업에 대해 긍정적 영향을 미치는 요인을 팀, 환경, 프로세스 등 세 가지 영역으로 구분하였다. 그밖에도 이상곤[28], Groenewegen[9], Horwath[11] 등의 연구에서 멤버특성, 신뢰, 조직 환경, 역할, 의사소통, 인센티브, 동기부여 등 협업에 영향을 주는 요인을 제시하였다.

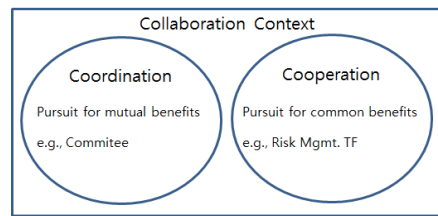
2.3 보안협업 성과

보안협업의 궁극적인 목적은 전사적 보안 수준을 향상시키는 것이라 할 수 있다[16,24]. 또한 보안협업은 전사적 활동을 통해 비즈니스의 목표 및 전략을 지원함으로써 비즈니스와의 연계성 높여야 한다[13]. 또한 조직협업은 협업 활동을 통해 조직변화에 대한 대처능력의 유연성이 증대될 수 있다[27].

위 연구들을 통해 본 연구의 종속변수인 보안협업의 성과는 전사적 보안수준 향상, 비즈니스와 정보보호 연계, 보안 대처능력의 유연성을 성과 척도로 설정하였다.

2.4 보안협업 모델 정의

본 연구에서는 정보보호 실무적 차원에서 활용할 수 있는 협업모델을 제시한다. 즉 협업(collaboration)은 [그림 1]에서 보는 바와 같이 조정(coordination)과 협동(cooperation)을 포함하는 광의의 개념으로 정의하였다. 조정은 전사적 보안을 위해 관련 부서간의 의견수렴 및 갈등해결을 위한 활동이라 말할 수 있다. 예를 들어, 정보보호 위원회, 보안 실무 협의회 등을 구성하여 보안 활동에서의 갈등 조정, 전사적 협력을 도모하기 위한 활동을 포함한다. 협동은 공통된 목적을 달성하기 위해 활발한 정보교환 및 책임할당, 역할 수행 등을 포함하는 활동이라 말할 수 있다. 예를 들어, 정보보호 위험분석 수행이라는 공동의 목표를 위해 보안부서, IT부서, 현업부서의 멤버들이 모인 작업팀을 구성하여 활동할 수 있다. 협업은 전사적인 정보보호 활동을 수행하기 위해 위와 같은 조정 및 협동 활동이 적절하게 수행되는 것을 말한다. 조정 활동과 협동 활동은 목적 및 조직 특성에 따라 능동적으로 선택할 수 있다.

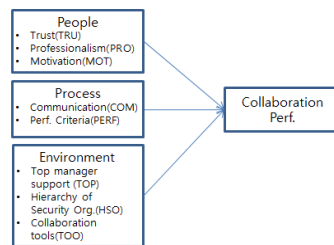


[Fig. 1] Security Collaboration Model

3. 연구 모형과 가설

3.1 연구 모형 및 가설 도출

본 연구는 '2. 관련연구'에 언급된 협업 요인 중 공통된 요인을 묶고 보안의 특성을 반영하여 8개의 보안협업 성공요인을 도출하였으며(<Table 1> 참고) 도출된 보안협업 성공요인과 보안협업 성과간의 관계를 연구모형으로 설계하였다([Fig. 2] 참조).



[Fig. 2] Research Model

<Table 1> Factors of Security Collaboration

People			Process		Environment			Auth.
TRU	PRO	MOT	COM	PERF	TOP	HSO	TOO	
			○	○	○		○	[32]
○	○	○	○				○	[31]
	○		○	○				[7]
○		○	○	○				[17]
○		○	○		○			[5]
	○	○	○	○	○		○	[11]
○	○	○	○	○	○			[26]
○		○	○	○	○			[1]
○		○	○					[6]
○	○	○	○	○			○	[12]
		○			○	○	○	[30]
	○		○	○	○		○	[27]
								[29]
○	○				○	○	○	[20]
								[24]
	○		○	○	○	○	○	[14]

3.1.1 협업 인력

인력(people) 영역은 협업 프로젝트 관련 인력에 대한 신뢰성, 전문성, 동기(motivation)의 세 요인으로 구성하였다. 신뢰성이란 조직 내에서 협동적 행동을 이끌 수 있는 요인으로 개인/팀의 행동이 긍정적 기대를 가져올 것이라는 의도 혹은 믿음을 말한다[5]. 멤버들의 신뢰가 부족하다면 성과에 부정적인 결과를 가져 올 수 있다 [7,9,11].

