기업 보안관리 강화의지 및 실행에 영향을 미치는 요인에 관한 연구

황종호*

〈요 약〉

본 연구는 기업의 보안관리의 중요성이 커지고 있는 반면 이에 대한 이해와 관심이 부족한 현실을 지적하고 보안관리를 유연하게 실행할 수 있는 적절한 해결안을 조사하고자 한다. 따라서 본 연구는 보안관리의 강화의지 및 실행에 영향을 미치는 요인으로 조직몰입, 보안위험 경험, 인지된 혜택, 파트너 의존성, 총 4가지의 외생변수를 제안하고 강화의지와 실행의 사이를 강화시켜줄 조절변수로 IT 불안정성을 제안하였다. 제안된 연구모형 검증하기 위해 AMOS 19.0을 사용하여 209개 설문을 구조방정식 접근을 통해 분석하였다. 연구결과 파트너 의존성을 제외한 나머지 변수들, 즉 조직몰입, 보안위험 경험, 인지된 혜택, 파트너 의존성은 보안관리 강화의지에 통계적으로 긍정적인 영향을 미치는 것으로 나타났다. 본 연구의 결과를 바탕으로 기업단위의 보안관리에 대한 새로운 학문적 근거를 제안하고 실무적 관리 지침에 중요한 역할을 할 수 있을 것이다.

핵심주제어: 보안관리, 인지요인, 강화의지 및 실행, IT불안정성

논문접수일: 2013년 05월 16일 수정일: 2013년 06월 17일 게재확정일: 2013년 06월 22일
* 동명대학교 경영대학 경영정보학과 부교수, jongho@tu.ac.kr

Ⅰ. 서 론

Dhillon과 Backhous(2001)에 의하면 현대의 기업들은 정보기술에 대한 의존도가 증가함에 따라 정보보안에 대한 위험 역시 지속적으로 늘어가고 있으며 Hsu 등(2012)은 정보기술이 기업 경영 전반에 생산성 및 효율성 확보에 중요한 역할을 하지만 정보보안의 실패는 기업의 존폐여부를 결정할 만큼 미치는 영향과 피해 규모가 상당하다고 한다. 그리고 Yildirim (2011), Finne등(2000)은 최근 이러한 정보의 노출과 보안관리와 관련해서 이전의 연구들은 잠재적 위험에 대한 인식이 높아지면서 보안 투자는 확대되고 있는 추세라고 한다.

한편 Cavusoglu 등(2009)은 시스템 혹은 외부의 해킹과 같은 사고에 의한 보안의 피해 사례가 급증해왔던 과거와 달리 조직원들의 도덕적 해이 혹은 충성심 결핍, 시스템의 오용, 남용 등 내부 원인 소재들이 보안관리의 부정적인 사례가 되고 있다. 다시 말해, Siponen와 Vance(2010), Straub와 Welke 등(1998)은 기술적, 물리적 도구에 의존만으로는 조직 내부의 보안관리를 충분히 설명할 수 없기 때문에 조직원들이 인식할 수 있는 요소들을 통해 정보 보안 문제를 사전에 제어할 필요성이 있다고 한다. 하지만 보안관리의 중요성이 대두된 반면 이에 대한 체계적 기준 및 구축 방법의 실행은 미비하다고 할 수 있다. 이전의 연구들에서는 기술적 관리에 중점을 둔 연구들로 조직의 내부 현상을 다룬 연구는 부족하다. 이에 따라 기업이 그들의 정보 자산을 점검하고 보안관리를 내부적으로 확산할 수 있는 이론적 정립이 제한적이었다.

Boss 등(2009)은 조직 내 보안은 전문가 혹은 기술적 해결책에 근거하는 것만으로 견고한 설계가 불가능하며, 모든 조직 시스템은 사람에 의해 운영 및 조정되는 것이 일반적인 사항이므로 강력한 보안 솔루션을 제시하기 위해서는 조직 내 문화와 인식을 변경하는 것이 중요한 역할을 한다고 주장하였다. 또한 Bulgurcu 등(2010)은 기존의 단편적인 솔루션은 내부의 완벽한 보안이 이루어지고 있다는 오해를 불러일으키고 보안 체계에 오히려 방해가 될 수 있기 때문에 조직적 측면에서 생각의 전환과 자발적 참여를 유도할 필요성이 있다고 강조하였다. 따라서 Anderson과 Agarwal(2010), Straub와 Welke(1998)은 보안관리에 대한 적절한 예방책을 찾기 위해서는 조직 전반의 보안 유효성에 영향을 미치는 요인들에 대한 다양한 접근과 시도가 필요하다. 특히 Von Solms(2004), Jahner와 Krcmar등(2005)은 기술적 약점에 편중되는 것이 아니라 보안관리에 있어서의 관리적 능력에 의한 역할과 책임이 필수적이라는 사실을 통해 성공적인 관리

가 가능하다.

본 연구는 조직의 보안관리를 계속적으로 유지하고 조직 내 정착시킬 수 있는 방안을 마련하고자 이에 대한 인지요인으로 조직몰입, 보안위험 경험, 인지된 혜택, 파트너 의존성을 제안하고 조직의 보안관리 강화의지 및 실행에 어떤 영향을 미치는지를 살펴보고자 하였다. 또한 IT 불안정성이 보안관리 강화의지와 보안관리 실행 사이에서 어떤 조절효과가 있는지에 대해서도 확인하였다. 즉 본 연구는 보안관리의 현실적인 이해와 발견을 제공하고 보안관리에 대한 조직들의 인식제고와 프로세스 결정에 대한 학문적 바탕을 제시하고자 한다.

Ⅱ. 선행연구

기업의 보안에 대한 연구는 다양한 각도에서 이루어져 왔다. 예를 들면, Lee와 Larsen등(2009)의 기술 및 물리적 설계, Straub(1990)의 시스템 보안 유효성, Gupta와 Hammond등(2005)의 보안투자 결정, Boss 등(2009)의 보안 정책준수, Spears와 Barki등(2010)의 보안대책 및 관리 등 여러 부분에서 시도되고 있다. 특히 Straub(1990), Lee 등(2004)의 보안의 관점은 정보시스템의 사용이 증가하면서 컴퓨터 사용과 관련 오용 및 남용과 같은 연구들에서 차츰 발전되어 보안 현상에 집중하는 형태로 나타나고 있다고 할 수 있다. 아울러 D'Arcy 등(2009)에 의하면 최근 연구들에서는 컴퓨터 오용의 억제이론(deterrence theory)을 활용한 개념을 확장하여 보안관련 연구를 통해 증명하는 형태로 설명하고 있다. 즉 컴퓨팅 오용과 같은 최종 사용자의 행동으로 사회적 범죄의 원인이 될 수 있기 때문에 이를 처벌의 강도 정도에 따라 통제할 수 있다고 주장한다.

