

Study about the Impact of Information Security Systems on Corporate Performance: Based on IT Relatedness Theory

Ja Myon Koo*, Joo Seok Park**, Jae Hong Park***

According to the development of new Information Technologies, firms consistently invest a significant amount of money in IT activities, such as establishing internal and external information systems. However, several anti-Information activities—such as hacking, leakage of information and system destruction—are also rapidly increasing, thus many firms are exposed to direct and indirect threats. Therefore, firms try to establish information security systems and manage these systems more effectively via an enterprise perspective. However, stakeholders or some managers have negative opinions about information security systems. Therefore, in this research, we study the relationship between multibusiness firms' performance and information security systems.

Information security indicates physical and logical correspondence of information system department against threats and disaster. Studies on information security systems suggested frameworks such as IT Governance Cube and COBIT Framework to identify information security systems. Thus, this study define that information security systems is a controlled system on enterprise IT process and resource on IT Governance perspective rather than independent domain of IT. Thus, Information Security Systems should be understood as a subordinate concept of IT and business processes.

In addition, this study incorporates information capability to information security system literature to show the positive relationship between Information Security Systems and Corporate Performance. The concept of information capability suggested that an interaction of human, information, technical and an effect on corporate performance using three types of capability (IT Practice, Information Management Practice, Information Behaviors and Values). Information capability is about firms' capability to manage IT infrastructure and information as well as individual employees who use IT infrastructure and information. Thus, this study uses information capability as a mediating variable for the relationship between information security systems and firms' performance.

* Ph.D., The School of Management, Kyung Hee University, Seoul, Korea

** Professor, The School of Management, Kyung Hee University, Seoul, Korea

*** Corresponding Author, Assistant Professor, The School of Management, Kyung Hee University, Seoul, Korea

To investigate the relationship between Information Security Systems and multibusiness firms' performance, this study extends the IT relatedness concept into Information Security Systems. IT relatedness provides understanding of how corporations cope with conflicts between headquarters and business units to create a synergy effect and achieve high performance using IT resources.

Based on the previous literature, this study develops the IT Security Relatedness model. IT Security Relatedness is our main independent variable, while Information Capability and Information Security Performance are mediating variables. To control for the common method bias, we collect each multibusiness firm's financial performance and use it as our dependent variable.

We find that Information Security Systems influence Information Capability and Information Security Performance positively, and these two variables consequently influence Corporate Performance positively. In addition, this result indirectly shows that corporations under a multibusiness environment can obtain synergy effects using the integrated Information Security Systems. This positive impact of Information Security Systems on multibusiness firms' performance has an important implication to various stakeholders. Therefore, multibusiness firms need to establish Information Security Systems to achieve better financial performance.

Keywords : Information Security Systems, Information Capability, IT Security Performance, IT Security Relatedness, Corporate Performance

정보보안체계 수립이 Multibusiness 기업 성과에 미치는 영향에 관한 연구: IT Relatedness 이론 관점에서

구 자 면, 박 주 석, 박 재 흥

I. 서 론

급변하는 경영환경으로 인하여 기업은 수많은 리스크에 노출되고 있다. 이런 리스크는 불확실성에 노출로 손해가 발생할 가능성[Lee et al., 1992]을 증대시켰으며, 경제적, 재정적 손실뿐만 아니라 물리적 손상, 손해 및 지연 등과 같은 다양한 손해가 발생할 가능성[APEC, 1999]을 증대시켰다. 특히 이런 리스크는 정보기술(IT) 분야에서도 예외라 할 수 없을 만큼 많은 영향을 미치고 있다. 이에 기업들은 정보보안 체계 수립을 위한 다양한 노력들을 진행하고 있지만, 아직도 많은 기업에서는 정보보안 체계와 같은 통제 체계의 구축이 기업의 성과에 반하는 노력으로 오해하는

경향이 있다. 이는 정보보안에 대한 투자가 기업 영업력이나 업무 효율성의 저하로 이어질 수 있다는 기우에 따른 것으로 정보보안이 기업 성과에 긍정적 영향을 미칠 수 있음을 간과하고 있는 것이다. 하지만, 일부 연구자들의 연구 결과에서 알 수 있듯이 정보보안의 성과는 자산손실의 감소나 비즈니스 손해 건 수 감소 등 다양한 형태로 긍정적인 영향을 미치고 있다[Sun, 2005]. 따라서, 정보보안 체계에 대한 투자는 단순히 보안 문제를 해결하고 침해 사고의 발생 가능성을 줄이는 정도에 만족하는 것이 아니라 정보보안 투자를 통해 기업에 더 큰 이익을 창출해 내는 영역으로 인식되어야 하는 것이다[Suh, 2008].

이에 본 연구에서는 기업의 정보보안에 대한

투자가 기업 성과에 어떠한 영향을 미치고 있는지, 어떠한 요인들이 그 영향선상에 있는지에 대한 보다 명확한 결론을 도출해 보고자 한다. 또한 이를 통하여 정보보안 체계 수립에 대한 효과에 대해 의문을 갖고 있는 다양한 기업내 이해관계자에게 그 해답을 제시해 보고자 한다.

본 연구는 정보보안 체계 수립이 기업 성과에 어떠한 영향을 미치는가에 대한 의문점을 가지고 출발하고 있다. 따라서, 본 연구의 목적은 Multi-business 기업¹⁾ [Huseyin, 2005]에서의 정보보안 체계 수립 이후 정보역량 및 정보보안 성과 향상과 기업성과와의 상관관계를 밝히는 것이다. 연구 모델은 설문조사를 통해 실증적으로 검증하였는데 정보보안 체계의 통합 수립/관리를 하고 있는 국내 상장 대기업 또는 30대 그룹 계열사를 대상으로 21개 기업의 정보전략, 정보기획, 정보보안 등의 담당자에게 설문지를 배포하여 데이터를 수집하였다. 또한, 수집된 데이터를 바탕으로 실증적 검증을 수행하여 정보보안 체계 수립의 기업성과에 대한 영향을 연구해 보았다.

II. 문헌연구

2.1 IT 통제 체계로서의 정보보안

정보보안이란 일반적으로 고의, 과실, 재해 등에 의해 정보시스템이 고장 및 파괴되는 등의 위해를 막기 위한 물리적/논리적 대응[Kwon *et al.*, 2007]이나 또는, 정보의 입력, 처리, 저장, 출력, 전송 등의 모든 단계에 걸쳐서 정보를 보호하는 것 [Suhn, 2005]을 의미한다. 전통적으로 정보보안은 IT 관점에서 스토리지, 프로세싱, 비즈니스 정보 자산의 처리 시의 보호 관점에서 그 중요성이 부

각되었으나[Posthumus *et al.*, 2004] 점차 기술적 이미지에서 벗어나 좀 더 넓은 의미인 전반적인 IT 환경을 보호하는 의미로 인식되고 있다[Basie, 2001]. 이에 더하여 경영층의 자각에 바탕을 둔 전략적, 법적 사항까지 고려해야 하는 인식[Posthumus *et al.*, 2004; Entrust, 2004; Birman, 2000]과 기업 거버넌스의 구성요소로 인식 되어야 하는 당위성 [Basie, 2005]으로 점차 발전되어 가고 있다.

