조직 내 비고의적 보안위반 인식에 영향을 미치는 자발적 및 비자발적 동기요인과 규제권자 압력의 조절효과에 관한 실증연구

김상현
경북대학교 경영학부 부교수
(ksh@knu.ac.kr)
김근아(교신저자)
경북대학교 경영학부 박사과정
(applenana@knu.ac.kr)

오늘날 기업의 보안 실패는 피해를 입은 기업에게 막대한 비용과, 신뢰와 명성에도 심각한 손상을 주고 심지어 파산에 이르는 등 부정적 결과의 초래로 기업경영에 큰 걸림돌이 되고 있다. 따라서 기업의 정보보안 목적은 불확실한 사건들로부터 보안 사고에 대한 예방을 최소화함으로써 조직 내부의 피해를 저감하는 것이라고 할 수 있다. 최근 이러한 보안과 관련된 공격 및 침해, 위반에 대한 잠재적인 위험 요소에 대한 관심이 확대되면서 기업의 이에 대한 투자가 증가하고 성공적인 보안설계를 위한 적용범위가 구체화되고 있다. 특히 정보보안 오·남용의 위반 행위 및 사고 발생의 원인은 조직의 정보보안에 대한 기본적 통제항목이 없기 때문으로 파악되고 있다. 또한 발견된 위반사고의 상당부분(절반 이상)이 비고의적 사고에 의한 결과로 나타나고 있다. 다시 말하면, 조직 보안문제의 모든 사례는 외부의 파괴적 공격과 일반적인 침해의 결과라기보다 비고의적 오용 및 인적 실수 등 종업원의 소홀한 감시와 조직 내 절차의 부재가 그 원인이 되고 있다. 따라서 조직 내 보안의 비고의적 위반에 대한 적절한 프로세스와 일련의 통제 장치의 실행이 필요하다. 이에 본 연구는 '조직은 무엇에 의해 비고의적 보안위반 통제를 위한 노력을 할 수 있는가?'의 주요 연구 질의에 대한 동기와 해답을 실증적 증명을 통해 찾고자 한다. 이와 같은 연구목적 달성을 위해 비고의적 보안위반의 인식제고를 위해 조직의 내재적 요소로 자발적 동기요인(조직의무, 보안위반경험, 업무이점)과 비자발적 동기요인(조직규범, 처벌강도, 보안위협)을 제안하고, 비고의적 보안위반에 대한 행동의 수정 및 억제 그리고 이로 인한 성과에 이르기까지 조직(기업)의 관점에서 어떤 영향을 미치는지에 대해 이론적으로 타당성을 평가하였다. 또한 규제권자 압력이 보안위반 인식 및 통제와 성과들 간의 관계에서의 어떤 역할을 하는지를 실증적 검정을 통해 본 연구의 차별화를 확보하였다. 제안된 연구모형의 구조방정식 분석결과, 자발적 동기의 조직의무, 보안위반경험, 업무이점, 비자발적 동기의 조직규범, 처벌강도는 보안위반인식에 긍정적인 영향을 미치는 것으로 나타났다. 하지만 보안위협은 보안위반인식에 긍정적인 영향을 미치지 않는다는 사실이 확인되었다. 뿐만 아니라 강압적/강제적 속성의 변수인 규제권자 압력의 조절효과 역시 기업의 보안 관리에 있어 중요한 영향을 미치는 것으로 나타났다. 이러한 연구결과는 이전 보안위반의 정성적 및 정량적 연구들에서 찾아 볼 수 없었던 내·외적 주요 변수들을 포함하고 있다. 이는 곧 보안사고의 실수적 측면의 손실을 최소화하기 위한 조사를 통해 보안위반에 대한 모니터링 및 진단과 사전 예방적 대응의 근거 마련 등 조직 및 사용자 행동의 관점에서 이론적, 실무적으로 중요한 시사점을 제시할 수 있다.

주제어: 비고의적 보안위반, 자발적/비자발적 동기요인, 규제권자 압력, 보안성과

논문접수일: 2012. 9 게재확정일: 2012. 12

Ⅰ. 서 론

오늘날 많은 기업들에게 정보보안의 위험은 지식정보사회로 점차 고도화하는 과정 속에서 큰 장애요소로 인식되고 있다(Baker and Wallance, 2007). 일반적으로 정보기술의 발달과 더불어 이로 인한 정보의 누수와 정보 침해에서 정보보안의 위험 원인을 찾고 있다. 즉, 정보로 인한 많은 혜택을 누리는 반면 등장한 다양한 역기능 및 위험(예, 사이버 테러, 개인정보 및 중요자산의 유출 등)에 노출되어 있다(Anderson and Agarwal, 2010; Ransbotham and Mitra, 2009). 이러한 기업의 보안 실패는 피해를 입은 기업에게 사회·경제적 손실뿐 아니라 조직의 존폐를 좌우하기도 한다(Johnston and Warkention, 2010; Hsu et al., 2012). 특히, 정보보안의 사고는 외부요인보다 내부요인에 따른 발생빈도가 높게 나타나고 이에 대한 내부위협이 조직에게 보다 치명적인 것으로 평가되고 있다(Bulgurcu et al., 2010). 또한, 보안사고 사례의 대부분이 종업원의 충성심 결핍, 도덕적 해이, 비고의적 오용 및 실수 등 종업원의 소홀한 감시와 구체적 지표 개발의 부재가 그 원인이 되고 있다(D'Arcy et al., 2009; Ifinedo, 2012; Workman et al., 2008). 따라서 기업은 그들 내부보안의 중요성에 대한 인식과 실천의 노력이 매우 절실하다.