또한 Pahnila 등(2007)의 연구들에서는 보안정책 준수의지에 대해 초점을 둔다. 예를 들면, Siponen 등(2006)은보호동기이론(protection motivation theory)을 적용하여 조직의 공식적인 제재를 명확히 하기 위해서는 환경적 요인(예, 지각된 위협 등)들에 대한 이해가 필요하다고 하였다. 뿐만 아니라 Herath와 Rao등(2009)은 대리인 이론(agency theory)에 바탕을 두고 패널티 혹은 사회적 압력과 같은 내·외부 요소들이 보안에 대한 조직적 분위기를 형성하고 나아가 조직원들이 보안을 위해 조직 내에 존재하는 관련 정책들을 준수하기 위해 노력한다고 주장하고 있다.

한편 Straub와 Welke등(1998)은 조직의 보안관리 차원을 내부의 중요자산을 보호하기 위해 위험의 발생여부를 사전에 파악하고 조사하기 위해서는 인지수준의 평가가 필요하다고 주장하고 있다. 예를 들면, Babatunde

와 Selamat(2012)는 조직 보안의 구조적 합리화와 의사결정의 효율성을 돕기 위해서는 관리체계가 구축되어야만 하는데 이를 위해서는 조직원의 보안에 대한 당혹감을 제거할 수 있는 요인에 대한 분석이 필요하다고 하였다. 이에 대해 정보보안관리의 평가요인으로 기술의 수준, 국제 보안표준, 정보보안 정책, 정보보안 인식, 정보보안 훈련 프로그램, 정보보안 문화, 조직원의 동기, 최고 경영자의 몰입 제안하였다. Hsu 등(2012)은 기업뿐 아니라 공공기관의 보안 침해가 빈번하다는 점을 지적하고 근본적인 솔루션을 제시하기 위해서는 제도적 이론에 기반 한 조직과의 일치가 어떻게 작용하는지 살펴볼 필요가 있다고 하였다. 즉 이 연구에서는 정보보안관리 도입과 정보보안관리 동화에 대한 제도적 영향과의 관계를 검증하였는데 제도적 영향의 요소로는 동료의 영향과 관리 권한상의 영향, 두 가지를 포함하였다. 더불어 경제적 기반 요소들이 제도적 영향과 정보보안관리 도입과 동화 사이에서 조절효과를 할 것이라는 가설을 제시하였다. 경제적 기반 요소로는 지각된 환경 불안정성, 지각된 경쟁 우위 획득, 자원의 유용성은 제도적 영향과 정보보안관리 도입 사이에 영향을 주며, 최고경영자의 지원, IT 능력, 문화적 접근성은 제도적 영향과 정보보안관리 동화 사이에서 영향을 미칠 것이라고 제안하였다. 결과적으로 이러한 변수들은 정보보안 관리에 유의미한 영향이 있는 것으로 나타났다.

Straub와 Welke등(1998)은 지금까지의 보안 관리에 관한 연구들은 조직의 의사결정의 최적화를 유도하고 위험 및 취약성을 제거하기 위해 대책과 대안들을 추적하고 조직 내·외부에 설득과 이해가 필요하다고 하였다. 특히 최근 많은 연구들을 통해 기술적 솔루션뿐만 아니라 그 이상의 포괄적인 노력이 이루어져야 한다고 주장한다. 보안에 대한 기본적인 접근으로는 기술적, 인적, 조직적, 크게 세 가지 관점에 근거하고 있는데 이전에는 기술적 방법에 우선하고 있다는 한계가 있다. 하지만 이는 단편적 해결책으로는 조직 전반의 보안 문제를 해소하기에는 역부족이라고 할 수 있다.

Beznosov와 Beznosova(2007)은 정보보안의 계속적인 유지를 위해서는 조직적 시각에서 보안을 대하는 자세가 필요하다고 주장하였다. 다시 말해 Kankanhalli 등(2003)은 보안은 한 쪽으로 편중되어서는 완벽한 안전망을 설계하기 어렵기 때문에 기술과 조직적 측면의 동시적으로 집중된 투자가 이루어질 때 현재의 보안 약점을 근본적으로 줄여나갈 수 있다. Werlinger 등(2009) 또한 조직, 기술, 인적 요소들의 전반을 통해 위험요소들을 발견하고 손실을 최소화할 수

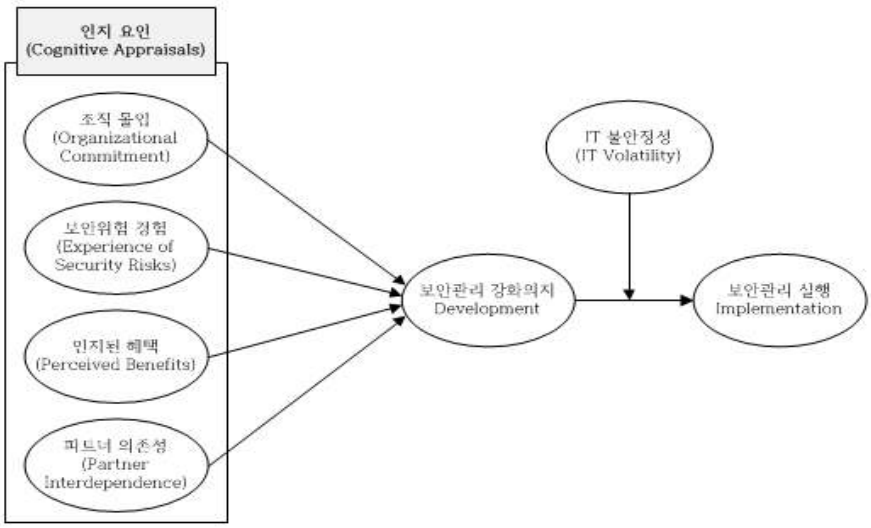
있다고 하였다. 즉 Dutta와 Roy등(2008)에 의하면 조직이 보안을 효과적으로 지켜나가기 위해서는 관리상의 어떠한 잠재요소들이 보안책임과 역할에 영향을 미칠 수 있는가에 대한 조사가 중요하다.

최근 몇몇 실증적 연구들에 의해 보안관리에 대한 중요성과 심각성에 대한 인식제고를 주장하고 있지만 여전히 보안 솔루션에 대한 조직적 행동의 효과에 대한 연구는 미비하다고 할 수 있다. 따라서 본 연구에서는 사람의 인식에 의해 보안관리가 좌우될 수 있음을 강조하고 기존의 연구들을 참고로 인지 요인을 도출하여 보안관리 연구에 새로운 이론적 근거를 제시하는데 주요 목적이 있다.