또한, 정보보안 체계는 기업의 IT 거버넌스 관점에서 그 영역을 이해해야 한다. IT Governance Cube[Koen and Harry, 2004]에서는 IT 거버넌스를 크게 IT 프로세스, IT 자원, 그리고 품질기준의 관점인 3차원으로 정의하고 있다. 이중 품질 영역의 보안성, 컴플라이언스, 신뢰성 영역이 각 차원[프로세스, IT 자원]과 결합하여 정보보안 관점의 IT 관리체계가 형성됨을 알 수 있다. 따라서, 정보보안 체계는 그 자체가 독자적인 IT의 한 영역이라기보다는 전체 IT 거버넌스 관점에서 전사 IT 프로세스, 자원에 대한 하나의 통제 체계임을 알 수 있는 것이다. 이는 또한 가장 권위 있는 IT 거버넌스 프레임워크로서 활용되고 있는 COBIT [Control Objectives for Information related Technology] 프레임워크[‘운영과 지원 그룹’에 포함된 프로세스인 ‘시스템 보안성 확보’ 등]를 통해 다시 확인해 볼 수 있다. COBIT과 정보보안 체계에 대한 관계성은 Basie[2005]의 연구를 통해서 나타난다. 우선 Basie는 COBIT이 IT 거버넌스를 위한 Tool이기 때문에 그 자체로 정보보안에 대한 독자적인 프레임워크가 될 수 없다고 말한다. 하지만 COBIT의 세부 통제 항목들 중 일부인 보안 측정 관리, 확인 및 권한/접근 등의 항목 등은 정보보안 체계를 상당히 포함하고 있다고 설명하고 있다. 따라서, 정보보안 체계는 IT Governance Cube와 COBIT 프레임워크를 통해 IT 관리체계 중 하나의 통제 체계로 인식할 수 있다. 이에 더하여 Basie와 Rossouw[2004]는 정보보안 체계를 Corporate Governance Responsibility로 정의하고 기업의 근간을 이루는 비즈니스, 조직, IT 등

1) Multibusiness 기업은 다양한 자회사 또는 다양한 Business Unit을 포함하고 있는 대단위 기업을 의미하는 것으로써 본 연구에서는 국내 30대 그룹 자회사 또는 한국거래소에 상장된 국내 기업에 한정하여 Multibusiness 기업을 정의함.

전영역에 있어 정보보안 체계가 영향을 미치고 있음을 설명함으로써 다차원적 통제 체계 특성을 통한 정보보안 체계의 중요성을 역설하고 있다.

2.2 Multi-business 기업의 IT Relatedness

IT Relatedness 개념은 Huseyin[2005]의 연구에서 처음 제시된 개념으로 Multibusiness 환경 하에서 기업이 어떻게 IT 자원을 활용하여 Head Quarter와 사업단위 간의 대립적인 목적에 균형을 맞추고, 높은 성과를 달성할 수 있을지에 대한 이해를 제공해 주고 있다. 즉, IT Relatedness란 다수의 사업단위가 존재하는 기업 또는 기업집단에서 자신들이 보유한 IT 전략, 프로세스, 자원 등을 연계성, 공유성 관점에서 활용하여 기업 성과를 극대화하는 관리 방안이다. Huseyin은 2005년, 2006년 2편의 논문을 통해 Multibusiness 기업의 시너지 창출과정을 입증하였다.

Huseyin[2005; 2006]은 먼저 IT Relatedness를 정의함에 있어 해당 변수를 구성하는 네 가지 영역을 정의하였다. 네 가지 영역은 (1) IT 인프라의 Relatedness, (2) IT 전략수립 프로세스의 Relatedness, (3) IT 인적자원 관리 프로세스의 Relatedness, (4) IT 벤더 관리 프로세스의 Relatedness이다.

IT 인프라 Relatedness는 개별 사업단위에게 IT 인프라에 대한 모든 자율성을 부여하는 것은 옳지 않으며, 일반적인 하드웨어, 소프트웨어나 커뮤니케이션 기술들은 전사적 표준을 사용하는 것[Huseyin, 2005; 2006]이 기업성과에 긍정적 영향을 미친다는 주장이다. IT 전략수립 프로세스 Relatedness는 Multibusiness 기업이 본부 부서의 간섭을 배제한 사업단위의 자율성을 부여하고, IT 관련 결정을 위한 일반적인 전략적 방향성을 제시할 수 있는 공동의 IT 전략수립 프로세스의 수립이 기업 성과에 긍정적인 영향을 미친다는 내용이다[Huseyin, 2005; 2006]. 이는 사업단위에게 IT 전략 개발을 허용하면서 본부 부서의 전략적 방향성에 부합하게 조정하는 방식으로 기업

내에 적용될 수 있다. IT 인적자원 관리 프로세스 Relatedness는 IT 인적자원이 전사적 방향성을 이해하고 공동의 가치, 목표, 목적, 동기부여를 공유할 때, 기업 성과 시너지 창출에 공헌한다는 개념[Huseyin, 2005; 2006]이다. 사업단위 내에서 공동의 목적, 원칙, 가치, 언어를 공유하는 것은 조직간 공동의 IT 인프라의 창출 및 유지에 중요한 요소이며[Hyuseyin, 2005], 이는 기업 성과에 직접적인 영향을 미칠 수 있는 요인이다.

IT 벤더 관리 프로세스 Relatedness는 사업단위들이 기술과 서비스의 필요성에 따라 IT 벤더와 맺는 여러 관계들에 대해 공동의 목표, 공동의 협상/관리 프로세스를 공유함으로써 기업의 성과에 긍정적 영향을 미치는 것을 의미한다[Huseyin, 2005; 2006]. 성공적으로 IT 벤더(IT 아웃소싱)와의 관계를 유지하는 것은 기업의 원가절감, 유연성 확보, 양질의 서비스 제공, 신기술 습득에 있어 중요한 영향을 미치게 된다[Lee, 1996]. 하지만, 벤더와 기업은 근본적으로 그들 간의 이익을 공유하지 않는 성향 때문에 파트너[협력자]로서의 관계 유지가 매우 힘들다[Lacity and Hirschheim, 1993]. 이런 어려움 속에서도 기업성과의 시너지 창출을 위하여 Huseyin[2005]은 전사 차원의 공동된 관리 프로세스의 수립과 이에 따른 공동적 대응을 주장하고 있는 것이다.

위의 내용에서 알 수 있듯이 IT Relatedness 개념은 Multibusiness 기업의 IT 자원에 대한 연계성, 공유성 관점에서의 시너지 극대화를 위한 관리 및 활용의 개념이다. 즉, Multibusiness 기업의 성과 극대화를 위하여 IT 자산 및 프로세스 등을 종합적으로 관리하는 IT 거버넌스의 또 다른 모형으로 그 개념을 이해할 수 있다.

2.3 정보역량(Information Capability)과 기업성과

정보역량의 개념은 Marchand의 2000년, 2002년 연구에서 그 개념이 정립되었다. Marchand는

사람, 정보, 기술이 어떻게 상호 작용을 하여 기업 성과에 긍정적인 영향을 미칠 것인가에 대한 질문을 토대로 기업 성과와 세 가지 정보 역량 [IT 정보자산 관리, 정보의 관리, 직원의 행동 및 정보사용에 따른 가치] 사이의 관계를 연구하였다 [Marchand, 2000]. Marchand는 우선 기업들이 정보기반 경영을 위하여 정보기술에 많은 투자를 하고 있지만, 그런 기술 중심 관점이 인간 중심 경영활동[좀더 효과적으로 정보를 사용하기 위하여 행동과 가치 개선을 추구]에 영향을 미치지 못하고 있는 현실을 파악하였다. 그에 따라, 효과적인 관리와 정보사용에 대한 기업의 역량을 측정하기 위하여 'Information Orientation(이하 IO)'이라는 상위 개념을 통해 세 가지 정보역량을 연구하였다.

IT 정보자산 관리(IT Practice: ITP)는 적절한 IT 어플리케이션과 인프라를 효과적으로 관리하는 역량을 의미하며 비즈니스 운영 및 프로세스, 혁신과 경영활동을 지원하는 정보시스템 및 인프라에 대한 효과적 관리역량이다. 정보의 관리(Information Management Practice: IMP)는 정보의 라이프사이클에 대한 효율적 관리역량으로써 정보의 발견, 수집, 조직화, 지식의 구성, 유지/관리로 구성되어 있다. 직원의 행동 및 정보사용에 따른 가치(Information Behaviors and Values: IBV)는 효과적인 정보사용을 위해 조직원들에게 행동과 가치를 촉진하고 주입시키기 위한 기업의 역량을 의미하며 정보의 진실성, 형식성, 통제, 정보의 공유 및 투명성, 정보의 사전준비성에 대한 내용을 담고 있다.

Marchand는 연구의 결론으로 기술 중심 보다는 인간 중심으로 운영되는 회사가 정보사용 관점에서 더욱 좋으며, 세 가지 정보 역량은 비즈니스 성과를 증대시킨다고 연구하여 정보역량의 기업성과에 대한 긍정적 영향을 입증하였다.

