Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.4, Aug. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.4.915

정보보호 위원회 활동에 따른 정보보호 거버넌스 구현 효과에 관한 연구*

김 건 우,† 김 정 덕‡
중앙대학교

A study on effects of implementing information security governance by information security committee activities*

Kunwoo Kim,† Jungduk Kim‡
Chung-Ang University

요 약

정보보호 거버넌스의 주체는 최고경영층이지만 여전히 정보보호 활동에 대한 최고경영층의 참여는 미흡한 실정이다. 이러한 상황에서 정보보호 위원회는 최고경영층의 정보보호 활동 참여를 활성화 하는데 좋은 방법이 될 수 있으며, 결국 정보보호 위원회 활동은 정보보호 거버넌스 구현을 위한 필수 요소라 할 수 있다. 본 연구의 목적은 정보보호 위원회의 활동이 정보보호 거버넌스 구현과 보안효과에 미치는 영향을 확인하는 것이며, 실증연구 분석을 위해 설문조사를 실시하였고, 수집된 자료는 PLS(Partial Least Square)를 이용하여 측정모형 및 구조모형 검정을 실시하였다. 연구 결과, 가치전달과 관련된 가설이 기각되었으며, 향후 정보보호가 비즈니스에 긍정적인 가치를 전달할 수 있는 방안에 대한 연구가 필요하다.

ABSTRACT

The commitment of top management is still insufficient for information security even the core of information security governance is dependent on the leadership of top management. In this situation, information security committee can be a good way to vitalize the commitment of top management and its activities are essential for implementing information security governance. The purpose of this study is to test that information security committee affects implementing information security governance and security effect. For a empirical analysis, questionnaire survey was conducted and the PLS(Partial Least Square) was used to analyze the measurement and structural model. The study result shows that a hypothesis related value delivery is not accepted and it is required to study various methods about how the information security provides positive value to business.

Keywords: Information Security Governance, Information Security Committee

I. 서 론

비즈니스 환경이 복잡해지고 위험이 다변화되고 있으며, DDoS 공격, 카드사 개인정보 유출 등과 같은 대형 보안사고가 끊이지 않고 발생하고 있다[1]. 최근에는 정보보호를 위한 최고경영층의 역할 및 책임이 중요시되고 있으며 정보보호 거버넌스 구현에 대한 관심이 높아지고 있다. 하지만 정보보호 거버넌

접수일(2015년 7월 2일), 수정일(2015년 7월 21일), 게재확정일(2015년 8월 3일)
* 본 논문은 2015년도 중앙대학교 CAU GRS 지원에 의하여 작성되었습니다.
† 주저자, kunwoo.kim317@gmail.com
‡ 교신저자, jdkimsac@cau.ac.kr(Corresponding author)

스의 핵심인 최고 경영층의 참여는 여전히 미흡한 실정이다. 정보보호 위원회 활동은 정보보호 거버넌스 구축에 필수적이고 최고 경영층 참여를 위한 좋은 방법이 될 수 있다[2]. 하지만 국내에서는 정보보호 위원회 관련 연구가 거의 이루어지고 있지 않으며, 해외에서는 시장조사 기관인 Gartner 등에서 일부 연구가 진행되고 있다[3].

이에 본 연구에서는 정보보호 위원회 및 정보보호 거버넌스에 대한 개념을 알아보고, 정보보호 위원회 활동이 정보보호 거버넌스 구현 및 보안효과에 미치는 영향을 확인하고자 한다. 이를 위하여 국내 정보보호 담당자 및 전문가에 대한 설문조사를 통해 수집된 자료를 이용하여 이를 실증적으로 분석하였다.