더욱이 최근 들어 보안의 성공적 관리를 설명하기 위한 방법으로 최종 사용자(end-user)에 초점을 두고 있다(Guo et al., 2011). 최종 사용자는 보안체계가 아무리 잘 구축되어 있다 하더라도 누구나 실수를 할 잠재적, 우발적 가능성이 존재한다(Herath and Rao, 2009b). 비록 악의적인 결과는 아니지만 정보의 손실 및 관련 보안사고 차원에서는 매우 중요한 요인으로 평가되고 있다(Siponen and Vance, 2010). 문제의 원인이 작고 사소한 역할 또는 오류일지라도 큰 문제를 야기할 위험이 있기 때문에 이를 미연에 억제, 제어할 수 있는 비고의적 보안위반에 대한 인식 수준을 제고하기 위한 노력이 필요하다(Guo et al., 2011). 다시 말해, 직접적인 원인이 되는 요인들에 대한 철저한 사전 분석과 지속적인 모니터링, 그리고 보안인식의 수준 향상 등 다양한 수단과 도구를 적용한 적절한 예방책이 시행되어야만 한다(Straub and Welke, 1998; Lee and Larsen, 2009; Hsu, 2009).

하지만 기업 경쟁력의 하나로 보안 관리에 대한 상당한 투자가 이루어지고 있는 반면 종업원의 이들이 조직 보안성과를 얼마나 달성하였는지에 대한 효과의 측정, 구체적인 평가기준과 방법의 구축 및 실행은 미비하다(Boss et al., 2009). 기존의 단편적인 보안솔루션 도입이나 관련 정책 및 지침만으로는 내부의 실질적이고 성공적인 정보보안의 실현을 설명하기에는 역부족이다(Li et al., 2010). 구축된 조직 내 보안체계에 의지해야 하는 종업원은 형식적인 활동에 머무르고, 보안통제는 무너질 수밖에 없다(Spears and Barki, 2010). 현재 보안에 대한 종업원의 자발적 참여와 관심을 유도하고 있지만 이에 대한 경제적 가치의 인식 결여 등의 이유로 참여는 매우 저조한 것으로 나타나고 있다. 즉, 비고의적 보안위반의 관리를 통한 경제적·사회적으로 기업에게 미치는 가시적인 효과는 미미하다고 할 수 있다. 효과적으로 종업원의 무관심과 실수를 방지하기 위해서는 조직의 전반적인 보안에 대한 인식의 전환과 프로세스의 개선이 필요하다는 것을 의미한다(Stanton et al., 2005; Baker and Wallace, 2007; Rhee et al., 2009; Siponen and Vance, 2010; Liang and Xue, 2010; Nelms, 2011).

따라서 보안위반 인식에 대한 필요성이 부각되고 있는 현시점에서 전체적인 조직 보안의 유효성에 영향을 미칠 수 있는 종업원들의 행동에 대한 구체적인 이해가 요구된다. 또한, 조직의 비고의적 보안위반에 대한 그 역할과 책임, 해결이 필수적이라는 사실을 강조하고 보안 관리에 대한 변화를 반영하는 절차 및 주체를 정의할 필요성이 있다. 이에 본 연구는 비고의적 보안위반 통제에 영향을 미칠 수 있는 자발적(조직의무, 보안위반경험, 업무이점) 및 비자발적(조직규범, 처벌강도, 보안위협) 동기요인을 제시하였다. 종업원의 보안에 대한 인식을 위해서는 최종 사용자의 내·외적의 요소에 대한 설명이 동시에 필요하다. 본 연구는 외부의 강제적 영향으로 인한 행동의 경각심을 일깨우기 위해 규제권자 압력을 조절변수로 제안하였다. 이는 곧 비고의적 보안위반 인식 및 통제 그리고 나아가 이로 인한 기업의 경제적 이득에 까지 영향을 미칠 수 있다.

본 연구는 비고의적 보안위반에 실질적으로 미치는 영향을 분석하고 이에 대한 파급효과를 측정함으로써 종업원의 부적절한 행동 범위를 최소화하고 보안의 위험에 대한 종업원의 바람직한 인식제고에 기반이 될 수 있다. 또한, 조직 보안의 이해와 솔루션의 조정도구로 조직의 현 보안상태의 점검 수행 및 현재 설정된 내부 프로세스를 평가하고, 기업의 생존과 장기적인 내적 가치 및 경쟁력 증대에 중요한 의미가 될 수 있다.