정보역량을 활용한 추가적 연구들로 Bharadwaj [2000]는 정보역량이 기업 성과에 긍정적인 영향을 미침을 주장하며 정보역량의 긍정적 효과를 뒷

받침 하고 있다. 국내 연구에서는 Lee, and Lee [2007]는 정보역량 개념을 활용한 연구를 진행하였는데 그들은 Marchand와 달리 ERP 도입 이후 변화관리 효과가 정보역량에 미치는 연구를 진행하여 정보역량으로 인한 기업 성과가 아닌 정보역량 그 자체의 효과를 확인하였다. 즉, ERP 도입 효과를 변화관리를 통한 정보역량의 향상으로 보고 연구를 진행하여 긍정적 효과의 결과에 도달하였다.

2.4 정보보안 체계에 대한 Multibusiness 시너지 관점 적용 필요성

정보보안 체계는 각종 규제에 따라 대기업 (Multibusiness) 특히 금융권에서 보다 적극적(방대한 고객정보, 해킹 위협, 정부 규제 등)으로 수립 중에 있다. 이는 2012년 개인정보보호법 제정과 금융감독원 모범규준[전산장비 이용관련 내부 통제] 등의 통제에 따른 영향이다. Kim and Kim [2012]의 연구에 따르면 인터넷 해킹 공격 및 개인정보 유출 사고 등의 이슈화로 대부분 대기업의 경우 개인정보보호에 대한 인식에 따라 기업의 지침 및 규정을 강화하고자 노력 하고 있으나, 중소기업의 경우 현실적으로 개인정보보호에 대한 인식이 미비하다고 말하고 있다. 이는 정보보안에 대한 투자의지가 대기업에서 보다 적극적이라는 것으로 판단할 수 있는 내용이다.

하지만, 이런 의지와는 별개로 대기업들의 경우에도 기 수립한 정보보안 체계의 일부 영역(DRM, 통합권한관리, 고객정보 관리 등)을 제외하고는 전사 통합관리가 미흡한 상황이다(보안 각서 준수 미흡, 부서별 벤더 관리, 일부 업무 효율성 강조로 보안 미준수 등). Jang and Lee[2010]은 이런 상황을 보다 구체적으로 연구하였는데 대기업은 정보보안 체계의 수립에도 불구하고 각종 정보자산 관리 미흡 및 규정 미준수, 내부 보안 대책 미흡 등의 문제점이 발견되고 있다고 조사 결과를 발표하였다. 따라서, 보다 적극적인 정보

보안 체계 수립에도 불구하고 정보보안 체계 수립 및 통합관리 수준이 높지 않은 Multibusiness 기업[대기업]에 대하여 Multibusiness 시너지 관점에서의 정보보안 체계에 대한 연구가 필요한 것이다.

Ⅲ. 연구모형 및 가설 수립

3.1 연구모형

본 연구의 모형은 IT Security Relatedness라는 독립변수가 정보역량[Information Capability]과 정보보안성과(Information Security Performance)에 영향을 미치고, 이를 통해 기업의 성과(Corporate Performance)가 향상되는 것으로 설정되어 있다(<그림 1> 참조). 독립변수는 IT 정보보안 전략 수립 프로세스(IT Security Strategy Making Process), IT 정보보안 관계관리 프로세스(IT Security Relationship Management Process), IT 정보보안 인적자원 관리 프로세스(IT Security Human Resource Management Process), IT 정보보안 인프라(IT Security Infrastructure)로 구성되어 있다. 정보보안체계가 단순히 어느 특정 영역의 수립만으로 효과를 발휘하는 것이 아니라 위의 네 가지 구성요소 모두를 만족할 때 정보역량 및 정보보안성과에 유효한 영향을 미친다는 것을 시사하는 것이며, 정보보안체계 수립이 궁극적으로 기업성과에 연계되기 위해서는 정보역량과 정보

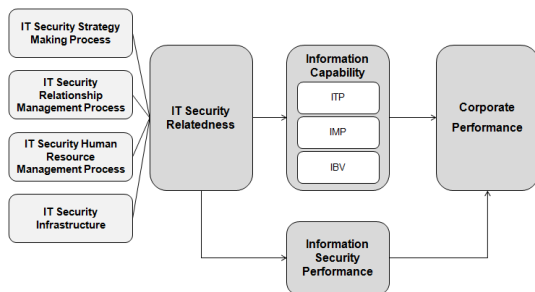
보안성과에서 유효한 결과가 확인되어야 하는 것이다.

3.2 연구 변수 및 가설

3.2.1 IT 정보보안 Relatedness (IT Security Relatedness)

IT Security Relatedness는 Multibusiness 기업 환경에서의 통합된 정보보안체계 수립 및 시너지가 기업의 성과에 긍정적인 영향을 미친다는 개념이다. 본 연구에서는 IT Governance Cube[Koen and Harry, 2004], COBIT 프레임워크, Basie의 문헌 연구를 통해 정보보안체계가 IT의 일부 영역이 아닌 전체 IT 거버넌스에 대한 통제체제를 확인해 보았다. 즉, 정보보안 체계 그 자체가 이미 IT 거버넌스의 구성요소를 모두 포함하고 있는 것이며, 해당 구성요소들에 대한 정보보안 관점의 활용을 통해 Multibusiness 기업의 정보 통제 시너지 효과에 대한 연구를 가능하게 하는 것이다. 이에 본 연구에서는 IT Relatedness 개념을 통제 체계인 IT Security Relatedness의 기본 모형으로써 참조 및 활용하였다. 따라서, IT Security Relatedness의 구성요소는 IT 정보보안 전략 수립 프로세스(IT Security Strategy Making Process), IT 정보보안 관계관리 프로세스(IT Security Relationship Management Process), IT 정보보안 인적 자원 관리 프로세스(IT Security Human Resource Management Process), IT 정보보안 인프라(IT Security Infrastructure)로 정의할 수 있다.

IT Security Relatedness는 정보보안의 각 구성 요소들에 대한 전사 통합적 관리체계를 통한 시너지(효과성)에 초점을 맞추고 있다. Lee et al.[2007]은 조직시민행동, IS혁신 저항, 사용자 IT 역량이 정보시스템 사용에 대한 내부통제 효과성에 긍정적인 영향을 미치고 이런 내부통제 효과성이 정보역량에 긍정적인 효과가 있음을 연구하였다. 여기서 IT 역량은 조직원들이 갖는 일반적인 IT



<그림 1> 연구 모형

기술 및 그 이해도이다. Lee and Lee[2007]은 법적 환경과 정보시스템의 내부통제 활동이 기업의 정보역량에 긍정적인 영향을 미친다고 주장하였다. 여기서 정보시스템의 내부통제 활동이란 정보자산에 대한 보안 및 통제에 관련한 이슈 [Kim *et al.*, 2007; Bloem *et al.*, 2006]를 해결하는 활동으로써 정보기술 컴플라이언스로 지칭하고 있다.

가설 1: IT Security Relatedness는 Information Capability에 정[+]의 영향을 미칠 것이다.

Ramnath and Pavlou[2002]은 인지된 정보보안이 전자상거래에 미치는 영향을 연구하며 사적 정보 전송과 관련된 위험을 다루는 Encryption, 기업의 정보저장소에 대한 소비자의 정보 신뢰성을 다루는 Protection, 신분 확인과 권한에 대한 역량을 측정하는 Authentication, 도메인명칭의 정확성을 검증하기 위한 Verification으로 변수를 구성하고 해당 변수들이 인지된 정보보안[정보보안 성과]에 영향을 미친다고 연구하였다. Suh[2005]은 정보보호 정책요인, 정보보호 조직요인, IT 아웃소싱, 정보보호 문화요인을 통하여 정보보안의 성과를 측정하였다. 해당 연구에서는 정보보호의 정책요인이 IT Security Relatedness의 IT Security Strategy Making Process의 전사 공통 정보보안 전략 수립 프로세스 및 그 활동과 연관이 있으며, 정보보호 조직 및 인적 정보보호는 정보보안 인적자원 관리와 연계되어 있다. 또한, 물리적 정보보호는 정보보안 인프라와, 협력업체 신뢰도는 정보보안 벤더 관리와 연관성이 있다고 할 수 있으며 이 모든 요인들은 정보보안 성과에 긍정적인 영향을 미치고 있다. 백민정, 손승희[2011]는 정보보안 인식과 행동이 정보보안 성과에 영향을 미친다고 연구하였다. 정보보안 인식은 정보보안에 대한 중요성 인식, 관심 정도이며 정보보안 행동은 정보보안 기술, 관리, 시스템으로 구성하였다. 정보보안 행동은 IT Security Relatedness

의 정보보안 인프라와 그 의미가 같으며, 그것을 관리하는 인력 등의 의미 또한 내포되어 있다고 할 수 있다. 해당 연구의 결과 또한 해당 구성 변수들이 정보보안 성과에 긍정적인 영향을 미치고 있음을 알 수 있다.