II. 이론적 배경 및 연구가설

2.1 정보보호 위원회

정보보호 위원회는 지속적이고 포괄적인 정보보호 프로그램 지원을 위한 협의체를 의미하며[2], 일반적으로 CISO 및 CIO 등 정보보호 관련 임원과 HR, 법무 등 지원부서의 임원, 현업 임원 및 담당자로 구성된다. 국내 정보보호 분야의 학위논문 및 학술지에는 정보보호 위원회 관련 연구가 없으며, 정부차원에서 개인정보보호 위원회 등에 대한 일부 연구 존재하고, 해외의 경우 이론적으로는 Todd Fitzgerald의 연구, 실무적으로는 Gartner의 연구가 대표적이라고 할 수 있다[2][3].

Todd Fitzgerald는 정보보호 위원회에 대하여 형성기, 갈등기, 규범기, 성과기의 라이프 사이클 관점에서 연구를 수행하였으며[2], Gartner에서는 정보보호 정책 및 전략 승인, 정보보호 예산 할당 및 승인, 정보보호 활동 결과 및 예외사항 검토, 갈등 조정의 정보보호 위원회의 6가지 활동을 제시하고 있다[3]. 또한 전사적 정보보호 활동을 위해서는 정보보호와 비즈니스와의 전략적 연계, 정보보호 위험 완화 등 정보보호 거버넌스 요구사항과 상충되는 다양한 갈등을 조정하는 것을 정보보호 위원회의 핵심으로 설명하고 있다.

2.2 정보보호 거버넌스

2013년 제정된 정보보호 거버넌스 관련 국제표준인 ISO/IEC 27014에서는 정보보호 거버넌스를 정보보호 활동을 지시/감독하기 위한 원칙 및 프로세스의 집합으로 정의하고 있으며, 정보보호 거버넌스의 목표를 비즈니스와의 전략적 연계, 가치 전달, 정보보호 위험 보증을 위한 책임성 수립으로 제시하고 있다[4]. 정보보호의 비즈니스 목표 달성 지원을 보증하기 위해서는 정보보호와 비즈니스를 전략 차원에서 연계해야하며, 이를 위해서 우선 최고경영층은 정보보호 전략 수립 시 비즈니스 요구사항을 반영해야 한다[5]. 또한 업무 프로세스에 정보보호 활동이 포함되어 비즈니스 성과측정 기법을 통해 평가되어야 하며[6], 비즈니스 관련 보안위험이 적절한 수준으로 관리되고 있음을 이해관계자들에게 주기적으로 보고해야 한다[7].

가치 전달이란, 정보보호가 비즈니스 목표달성에 긍정적인 가치를 제공함을 보증하는 것으로, 우선 최고경영층은 정보보호가 조직의 목표달성에 긍정적인 가치를 제공함을 인식해야 하며, 정보보호 투자의사결정 시 조직의 위험과 전략을 고려해야 한다[8]. 또한, 계획에 따라 정보보호 투자를 최적화해야 하며[9], 정보보호 활동의 성과평가를 통해 미흡한 사항을 지속적으로 개선해야 한다[10]. 그리고 정보보호 위험 수준의 보증을 위하여 최고경영층은 업무상의 위험을 포함한 전사적 측면의 보안위험을 고려해야 하며[11], 위험관리 전략 수립 시 조직의 위험성향을 고려해야 한다[12]. 또한, 정보보호 관련 위험 완화를 위한 이해관계자들의 역할 및 책임을 명확히 정의해야 하며[13], 이에 따른 충분한 자원을 할당해야 한다[8]. 결국 정보보호 거버넌스의 성공적인 구현을 위해서는 위와 같은 목표달성 및 최고경영층의 활동이 전제가 되어야 한다고 할 수 있다.

2.3 보안 효과

Jacqueline H. Hall 등은 보안 효과와 관련하여 정보자산의 보호, 관련 법/제도 준수, 보안정책 및 표준 유지, 외부 공격으로부터 즉각적인 대응, 시스템 장애의 신속한 복구, 보안 위험 최소화, 비즈니스 연속성 유지, 정보자산 피해 예방, 정보자산의 효과적인 통제의 9개의 효과를 제시하였다[14]. 하지만, 보안정책 및 표준 유지와 정보자산의 효과적인 통제는 보안 효과가 아닌 선행 활동이며, 시스템 장애의 신속한 복구는 정보보호 보다는 IT 운영 효과에 가까우므로, 본 연구에서는 상기의 보안 효과 중 6개의 효과를 채택하여 측정하였다.