II. 이론적 배경

2.1 비고의적 보안위반의 개념

조직의 보안은 정보자산을 보호하기 위한 제반 제도 및 도구에 의해 실현되며, 활동의 주체와 중심에는 사람이 존재한다(Anderson and Agarwal, 2010; Johnston and Warkention, 2010). 최근 많은 발견된 보안사고의 원인 소재들이 종업원(최종 사용자)의 행동에 편중되어 나타나고 있다(Bulgurcu et al., 2010; Zhang et al., 2009; Stanton et al., 2005). 특히, 종업원 그들의 무심한 실수로부터 비고의적 사고에 치중되어 나타나고 있다(Siponen and Vance, 2010). 즉, 조직이 경계할 수 있는 적절한 규제 항목 및 인식의 부족으로 인해 보안의 규칙과 정책의 위반으로 이어지고 있는 것이다(Guo et al., 2011; Herath and Rao, 2009a). 뿐만 아니라 크고 치명적인 실수는 기술적인 수정에 과도하게 의존하는 대신 실제 사용에 무심하기 때문인 것으로 파악되고 있다(Nelms, 2011).

보안 문제는 종업원의 일련의 행위, 즉 의도적, 악의적 혹은 무심한 행동으로 조직에게 손상을 입히고 기업의 존립이나 명예, 영리 등 전반에 영향을 미친다(Guo et al., 2011). 하지만 보안을 직접 행하는 대상이 어떠한 이유로 악의적인 목적과 관점 없이 손상을 일으키는가에 대한 이해의 전제는 매우 미비하다. 물론 정보의 개인적 이득을 목적으로 한 의도적인 유출이나, 위변조, 훼손, 파괴 및 지체에 대한 견제 장치 및 조치는 어느 정도 구현되고 있지만 종업원의 무의식 혹은 실수 등의 위반사례에 대한 노력과 설득이 필요하다(Guo et al., 2011; Herath and Rao, 2009b). 이는 종업원의 비즈니스 운영과 보안을 일부러 해치려는 것은 아니지만 시간과 노력을 절약하는 등 자신을 돕기 위한 행동으로부터 특정 규칙과 정책을 불가피하게 어기게 되는 일체의 사건들을 포함한다(Nelms, 2011). 또한, 보안위반 및 비윤리적 사용 혹은 오용 등 바람직하지 않은 보안관련 동작들이 해당될 수 있다(Myyry et al.,

2009). 많은 조직들은 종업원들이 자발적으로 할 수 있는 일련의 보안위반에 대한 구조의 합리적 조정이 크게 개선되지 않고 있다. 비고의적 보안위반은 보안정책의 위반보다 노출 정도나 범위에 대해 한정적이다(Herath and Rao, 2009b). 즉, 비고의적 보안위반을 방지하기 위해 보안 정책을 구현하는 이유이다. 비고의적 보안위반의 행위는 불법이나 악의적 결과라기보다 종업원의 의식 부족에서 상당한 문제점들을 발견할 수 있다(Guo et al., 2011). 따라서 최종 사용자의 잠재적 위험요소로부터 발생되는 비고의적 보안위반에 대한 의식적인 결정을 만들 수 있는 논의가 필요하다.

2.2 보안행동 문헌연구

정보보안과 관련된 연구동향은 기술적 · 물리적 보안 설계 및 구축(Lee and Larsen, 2009), 정보시스템 보안을 위한 투자의 효과 및 투자 결정(Gupta and Hammond, 2005), 정보보안지표 개발 및 계량화 연구(Baker and Wallace, 2007; Ransbotham and Mitra, 2009; Hsu, 2009), 정보보안정책의 역할 및 성숙도(Bulgurcu et al., 2010; Boss et al., 2009), 정보보안 및 위험 관리(Hsu et al., 2012; Spears and Barki, 2010) 등 다양한 연구가 시도되고 기업의 전사적 차원에서 정보보안 전략 수립을 위한 가이드라인 역할을 해왔다. 하지만 방대한 연구결과에도 불구하고 최종 사용자 행동에서의 정보보안 수립 및 검토는 여전히 부족하다. 즉, 인적 요소, 관리적 측면에서의 조직 보안에 대한 노력과 지침의 부재로 인해 조직 내 잠재적인 위험에 대한 안정된 해결책이 제시되지 못하고 있는 실정이다.

최종 사용자의 보안과 관련된 행동에 대한 선행연구는 종업원의 부적절한 컴퓨팅 사용을 억제하기 위한 대책의 효과를 조사하기 위해 적용되어 왔다. 예를 들면, 억제이론(deterrence theory)에서는 종업원의 보안에 대한 영향 모델을 제안하기 위해 조직의 보안위험에 대한 억제 조치는 조직의 잠재적인 범죄 행동의 컴퓨터 남용을 줄일 수 있다고 주장한다(Straub, 1990). 이는 곧 위반에 대한 벌칙의 확실성(deterrent certainty)과 심각성(deterrent severity)을 제안하였다. 아울러 최근 몇몇 연구에서는 억제이론을 확장한 개념을 적용하여 사용자의 컴퓨팅 오용의도를 조사하기 위해 제안되고 있다(Lee et al., 2004; D'Arcy et al., 2009). 이들 연구에서는 범죄의 원인을 처벌의 강 · 약 정도에 의지하고, 사회통제의 처벌에 주목하여 범죄가 설명될 수 있다는 견해를 일관되게 주장하고 있다(D'Arcy et al., 2009).