Ⅲ. 연구모형과 연구가설

1. 연구모형

본 연구는 선행연구에서 살펴본 바와 같이 기업의 보안관리 인식과 책임이 강조되고 있다는 사실을 지적하고 이에 적합한 변수들을 도출하여 연구모형을 개발하였다. Babatunde와 Selamat(2012)는 보안관리의 범위를 구체화하기 위해서는 조직원들이 인지할 수 있는 요소들에 의한 접근이 우선되어야 한다고 주장하였다. 이에 Herath와 Rao(2009), Anderson과 Agarwal 등(2010)의 보안관리 강화의지의 인지 요인으로 조직몰입(Organizational Commitment), 보안위험



<그림 1> 연구 모형

경험(Experience of Security Risks), 인지된 혜택(Perceived Benefits), 파트너의존성(Partner Interdependence)을 제시하여 어떠한 기업 내 잠재적 동기에 의해 보안을 실천하고자 하는지에 대해 알아보고자 하였다. 또한 Walker와 Weber 등(1984)에서의 제시처럼 기업의 IT에 대한 의존도가 상당히 높아짐에 따른 IT의 불확실한 상황이 보안관리 강화의지에서 실행에 이르기까지 어떠한 요인이 강화에 영향을 미치는지에 대해 살펴보고자 하였다. 따라서 이에 대한 모형과 가설을 나타내면 다음의 <그림 1>과 같다.

2. 연구가설

본 연구에서 제안하는 인지 요인의 첫 번째 변수는 조직 몰입이다. Herath와 Rao 등(2009)은 조직 몰입은 조직 구성원의 업무 태도와 조직 행동 개념을 효율적으로 설명한다. 즉 조직의 목표와 가치관을 받아들이고 희생을 기꺼이 동의하는 정도라고 할 수 있다. Stanton 등(2003)은 조직과의 관계에서 계산과 교환 등 자신이 지불해야 할 비용의 부담을 최소화시키고 개인적 이득이나 관심에 가치를 두는 것이 아니라 조직에 대한 의무감을 갖고 행동을 수행하는 내적인 가치관을 말한다. 따라서 Lee 등(2004)은 조직의 경영에 조직원들이 형성하는 일체감 혹은 충성심은 조직에 대한 부정적인 결과를 감소시키고 조직에게 더욱 집중할 수 있는 동기를 제공하여 생산성 증대와 경쟁력 향상에 도움이 될 수 있다. 마찬가지로 이와 같은 조직 몰입은 조직 내 보안관리에 중요한 동기요인이 될 수 있을 것이다.

[가설 1]: 조직몰입은 보안관리 강화의지에 정(+)의 영향을 미칠 것이다.

다음으로 제안하는 두 번째 변수는 보안위험 경험이다. 경험은 정보시스템 분야에서 많은 설득력을 갖는 주요 변수로 채택되어 왔다. Venkatesh (2000)의 직접경험, Thompson 등(1994)의 이전경험, Bajaj와 Nidumolu 등(1998)의 과거사용 또는 Thompson과 Higgins 등(1991)의 습관을 의미하거나, Hartwick와 Barki 등(1994)의 시스템 개발 과정에 있어서는 사용자 참여를 경험이라고도 한다. 경험의 관점은 시스템의 사용시간, 빈도, 패키지의 수 등 경험의 양적인 면에 치중되어 연구되어 왔다고 할 수 있다. 마찬가지로 본 연구에서의 경험은 보안관리를 인지하기 위한 요소로 과거의 보안위험을 얼마나 겪었는가에 초점을 두었다. Compeau와 Higgins 등(1995)은 이러한 위험에 대한 과거의 경험 정도는 현재의 보안에 대한 심각성과

중대함을 각인시킴으로써 현재의 보안관리에 대한 실수 및 무지의 행동을 수정하고 나아가 자율적 예방 활동을 촉진 할 수 있을 것이다.

[가설 2] 보안위험 경험은 보안관리 강화의지에 정(+)의 영향을 미칠 것이다.

보안관리 강화의지의 영향에 관한 세 번째 변수는 인지된 혜택이다. Kuan과 Chau 등(2001)은 조직 내부의 절제를 위해서는 해당 시스템 혹은 프로세스에 대한 상대적인 이익이 어느 정도인가가 우선된다. 조직 내 전반 혹은 개인들에게 현재 제시되는 새로운 대안이 어떠한 효율적인 측면을 제공함으로써 경제적 인센티브와 혜택을 발생시킬 수 있는가는 고려되어야 할 주요 사안이 될 수 있다. Anderson과 Agarwal 등(2010)은 정보시스템 뿐 아니라 보안관리의 연구에서도 조직 내 올바른 보안에 대한 경각심을 불러일으키기 위해서는 보안상의 발생될 수 있는 직·간접 이득에 대한 충분한 이해가 필요하다고 하였다.

[가설 3] 인지된 혜택은 보안관리 강화의지에 정(+)의 영향을 미칠 것이다.

본 연구에서 제안하는 네 번째 변수는 파트너 의존성이다. 현대의 기업 환경은 협력의 관계에 놓여 있다고 할 수 있다. 즉 Zhu 등(2006)은 조직이 경영을 위해서는 내부 뿐 아니라 외부의 계열 혹은 동종 산업에 존재하는 다른 조직과의 구조를 중요하게 생각하고 이에 대한 영향을 무시할 수 없다. Lee(2009)는 동종 계열의 정보기술 변화 혹은 도입은 조직 내 전략 및 목표에 많은 영향을 미치고 조직 역시 이러한 환경을 수용하기 위해 여러 노력과 대처 방안을 모색하고 새로운 관리 방식을 찾고 모방하려 한다. 특히 DiMaggio와 Powell 등(1983)은 파트너 기업들의 기술 및 프로세스 도입과 관련한 혁신적이거나 성공적인 결과를 따르려는 경향이 있다. 이러한 관점에서 협력 기업들의 관계 및 의존은 조직의 보안관리에도 중요한 영향 요인이 될 수 있다. 이와 같은 논의를 바탕으로 다음과 같은 가설을 설정하였다.

[가설 4] 파트너 의존성은 보안관리 강화의지에 정(+)의 영향을 미칠 것이다.

Venkatesh 등(2003)은 정보시스템 관련 많은 연구에서 최종 사용자의 의지는 실제 행동으로 나타나난다는 결과가 확인되었다. Spear와Barki 등(2010)은 정보시스템 보안에 관한 연구에서도 최종 사용자들의 지각에 의해 내부의 보안 의지가 강화 되고 나아가 실질적인 관리 수준이 향상된다고 주장한다. Whitman(2004)은 보안

관리 강화의지, 즉 보안의 통제와 강화에 대한 의지는 보다 나은 보안 설계와 오류의 감소에 대한 긍정적인 평가를 기대하고 이러한 보안에 대한 걱정과 우려는 보안관리가 실행될 수 있도록 한다. 따라서 Spear와 Barki 등(2010)은 보안관리에 대한 인식과 노력은 개발로 이어지고 이는 보안관리의 적극적인 수행에도 의미있는 결과를 도출하는데 영향을 미칠 것이다. 이와 같은 논의를 바탕으로 다음과 같은 가설을 설정하였다.

[가설 5] 보안관리 강화의지는 보안관리 실행에 정(+)의 영향을 미칠 것이다.