가설 2: IT Security Relatedness는 Information Security Performance에 정[+]의 영향을 미칠 것이다.

3.2.2 정보역량(Information Capability)

정보역량은 조직의 목표 및 전략적 방향을 달성하기 위하여 정보기술을 관리하고, 정보 Life Cycle에 따라 정보를 관리하며 조직원들이 효과적으로 정보를 활용하고 가치를 증대시키기 위한 활동 수행 역량을 의미한다. 정보역량과 비교되는 의미로 IT 역량이 있는데, IT 역량은[Bharadwaj, 1999b] IT 비즈니스 파트너십, 외부와의 IT 연계, 비즈니스 IT 전략적 사고, IT 비즈니스 프로세스 통합, IT 관리, IT 인프라의 6가지 요소로 구성되어 있다. Bharadwaj는 이를 통해 IT 역량이란 기업 역량 향상을 위한 전사 IT의 구성 및 관리이며, 정교한 기술적 기능들의 집합이 아닌 차별성을 위한 전사적 역량이라고 정의하였다[Bharadwaj, 2000]. 따라서, 본 논문에서는 정보보안 체계에 대한 기업의 정보관리/활용 역량 향상측면에서 IT 역량 개념이 아닌 정보역량 개념으로 변수를 구성하였다. 또한, 정보역량의 구성요소는 정보자산/정보의 관리, 활용, 가치 창출 측면에서 Marchand[2000; 2002]의 IO[Information Orientation] 개념을 활용하였다. 본 변수의 세부 구성항목은 Marchand 연구를 참조하여 Information Technology Practices[ITP], Information Management Practices[IMP], Information Behavior and Value[IBV]로 구성하였다.

정보역량은 기업 성과에 직접적인 영향을 미치는 요인이다. Marchand의 연구[2000; 2002]에서는 정보역량의 개념 구성뿐만 아니라 기업성과에

미치는 긍정적인 영향을 확인하였고 이를 달성하기 위한 가이드라인을 제시하고 있다. 홍성찬[2005]은 ERP 시스템 활용이 정보활용역량과 사업성과에 미치는 영향을 연구하여 ERP 시스템 활용이 정보 기술 역량, 정보관리 역량, 정보행위 역량 등 정보활용 역량에 긍정적인 영향일 미치고 이는 기업의 사업성과에도 긍정적인 영향을 미친다고 연구하였다.

가설 3: Information Capability는 Corporate Performance에 정[+]의 영향을 미칠 것이다.

3.2.3 정보보안 성과(Information Security Performance)

정보보안 성과는 정보보안 체계 수립으로 기업이 얻을 수 있는 직접적인 정보보안 관련 성과이다. 정보보안체계는 기업의 성과에 영향을 미치는 요인으로써 정보보안 사고 발생 시 기업 가치 및 주가의 하락 등[권영욱 등, 2007; Ettredge and Richardson, 2002; Bharadwaj and Keil, 2001; Cavusoglu etc., 2004] 직접적인 재무적/비재무적 피해를 입게 된다. 따라서, 정보보안의 성과에 대해 Ramnath and Pavlou[2002]은 인지된 정보보안이 전자상거래에 미치는 영향을 연구하며 해당 Construct들이 인지된 정보보안에 영향을 미친다고 연구하였다. 선한길[2005]은 정보보호 정책요인, 정보보호 조직요인, IT 아웃소싱, 정보보호 문화요인을 통하여 정보보안의 성과를 측정하였다. Shi-Ming 등[2006]은 정보보안에 대한 관리 및 투자효과 측정을 위한 방안을 연구하여 BSC 기법을 활용한 정보보안 성과 측정 지표를 개발하였고 재무적 손실 감소와 이익 촉진에 영향을 주는 다양한 지표로써 거래보안 강화, 불법 감소, 시스템 역량 강화 등을 제시하였다. Baek and Sohn[2011]는 정보보안 인식과 행동이 정보보안 성과에 영향을 미친다고 연구하였다. 정보보안 인식은 정보보안에 대한 중요성 인식, 관심 정도

이며 정보보안 행동은 정보보안 기술, 관리, 시스템으로 구성하였다. Kwon and Kim[2007]는 정보보안 사고와 방지 투자의 영향을 연구하여 정보보안 사고가 기업가치에 통계적으로 유의한 영향을 미친다는 결론을 도출하고 정보보안에 대한 투자의 인식이 전환되어야 함을 주장하고 있다.

가설 4: Information Security Performance는 Corporate Performance에 정[+]의 영향을 미칠 것이다.

3.2.4 기업 성과(Corporate Performance)

기업 성과 측정과 관련하여 일부 연구자들은 IT Security Relatedness나 정보역량, IT 정보보안 성과 같은 무형의 가치에 대한 측정은 Tobin's q로 측정하는 것이 보다 효율적인 측정 방법이라고 [Huseyin 2005; Bharadwaj et al., 1999a] 주장한다. 하지만, 본 연구에서는 30대 그룹의 자회사가 표본으로 일부 포함되어 있으며 해당 기업의 특성상 한국거래소에 상장되지 않은 기업들이 있어 Tobin's q로의 기업 성과측정은 적절하지 못하다. 따라서, 기업 성과를 측정하는 지표로써 본 연구에서는 총자산이익률(Return On Assets: ROA)을 활용하고자 한다. 총자산이익률은 기업성과를 측정하는 지표로써 순이익을 총자산으로 나눈 비율로 수익성을 평가하는 종합지표이다[Yi et al., 2007]. 즉, 기업이 총자산을 수익창출활동에 있어 얼마나 효율적으로 이용했는지 측정하는 것으로써 ROA가 높다는 것은 자산을 효율적으로 관리/운영하고 있다는 것을 나타내는 것이다[Lee and Lee, 2007; Jeon and Kim, 2005]. 이를 뒷받침하는 주장으로써 Weill과 Ross[2004]는 IT 체계가 기업 성과에 미치는 영향을 확인하기 위해서는 수익성, 자산의 활용, 성장률 등의 재무성과를 파악하여야 한다고 주장함으로써 기업이 자산을 활용하여 얼마나 많은 수익성에 기여해야 하는지를 연구하였다.

3.3 통제변수

재무데이터 또는 주가 데이터에 근거한 기업 가치 및 성과 측정은 기업의 진정한 성과측정을 왜곡할 수 있는 위험이 있다. 따라서, 다각적으로 Multibusiness기업의 성과 측정을 위한 통제 변수를 설정하고 이를 실험에 반영하여 왜곡이 최소화된 결과를 도출하고자 한다. 통제 변수 선정은 IT Relatedness의 기업성과에 대한 영향을 연구한 Huseyin[2006]연구 방법을 참고하였으며 그에 따라 기업 규모[Firm size], 산업 성과[Industry Performance]를 선정하였다. 본 연구에서 기업 규모는 매출액[Huseyin, 2005; 2006]을 활용하고, 산업 성과는 실험 대상 기업이 속한 산업 모든 기업의 ROA 가치 평균[Huseyin, 2006; McGahan and Porter, 1999]을 통제 변수로 사용하였다.

3.4 변수의 조작적 정의

본 연구에서는 개념적 연구모형의 변수들을 측정하기 위하여 문헌연구에 기반한 측정항목을 개발하였으며, 연구의 목적에 부합하도록 변수에 대한 조작적 정의를 수행하였다.