2.4 연구가설 및 모형

본 연구에서는 Fig. 1.과 같이 정보보호 위원회의 활동이 정보보호 거버넌스 구현에 긍정적인 영향을 미칠 것이라는 가설(H1~H3)과 정보보호 거버넌스 구현이 보안 효과에 긍정적인 영향을 미칠 것이라는 가설(H4~H6)을 설정하였으며, 각각의 연구가설은 다음과 같다.

H1(+): 정보보호 위원회 활동은 비즈니스와 정보보호의 전략적 연계에 긍정적인 영향을 미칠 것이다.
H2(+): 정보보호 위원회 활동은 정보보호 가치 전달에 긍정적인 영향을 미칠 것이다.
H3(+): 정보보호 위원회 활동은 정보보호 위험 보증을 위한 책임성 수립에 긍정적인 영향을 미칠 것이다.
H4(+): 비즈니스와 정보보호의 전략적 연계는 보안 효과에 긍정적인 영향을 미칠 것이다.
H5(+): 정보보호 가치 전달은 보안 효과에 긍정적인 영향을 미칠 것이다.
H6(+): 정보보호 위험 보증을 위한 책임성 수립은 보안효과에 긍정적인 영향을 미칠 것이다.

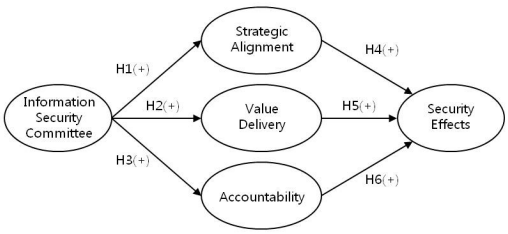

Fig. 1. Research Model

III. 연구 방법

3.1 자료수집 및 표본 특성

본 연구에서는 정보보호 거버넌스에 대한 이해도가 비교적 높은 국내 정보통신, 금융, 제조 등 산업체의 정보보호 담당자(43명) 및 정보보호 컨설턴트(27명) 등 총 70명의 전문가를 대상으로, 2015년 6월 6일부터 13일까지 약 1주간 온라인 설문도구를 이용하여 자료를 수집하였다. 설문대상은 대부분 남성(63명)이었으며, 10년 이상의 정보보호 분야 경력 보유자가 38명 이었다. 또한 산업체의 정보보호 담당자 중 31명이 대기업에 종사하고 있었으며, 임원급 이상이 24명이었다. 설문지는 5점 리커드 척도를 이용하였으며, 총 23개의 항목으로 구성되었다. 완료된 온라인 설문 중 결측치를 포함하는 7개의 설문을 제외한 총 63개의 표본이 분석에 이용되었다.

3.2 변수의 조작적 정의

본 연구에서 사용된 연구변수들의 조작적 정의는 Table 1.과 같으며, 측정도구와 관련된 선행연구를 함께 표기하였다.

Table 1. Definition of Constructs

Construct	Definition	Ref.
Information Security Committee (ISC)	Required activity to information security committee	[3]
Strategic Alignment (SA)	Required activity for alignment with business	[5][6] [7]
Value Delivery (VD)	Required activity for managing value of security	[8][9] [10]
Accountability (AC)	Required activity to ensure level of information risk	[8][11] [12][13]
Security Effects (SE)	Expected effect from information security activity	[14]

본 연구의 독립변수인 정보보호 거버넌스 구현에 요구되어지는 정보보호 위원회의 활동을 측정하기 위하여 정보보호를 위한 역할 및 책임 수립, 정책 승인, 거버닝 프로세스 보증, 예산 승인 및 할당, 전략 검토 및 승인, 성과 검토 여부의 6개의 항목을 선정하였다. 매개변수인 정보보호와 비즈니스의 전략적 연계 정도를 측정하기 위하여 정보보호 전략 수립 시 비즈니스 요구사항 반영, 정보보호 활동의 비즈니스 성과측정 기법을 통한 평가 여부, 비즈니스 관련 보안위험의 주기적인 보고 여부의 3개 항목을 선정하였다.