Duncan(1972)은 정보기술의 발전은 현존하는 기업들에게 다양한 기회를 제공하는 반면 빠른 변화로 인해 새로운 형태의 문제를 양산하기도 한다. Bichteler(1987)는 문제발생의 경우 기업들에게 혜택을 제공하기 이전에 실질적인 장벽으로 존재할 수가 있기 때문에 IT의 불확실한 상황에 대한 기업들의 인식능력이 간과되어서는 안 된다고 할 수 있다. 즉 Walker와 Weber 등(1984)은 IT 불안정성이란 시스템 및 기술적 인프라와 같은 신기술의 지속적인 변화와 업그레이드되는 정도를 의미한다. Tarafdar와 Ragu-Nathan 등(2011)은 IT의 이러한 변동은 기업에게 자칫 혼란을 일으키고 스트레스를 유발할 수 있지만 이러한 요인에 대해 일시적이고 도전거리로 인식할 때 긍정적인 효과가 나타날 수 있다. 다시 말해, 직면한 상황을 이해하고 학습하기 위한 시간과 노력을 기꺼이 투자하는 호의적인 태도가 잠재되어 있다는 것이다. Walker와 Weber 등(1984)은 기업은 둘러싼 환경이 불확실하다고 느끼면 여러 정보들을 신속, 정확하게 수집하고 처리 및 전달하기 위해 경영전반에 총체적인 관심을 기울일 수 있다. 따라서 경영의 주요한 부분이라 여기는 보안관리 역시 이러한 효과가 발생될 것이라 예측할 수 있다. 이와 같은 논의를 바탕으로 다음과 같은 가설을 설정하였다.

[가설 6] IT 불안정성은 보안관리 강화의지와 실행 사이의 관계를 더 강화시켜 줄 것이다.

<표 1> 변수의 조작적 정의 및 관련연구

변수	조작적 정의	관련연구
조직 몰입	조직 보안에 대한 책임 및 의무감을 갖는 정도	Herath와 Rao(2009)
보안위험 경험	보안의 위험 및 문제에 대한 직·간접적인 경험의	Li 등(2010)

	정도	
인지된 혜택	보안관리로 조직이 얻을 수 있는 상대적 이익에 대한 인식 정도	Chau과 Tam(2000)
파트너 의존성	협력기업에 대한 기술적, 전략적 조직의 의존 정도	Lee(2009)
IT 불안정성	IT의 빠른 발전과 변화에 대한 기업의 인식 정도	Chen과 Paulraj(2004)
보안관리 강화의지	조직의 보안관리 강화 및 통제에 대한 의지 정도	Spears와 Barki(2010)
보안관리 실행	조직의 보안관리 활동의 실행 정도	Spears와 Barki(2010)

Ⅳ. 실증분석

1. 자료수집 및 인구통계학적 특성

가설검증을 위해 국내 보안관리를 전략적 요소로 간주하여 실행하는 조직을 대상으로 설문하였다. 설문 대상은 코스피 와 코스닥에 등록된 기업 및 그 밖의 기업을 대상으로 우편, 이메일, 전화, 방문 등을 사용하여 설문을 실시하였다. 총 2,000부의 설문이 배포되어 이 중 238부(회수율 11.9%)가 회수 되었다. 하지만, 본 연구의 내용과 관계없거나 응답이 불성실한 29부를 제외한 총 209부를 사용하였다.

각 잠재변수들을 측정하기 위한 측정항목들은 일차적으로 국외 선행연구들을 바탕으로 도출한 후 본 연구의 목적에 맞게 수정 및 보완을 하였다. 최종 도출된 모든 측정항목은 (1)강한 부정에서부터 (5)강한 긍정에 걸친 5점 리커트(5-point Likert) 척도를 사용하였다. 본 연구에서 사용한 변수의 조작적 정의와 관련 연구에 관한 설명은 <표 1>에 제시하였다.

<표 2>는 표본의 인구통계학적 특징을 나타내고 있다. 설문대상자들의 인구 통계적 특성은 다음과 같다. 우선, 응답자의 해당기업 업종은 물류/유통/서비스(40.7%)가 가장 많았고, 그 다음으로 제조(32.5%), 정보통신(12.4%), 건설(9.1%)순으로 나타났다. 종업원 수는 500-1,000명 미만(27.3%), 100명-500명 미만(23.9%), 1,000명-3,000 미만(21.5%)등의 순으로 나타났으며, 연 매출액은 1,000억

<표 2> 응답자의 인구통계학적 특성

분류		빈도	응답비율(%)
업종	제조	68	32.5%
	물류/유통/서비스	85	40.7%
	정보통신	26	12.4%
	건설	19	9.1%
	기타	11	5.3%

성별	남자	164	78.5%
	여자	45	21.5%
학력	고졸	36	17.2%
	전문대/대학졸	117	56.0%
	대학원졸	56	26.8%
직위	이사급 이상	54	25.8%
	부장. 차장	69	33.0%
	과장. 대리	81	38.8%
	기타	5	2.4%
종업원 수	50명 미만	12	5.7%
	50명 - 100명 미만	17	8.1%
	100명 - 500명 미만	50	23.9%
	500명 - 1,000명 미만	57	27.3%
	1,000명 - 3,000명 미만	45	21.5%
	3,000명 이상	28	13.4%
연 매출액	10억 미만	11	5.3%
	10억 - 50억 미만	18	8.6%
	50억 - 100억 미만	14	6.7%
	100억 - 500억 미만	28	13.4%
	500억 - 1,000억 미만	64	30.6%
	1,000억 이상	74	35.4%
합계		209	100.0%

이상인 기업(35.4%)이 가장 많은 분포를 나타냈으며 그 다음으로 500억-1,000억 미만(30.6%), 100억-500억 미만(13.4%), 10억-50억 미만(8.6%)의 분포를 보였다. 직위는 과장/대리(38.8%), 부장/차장(33.0%), 이사급 이상(25.8%)의 순으로 나타났다.

2. 측정모형의 신뢰성 및 타당성 검증

최종 수집된 데이터(n=209)로 측정모형의 신뢰성과 타당성 검증을 실시하였다. 특히 타당성은 동일한 개념을 측정한 상이한 설문 항목 간에 상관관계가 존재하는지를 검증하는 집중타당성(convergent validity)과 유사한 두 개의 개념이 뚜렷이 구별되는 정도를 검증하는 판별타당성(discriminant validity)을 검증하였다. 신뢰성 검증 방법은 일반적으로 사회과학 연구 에서 가장 많이 사용되고 있는 Cronbach's Alpha 계수(0.7 이상)를 이용하였다. 집중타당성은 확인적 요인분석 결과 중 요인적재값(factor

<표 3> 신뢰성 및 집중타당성 분석

변수	항목	요인값	C.R	Cronbach's - α
조직 몰입 (Organizational Commitment)	oc1	0.753	-	0.763
	oc2	0.707	10.621	
	oc3	0.718	12.342	