<표 1> 변수의 조작적 정의 결과

Construct	변수	출처
IT Security Relatedness	IT Security Strategy Making Process	Huseyin[2005], Huseyin[2006], Huseyin and Venkatraman[2005]
	IT Security Relationship Management Process	
	IT Security Human Resource Management Process	
	IT Security Infrastructure	
Information Capability	Information Technology Practices	Marchand <i>et al.</i> [2000] Marchand <i>et al.</i> [2002] 이승창, 이호근[2007]
	Information Management Practices	
	Information Behavior and Value	
Information Security Performance		백민정, 손승희[2011], 선한길[2005]

IV. 연구 방법 및 분석 결과

4.1 데이터 수집 및 표본 특성

본 연구는 연구모형과 가설검증을 위해 설문조사를 통한 실증 검증을 수행하였다. 설문항목은 문헌 연구를 기반으로 작성하였고, 전문가 인터뷰 및 예비조사를 통해 내용 타당성 검증 후 설문조사를 진행하였다. 표본조사 대상은 본 연구의 목적에 부합하고 이해도가 높은 국내 30대 대기업 및 그 자회사에 근무하는 정보전략, 정보기획, 정보보안 등 정보보안 업무와 관련된 IT 담당자들을 대상으로 실시하였다. 설문 대상 표본은 21개 기업을 대상으로 설문지를 발송하여 총 3주간의 기간 동안 121명에게 설문을 진행하였다. 수거된 설문지 중 표본조사 대상이 아니거나 설문의 일관성이 심각하게 결여된 표본을 제거하고 총 115부의 설문지를 본 연구를 위한 표본으로 선택하였다.

4.2 구조타당성: 확인적 요인분석

본 연구는 구조타당성의 확인을 위하여 확인적 요인분석을 수행하였다. 일반적으로 요인 적 재량이 통계적으로 유의하면 단일 차원성이 존

제한다고 할 수 있다. Factor Loading 도출 결과 모든 요인과 변수에 대한 Factor Loading 값이 최소 요구치 0.5를 크게 상회함으로 연구 모형에 사용된 모든 측정항목이 타당함을 확인하였다.

각 요인에 대한 신뢰도는 확인적 요인분석 결과를 활용한 AVE(Average Variance Extracted: 평균 분산 추출)값과 Cronbach's α 계수 값을 이용하여 확인하였다. AVE는 잠재개념에 대해 지표가 설명할 수 있는 분산의 크기를 나타내며 AVE 값이 0.5 이상일 경우 신뢰도가 있는 것으로 판단한다. 또한, 각 요인에 대한 신뢰도는 Cronbach's α 계수를 통하여 검증이 가능하다[Cronbach, 1951]. 일반적으로 Cronbach's α 계수 값이 0.6 이상이면 신뢰도가 있는 것으로 판단하고 0.8~0.9 이상이면

신뢰도가 높은 것으로 판단한다[Van de Van and Ferry, 1980]. <표 2>를 확인해 보면 모든 요인들의 AVE 값은 대부분 0.8에서 0.9 이상이며, Cronbach's α 계수 값은 최하 0.803 이상이므로 신뢰도가 대단히 높다고 할 수 있다.

판별타당성은 AVE를 이용한 VE 검증으로 판단하게 된다. VE 검증은 AVE 값의 제곱근을 이용하여 확인하며, 보통 AVE 제곱근 값이 0.5 이상 [Bagozzi and Yi, 1998; Fornell and Larcker, 1981] 이고 다른 구성개념의 상관관계 값보다 높아야 타당성이 성립한다[Barclay 외, 1995]. <표 3>은 판별 타당성 검증을 위하여 AVE 제곱근 값과 각 요인별 상관계수 값을 정리한 표로 본 연구의 모형은 판별 타당성을 확보한 것으로 판단할 수 있다.

<표 2> 요인별 기술통계량 및 신뢰도, AVE 분석 결과

유형	Mean	S.D.	Cronbach Alpha	AVE
IT Security Relatedness	4.173	1.561	0.956	0.908
IT Security Strategy Making Process	4.548	1.546	0.954	0.958
IT Security Relationship Management Process	3.986	1.592	0.943	0.947
IT Security Human Resource Management Process	3.641	1.523	0.867	0.847
IT Security Infrastructure	4.693	1.595	0.881	0.900
Information Capability	5.241	1.042	0.919	0.794
Information Technology Practices	5.335	1.046	0.847	0.829
Information Management Practices	5.167	1.002	0.838	0.819
Information Behavior and Value	5.224	1.072	0.803	0.748
IT Security Performance	5.472	0.991	0.876	0.896
Corporate Performance	1.67	2.91		

<표 3> 판별 타당성 검증

Constructs	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[1] IT Security Strategy Making Process	0.98								
[2] IT Security Relationship Management Process	0.755	0.97							
[3] IT Security Human Resource Management Process	0.739	0.714	0.92						
[4] IT Security Infrastructure	0.717	0.675	0.708	0.95					
[5] Information Technology Practices	0.493	0.492	0.473	0.494	0.91				
[6] Information Management Practices	0.434	0.392	0.459	0.409	0.721	0.9			
[7] Information Behavior and Value	0.399	0.409	0.449	0.351	0.662	0.734	0.86		
[8] IT Security Performance	0.384	0.400	0.333	0.397	0.442	0.552	0.507	0.95	
[9] Corporate Performance	0.104	0.176	0.050	0.181	0.245	0.305	0.275	0.343	1

4.3 구조모델: SEM분석

구조 타당성(확인적 요인분석) 분석을 통하여 본 연구에 활용된 측정 변수들의 신뢰성과 타당성이 성립함을 확인하였으므로 Amos 18.0을 활용하여 가설 검증을 위한 경로분석을 수행하였다. 경로분석 결과는 경로 상 표준화 되지 않은 회귀 계수 값(Estimates of regression weights)이 'Sales(기업규모-통제변수)'를 제외하고는 모두 유의한 값을 보이고 있으며, T값이 P = 0.01, 0.05 이하에서 유의함으로 해당 연구의 모든 경로는 유의한 정(+)의 효과를 보이고 있음을 알 수 있다. 또한, Sales(매출액-통제변수)는 기업성장에 있어 유의한 통제변수가 아님을 알 수 있다. <표 4>는 가설 검증에 앞서 수행한 구조모델의 적합도 검증 결과이다.

각 적합도 항목에 대한 측정값은 권고 측정기준에서 대부분 부합하고 있으며 권고 수용기준에서 크게 벗어나지 않아 전반적으로 본 연구 모

델은 적합성에 충족한 것으로 판단된다. SRMR은 Hu와 Bentler[1999]의 의견에 따르면 0.08 이하의 측정값이 적합하다고 제시하였으나 일반적으로 0.085 이하의 기준이면 모형의 적합성이 있다고 판단할 수 있다. 카이스퀘어 값을 자유도로 나눈 CMIN/DF는 1.0 이상, 4.0 이하의 권고 수치를 만족하고 있으며(Chi-square = 394.584, Degrees of freedom = 201), GFI의 경우 또한 권고 수용기준 내에 위치하고, TLI와 CFI는 0.9 이상의 기준에 부합하거나 비슷한 측정값을 보이고 있어 본 연구 모형이 수용 가능함을 보여 주고 있다.

경로분석 결과 모든 변수들의 경로상 표준경로계수 값은 각 변수에 정(+)의 영향을 미치는 것으로 분석되었으며 T값과 P값의 확인을 통해 표준경로계수 값은 유의한 결과임을 확인할 수 있다. 경로분석 결과 중 가설과 관련된 경로분석 결과값은 아래 <그림 2>, <표 5>의 내용과 같다.