협업을 구성하기 위해선 개인/팀의 기술이 숙련되었는지 그리고 적절하게 배치되었는지 확인해야 한다[7]. 협업을 운영하는 기술-적절한 관리감독, 협업의 목표설정 등-또한 중요하다[1]. 즉 협업관련 전문성이 높을수록 협업 목표를 달성하기 용이하다.

협업의 운영은 직원의 동기부여에 따라 상이하게 나타난다. 개인/팀의 태도와 동기부여는 협업을 구성 시 고려해야하는 측면으로 중요하다[11].

따라서 인력 관련해서 아래와 같은 3가지 가설을 도출할 수 있다. 즉, **보안 협업에 참여하는 인력의 신뢰성이 높을수록(H1-1), 전문성이 높을수록(H1-2), 동기부여가 높을수록(H1-3), 보안협업 성과에 긍정적 영향을 미칠 것이다.**

3.1.2 협업 프로세스

협업 프로세스란 협업을 위한 의사소통, 성과측정 등의 방법을 통한 일련의 협업과정을 의미한다. 협업이 성공하기 위해서는 협업 구성원 간의 의사소통이 원활하게 가능해야하며 협업 구성원간의 형식적/비형식적인 상호작용을 하는 방법에 따라 협업의 결과가 다르게 나타날 것이다[9,10]. 또한 협업 구성원들 간의 갈등해소는 협업 성과에 긍정적인 영향을 끼칠 것이다[1,22].

협업조직의 지속적인 수행을 위해선 조직의 성과측정을 수행해야 하고 그에 상응하는 보상체계가 필요하다 [15]. 또한 협업의 성공을 위해선 협업 업무의 평가와 반영을 수행하는 프로세스가 요구된다.

따라서 협업 프로세스 관련해서 아래와 같은 2가지 가설을 도출할 수 있다. 즉, **보안 협업조직의 성과측정 프로세스가 잘 정립될수록(H2-1), 협업 의사소통(H2-2)이 활발할수록, 보안협업 성과에 긍정적 영향을 미칠 것이다.**

3.1.3 협업 환경

협업 환경이란 공동체에서 업무성과를 낼 수 있는 환경을 조성하는 것으로 협업성과에 영향을 미친다[22]. 특히 전사적 보안을 위해서는 최고경영자의 의지와 지원이 매우 중요하며 협업 활동에 대한 적극적인 격려가 요구된다[10]. 또한 전사적 보안을 수행하고 여러 부서와의 협업을 가능하게 하기 위해서는 정보보호 부서의 위상이 높아야 한다[18].

그룹웨어, 메신저 등 성공적인 협업을 지원해주는 IT 도구는 협업을 유기적이며 효율적인 의사전달을 가능하게 한다[3]. 특히, 높은 수준의 협업일수록 수행 문제를 해결하기 위한 지원 시스템이 필요하다[11]. 따라서 협업 환경 관련해서 아래와 같은 3가지 가설을 도출할 수 있다. 즉, **최고경영자의 협업수행 의지가 높을수록(H3-1), 정보보호부서의 위상이 높을수록(H3-2), 협업지원 도구의 활용도가 높을수록(H3-3), 보안협업 성과에 긍정적 영향을 미칠 것이다.**

4. 실증 분석

본 연구에서 제시한 가설을 검증하기 위해 구조방정식을 사용하였다. 구조방정식은 각 경로계수를 비교 분석하기에 용이하기 때문에 본 연구에 적합하다. 본 연구의 위해 수집된 자료는 SPSS 18.0을 활용하여 기본 통계 분석을 실시하였고 본 연구가설의 검증을 위한 모형전체의 적합도, 타당도, 신뢰도, 요인별 상관관계, 경로계수 값 등은 Smart PLS 2.0 사용하여 추정하였다.