보안위험 경험 (Experience of Security Risks)	esr1	0.719	-	0.816
	esr2	0.829	15.798	
	esr3	0.764	9.477	
인지된 혜택 (Perceived Benefits)	pb1	0.806	-	0.841
	pb2	0.728	12.242	
	pb3	0.735	14.021	
파트너 의존성 (Partner Interdependence)	pi1	0.881	-	0.838
	pi2	0.792	12.637	
	pi3	0.765	10.511	
IT 불안정성 (IT Volatility)	itv1	0.854	-	0.787
	itv2	0.823	15.873	
	itv3	0.867	17.131	
	itv4	0.718	13.273	
보안관리 강화의지 (Development)	d1	0.839	-	0.852
	d2	0.776	14.565	
	d3	0.812	14.639	
	d4	0.746	12.275	
보안관리 실행 (Implementation)	i1	0.835	-	0.915
	i2	0.867	16.898	
	i3	0.853	11.769	
	i4	0.860	12.234	

loading)을 사용하였으며, 일반적으로 요인적재량은 ±0.4 이상이면 유의한 것으로 판단된다(Barclay 등, 1995). 판별타당성 검증을 위해 Fornell와 Larcker(1981)가 제시한 평균분산추출(Average Variance Extracted: AVE)과 Pearson 상관관계분석 방법을 사용하였다. 각 구성개념에서 AVE의 제곱 값이 해당 구성개념과 다른 구성개념간의 상관계수 값을 초과하면 판별타당성이 존재하는 것으로 본다.

<표 3>과 <표 4>는 본 연구에서 사용된 변수들의 신뢰성 및 타당성 검사 결과를 보여주고 있다. 우선 신뢰성 측정 결과 신뢰성을 저해하는 항목은 없었으며, 신뢰성 검증에 사용된 Cronbach's Alpha 값은 0.763에서 0.915로 분포되어 권장치(0.7 이상) 이상으로 나타나 측정항목의 신뢰성은 확보된 것으로 판단된다. 다음으로 모든 항목에 대한 요인 적재 값 역시 기존 연구에서 제시하는 기준치 이상으로 나타나 측정항목에 대한 집중타당성의 문제가 없는 것으로 나타났다.

<표 4> 잠재변수의 판별타다성과 분석 결과

변수	1	2	3	4	5	6	7
1. 조직 몰입	**0.847**						
2. 보안위험 경험	0.302	**0.843**					
3. 인지된 혜택	0.132	0.225	**0.815**				
4. 파트너 의존성	0.238	0.350	0.376	**0.869**			

5. IT 불안정성	0.181	0.244	0.160	0.311	**0.856**		
6. 보안관리 강화의지	0.421	0.198	0.119	0.287	0.360	**0.878**	
7. 보안관리 실행	0.273	0.194	0.399	0.262	0.131	0.345	**0.881**

주) 진하게 표시된 대각선 값은 AVE의 제곱근 값임.

마지막으로 AVE값을 이용한 판별타당성 검증결과 역시 대각선 AVE값의 제곱근이 종과 횡의 상관계수 값이 보다 높이 나타나 판별타당성 역시문제가 없는 것으로 나타났다. 이와 같은 결과는 설문문항의 내적 일관성 및 타당성을 통계적으로 증명 하고 있다.

3. 적합도 및 가설 검증

측정모형의 신뢰성과 타당성 검증에 후, 수집된 데이터의 특징과 측정모형의 특징이 어느 정도 일치하는지를 검증하기 위해 AMOS 19.0을 사용하여 적합도 검증을 실시하였다. 초기 측정모형의 적합도 검증은 연구모형에서 제안하는 총 7개 변수를 측정하기 위한 24개의 측정항목으로 실시하였다. 적합도 검증의 판단 기준은 기존 연구에서 일반적으로 많이 사용하는 상대적 카이스퀘어(X^2/df), 기초부합지수(GFI), 수정된 기초부합지수(AGFI), 비교부합지수(CFI), 증분적합지수(IFI), 표준적합지수(RMSEA)를 사용하였다. 초기 측정모형의 적합도를 검증한 결과의 산출물 중 수정지수(modification index)를 살펴본 결과 몇 항목이 적합도를 저해하는 요소로 판단되었다. 예를 들면,IT 불안정성을 측정하는 5번째 항목(itv5)과 6번째 항목(itv6), 보안관리 강화의지를 측정하는 5번째 항목(d5)들이 측정모형에서 원래 측정하기 위한 잠재변수 외에 다른 변수에도 적재되는 성향이 있어 이 세 항목을 제거한 후 적합도 검증을 다시 실시하였다. <표 5>에서 나타나듯이 재검증 결과 모든 지수가 권장치 이상이므로 적합도에 문제가 없는 것으로 나타났다. 총 209개의 데이터로 측정모형의 신뢰성과 타당성 검증 후 연구모형에서 제시한 변수들 간의 영향을 검증하기 위해 구조방정식 분석(Structural Equation Modeling: SEM)을 실시하였다. SEM 분석을 통해 연구목적을 증명하기 위한 3 가지 중요한 결과를 도출해 낼 수 있다. 첫 번째 결과는 구조모형의 적합도 정도이다. 구조모형의 적합도

<표 5> 적합도 검증

Model	IFI	GFI	AGFI	CFI	X^2/df	RMSEA
초기측정모형	0.919	0.876	0.840	0.939	1.868	0.045
수정모형	0.940	0.915	0.910	0.959	1.982	0.036

권장치	≥0.9	≥0.9	≥0.8	≥0.9	≤3.0	≤0.05

결과는 상대적 카이스퀘어(X^2/df) = 2.601, 기초부합지수(GFI) = 0.941, 수정된기초부합지수(AGFI) = 0.916, 비교부합지수(CFI) = 0.953, 증분적합지수(IFI) = 0.948, 표준적합지수(RMSEA) = 0.035로 나타나 연구가설의 검증에는 별무리가 없을 것으로 판단되었다. 두 번째는 연구모형의 변수들 간의 영향 정도를 알 수 있는 경로계수(β)이다. 즉, Wixom과 Watson 등(2001)의 경로계수는 두 변수간 인과관계에 대한 정보를 보여준다. 마지막으로 SEM은 내생변수에 대한 결정계수 즉 R2 결과 값도 보여준다. 결정계수 R2는 총 변동 중에서 회귀선 즉 변수들에 의해 설명되는 비율을 의미한다.

분석 결과를 살펴보면, 본 연구에서 제안한 연구모형의 보안관리 인지 요인의 조직 몰입, 보안위험 경험, 인지된 혜택은 각각 경로계수 0.378, 0.429, 0.552에서 유의수준 0.001, 0.01, 0.001에서 지지되었다. 따라서 가설 1, 가설 2, 가설 3은 채택되었다. 하지만 인지 요인의 파트너 의존성은 경로계수 0.102로 기각되었다.