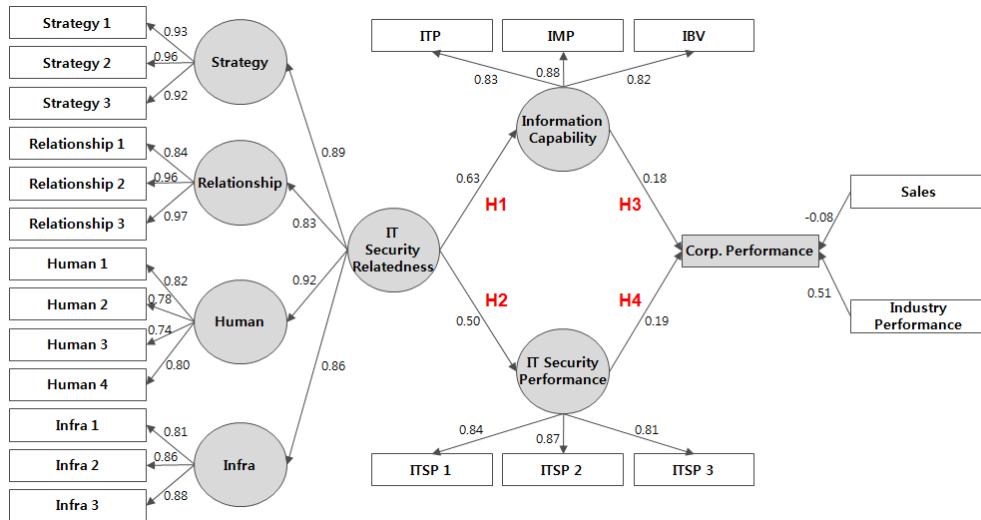
<표 4> 구조모델의 적합도 검증

적합도 항목	Standardized RMR(SRMR)	CMIN/DF (χ^2/df)	RMSEA	GFI	Baseline Comparisons	
					TLI	CFI
측정값	0.0838	1.963	0.092	0.773	0.894	0.907
권고 수용기준	0.085 이하	1.0 이상 4.0 이하	0.1 이하	0~1.0	0.9 이상	0.9 이상

<표 5> 경로분석 결과

가설		표준경로계수	T값	가설채택여부
H1	IT Security Relatedness는 Information Capability에 정(+)의 영향을 미칠 것이다.	0.626***	5.597	채택
H2	IT Security Relatedness는 Information Capability에 정(+)의 영향을 미칠 것이다.	0.505***	4.603	채택
H3	Information Capability는 Corporate Performance에 정(+)의 영향을 미칠 것이다.	0.175**	2.084	채택
H4	Information Security Performance는 Corporate Performance에 정(+)의 영향을 미칠 것이다.	0.194**	2.297	채택

*** p < 0.01, ** p < 0.05.



<그림 2> 연구모형의 경로분석 결과

V. 결론

5.1 연구결과

본 연구는 기업에서 수립하는 정보보안 체계가 정보역량 및 정보보안 성과에 긍정적인 영향을 미치며 궁극적으로는 기업성과에 긍정적인 영향을 미치고 있음을 밝혀내고 있다. 이는, Multi-business 환경 하의 기업들이 통합된 정보보안 체계를 통하여 시너지 효과를 누릴 수 있음을 증명하는 것으로써 정보보안 체계 수립의 당위성에 대한 개념적 틀을 제시해 주고 있다. 따라서, 본 연구의 결과는 크게 세 가지 관점에서 그 결과를 분석할 수 있다.

첫째, IT Security Relatedness의 구성 요소 확인이다. 문헌 연구 과정에서 IT(IT 거버넌스)와 정보보안 체계에 대한 관계를 확인하였고, 이를 통해 기업의 자산으로써 정보보안 체계의 위상을 확인할 수 있게 되었다. 따라서, IT Relatedness 이론과 마찬가지로 정보보안 체계 또한 4가지 요인 (Strategy, Relationship, Human, Infra)으로 구성되어 있으며, 통합된 정보보안 체계 수립이 기업 성과에 긍정적인 영향을 미침을 알 수 있게 되었다.

둘째, IT Security Relatedness와 Information Capability와의 연관성이다. 정보보안 체계 수립이 기업의 정보자산관리 역량과 정보 라이프사이클에 대한 효율적 관리역량, 직원들에 대한 효율적 정보사용 관리역량에 긍정적 영향을 미치는 주요 변수임이 확인됨으로써, 기업의 정보 관리 역량 향상 관점에서 정보보안에 대한 투자의 당위성을 설명해 주고 있다.

셋째, Information Capability와 IT Security Performance의 직접적인 기업 성과에 대한 영향이다. 이는 IT Security Relatedness 수립의 긍정적 영향에 대한 연장선상에서 정보역량 및 정보보안 성과와 기업 성과와의 상관관계를 명확히 보여주는 결과인 것이다. 특히 이런 사항은 정보보안 투자가 기업의 성과에 있어 긍정적인 영향이 부족하다고 가정하는 기업들에게 정보보안의 효용성을 명확히 알려주는 계기라 할 수 있다.

5.2 시사점

본 연구의 시사점은 크게 학문적 시사점과 산업계 관점의 시사점으로 나누어 설명할 수 있다. 학문적 관점에서는 첫째, 정보보안 성과와 기업성

과와의 관련성이다. 그간 정보보안 체계에 대한 연구는 상당수가 정보보안 성과로 초점이 맞추어져 진행되어 왔다. 하지만, 본 연구에서는 정보보안 체계 수립과 정보보안 성과, 그리고 기업 성과까지 그 직접적인 영향도를 확인해 봄으로써 정보보안 체계 수립의 필요성과 당위성에 대한 논리적 방향성을 제시해 주었다. 특히 기업성과에 대한 검증에 있어 실제 기업의 재무 데이터인 총자산이익률(Return On Assets: ROA)을 활용하였으며, 수익성 종합 평가 지표와 정성적 설문 문항의 경로 분석을 통해 기업의 Additional Value에 대한 정보보안 성과 및 정보역량의 관계성을 확인하였다.

둘째, 정보보안 체계 수립을 통한 기업 정보 역량(Information Capability) 향상에 대한 연구이다. 기존 Marchand[2000]의 연구는 주로 기업 성과나 정보화 등의 효과에 초점이 맞추어져 연구에 활용되어 왔다. 하지만, 본 연구에서는 정보보안 체계와 정보 역량의 관련성을 처음으로 연구하여 긍정적인 효과가 있음을 밝혀내었고, 정보 역량 관점에 영향을 줄 수 있는 기업내 다양한 환경에 대한 인식 범위를 넓힐 수 있게 하였다.

산업계 관점에서의 시사점은 첫째, 정보보안 투자에 대한 당위성 제공이다. 정보보안 투자시 갖게 되는 기업 CEO의 다양한 의문[Suh, 2008]들에 대하여 본 연구는 가장 근원적인 대답을 제시해 줌으로써 정보보안 투자에 대한 올바른 인식을 제공해 줄 수 있는 것이다. 둘째, 시너지 관점에서의 네 가지 정보보안 구성요소 제시를 들 수 있다. 정보보안 담당자들은 정보보안 체계 수립시 정보보안 관련 다양한 기준/표준들을 참고하지만, 다양한 이해관계자에 대한 시너지 관점에서 명확한 구성 요소를 확인시켜 주는 영역이 부재

하였기에 본 연구의 효용성이 크다고 할 수 있다.

5.3 연구한계

본 연구의 진행에 있어 한계점은 세 가지 측면에서 고려해 볼 수 있다. 첫째, 표본의 한계성이다. 본 연구는 특정 산업군에 대한 심도 있는 표본 수집 및 분석을 진행한 것이 아니라 Multi-Business 환경의 기업을 표본의 대상으로 진행하여 일부 산업은 다수 기업이 표본으로 선정되고 일부 산업에서는 소수의 기업이 표본으로 선정되어 산업간 균형 및 대표성에 한계점을 보이고 있다. 또한, 설문 응답자의 구성이 정보보안 담당자라는 직책의 모호성에 기인하여 정보기획부터 정보시스템 운영자 중 정보보안 관련 업무수행자로 다양하게 구성하게 되었다. 둘째, IT Security Relatedness와 기업 성과간의 연관 관계를 직접적으로 분석하지 않은 것이다. 이는 연구 진행 과정에서 해당 경로 분석을 추가(가설 추가)하였을 경우 해당 가설이 기각되었으며, IT Security Relatedness의 개념 자체가 처음 제시되는 개념임에 따라 관련 문헌 연구 및 변수의 조작적 정의에 있어 한계점이 있었기 때문이다.

셋째, Information Capability에 대한 구조/경로 분석 시 정보역량의 각 하위 변수들을 개별적으로 연구 분석에 활용한 것이 아니라 ITP, IMP, IBV를 단일 변수로 한 요인점수 값을 활용하여 분석을 수행한 것이다. 각 변수에 대한 설문문항은 세 변수에 대해 총 13개 문항을 조사하였지만, 분석의 복잡성 및 레벨에 대한 한계점을 고려하여 Lee and Lee[2007]의 연구 방법을 참고한 후 분석을 진행하였다.