또한, 일부 연구에서는 윤리적 관점에서 사용자의 보안 행동을 연구하였다(Banerjee et al., 1998). 비공식적인 규범과 최종 사용자의 윤리적 행동의 내용을 제시한다(Harrington, 1996). 윤리는 보안과 관련된 아무런 공식적인 규칙이나 정책, 혹은 장소에 무관하게 어떤 상황에 대해 합리적 결정을 하는데 도움이 될 수 있다(Leonard and Cronan, 2001; Myyry et al., 2009; Dhillon and Backhouse, 2000). 하지만 몇몇 다른 연구자에 의해 이러한 사용자의 주관적 판단 및 개입에 의존하는 것은 위험인자를 최소화하기에는 많은 제약이 뒤따를 수 있다는 주장에 제기되고, 이에 대한 논리적 합의의 결과로 보안정책에 대한 사용자 준수에 초점을 두고 있다(Siponen and Vance, 2010; Bulgurcu et al., 2010). 보안정책 준수 모델에서는 사용자 태도에 미치는 영향에 대해 연구하였다. 조직의 보안정책의 필요성과 이에 대한 위반을 조정하기 위해 그들의 생산적 행동 및 일반적인 정책에

집중하고 있다(Ng et al., 2009; Herath and Rao, 2009a; Ifinedo, 2012).

하지만 이들 연구만으로는 종업원들의 조직 보안의 중요성을 일깨우기에는 많은 제한과 격차가 존재할 수 있다는 의견이 제기되었다(Workman et al., 2008). 즉, 보안 행동의 유형은 매우 다르게 나타날 수 있고 규칙이나 정책은 단순한 상식선에서 해석되고 최종 사용자는 자신들의 목적과 변명에 대해 거래할 수 있다(Ransbotham and Mitra, 2009; Boss et al., 2009). 이미 사고의 발생 후 그들 내부에 부여하는 징계 조치에 의해서는 그들의 행동을 제어하고 올바른 행동의 설득력을 얻기에는 충분하지 않다(Herath and Rao, 2009b). 따라서 근본적인 의식의 전환을 가져오기 위해서는 종업원의 위반 행동에 대해 적절한 보안 조치와 방해요소들을 제거하기 위한 처방이 필요하다(Guo et al., 2011). 특히, 최종 사용자가 자신들의 일탈 행위에 대해 예측할 수 없는 부분을 설명하는 것은 보다 효과적이고 좋은 예방책이 될 수 있다(Anderson and Agarwal, 2010; Johnston and Warkention, 2010; Liang and Xue, 2010).

Guo et al.(2011)은 최종 사용자의 작업환경에서의 비고의적 보안위반의 복합적인 행동 모델을 제안하였다. 즉, 비고의적 보안위반을 관리하고 정보보안의 실질적인 강화를 위해서는 기대되는 내적 산출물과 종업원들의 태도를 동시에 살펴볼 필요가 있다고 주장하였다. 또한, 잠재된 정보보안의 위험통제와 단계적으로 관리할 수 있는 기업 경영상의 현실적 설계를 통해 직원들의 보안 인식과 능력을 고취시키고, 비고의적 실수로부터 발생되는 보안 사고에 대한 예측과 차단이 가능하다고 보고하였다. Spionen and Vance(2010)은 정보보안 정책 위반은 범죄적 심리의 중화를 통해 사용자의 스스로 합리화가 가능하다고 주장하였다. 즉, 모든 범죄는 그들 자신의 그릇된 행위의 합리화에 의해 발생할 가능성이 있다는 중화이론(neutralization theory)에 바탕을 두었다. 사용자는 각종 이유들을 열거함으로써 자신의 범죄 행위를 중화시키고, 범죄를 억제하는 도덕 및 양심 등의 기제들을 무력화시킨다고 하였다. 종업원들은 자신이 기업에게 받을 마땅한 자격에 대해 피해의식을 느낄 수 있고, 이러한 불만을 보상받기 위해 반사회적 행동을 정당화시키는 방법으로 중화를 선택한다고 하였다. 따라서 종업원에게 그들 조직 내 존재하는 규범과 책임의 중요성을 호소할 필요성이 있다고 주장하였다. Herath and Rao(2009b)는 정보보안정책의 효과적 실행을 위해 보안위반 수준의 정도를 고려하였다. 보안의 피해로 인한 많은 유사한 상황들을 보다 정확히 진단하기 위해서는 보안위반 차이를 분석할 필요성을 제안하고 이들로부터 종업원에게 과제를 부여하고 해결안을 찾기 위해 보안정책의 실천이 이루어질 수 있다고 주장하였다. 즉, 조직의 업무가 고도화 될수록 비례하여 증가하는 보안 위해 요소에 대응하기 위해서는 종업원의 위반에 대한 내부구조를 우선 파악하고, 사전적 안전망을 구성하여 이중적인 보안체계를 구축할 수 있다고 하였다.