또한 가치전달의 경우, 최고경영층의 정보보호 가치 인식, 지속적 개선, 투자 위험을 고려한 투자 의

사결정, 계획에 따른 투자 최적화 여부의 4개 항목으로 측정하였으며, 책임성의 경우, 위험 완화를 위한 역할 및 책임 정의, 전사적 보안위험 고려, 조직의 위험성향 고려, 충분한 자원 할당 여부의 4개 항목을 통하여 측정하였다. 끝으로 종속변수인 보안효과는 정보자산 보호, 법·제도 준수, 위험 최소화, 비즈니스 연속성 유지, 피해 예방의 6가지 항목을 통하여 측정하였다.

IV. 연구의 분석 및 결과

본 연구에서는 가설검정을 위하여 PLS 방식을 채택하였으며, SmartPLS 3.0을 이용하여 분석하였다. PLS를 사용한 이유는 상대적으로 적은 표본 수로 복잡한 인과모형의 설명할 수 있으며, 측정모형과 구조모형을 동시에 측정할 수 있기 때문이다[15]. PLS 방법의 경우, 표본 수는 가장 많은 경로를 가진 변수의 경로수의 10배를 초과해야 하는데[15], 본 연구에서는 구성개념 중 정보보호 위원회 활동, 보안효과와 관련된 잠재변수가 6개이고 표본 수는 60개를 초과해야 하므로 최소 표본 수 요구사항을 만족한고 할 수 있다.

4.1 측정 모형의 검정

측정 모형에 대한 평가는 일반적으로 신뢰성, 집중 타당성(Convergent Validity), 판별 타당성(Discriminant Validity)으로 평가할 수 있다. 신뢰성은 크론바하 알파(Cronbach's Alpha) 값이 0.7 이상일 경우, 신뢰성에 문제가 없는 것으로 판단하며[16], 본 연구의 모든 측정항목의 크론바하 알파 값이 Table 2.와 같이 모두 0.7을 상회하므로 신뢰성을 확보했다고 할 수 있다.

집중 타당성은 각 요인의 요인적재값(Factor Loading), 구성개념의 복합신뢰도인 CR(Composite Reliability), 평균분산추출값인 AVE(Average Variane Extracted)로 평가 가능하고, Table 2.와 같이 요인적재 값이 모두 0.7 이상으로 통계적으로 유의하여 단일 차원성이 존재한다고 할 수 있으며, 복합신뢰도(CR)가 모두 0.7 이상이고, 평균분산추출값(AVE)이 0.5 이상이므로, 집중 타당성을 확보한 것으로 나타났다[16].

판별 타당성은 일반적으로 AVE의 제곱근 값과 잠재변수들 간의 상관관계 분석을 통해 평가하며, AVE 제곱근 값이 인접하고 있는 변수들 간의 상관관계보다 클 경우 판별 타당성에 문제가 없는 것으로 판단할 수 있다[16]. 본 연구의 판별 타당성 분석 결과, Table 3.의 진하게 표시된 대각선 값과 같이 AVE 제곱근 값이 인접 변수들의 상관관계보다 크기 때문에 판별 타당성 역시 확보된 것으로 나타났다.