〈References〉

- [1] Andersen, P.W., "Information Security Governance," *Information Security Technical Report*, Vol. 6, No. 3, 2001, pp. 60-70.
- [2] APEC, *APEC Risk Management Theory Workshop Report*, 1999.
- [3] Baek, M.J. and Sohn, S.H., "A Study on the

- Effect of Information Security Awareness Behavior on the Information Security Performance in Small Medium Sized Organization," *Asia Pacific Journal of Small Business*, Vol. 33, No. 2, 2011, pp. 113-132.
- [4] Bagozzi, R.P. and Yi, Y., "On the Evaluation of Structural Models," *Journal of Academy of Marketing Science*, Vol. 16, No. 1, 1988[Spring], pp. 74-94.
- [5] Barclay, D., Higgins, D., and Thompson, R., "The Partial Least Squares Approach to Casual Modeling: Personal Computer Adoption and Use as an Illustration," *Technology Study*, Vol. 2, No. 2, 1995, pp. 285-309.
- [6] Basie von Solms, "Information Security-A Multidimensional Discipline," *Computers and Security*, Vol. 20, 2001, pp. 504-508.
- [7] Basie von Solms, "Information Security governance: COBIT or ISO 17799 or both?," *Computers and Security*, Vol. 24, 2005, pp. 99-104.
- [8] Basie von Solms, Rossouw von Solms, "The 10 deadly sins of information security management," *Computers & Security*, Vol. 23, 2004, pp. 371-376.
- [9] Bharadwaj, "A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation," *MIS Quarterly*, Vol. 24, No. 1, 2000, pp. 169-196.
- [10] Bharadwaj, A.S. and Keil, M., "The Effect of Information Technology Failures on the Market Value of Firms: An Empirical Examination," *INFORMS 2001 Miami*, November, 2001.
- [11] Bharadwaj, A.S., Bharadwaj, S.G., and Konsynski, B.R., "Information Technology Effects on Firm Performance as Measured by Tobin's q," *Management Science*, Vol. 45, No. 7, 1999a, pp. 1008-1024.
- [12] Bharadwaj, A.S., Sambamurthy, V., and Zmud, R.W., "IT CAPABILITIES: THEORETICAL PERSPECTIVES AND EMPIRICAL OPERATION-LIZATION," *ICIS '99 Proceedings of the 20th international conference on Information Systems*, 1999b.
- [13] Birman K.P., "The Next-generation Internet: Unsafe at any speed," *IEEE Computer*, Vol. 33, No. 8, 2000, pp. 54-60.
- [14] Bloem, J., Van Doorn, M., and Mittal, P., "Making IT Governance Work in a Sarbanes-Oxley World," John Wiley and Sons, Inc., Hoboken, NJ, 2006.
- [15] Cavusoglu, H., Mishra, B., and Raghunathan, S., "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developer," *International Journal of Electronic Commerce*, Vol. 9, No. 1, 2004, pp. 69-104.
- [16] Cronbach, L.J., "Coefficient Alpha and the Internal Structure of Tests," *Psychometrika*, Vol. 16, No. 3, 1951, pp. 297-334.
- [17] Entrust. Information Security Governance [ISG]: an essential element of corporate governance. Available from: <http://itresearch.forbes.com/detail/RES/1082396487_702.html>; 2004.
- [18] Ettredge, M. and Richardson, V., "Assessing the Risk of in E-Commerce," Proceedings of the Thirty Fifth Hawaii International Conference on Systems Sciences, Los Alamitos, CA: *IEEE Computer Society Press*, 2002.
- [19] Fornell, C. and Larcker, D.F., "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, Vol. 18, No. 1, 1981, pp. 39-50.
- [20] Hong, S.-C., "Impacts of ERP Systems on Information Capabilities and Business Perfor-

- mance," *Korean Society for Internet Information*, Vol. 6, No. 6, 2005, pp. 45-56.
- [21] Hu, L.T. and Peter, M.B., "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," *Structural Equation Modeling: A Multidisciplinary Journal*, Vol. 6, No. 1, 1999, pp. 1-55.
- [22] Huang, S.M., Lee, C.L., and Kao A.C., "Balancing performance measures for information security management," *Industrial Management and Data Systems*, Vol. 106, No. 2, 2006, pp. 242-255.
- [23] Huseyin, T. and Venkatraman, N., "Knowledge Relatedness and The Performance of Multibusiness Firms," *Strategic Management Journal*, Vol. 26, 2005, pp. 97-119.
- [24] Huseyin, T., "Information Technology Relatedness, Knowledge Management Capability, and performance of Multibusiness firms," *MIS Quarterly*, Vol. 29, No. 2, Special Issue on Information Technologies and Knowledge Management, 2005, pp. 311-334.
- [25] Huseyin, T., "Performance effects of information technology synergies in multibusiness firms," *Management information systems quarterly*, Vol. 30, No. 1, 2006, p. 57.
- [26] Jang, S.S. and Lee, H.S., "Study About ISMS Certificate Evaluation Analysis", *Korea Institute of Information Security and Cryptology*, Vol. 20, No. 1, 2010, pp. 31-38.
- [27] Jeon, I.S. and Kim, H.J., "Return on Customer Satisfaction Investment: Is CSI Financially Accountable?," *Korea Marketing Association*, Vol. 20, No. 3, 2005, pp. 65-84.
- [28] Kim, J.H. and Kim, H.J., "A Study on the way for Handling for Personal Information Protection considering the Scale and Characteristic of Companies' Status," *Journal of Security Engineering*, Vol. 9, No. 1, 2012, pp. 99-108.
- [29] Kim, S.S., Lee, J.B., and Lim, B.W., "A Study on How Internal Control can have an Impact on Firm Performance by Institutional Influence," *Joint Conference of THE KOREAN ACADEMIC SOCIETY OF BUSINESS ADMINISTRATION/Korean Institute of Industrial Engineers*, 2007, pp. 1061-1068.
- [30] Koen, B. and Harry, B., *"IT Governance: A Pocket Guide Based on COBIT"*, Van Haren Publication, 2004.
- [31] Kwon, Y.K. and Kim, B.D., "The Effect of Information Security Breach and Security Investment Announcement on the Market Value of Korean Firms," *Information System Review*, Vol. 9, No. 1, 2007, pp. 105-120.
- [32] Lacity, M. and Hirschheim, R., "The Information systems Outsourcing Bandwagon," *Sloan Management Review*, Vol. 35, No. 1, 1993, pp. 73-86.
- [33] Lee, J.B., Kim, S.S., and Lee, J.C., "The Study about the Influence of Effective Internal Control Systems on IT Capability," *Journal of the Korean Operations Research and Management Science Society*, 2007[Fall], p. 3.
- [34] Lee, MKO., "IT outsourcing contracts: practical issues for management," *Industrial Management and Data Systems*, 1996, pp. 1-17.
- [35] Lee, S.C. and Lee, H.G., "The Impact of Change Management after ERP Implementation: An Information capability perspective," *Asis Pacific Journal of Information System*, Vol. 17, No. 1, 2007, pp. 1-31.
- [36] Marchand, D.A., Information Orientation: People, Technology and the Bottom Line, *Sloan Management Review*, Vol. 41, No. 4, 2000[Summer], p. 69.
- [37] Marchand, D.A., Kettinger, W.J., and Rolins,

- J.D., *Information Orientation: The Link to Business Performance*, Oxford University Press, 2002.
- [38] McGahan, A.M. and Porter, M.E., "The Persistence of Shocks to Profitability," *The Review of Economics and Statistics*, Vol. 81, No. 1, 1999, pp. 143-153.
- [39] Ramnath, K.C. and Pavlou, P.A., "Perceived information security, financial liability and consumer trust in electronic commerce transactions," *Logistics Information Management*, Vol. 15, No. 5/6, 2002.
- [40] Shaun, P. and Rossouw, von S., "A framework for the governance of information security," *Computer & Security*, Vol. 24, 2004, pp. 638-646.
- [41] Suh, S.W., "A Practical Guide to Information Security Investment for CEO," *Seoul National University Press*, 2008.
- [42] Sun, H.G., "A Study on the Effect of Information Security Policy and Organization on the Performance of Information Security," *Conference of Korea Management Information System*, 2005[Spring].
- [43] Van de Van, A.H. and Ferry, D.L., *Measuring and Assessing Organization*, Wiley Inter-Science, New York, 1980.
- [44] Weill, P. and Ross, J.W., *IT governance: How Top Performers Manage IT Decision Rights for Superior Results*, Watertown, MA: Harvard Business School Press, 2004.
- [45] Yi, Y.J. and Lee, C.L., "The Role of Customer Loyalty Variables in the Effects of Customer Satisfaction on Firm's Performance," *Korea Marketing Association*, March, 2007, pp. 81-102.