이와 같은 이론적 모델들은 종업원의 위반 행동을 설명하는데 일부 성공적이긴 했지만 반면 최종 사용자의 보안위반 이유에 대한 잠재요인을 관찰하고 측정하기에는 다소 제한적이라고 할 수 있다. 또한, 일련의 정책을 실행하기 위한 중간 단계로의 설명 밖에 지나지 않기 때문에 보안위반에 대한 기존 연구의 시각은 한정되어 있다. 이는 곧 사용자의 보안을 유지하고 위협을 다루는 관점에 있어 그들의 책임이나 과제로 인식되고 있지 않기 때문이다. 더욱이 본 연구에서 제안하는 비고의적 보안위반에 대한 접근

은 충분한 이론적 설명을 제공하고 있지 않다. 즉, 최종 사용자들의 비고의적 보안위반에 대한 동기요인의 이해는 여전히 제한적이다. 따라서 이러한 이전연구의 격차를 보완하기 위해 본 연구는 최종 사용자의 실수와 비고의적 측면의 주제에 대해 실증적 검정을 하고자 한다. 왜냐하면 아무리 좋은 보안 솔루션을 도입하더라도 그것을 실행하는 최종 사용자의 수정 및 배치가 적절하게 이루어지지 않는다면 최종적인 보안의 이익은 기대하기 어렵기 때문이다.

Ⅲ. 연구모형 및 가설

3.1 연구모형

비고의적 보안위반에 대한 통제는 개인 또는 기타 최종 의사결정 단위에게 정보의 채택과 실행을 효과적으로 돕고 보안 관리에 대한 노력을 계속적으로 실천하는 과정이다. 하지만 이전 연구들은 비고의적 보안위반의 단계와 영향을 미치는 요인들을 구체적으로 구별 및 분석하지 않았다. 즉, 어떤 과정에 의해 보안위반이 통제되는지에 대한 전제들을 찾아볼 수 없었다. 따라서 본 연구는 비고의적 보안위반의 본질적 이해와 보안위반의 인식 전·후에 어떤 요인에 의해 긍정 혹은 강화되는지에 대해 살펴보고자 한다. 이는 조직의 비고의적 보안위반을 관리하기 위한 동기를 찾고, 주요 연구 질의인 '조직은 무엇에 의해 비고의적 보안위반 통제를 위한 노력을 할 수 있는가?'에 대한 해답을 제공하는데 도움이 될 수 있다.

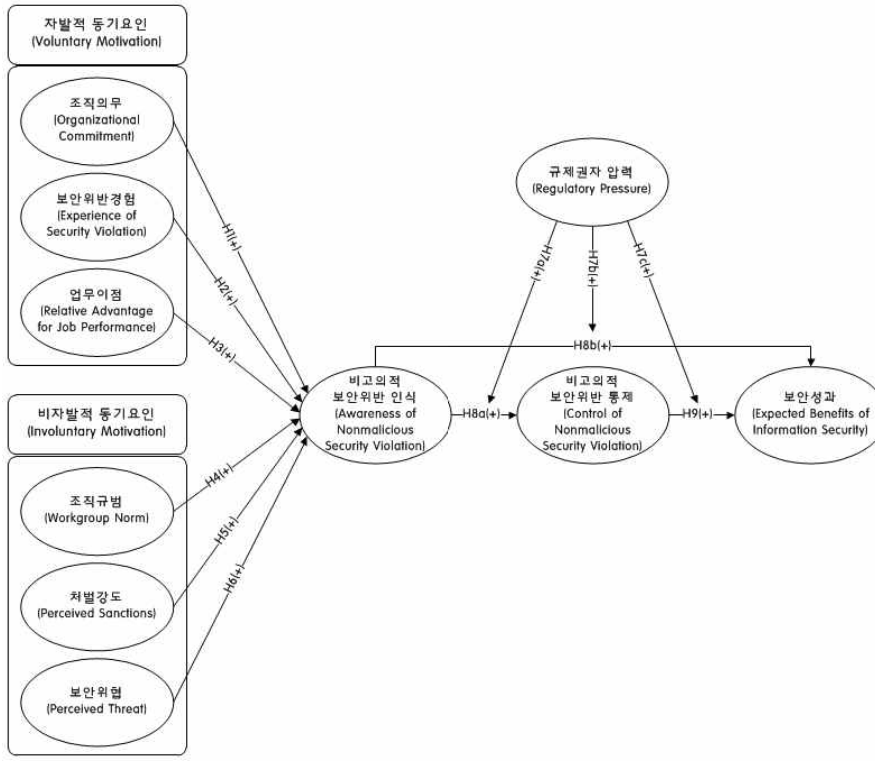
이와 같은 목적을 달성하기 위해 본 연구는 보안관리에 중요한 역할을 하는 자발 및 비자발적(내·외재적) 동기 이론을 제시하여 비고의적 보안위반 통제에 대한 잠재적 동기와 추진 효력을 결정할 수 있는 변수들(조직의무, 보안위반경험, 업무이점, 조직규범, 처벌강도, 보안위협, 총 6 외생변수)을 살펴보고자 한다. 또한, 조직은 내부 요인에 의해 보안통제의 압력을 요구 받을 수 있지만 만약 조직 외부의 정책 및 사회적 제도가 뒷받침되지 않는다면 그 의미가 없어진다. 이에 본 연구는 규제권자 압력의 조절효과를 살펴봄으로써 보안위반 통제의 효과적인 과정(인식, 통제, 성과)에 대한 통찰력을 제공하고자 한다. 본 연구에서 제안한 연구모형과 가설은 〈그림 1〉에서 보여주고 있다.