4.1 표본 구성 및 측정 도구 개발

보안 및 IT 관련 전문가를 대상으로 총 127개의 설문 수집을 하였다. 설문 방법은 온라인과 오프라인으로 나누어 진행하였으며 무응답, 불성실 응답 및 3년 미만의 경력의 응답자를 제외한 총 106개의 설문을 검증자료로 사용했다. 일반 통계결과의 결과는 다음과 같다. 실무경력은 '15년 이상' 42.5%, '7년 이상 11년 미만' 23.6%, '7년 미만' 17.9%, '11년 이상 15년 미만' 16.0% 등의 순으로 나타났다. 담당업무는 '컨설팅업무'를 하는 사람이 가장 높게 나타났으며(39.6%) 조정 및 협동 두 협업유형을 경험한 비율은 51.9%로 나타났다. 현재 협업 조직에 참여

하고 있는 비율은 ‘예’ 62.3%, ‘아니오’ 36.8%로 나타났다.

본 설문문의 모집단을 대표하는 적정 수준의 표본크기를 Chin[34]과 G*Power 방법을 통해 구하였다. Chin[34]은 PLS를 위한 적정 표본크기는 변수 당 10개 이상이 좋다고 말하였으며, G*power를 통해 도출한 표본크기는 (효과크기 0.15, 유의수준 0.05, power 0.8) 50개 이상이면 검증에 유의한 표본크기임으로 본 조사에서의 표본 사이즈는 두 요구사항 모두 만족하는 것으로 나타났다.

협업 성공요인의 측정도구는 기존 연구를 바탕으로 설문지를 작성하였다. 모든 측정 도구는 리커트 7점 척도를 사용하였다. 각 변수의 조작적 정의 및 측정 도구의 키워드는 <Table 2>와 같다.

4.2 연구의 타당성 및 신뢰성

본 연구에서 제시한 독립변수의 타당성 및 신뢰성을 확인하기 위해 집중타당도와 판별타당도를 사용하였다. 집중 타당도는 측정항목의 요인분석, 구성개념 (Construct)의 조합 신뢰성, Cronbach's α 및 AVE값에 의해 평가 가능하다. PLS 분석에서 COM2, TRU1 척도는 해당 변수를 정확히 반영하지 못하고 있어 제외한다. 본 연구의 조합 신뢰성은 다음 <Table 3>와 같이 모든 변수는 0.7이상을 나타내기 때문에 모든 변수는 기준을 통과하였다[2]. Cronbach's α 은 역시 일반적으로 0.6이상이면 측정항목에 대한 신뢰도는 만족할 만한 수준으로 보고 있기 때문에 신뢰도는 만족한다. AVE값도 모든 변수는 임계치 0.5를 상회하므로 각 요인별 신뢰성을 확보했다 볼 수 있다. 판별 타당도는 요인분석과 구성개념 (Construct)간의 상관관계로 평가할 수 있는데 평균분산 (AVE)의 제곱근과 요인 간 상관계수로 평가 가능하다 [6]. 본 연구의 상관계수는 한 변수 내에서 AVE 제곱근이 다른 변수들 간의 상관관계보다 크기 때문에 판별 타당성이 충족된다. 그리고 공통성(Communality) 수치는 측정모형의 적합도를 판단하는 기준으로 최소 0.5 이상의 기준을 모두 충족한다.

PLS 경로 모형의 전체 적합도(Goodness of Fit)은 0.25 이상이면 적합하다[27]. 위의 기준으로 본 연구의 전체 모델 적합도는 0.731로 나타나 전체 적합도를 만족한다. 또한 PLS 경로 모형의 주목적인 예측을 위해 Stone-Geiser Q^2 검증 통계량인 교차 검증된 Redundancy 값이 양수를 가리키기 때문에 예측을 충분