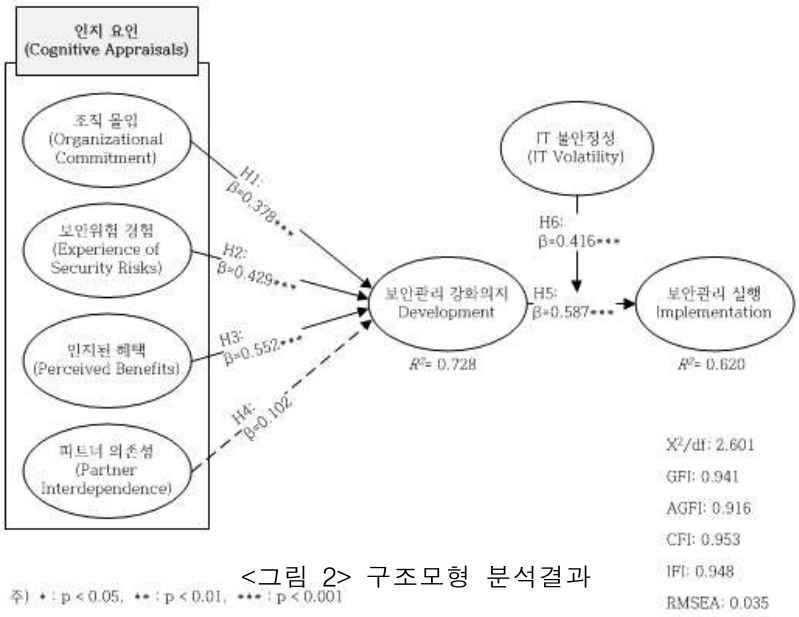
보안관리 강화의지가 실행에 미치는 영향에 대한 가설 5는 경로계수 0.587, 유의수준 0.587에서 지지되었다. 마지막으로 Baron and Kenny 등(1986)이 조절변수로 제안한 IT 불안정성에 대한 가설 6은 보안관리 강화의지와 실행 사이에서 경로계수 0.416, 유의수준 0.001에서 지지되었다. 연구모형에서 제안한 인지요인의 4 변수 중 파트너 의존성을 제외한 나머지 변수는 보안관리 강화의지를 표현하는 분산의 72.8%를 설명하고 있다. 즉, 보안관리 강화의지 변수가 가지고 있는 정보 중 72.8%는 인지요인의 3 변수의 변동으로 설명할 수 있다는 것을 의미한다. 또한, 보안관리 강화의지는 보안관리 실행을 분산의 62.0%를 설명하고 있다. <표 6>

<표 6> 가설검증 결과

가설	경로	표준화된 경로계수	t 값	채택 유·무
가설 1	조직 몰입 --> 보안관리 강화의지	0.378***	5.890	채택
가설 2	보안위험 경험 --> 보안관리 강화의지	0.429**	6.562	채택
가설 3	인지된 혜택 --> 보안관리 강화의지	0.552***	7.563	채택
가설 4	파트너 의존성 --> 보안관리 강화의지	0.102	1.017	기각
가설 5	보안관리 강화의지 --> 보안관리 실행	0.587***	8.950	채택
가설 6	보안관리 강화의지 --> 보안관리 실행 ↑ IT 불안정성	0.416***	6.132	채택

주) *p < 0.05, **p < 0.01, ***p < 0.001

과 <그림 2>는 가설검정의 결과와 채택 유·무의 요약을 보여주고 있다.



<그림 2> 구조모형 분석결과

Ⅴ. 결 론

정보시스템 및 네트워크를 활용한 현대 조직 환경은 조직 내 보안의 중요성을 필수적인 요소로 인식하게 되었다. 하지만 보안실태에 대한 걱정과 우려의 시선은 여전히 문제화되고 있다. 지금까지 많은 조직들은 매우 체계적인 기술적 보안체계를 갖고 있으며, 제시되고 있는 보안과 관련된 가이드라인을 잘 준수하고 있기 때문에 보안을 외부의 침해로부터의 문제 요소로 다루고 있는데 집중하고 있지만 상당부분이 조직 내 인식의 결여라는 오해를 상기시킬 필요가 있다. 이를 위해서는 검증된 솔루션을 확인시키고 보안상황을 파악할 수 있는 이론적 정립을 통해 실효성 있는 방안을 마련해야 한다. 따라서 본 연구에서는 이러한 보안관리의 중요성을 강조하기 위해 이에 대한 인지요인을 도출하고 특히 불확실한 기술 변화에 조직이 어떠한 영향을 받는지에 대해서도 살펴보고자 하였다. 우선 인지요인으로는 조직 몰입, 보안위험 경험, 인지된 혜택, 파트너 의존성을 제안하였으며 이들이 보안관리 강화의지에 어

떤 영향을 미치고 나아가 보안관리 실행에 미치는 영향을 검증하였다. 뿐만 아니라 IT 불안정성이 보안관리 강화의지와 실행 사이에서의 조절효과에 대해서도 분석하였다. 국내 기업들을 대상으로 총 209개의 표본을 수집하여 분석한 결과를 살펴보면 다음과 같다.

연구결과를 요약하면, 첫째, 인지요인의 조직 몰입, 보안위험 경험, 인지된 혜택은 보안관리 강화의지에 긍정적인 영향을 미치는 것으로 나타났다. 하지만 파트너 의존성은 유의한 영향을 미치지 않는 것으로 나타났다. 이는 본 조직이 인식 할 수 있는 요소로써 외부의 환경적인 측면보다는 직접적 인식 혹은 조직 자체에서 발생하고 수 있는 보안상의 기능과 역할이 더욱 중요하게 작용하고 있다는 것을 알 수 있다. 다시 말해 보안관리 강화의지에 있어 동종 업계와의 관계적 영향보다는 조직 내부적 요소들인 조직 몰입, 보안위험 경험, 인지된 혜택과 같은 요소들이 우선시 되고 있다는 사실을 알 수 있다. 둘째, Spears와 Barki 등(2010)의 연구에서 검증된 바와 같이 보안관리 강화의지는 보안관리 실행에 긍정적인 영향을 주는 것으로 밝혀졌다. 마지막으로 IT 불안정성은 보안관리 강화의지와 실행사이에서 이들 사이의 관계를 강화시키는 것으로 나타나 조절효과가 검증되었다. 조직의 모든 업무들이 정보시스템과 네트워크와 같은 기기들에 대한 의존정도가 상당히 높은 영향을 미친다는 결과를 반영하고 있다는 것을 의미한다. 즉 급변하는 환경의 불안정 속에서 특히 IT 기기의 변화 속도와 다양성은 보안관리에도 매우 중요하다는 것을 알 수 있다.

결과적으로 완벽한 보안이란 존재할 수 없기 때문에 조직적 측면의 인식 수준 향상을 위한 노력이 필요하다는 것이다. 이를 위해서는 조직이 인지할 수 있는 여러 내·외적 요소들의 조화에 의해 피해를 최소화하고 사고 발생 시 이에 대한 관리 체계가 잘 정립이 될 수 있다. 아무리 철저한 기술로 무장한 솔루션이 있다고 할지라도 실질적인 보안 문제를 해결하기 위해서는 조직이 보안에 대해 고민하는 관리 태도가 중요하다고 할 수 있다. 즉 관리부재의 허점으로 인해 조직의 보안실패가 가장 큰 원인이 될 수 있다는 사실을 인지해야만 한다.