3.2 가설설정

3.2.1 자발적 동기

본 연구는 조직의 새로운 패러다임에 대한 종업원의 긍정적인 내적 상태를 의미하는 자발적 동기요인으로 조직의무, 보안위반경험, 업무이점을 제안한다. 이는 곧 조직의 장기적이고 지속적인 힘을 유지할 수 있다(Herath and Rao, 2009a).

현대의 조직은 종업원의 업무성과 제고방안과 조직에 대한 협력적 결과에 주목한다. 그들 경영환경에 종업원들이 가지는 조직에 대한 의무감 및 충성심은 조직에 우호적이거나 바람직한 영향을 미친다고 제시하고 있다(Mowday, 1998). 개개인이 가질 수 있는 조직의무에 대한 개념을 일치된 합의로 정의하기는 어렵지만, 이전의 연구에서는 조직의무에 대해 조직에 헌신하려는 태도 및 경향의 정도라고 정의하고 있다(Stanton et al., 2003) 즉, 한 조직의 목표 및 내적 가치에 수반하는 역할과 자신들의 에너지를 투자하고 노력하려는 의사의 상대적 강도를 의미한다(Basu et al., 2002). 일반적으로 종



〈그림 1〉 연구모형 및 가설설정

업원의 조직에 대한 소신 있는 행동은 조직의 손실을 고려하고 경제적인 측정이 가능하다고 주장하고 있다(Herath and Rao, 2009b). 이는 곧 조직의무가 높은 종업원은 나아가 사회적으로 책임감 있는 존재로 생산적인 활동과 조직에 적당하고 합리적인 실천을 예측할 수 있다(Newman and Sabherwal, 1996; Lee et al., 2004).

합리적인 도구 사용의 행위와 예측을 설명하기 위한 가장 좋은 변수로 최종 사용자의 경험은 행동 발생 전·후의 인과관계를 효과적으로 이해하는데 도움을 준다(Li et al., 2010). 경험에 대한 보편적 관점은 기술이나 사건에 노출되어 얻는 현실적 관찰이나 지식을 의미한다(Rhee et al., 2009). 종업원은 보안위반의 경험으로부터 현재 상태를 진단하고 언제, 어디서, 어떤 모습으로 발생할지 알 수 없는 행동에 대해 시행착오의 접근으로 예방이 가능하다(Potosky, 2002). 이는 곧 이전의 영향으로부터 실제의 부조화와 심리적 불편을 감소시키고, 종업원이 만약 자신의 경험을 유효하게 받아들인다면 그에 따라 태도와 인식에도 영향을 미칠 수 있다(Marakas et al., 1998). 즉, 종업원의 비고의적, 실수 및 무지에 의한 행동에 대해 사전경험으로부터 자율적 예방과 경감 활동을 촉진하고 조율하기 위한 처방이 될 수 있다(Compeau and Higgins, 1995).

마지막으로 비고의적 보안위반의 인식을 위한 자발적 동기의 주요변수로 업무이점을 제시한다. 조직

이 그들의 내부에 새로운 솔루션을 제시하기 위해서는 이에 대한 직·간접적 이득에 대한 인식의 전환이 이루어져야만 성공적인 적용과 도입이 가능하다(Guo et al., 2011). 특히, 종업원은 그들의 업무에 도움이 되고 개선을 가져올 수 있는 방향을 고려할 필요성을 가진다(Ng et al., 2009). 조직 내 새로운 프로세스의 개입이 성공적으로 구현되기 위해서는 종업원의 직무 내용과 업무환경의 변화를 초래할 수 있는 효과적이고 견고한 설계가 필요하다(Besnard and Arief, 2004). 왜냐하면 종업원들은 그들의 행동의 전개로부터 어떤 경제적 인센티브와 혜택이 있는가를 주요하게 평가하기 때문이다(Hsu et al., 2012). 즉, 새로운 해결책에 대한 상당부분의 조직 내 문제들이 그들의 업무와 목표와 일치되지 않기 때문인 것으로 지적되고 있다(Post and Kagan, 2007). 따라서 보안위반에 대한 특정 행동을 수정하고 갈등을 발견하기 위해서는 예상될 수 있는 업무이점의 잠재력 확보에 대한 설득이 중요한 논리가 될 수 있다. 따라서 이와 같은 논의를 바탕으로 본 연구의 비고의적 보안위반의 자발적 동기요인 세 변수와 비고의적 보안위반 인식간의 관계를 실증적으로 검정하기 위해 다음과 같은 가설을 설정하였다.

가설 1: 조직의무는 비고의적 보안위반 인식에 정(+)의 영향을 미칠 것이다.
가설 2: 보안위반경험은 비고의적 보안위반 인식에 정(+)의 영향을 미칠 것이다.
가설 3: 업무이점은 비고의적 보안위반 인식에 정(+)의 영향을 미칠 것이다.