<Table 2> Collaboration Factors & Metrics

Domain	Var.	Oper. Define	Indicator	Auth.
People	Trust	The Intent to taking positive action of person or team	mutual respect (TRU1)	[10]
			trust in co-workers (TRU2)	
			expectation of goal achievement (TRU3)	
Professionism	Appropriate deployment of person and team	skilled worker (PRO1)	[10]	
		deployment of appropriate person (PRO2)		
Motivation	The support of action toward a desired goal	incentives (MOT1)	[11]	
		recognition of necessary (MOT1)	[1]	
Process	Communication	Interaction with co-workers	formal communication (COM1)	[10]
			informal communication (COM2)	
			conflict solution (COM3)	[1]
Perf. Criteria	Measurement process of collaboration working	compensation criteria of a person (PERF1)	[28]	
		compensation criteria of a team (PERF2)		
Environment	Support of Top manager	The support of top manager for collaboration	involvement top manager (TOP1)	[12]
			report system (TOP2)	[31]
	Division of status	The Status of collaboration division	status of manager for security (HSO1)	[31]
status of division (HSO2)				
Collaboration tools	Implementation of tools supporting collaboration	tools for communication (TOO1)	[11]	
		method for collaboration support (TOO2)		

〈Table 3〉 PLS analysis overview

변수	AVE	Composite Reliability	R ²	Cronbachs α	Communality	Redundancy	Path coefficient
COM	0.7602	0.8637	0	0.6849	0.7602	0	0.077
PERF	0.8174	0.8995	0	0.7766	0.8174	0	0.119
TOO	0.7335	0.8455	0	0.6512	0.7335	0	0.245
HSO	0.744	0.8522	0	0.6782	0.744	0	-0.011
MOT	0.7446	0.8531	0	0.6671	0.7446	0	0.144
PRO	0.7246	0.8393	0	0.6381	0.7246	0	0.164
Col-Perf	0.691	0.8694	0.5458	0.7756	0.691	0.0084	
TRU	0.8226	0.9026	0	0.7847	0.8226	0	0.207
TOP	0.7722	0.8712	0	0.7131	0.7722	0	0.414

Goodness of fit = 0.731

히 하고 있다고 말할 수 있다. 추가로 변수 간 상관관계를 나타내는 다중 공선성(Multi-Collinearity)의 기준치인 .80은 모든 변수에서 작게 나타났기 때문에 다중공선성의 문제는 없다고 말할 수 있다. 마지막으로 요인분석을 확인하면 각 요인별 값이 다른 측정항목에 비해 높게 나타나고 있고 COM2, TRU1을 제외한 나머지 값은 0.7 이상을 가리키기 때문에 COM2, TRU1을 제외한 나머지 척도들은 판별타당성을 갖는다고 할 수 있다.

4.3 연구 결과

본 연구의 가설 검증을 위해 보안 및 IT 종사자를 대상으로 PLS 구조모형 기법을 사용하여 결과를 도출하였다. 경로계수를 추정하기 위해 부트스트랩을 통해 표본수의 수를 입력 후 500회 샘플링 반복을 하였다. PLS 모델은 측정변수의 분포에 대한 가정이 없고 모수추정방법 또한 최소자승법이기에 때문에 표준오차가 계산되지 못한다. 그러므로 모수 추정 값에 대한 통계적 검증은 부트스트랩을 사용하였다[6].

실증분석 결과, 가설 4와 7을 제외하고는 모두 채택되었다<Table 4>. 즉 구성원 간 의사소통과 정보보호 부서의 위상은 통계적으로 유의한 차이가 없는 것으로 나타났다. 그 밖의 가설은 통계적으로 유의한 차이를 보였다. 구성간의 의사소통이 협업을 위해서 중요하다고 판단되었으나, 상대적으로 타 요인에 비해 덜 중요한 것으로 판명되었으며, 정보보호 부서의 위상은 협업의 성과와 크게 관계가 없다는 시사점을 도출할 수 있었다.