이러한 현 실태를 반영한 본 연구의 시사점을 제시하면 다음과 같다. 첫째, 기업의 보안관리 실증적 연구에 대한 새로운 변수(예, 조직 몰입, 인지된 혜택, 파트너 의존성)를 도출하여 이론적으로 검증하여 그 의미가 크다고 할 수 있다. 뿐만 아니라 IT 불안정성의 조절효과를 제안하여 이전의 연구들에서 찾아 볼 수 없었던 인과관계를 설명하였다. 이와 같은 본 연구의 시도는 향후 기업 보안관리

실행에 대한 필요 요소를 설명하는 이론적 바탕이 될 수 있을 것이다. 둘째, 기업들의 보안의 인식이 부족한 상태를 점검하고 실제 기업들이 보안 프로세스에 적용할 수 있는 기회와 동기를 제시할 수 있는 정보를 알 수 있다. 이는 기업들이 그들 환경에 도출된 요소들을 활용하여 유용한 결과를 얻고 기존에 내부에 존재하던 부정적인 기능들을 최소함으로써 성공적인 보안관리를 도울 수 있을 것이다. 반면 본 연구의 몇 가지 한계점으로는 우선 본 연구에서 사용된 인지요인 이 외의 변수의 다양화와 측정도구의 개발을 통해 보안관리를 설명하기 위한 요소의 타당성을 추가적으로 검정할 필요가 있다. 또한 기업 대상의 설문일 경우 공공기업과 민간기업의 분류된 형태로도 조사하여 어떤 결과가 나타나는지를 비교해 볼 수 있을 것이다. 마지막으로 본 연구의 변수는 자기보고방식(self-report)에 의존하여 동일방법편의(common method bias)의 가능성이 있을 수 있다. 향후 연구에서는 이러한 부분들을 보완하여 보다 심도있는 연구결과를 제시할 수 있을 것으로 기대한다.

참고문헌

1. Anderson, D. L., & R. Agarwal (2010), “Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions,” MIS Quarterly, 34(3), 613-643.
2. Babatunde, D. A., & M. H. Selamat(2012), “Investigating information security management and its influencing factors in the nigerian banking industry: a conceptual model,” International Journal on Social Science, Economics & Art, 2(2), 5-59.
3. Bajaj, A., & S. Nidumolu(1998), “A feedback model to understand information system usage,” Information & Management, 33 (4), 213-224.
4. Barclay, D., R. Thompson, & C. Higgins(1995), “The partial least squares(pls) approach to casual modeling: personal computer adoption and use as an illustration,” Technology Studies, 2(2), 285-309.
5. Baron, R. M. & D. A. Kenny (1986), “The Moderator-Mediator Variable Distinction in social psychological research: conceptual, strategic, and statistical considerations,” Journal of Personality and Social Psychology, 51(6), 1173-1182.
6. Beznosov, K., & O. Beznosova (2007), “On the imbalance of the security problem space and its expected consequences,” Information Management and Computer, 15(5), 420-431.
7. Bichteler, J.(1987), “Technostress in libraries: causes, effects and solutions,“ Electronic Library, 5(5), 282-287.
8. Bulgurcu, B., H. Cavusoglu, & I. Benbasat(2010), “Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness,” MIS Quarterly, 34(3), 523-548.
9. Boss, S. R., L. J. Kirsch, I. Angermmeier, R. A. Shingler, & R. W. Boss(2009), "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security," European Journal of Information Systems, 18(2), 151-164.
10. Chau, P. Y. K., & K. Y. Tam(2000), “Organizational adoption of open systems: a 'technology-push, need-pull' pers-

pective," Information & Management, 37(5), 229-239.
11. Cavusoglu, H., H. Cavusoglu, J. Y. Son, & I. Benbasat(2009), "Information security control resources in organizations: a multidimensional view and their key drivers," Working paper, Sauder School of Business, University of British Columbia.
12. Chen, I. J., & A. Paulraj(2004), "Towards a theory of supply chain management: the constructs and measurements," Journal of Operations Management, 22(2), 119-150.
13. Compeau, D., & C. Higgins (1995), "Computer self-efficacy: development of a measure and initial test," MIS Quarterly, 19(2), 189-211.
14. D'Arcy, J., A. Hovav, & D. Galletta(2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," Information Systems Research, 20(1), 79-98.
15. Dhillon, G., & J. Backhouse (2001), "Current directions in IS security research: towards socio-organizational perspectives," Information Systems Journal, 11(2), 127-153.
16. Dunca, R. B.(1972), "The characteristics of organizational environment and perceived environment uncertainty," Administrative Science Quarterly, 17(1), 313-327.
17. DiMaggio, P. J., & W. W. Powell(1983), "The iron cage revisited: institutional isomorphism and collective rationality in organizational fields," American Sociological Review, 48(2), 147-160.
18. Dutta, A., & R. Roy(2008), "Dynamics of organizational information security," System Dynamics Review, 24(3), 349-375.
19. Finne, T.(2000), "Information systems risk management: key concepts and business processes," Computer & Security, 19(3), 234-242
20. Fornell, C., & D. Larcker(1981), "Evaluating structural equation models with unobservable variables and measurement error," Journal of Marketing Research, 18(1), 39- 50.
21. Gupta, A., & R. Hammond(2005), "Information systems security issues and decisions for small

business: an empirical examination," Information Management & Computer Security, 13(4), 297?310.

22. Hartwick, J., & H. Barki(1994), "Explaining the role of user participation in information system use," Management Science, 40(4), 440-465.
23. Herath, T., & H. R. Rao(2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations," European Journal of Information Systems, 18(2), 106-125.
24. Hsu, C., J. N. Lee, & D. W. Straub(2012), "Institutional influences on information systems security innovations," Information Systems Research, 23(1), 1-22.
25. Jahner, S., & H. Krcmar(2005), "Beyond technical aspects of information security: risk culture as a success factor for IT risk management," in Proceedings of the 11th AMCIS, Omaha, NE.
26. Kankanhalli, A., H. H. Teo, B. C. Y. Tan, & K. K. Wei(2003), "An integrative study of information systems security effectiveness," International Journal of Information Management, 23(2), 139-154.
27. Kuan, K. K. Y., & P. Y. K. Chau(2001), "A perception-based model for EDI adoption in small businesses using a technology-organization-environment framework," Information & Management, 38(8), 507-521.
28. Lee, M. S.(2009), "An empirical study about RFID acceptance: focus on the employees in korea," World Academy of Science, Engineering and Technology, 55, 1048-1057
29. Lee, S. M., S. G. Lee, & S. Yoo(2004), "An integrative model of computer abuse based on social control and general deterrence theories," Information & Management, 41(6), 707-718.
30. Lee, Y., & K. R. Larsen(2009), "Threat of coping appraisal: determinants of SMB executives' decision to adopt anti-malware software," European Journal of Information Systems, 18(2), 177-187.
31. Li, H., J. Zhang, & R. Sarathy(2010), "Under- standing compliance with internet use policy from the perspective of rational choice theory," Decision Support Systems, 48(4), 635-645.