3.2.2 비자발적 동기

자발적 동기와 더불어 조직 내 문화 및 분위기와 같은 비자발적 동기의 방향이 동일하게 존재할 때 조직은 이상적인 프로세스의 개선을 추구할 수 있다(Herath and Rao, 2009a). 이에 본 연구는 비자발적 동기요인으로 조직규범, 처벌강도, 보안위협, 세 가지의 요소를 제안한다.

일반적으로 조직 활동은 규범을 주요 통제수단으로 구분한다(Knapp and Marshall, 2006). 특히, 종업원은 그들의 내적 가치 형성과 의사결정은 조직 내부의 규범에 의존하고, 동료 및 상사들의 영향에 의해 바람직한 경영모델을 실현시킨다(Guo et al., 2011). 즉, 조직규범은 기존의 프로세스를 수정하고 새로운 결정에 대해 정당성과 동조를 유도할 수 있다(Herath and Rao, 2009). 또한, 수단이나 행동의 결과가 사회적으로나 개인적으로 적합한 상태인지를 가늠하기 위해 종업원은 그들 그룹의 관계적 상호작용에 의해 조직을 관찰하고 이해한다. 이는 곧 조직은 본질적으로 계층을 이루고 있고, 종업원은 그들의 특정 신념이나 태도 및 행동을 위한 역할 모델로써 다른 멤버를 참고하려는 경향이 있다(Hsu et al., 2012). 따라서 종업원은 현재의 문제와 현상에 대해 규범적 결과로부터 보다 발전된 행동을 조직에 적합하게 표준화시킬 수 있다(Karahanna et al., 1999).

많은 보안 사건으로부터 행동을 일률적으로 관리하기 위한 조직 내 적절한 장치의 필요성이 증가하고 있다(Straub et al., 2004). 대부분 보안에 대한 정책적 처벌이 제 역할을 하지 못하기 때문에 종업원의 태만과 불성실이 불가피한 것이라는 주장에 제기되었다(Guo et al., 2011). 한편 억제이론에서는 처벌의 조절을 통해 최종 사용자의 불법행동의 수준을 감소시키고, 처벌의 위협으로부터 불필요한 행동이 통제될 수 있다고 주장한다(Straub and Collins, 1990). 이는 인간은 합리적이고, 경제적

선택, 즉 이득과 비용을 계산한 행동을 하고, 따라서 위험한 요소로 분류되는 행동이 적발되었을 때 생기는 신체적·재산적 피해의 잠재적 비용에 초점을 두기 때문에 이에 대한 비용을 최소화시키려는 반면 이익과 효용은 극대화하기 위해 노력한다는 것이다(Straub, 1990; Bulgurcu et al., 2010; Siponen and Vance, 2010). 즉, 종업원은 경제적 요인들을 그들에게 연결시키고 예상되는 평가와 이득에 주목하기 때문에 처벌이 가해진다면 문제의 행동에 긍정적인 답변을 기대할 수 있다(D'Arcy et al., 2009).

다음으로 본 연구에서 제안하는 비자발적 동기요인의 마지막 변수는 보안위협이다. 보안 관리에 대한 중대한 오해 중 하나가 위협은 외부로부터 발생하고, 위협의 요인은 언제든 식별이 가능하기 때문에 조직의 계획 수립과 시스템 구축이 적절하게 배치된다면 안전 수준은 어느 정도 보장될 것이라는 것이다(Anderson and Agarwal, 2010). 하지만 많은 보안위협의 본질적 원인은 내부 종업원들의 무지, 실수, 부주의, 그리고 규칙의 미준수에 의한 것으로 판단되는 반면 이에 대한 심각한 위험을 인식하지 못하고 있다(Johnston and Warkention, 2010). 이와 같은 경우 잠재된 반복적 위험이 존재하고, 이는 곧 보안관리 발전을 저해하는 요인으로 평가된다(Li et al., 2010). 따라서 종업원은 조직에 드러날 수 있는 실체적 위협으로부터 심각성과 현재의 흐름을 인식할 필요성이 있다. 왜냐하면 위협은 조직의 자산에 해를 줄 수 있는 위험의 원천이기 때문이다(Liang and Xue, 2009). 즉, 위협에 대한 구체적 구분과 발생의 빈도 및 손실의 크기에 대한 측정이 중요하다고 할 수 있다(Guo et al., 2011). 따라서 이와 같은 논의를 바탕으로 본 연구의 비고의적 보안위반의 비자발적 동기요인 세 변수와 비고의적 보안위반 인식간의 관계를 실증적으로 검정하기 위해 다음과 같은 가설을 설정하였다.

가설 4: 조직규범은 비고의적 보안위반 인식에 정(+)의 영향을 미칠 것이다.
가설 5: 처벌강도는 비고의적 보안위반 인식에 정(+)의 영향을 미칠 것이다.
가설 6: 보안위협은 비고의적 보안위반 인식에 정(+)의 영향을 미칠 것이다.