Table 2. Results of Validity and Reliability

Scale Item	Factor Loading	AVE	CR	Cronbach's Alpha
ISC 01	0.703	0.630	0.910	0.881
ISC 02	0.765			
ISC 03	0.898			
ISC 04	0.883			
ISC 05	0.755			
ISC 06	0.739			
SA 01	0.716	0.705	0.877	0.798
SA 02	0.901			
SA 03	0.890			
VD 01	0.752	0.595	0.855	0.775
VD 02	0.789			
VD 03	0.750			
VD 04	0.794			
AC 01	0.778	0.690	0.899	0.849
AC 02	0.909			
AC 03	0.810			
AC 04	0.820			
SE 01	0.823	0.647	0.916	0.890
SE 02	0.783			
SE 03	0.902			
SE 04	0.811			
SE 05	0.770			
SE 06	0.726			

Table 3. Results of Discriminant Validity

Construct	ISC	SA	VD	AC	SE
ISC	**0.794**				
SA	0.673	**0.840**			
VD	0.707	0.738	**0.771**		
AC	0.770	0.690	0.706	**0.831**	
SE	0.632	0.554	0.384	0.592	**0.804**

4.2 구조 모형 및 가설 검정

구조모형의 적합도를 확인하기 위하여 Fig. 2.와 같이 경로분석을 수행하였다. 각 구성개념들 간의 경로계수(Path Coefficient)와 t-값을 부트스트랩핑(Bootsrapping)을 통해 도출하였으며, 부트스트랩핑의 단일표본 복원횟수는 500회로 설정하였다[15].

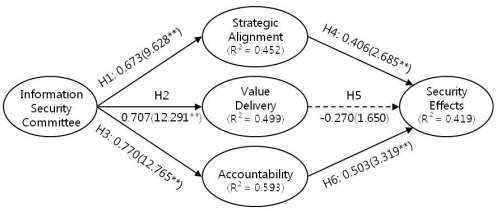

Fig. 2. Results of Path Analysis

분석결과 R^2값이 모두 0.1을 상회하여 각 구성개념에 대한 분산 설명력이 충분한 것으로 나타났다[17]. 또한 Table 4.와 같이 가설5(H5)를 제외한 나머지 경로계수들은 통계적으로 유의수준 0.01에서 지지되어 가설이 채택되었다. 하지만 가설5는 통계적으로 유의하지 않고, 가설 방향이 (-)로 나타나 가치 전달과 보안 효과 간의 직접적인 관계는 지지되지 않아 기각되었다.

정보보호 활동의 긍정적인 가치를 비즈니스 목표 달성을 저해하는 위험요인의 식별 및 조치라고 한다면, 정보유출 등 위험의 발생 가능성은 불확실하며, 보안효과에 대한 가시성이 확보되기 어렵기 때문에 가치전달과 관련된 가설이 기각되었다고 판단된다. 따라서 향후에는 정보보호 가치를 재무적 또는 비재무적으로 측정하고 비즈니스 성과에 반영할 수 있는 방법론에 대한 연구가 수행될 필요가 있다.

V. 결 론

본 연구에서는 최고경영층의 정보보호에 대한 활동 참여 활성화의 한 가지 방법으로 정보보호 위원회의 활동과 정보보호 거버넌스 구현의 관계를 살펴보았으며, 이에 따른 보안효과에 대하여 분석하였다. 본 연구는 정보보호 거버넌스의 중요성이 증대되고, 국내 정보보호 위원회 관련 연구가 미비한 실정에서 수행된 학술적 연구이며, 실무적으로 적용 가능한 정보보호 위원회의 역할을 식별하고 그 효과를 측정한 연구라는 점에서 의의가 있다. 하지만 PLS 방법을 적용함에 있어 최소 표본 수는 만족하였지만, 다른 방법론에 비하여 표본 수가 적기 때문에 일반화에 있어 신중한 접근이 필요하다.

연구 결과, 정보보호와 비즈니스와의 전략적 연계, 긍정적인 가치 전달, 책임성 수립을 위해서는 최고경영층이 참여한 정보보호 위원회 활동이 필요하며, 정보보호 거버넌스 구현을 통하여 정보보호 관련 법률 준수, 정보자산의 손실방지 및 비즈니스 연속성 유지 등의 긍정적인 효과가 있는 것으로 나타났다. 하지만, 가치 전달과 관련된 효과는 통계적으로 유의하지 않은 것으로 나타났으며, 따라서 향후에는 정보보호 활동에 대한 성과 평가, 투자 효과에 대한 타당성 분석 등 정보보호가 제공하는 비즈니스 측면의 긍정적인 가치에 대한 연구가 필요하다고 할 수 있다.