〈Table 4〉 Test Results

Hypothesis path	Path coef.	T-test	p	Accept /reject
TRU -> Perf	0.207	3.0267	**	Accept
PRO -> Perf	0.164	2.6009	**	Accept
MOT -> Perf	0.144	2.3034	*	Accept
COM -> Perf	0.077	1.0166		reject
CRI -> Perf	0.119	2.043	*	Accept
TOP -> Perf	0.414	6.0908	**	Accept
HSO -> Perf	-0.011	0.1702		reject
TOO -> Perf	0.245	2.8127	**	Accept

*p<.05 **p<.01

5. 결론 및 향후 연구

본 연구는 전사적 보안을 실행하기 위해 협업의 중요성을 강조하고 협업 성공요인을 파악하였다. 최고경영자의 의지, 협업지원도구, 협업 인력의 신뢰성, 전문성, 동기, 평가기준 등의 순으로 중요하다고 나타났다. 특히 최고경영자의 의지가 가장 높은 영향을 미친다는 연구결과는 많은 시사점을 주고 있다. 그리고 보안부서의 위상보다 보안기능을 효과/효율적으로 수행할 수 있는 도구(IT 활용 협업도구, 의사결정 방법론 등)나 동기부여에 따라 협업의 성과가 더 높게 나타난다는 점은 주목해야 할 것이다.

본 연구의 한계점은 다음과 같다. 첫째, 본 실증 연구는 협업 경험을 가지고 있는 관리자 또는 전문 인력을 대상으로 조사하였으나, 현재 협업 조직에 직접 참여하고 있지 않은 인력(36.%)를 포함하고 있기 때문에 향후에는 협업에 직접 참여하는 인력을 대상으로 연구를 진행할 필요가 있다.

둘째, 보안협업 유형을 정립하였으나 유형에 따른 협업요인의 유의성 차이를 밝히지 못했다. 협업의 유형을 조정과 협동 활동으로 구분하여 정의하였으나 본 연구에서는 별도로 구분하지 않고 협업 전반적 차원에서 실증 분석을 하였다. 향후에는 협업 유형별 실증분석을 함으로써 구체적 성공요인을 도출할 계획이다.

ACKNOWLEDGMENTS

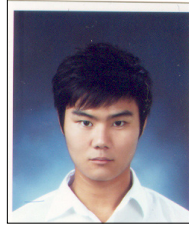
This study was supported by the Chung-Ang Univ. research scholarship in 2014.

REFERENCES

- [1] T.M. Amabile et al, "Academic-practitioner collaboration in management research: A case of cross-profession collaboration," *Academy of Management Journal*, vol. 44, no. 2, pp. 418-431, Apr 2001.
- [2] R.P. Bagozzi and Y. Yi, "On the evaluation of structural equation models," *Journal of the academy of marketing science*, vol. 16, no. 1, pp. 74-94, Spr 1988.
- [3] P.H. Carstensen and K. Schmidt, "Computer supported cooperative work: New challenges to systems design," 1999.
- [4] P. Danese, "Towards a contingency theory of collaborative planning initiatives in supply networks," *Int J Prod Res*, vol. 49, no. 4, pp. 1081-1103, Feb 2011.
- [5] K.S. Dean, "Strategies and Benefits of Fostering Intra-Organizational Collaboration," Dec 2010.
- [6] C. Fornell and F.L. Bookstein, "Two structural equation models: LISREL and PLS applied to consumer exit-voice theory." *Journal of Marketing Research (JMR)*, vol. 19, no. 4, Nov 1982.
- [7] C. Forest, "Empowerment skills for family workers: A worker handbook," Cornell University, 2003.
- [8] R. Gulati, F. Wohlgezogen and P. Zhelyazkov, "The two facets of collaboration: Cooperation and coordination in strategic alliances," *The Academy of Management Annals*, vol. 6, no. 1, pp. 531-583, May 2012.
- [9] Groenewegen L. (2013). "Factors influencing collaboration within a partnership of large infra-structural projects in the netherlands," *TU Delft*, Sep 2013.
- [10] N. Hara, P. Solomon, S. Kim and D.H. Sonnenwald, "An emerging view of scientific collaboration: scientists' perspectives on collaboration and factors that impact collaboration," *J.Am.Soc.Inf.Sci.Technol.*, vol. 54, no. 10, pp. 952-965, Aug 2003.
- [11] J. Horwath and T. Morrison, "Collaboration, integration and change in children's services: critical issues and key ingredients," *Child Abuse Negl.*, vol. 31, no. 1, pp. 55-69, Jan 2007.
- [12] ISO/IEC "27001:2013. Information security management," 2013
- [13] ISO/IEC "27014:2013. Information security governance," 2013
- [14] P. Mattesich, M. Murray-Close and B. Monsey, "Collaboration: What makes it work - areviewoftheresearchliteratureonfactorsinfluencing successfulcollaboration," *SaintPaul,MN:AmherstH.WilderFoundation*, May 2001.
- [15] X. Meng, M. Sun and M. Jones, "Maturity model for supply chain relationships in construction," *J.Manage.Eng.*, vol. 27, no. 2, pp. 97-105, Mar 2011.
- [16] R.T. Moulton and M.E. Moulton, "Electronic communications risk management: a checklist for business managers," *Comput.Secur.*, vol. 15, no. 5, pp. 377-386, 1996.
- [17] D.B. Parker, "The strategic values of information security in business," *Comput.Secur.*, vol. 16, no. 7, pp. 572-582, 1997.
- [18] S. Posthumus and R. Von Solms, "A framework for the governance of information security," *Comput.Secur.*, vol. 23, no. 8, pp. 638-646, Dec 2004.
- [19] B. Singh, "Collaboration and competition tensions in multi-unit organizations facing volatile business