Appendix: 연구설문지

설문지

정보보안체계 수립이 Multibusiness 기업 성과에 미치는 영향에 관한 연구 IT Relatedness 이론 관점에서

안녕하십니까?

바쁘신 와중에도 시간을 내주셔서 진심으로 감사드립니다. 본 설문지는 정보보안체계 수립이 기업[Multibusiness 관점] 성과에 미치는 영향에 관한 연구를 위하여 자료 수집을 목적으로 작성 되었습니다. 귀하께서 응답해 주시는 내용은 연구결과에 매우 중요한 영향을 미치게 되오니 어려우시더라도 잠시 시간을 내어 주셔서 정확한 판단과 의견을 제시해 주시기 바랍니다.

응답내용은 연구목적 이외에는 절대로 사용하지 않고 무기명으로 처리됩니다. 아무쪼록 바쁘시더라도 설문에 성의껏 응답해 주시면 저의 연구에 많은 도움이 되리라 생각되오니 협조를 부탁드립니다.

2012년 1월

경희대학교 경영대학 교수 박주석
연구원 구자면

■ 아래는 귀하가 소속된 기업에서 기수립한 정보보안 체계와 관련된 질문문항입니다. 소속 기업의 기업단위, 본부단위, 부서단위의 정보보안 체계를 고려하시어 기업내 정보보안 체계의 전사 통합성은 어떻게 되는지 해당 항목에 따라 설문에 응하여 주시면 감사하겠습니다.

설문은 주어진 7점 척도로 응답해 주시면 되며, 해당 질문에 따라 IT정보보안 체계가 전사적 통합이 아닌 본부/부서 단위로 개별적으로 수립되어 있을 경우 1점[질문에 대한 대답이 전혀 그렇지 않을 경우], IT정보보안 체계가 전사적으로 완전히 통합되어 수립/운영되고 있을 경우 7점[질문에 대한 대답이 매우 그렇다일 경우]을 선택하여 'O'표 해 주시기 바랍니다.

① 전혀 공유하고 있지 않다	② 대부분 공유하고 있지 않다	③ 60%~70% 수준에서 공유하고 있지 않다	④ 보통 수준에서 공유하고 있다	⑤ 60%~70% 수준에서 공유하고 있다	⑥ 대부분 공유하고 있다	⑦ 모두 공유하고 있다	
1. 당사는 IT정보보안 투자에 대한 전략적 근거를 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦
2. 당사는 IT정보보안 전략을 체계화하는 프로세스를 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦
3. 당사는 비즈니스 전략[규정]과 IT정보보안 전략의 연계를 위한 프로세스를 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦
4. 당사는 IT정보보안과 관련하여 아웃소싱을 하기 위한 전략적 목표들을 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦
5. 당사는 IT정보보안 관련 벤더 및 서비스 공급자들과의 협상에 사용되는 프로세스를 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦
6. 당사는 IT정보보안 관련 벤더 및 아웃소싱 회사를 관리하는 프로세스를 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦
7. 당사는 IT정보보안 관련 분야에서 일할 인재의 채용 프로세스를 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦
8. 당사는 IT정보보안 관련 인재의 훈련 프로그램을 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦
9. 당사는 IT정보보안 관련 인재에게 제공할 인센티브 방안을 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦
10. 당사는 IT정보보안 관련 인재를 유지할 전략을 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦
11. 당사는 IT정보보안과 관련된 인프라의 관리 정책을 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦
12. 당사는 IT정보보안 관련 소프트웨어의 표준을 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦
13. 당사는 IT정보보안 관련 하드웨어의 표준을 전사적으로 공유하고 있다.	①	②	③	④	⑤	⑥	⑦

■ 아래는 귀하가 소속된 기업의 전사적 정보 역량[관리, 활용, 사용자 측면]에 관한 질문문항입니다. **정보역량이란 IT부서에만 속한 개념이 아닌 전사에 해당하는 개념으로, 정보시스템의 효과적 관리, 정보의 관리, 효과적인 정보사용을 위한 정보사용자에 대한 관리의 개념**입니다. 소속 기업 내에서 직접 느끼시거나 간접 체험하신 경험, 지식을 활용하시어 해당 기업의 정보 역량은 어떻게 되는지 해당 항목에 따라 설문에 응하여 주시면 감사하겠습니다.

설문은 주어진 7점 척도로 응답하시면 되며, **해당 질문에 대해 완전히 동의하지 않으면 1점, 완전한 동의시 7점**을 선택하여 'O'표 해 주시기 바랍니다.

14. 당사는 정보활용을 통하여 전사 차원의 업무 처리와 효율성이 향상되고 있다.	①	②	③	④	⑤	⑥	⑦
15. 당사는 정보활용을 통하여 비즈니스 프로세스의 관리 효율성이 향상되고 일관성 있는 고품질로 업무를 처리할 수 있다.	①	②	③	④	⑤	⑥	⑦
16. 당사는 정보활용을 통하여 신제품 개발 및 조직원 창의성 개발 역량 등이 향상되고 있다.	①	②	③	④	⑤	⑥	⑦
17. 당사는 정보활용을 통하여 경영층의 의사결정 지원이 용이해 지고 있다.	①	②	③	④	⑤	⑥	⑦
18. 당사는 의사결정 전 적절한 정보원천과 DB를 통한 정보의 분석 및 평가가 가능하고 해당 정보에 접근이 가능하다.	①	②	③	④	⑤	⑥	⑦
19. 당사는 조직원의 정보요구를 프로파일링하여 해당 정보를 적절할 절차에 따라 수집하고 있다.	①	②	③	④	⑤	⑥	⑦
20. 당사는 체계적인 정보의 조직화 역량[정보의 색인, 분류, 체계화]을 통하여 정확하고 완벽한 정보를 관리하고 있다.	①	②	③	④	⑤	⑥	⑦
21. 당사는 중복 정보의 수집을 방지하고, 정보의 재사용성을 유지하며, 조직원들이 항상 최상의 정보를 이용할 수 있도록 갱신 등의 관리를 하고 있다.	①	②	③	④	⑤	⑥	⑦
22. 당사는 조직원이 개인의 이익을 위하여 정보를 임의 조작할 수 없도록 정보의 무결성을 유지하고 있다.	①	②	③	④	⑤	⑥	⑦
23. 당사는 제공한 정보에 대해 조직원들이 정보의 원천을 신뢰하고 있다.	①	②	③	④	⑤	⑥	⑦
24. 당사는 조직성과, 기업평판 등의 정보를 모든 조직 구성원들에게 지속적으로 제공하고 있다.	①	②	③	④	⑤	⑥	⑦
25. 당사는 조직간, 팀간에 정보[민감하거나 민감하지 않은]를 자유롭게 교환하고 있다.	①	②	③	④	⑤	⑥	⑦
26. 당사는 조직원들이 신제품/서비스 개발 및 기존 상품/서비스 강화 등을 위해 정보를 적극적으로 이용하고 있다.	①	②	③	④	⑤	⑥	⑦

◆ About the Authors ◆



Ja Myon Koo

Ja Myon Koo is a senior manager at the KPMG Samjong Accounting Corporation. He perform the IT consulting services at the area of Process Innovation, information strategy planning, enterprise architecture, IT investment evaluation, and others. He earned degree of master and Ph.D. from the Kyunghee University. His research interests are consulting service quality, data reference model and information security systems.



Joo Seok Park

Joo Seok Park Dr. Jooseok Park is a professor at the school of management at Kyung-Hee University. He received his Ph.D. in Management Information Systems from the Haas School of Business, University of California at Berkeley. His current research area examines data model, enterprise architecture, and business analytics.



Jae Hong Park

Jae Hong Park is an assistant professor at the School of Kyung Hee University. His research interests are business analytics, social media analysis, online word-of-mouth effect, IT investment evaluation, and others. He earned master's degree from the Stanford University, and earned his Ph.D. degree from the University of Texas at Austin. His works have been published at various journals and conference proceedings such as Information Systems Research, Electronic Commerce Research and Applications, and International Conference on Information Systems.

Submitted : July 20, 2013

1st revision : September 28, 2013

Accepted : December 03, 2013

2nd revision : November 26, 2013