32. Pahnila, S., M. Siponen, & A. Mahmood(2007), “Employees’ behavior towards IS security policy compliance,” 40th Hawaii International Conference on System Sciences.
33. Siponen, M., & A. Vance(2010), “Neutralzation: new insights into the problem of employee information systems security policy violations,” MIS Quarterly, 34(3), 487-502.
34. Siponen, M., S. Pahnila, & A. Mahmood(2006), “Factors influencing protection motivation and IS security policy compliance,” Innovations in Information Technology, 1-5.
35. Spears, J. L., & H. Barki(2010), “User participation in information systems security risk management,” MIS Quarterly, 34(3), 503-522.
36. Stanton, J. M., K. Stam, I. Guzman, & C. Caldera(2003), “Examining the linkages between organizational commitment and information security,” In IEEE Systems, Man, and Cybernetics Conference Washington DC, USA.
37. Straub, D. W.(1990), “Effective IS security: an empirical study,” Information Systems Research, 1(3), 255-276.
38. Straub, D. W., & R. J. Welke (1998), “Coping with systems risk: security planning models for management decision making,” MIS Quarterly, 22(4), 441?469.
39. Tarafdar, M., Q. Tu., & R. Ragu-Nathan(2011), “Impact of technostress on end-user satisfaction and performance,” Journal of Management Information Systems, 27(3), 303-334.
40. Thompson, R. & C. Higgins (1991), “Personal computing: toward a conceptual model of utilization,” MIS Quarterly, 15(1), 125-142.
41. Thompson, R., C. Higgins, & J. Howell(1994), “Influence of experience on personal computer utilization testing a conceptual model,” Journal of Management Information Systems, 11(1), 167-187.
42. Venkatesh, V.(2000), “Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model,” Information Systems Research, 11(4), 342-365.

43. Venkatech, V., M. G. Morris, G. B. Davis, & F. D. Davis(2003), “User acceptance of information technology: toward a unified view,” MIS Quarterly, 27(3), 425-478.
44. von Solms, B., & R. von Solms(2004), "The 10 deadly sins of information security management," Computers & Security, 23(5), 371-376.
45. Walker, G., & D. Weber(1984), “A transaction cost approach to make-or-buy decisions,” Administrative Science Quarterly, 29 (3), 374-391.
46. Werlinger, R., K. Hawkey, D. Botta, & K. Beznosov(2009), “Security practitioners in context: their activities and interactions with other stakeholders within organizations,” International Journal of Human-Computer Studies, 67(7), 584-606.
47. Whitman, M. E.(2004), “In defense of the realm: understanding threats to information security,” International Journal of Information Management, 24(1), 43-57.
48. Wixom, B., & H. Watson(2001), “An empirical investigation of the factors affecting data warehousing success”, MIS Quarterly, 21 (2), 17-41.
49. Yildirim, E. Y., G. Akalp, S. Aytac, & N. Bayram(2011), "Factors influencing information security management in small- and medium-sized enterprises: a case study from turkey," International Journal of Information Management, 31(4), 360-365.
50. Zhu, K., K. L. Kraemer, S. Xu(2006), “The process of innovation assimilation by firms in different countries: a technology diffusion perspective on e-business,” Management Science, 52(10), 1557-1576.

<부록> 설문 문항

변수	측정항목	
조직 몰입	oc1	정보보안의 문제 및 위협에 대한 충분한 이해와 지식을 가지고 있다.
	oc2	정보보안 및 잠재적인 보안위험의 기업의 자세에 대해 완전히 이해하고 있다.
	oc3	기업의 정보보안을 위해 규정한 보안 정책 및 규칙에 대해 알고 있다.
보안위험 경험	esr1	기업의 보안위험관리의 중요성에 대해 자주 들었다.
	esr2	산업 내 기업의 보안위험에 대한 경고를 알고 있다.
	esr3	보안문제로 인해 기업이 어려움에 처할 수 있다는 것을 직간접적으로 경험해 본적이 있다.
인지된 혜택	pb1	정보보안관리는 기업의 데이터 관리 오류를 줄여준다.
	pb2	정보보안관리는 기업 이미지 개선에 도움 된다.
	pb3	정보보안관리는 기업의 불필요한 비용을 전반적으로 감소시킨다.
파트너 의존성	pi1	파트너/거래 기업과의 지속적인 경영관계 유지는 사업목표 달성을 위해 중요하다.
	pi2	기업 전체 수익의 상당 부분은 파트너/거래 기업과의 거래에 의한 수익이다.
	pi3	파트너/거래 기업들은 그들의 사업 목표를 성취하기 위해 우리기업의 공급/서비스에 많이 의존한다.
IT 불안정성	itv1	우리 기업이 필요한 IT 기술은 빠르게 변하고 있다.
	itv2	우리 기업의 새로운 IT 기술 도입 주기가 점점 더 짧아진다.
	itv3	경영상 요구되는 IT 기술이 자주 바뀐다.
	itv4	우리 기업의 새로운 IT 기술 사용이 자주 바뀐다.
	itv5	경쟁기업의 새로운 IT 기술 도입 주기가 더 짧아진다.
	itv6	파트너 기업의 IT 기술은 빠르게 변하고 있다.
보안관리 강화의지	d1	우리 기업은 정보시스템 사용자들에 대한 접근 관리 및 감시 시스템을 개발할 것이다.
	d2	우리 기업은 정보시스템 사용자의 보안위험관리에 대한 의무를 강화할 것이다.
	d3	우리 기업은 정보보안에 대한 인적/기술적 투자를 높일 것이다.
	d4	우리 기업은 정보보안정책 및 규율을 엄격히 할 것이다.
	d5	우리 기업은 정보보안위험에 대한 직원교육을 강화할 것이다.
보안관리 실행	i1	우리 기업은 보안위험관리를 수행하고 있다.
	i2	우리 기업의 보안위험 관련 시스템 및 모니터링이 잘 실행되고 있다.
	i3	조직원들이 보안위험관리 의무 및 규율을 잘 지키고 있다.
	i4	기업의 보안위험관리에 대한 투자가 예전에 비해 높아졌다.

Abstract

An Empirical Study on Influential Factors of the Development and Implementation in Firm Security Management

Hwang, Jong-Ho*

This study investigates proper solution available for flexibly management pointing out reality a lack of understanding and interest for executing security management while importance of firm security management gets bigger. Accordingly, this study suggests 4 exogenous variables such as organizational commitment, experience of security risks, perceived benefits, partner interdependence as factors of having influence upon development and implementation in security management. It suggests IT volatility as moderating variable, which will intensify between development and implementation. The research model was tested by using Structural Equation Modeling, via Amos 19.0 analysis on a sample collected from 209 firms. As a result, the remaining variables except partner interdependence showed statistically positive influence. The implications of the findings suggest a new theoretical framework of the security management and offers important solutions for the practical application guidelines.

Key Words: Security Management, Cognitive Appraisals, Development, Implementation, IT volatility

* Professor, Dept.of Management Information System, Tongmyong University, Busan, Korea