References

[1] Richard A. Caralli, Julia H. Allen, Pamela D. Curtis, David W. White, and Lisa R. Young, "CERT resilience management model version 1.0," Technical Report, CMU/SEI - 2010 - TR - 012, Carnegie Mellon University, May 2010.

[2] Todd Fitzgerald, "Building management commitment through security councils," Information Systems Security, vol. 14, no. 2, pp. 27-36, Feb. 2015.

[3] Tom Scholtz and F. Christian Byrnes, "Information security and governance: forums and committees," G00207477, Gartner, Oct. 2010.

[4] ISO/IEC 27014, "Governance of information security," May 2013.

[5] Shaun Posthumus and Rossouw von Solms, "A framework for the governance of information security," Computers and Security, vol. 23, no. 8, pp. 638-646, Dec. 2004.

[6] Paul Williams, "Information security governance," Information Security Technical Report, vol. 6, no. 3, pp. 60-70, Sep. 2001.

[7] Basie von Solms, "Information security governance: compliance management vs operational management," Computers & Security, vol. 24, no. 6, pp. 443-447, Sep. 2005.

[8] Corporate Governance Task Force, "Information security governance: a call to action," USA, 2004.

[9] Joan Hash, Nadya Bartol, Holly Rollins, Will Robinson, John Abeles, and Steve

Batdorff, "Integrating IT security into the capital planning and investment control process," Special Publication 800-65, National Institute of Standards and Technology, USA, Jan. 2005.
〔10〕 Rossouw von Solms and Basie von Solms, "Information security governance: a model based on the direct - control cycle," Computers & Security, vol. 25, no. 6, pp. 408-412, Sep. 2006.
〔11〕 Rolf Moulton and Robert S. Coles, "Applying information security governance," Computers & Security vol. 22, no. 7, pp. 580-584, Oct. 2003.
〔12〕 Richard M. Steinberg, "Enterprise risk management: integrated framework," COSO, Sep. 2004.
〔13〕 W. Krag Brotby, "Information security governance guidance for boards of directors and executive management," IT Governance Institute, 2006.
〔14〕 Jacqueline H. Hall, Shahram Sarkani, and Thomas A. Mazzuchi, "Impacts of organizational capabilities in information security," Information Management & Computer Security, vol. 19, no. 3, pp. 155-176, 2011.
〔15〕 Chin W.W., "The Partial Least Squares Approach to Structural Equation Modeling," in G. A. Marcoulides(Ed.) Modern Methods for Business Research, Lawrence Erlbaum Associates, pp. 295-336, 1998.
〔16〕 Claes Fornell, and David F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," Journal of Marketing Research, vol. 18, no. 1, pp. 39-50, Feb. 1981.
〔17〕 Falk R.F. and Miller N.B., A Primer for Soft Modeling, The University of Akron Press, Akron, 1992.

〈저자소개〉

김 건 우 (Kun-Woo Kim) 정회원
2008년 8월: 중앙대학교 정보시스템학과 졸업
2010년 2월: 중앙대학교 정보시스템학과 석사
2015년 3월~현재: 중앙대학교 융합보안학과 박사과정
〈관심분야〉 정보보호 거버넌스, 정보보호 관리, 디지털 포렌식

김 정 덕 (Jungduk Kim) 종신회원
1979년 2월: 연세대학교 정치외교학과 졸업
1981년 8월: 연세대학교 경제학과 석사
1986년 5월: University of S. Carolina, MBA
1990년 12월: Texas A&M University, Ph.D. in MIS
1995년 3월~2014년 8월: 중앙대학교 정보시스템학과 교수
2014년 9월~현재: 중앙대학교 산업보안학과 교수
〈관심분야〉 정보보호 거버넌스, 정보보호 관리, 디지털 비즈니스