- environments." CASE WESTERN RESERVE UNIVERSITY, Dec 2005.
- [20] B. von Solms, "Information security - the fourth wave," *Comput.Secur.*, vol.25, no.3, pp.165-168, May 2006.
- [21] J.R. Westby, "How boards & senior executives are managing cyber risks," *Governance of Enterprise Security: CyLab 2012 Report*, pp. 1-28, May 2012
- [22] M.B. Winer and K.L. Ray, "Collaboration handbook," Amherst H. Wilder Foundation, Apr 1994.
- [23] K.K. Wong, "Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS." *Marketing Bulletin*, vol. 24. 2013
- [24] K W Kim and J D Kim, "A Study on Critical Success Factors for Implementing Information Security Governance," *Journal of Digital Convergence*, Vol.8, no.4, pp.97-108, Dec 2010.
- [25] J D Kim and S I Lee, "A study on cases of nation introduction and international standardization for security governance," *KIISC REVIEW*, vol.22, no.6, pp.9-14, Oct 2012.
- [26] J D Kim and K H Hong, "A Review on security issues and research," *KIISC REVIEW*, vol.17, no.4, pp.18-25, Aug 2007.
- [27] D H Lee, "An Exploratory Study on Information Security Governance Components in the View of Manager," *The University of Chung Ang*, 2012.
- [28] S G Lee & S B Cho, "A Study on the Success Factors of On-line Collaboration for Manufacturing Innovation Using AHP Analysis," *KITS*, vol.10, no.3, pp.1-19, Sep 2011.
- [29] E C Lee & M I Chae, "A Study on Key Success Factors of SCM Applying AHP," *Korean Journal of Logistics*, vol.17, no.1, pp.53-77, 2009.
- [30] W.W. Chin, "Commentary: Issues and opinion on structural equation modeling." *MIS Quarterly*, Vol. 22, No. 1, pp. 7-16, Mar 1998.
- [31] "5 critical instructions for innovation of security ", <http://korea.emc.com/about/news/press/korea/2014/20140107.htm>, EMC

도 정 민(Do, Jung Min)



- 2012년 8월 : 중앙대학교 정보시스템학과 학사
- 2012년 9월 ~ 현재 : 중앙대학교 경영학과 석사과정
- 관심분야 : 정보보호 거버넌스, 정보보호 조직, 보안 관리
- E-Mail : ehwjalds@naver.com

김 정 덕(Kim, Jungduk)



- 1979년 2월 : 연세대학교 정치외교학과(학사)
- 1981년 8월 : 연세대학교 경제학과 대학원(석사)
- 1986년 8월 : Univ. of S. Carolina, MBA
- 1990년 12월 : Texas A&M Univ., Ph. D. in MIS
- 1995년 3월 ~ 현재 : 중앙대학교 교수
- 관심분야 : 정보보호 거버넌스, 정보보호 관리, IT 감사
- E-Mail : jdkimsac@cau.ac.kr