3.2.3 규제권자 압력의 조절효과

기업들은 보안과 관련된 지속적으로 증가하는 국가 및 산업의 요구사항을 준수할 필요성이 있다. 실제로 조직은 그들의 목표와 유효성이 불확실한 환경 아래에서 사회적 가치체계나 규칙 등과 일치되도록 조직의 형태 및 구조를 변경하도록 압력을 받는다(Teo et al., 2003; DiMaggio and Powell, 1983; Khalifa and Davison, 2006). 즉, 불확실한 환경 하에서 규제기관의 강제는 조직의 특정구조나 전략 채택을 도울 수 있다(Gosain, 2004). Appari and Johnson(2009)은 조직들의 규제자에 대한 의존이 결국 산업 내 권력을 강화시키고 조직의 내·외부 환경에서 발생되는 보안위험으로부터 회피할 수 있는 중요한 요인이라고 강조하였다. 또한, Hsu et al.(2012)은 정보보안관리의 실행을 위한 합리적 도구로써, 종업원의 구조적, 행동적 변화에 영향을 미치는 요인으로 제도적 압력을 제안하였다. 특히, 그들은 규제감독자의 영향은 핵심조직이 활동하고 있는 산업 내에서의 기대 혹은 그 조직이 의존하고 있는 다른 조직에 의한 외부적인 압력으로 정의하고, 이는 조직 보안 관리의 변화를 촉진하고 성공적으로 보안성과를 달성할 수 있다고 주장하였다.

이처럼 기존의 연구들에서는 조직이 속한 사회 즉, 다른 조직의 사회적, 문화적, 정치적 요인 등에 의해 부과되는 공식적·비공식적 압력이 종업원의 정보보안관리 실천에 긍정적인 영향을 미치는 것으로 나타났다. 이러한 압력은 외부의 힘이나 설득 등을 통해 작용되는데, 실제 사례에서도 조직의 현재 환경 변화는 정부의 정책, 사회적 제도 등의 변화에 의해 통제되는 경우가 상당 부분을 차지하고 있다(Scott, 1987; Liang et al., 2007; Hu et al., 2007). 따라서 이와 같은 논의를 바탕으로 본 연구의 비고의적 보안위반 인식, 통제, 성과 사이의 관계에서 규제권자 압력이 어떤 역할을 하는지에 대해 실증적으로 검정하고자 다음과 같은 가설을 설정하였다.

가설 7a: 규제권자 압력은 비고의적 보안위반 인식과 통제 사이의 관계를 더 강화시켜 줄 것이다.

가설 7b: 규제권자 압력은 비고의적 보안위반 인식과 성과 사이의 관계를 더 강화시켜 줄 것이다.

가설 7c: 규제권자 압력은 비고의적 보안위반 통제와 성과 사이의 관계를 더 강화시켜 줄 것이다.

3.2.4 비고의적 보안위반 통제

최종 사용자는 그들이 어떻게 무엇을 해야 하는지에 대한 실제적 행동을 위해 인지적 능력에 의지한다(Spears and Barki, 2010). 부정적이든 긍정적이든 상황에 대한 노력을 위해서는 현 시점의 정확한 이해와 평가 등의 인식 확립을 통해 역할에 집중할 수 있는 동기를 제공한다(Siponen and Vance, 2010). 더욱이 자신의 무지나 실수에 대한 종업원의 극복할 노력과 환경은 문제를 원천적으로 제거 및 차단하고, 환기와 주의를 각성하는 도구로 적절한 효과가 있다. 다시 말해, 비고의적 보안위반을 스스로 분석, 예방하고, 사고 시 이를 최소화하거나 방지하기 위한 과정은 실천적 의미로 종업원의 올바른 의식과 행동에 크게 좌우될 수 있다(Karyda et al., 2005). 결과적으로 종업원 개별의 통제노력에 의해 집합의 결과를 야기 시킬 수 있다(Kankanhalli et al., 2003). 따라서 종업원의 철저한 실천을 바탕으로 조직 전반의 관리수준이 제고될 수 있다(Gupta and Hammond, 2005). 뿐만 아니라 Hong et al.(2006)은 단계적 접근에 의해 보안의 효과적인 평가가 가능하다고 주장하였다. 이와 같은 논의를 바탕으로 본 연구의 비고의적 보안위반 인식, 통제, 성과 간의 관계를 실증적으로 검정하기 위해 다음과 같은 가설을 설정하였다.

가설 8a: 비고의적 보안위반 인식은 통제에 정(+)의 영향을 미칠 것이다.

가설 8b: 비고의적 보안위반 인식은 성과에 정(+)의 영향을 미칠 것이다.

가설 9: 비고의적 보안위반 통제는 성과에 정(+)의 영향을 미칠 것이다.

Ⅳ. 연구방법 및 실증분석

4.1 연구대상 및 측정방법

본 연구는 조직의 비고의적 보안위반에 대한 중요성에도 불구하고 국내에서는 보안위반 관리에 대한

실행과 확산이 산업 전반적으로 이루어지지 않고 있다는 점을 지적하고, 정보보안 보안위반 인식과 통제를 통해 보안성과에 미치는 요소들을 실증적으로 연구하고자 한다. 따라서 본 연구의 대상은 현재 정보시스템의 정보보안에 대해서 조직 차원의 활동 및 실행을 하고 있는 국내·외 기업을 대상으로 어떤 요소와 과정을 거쳐 보안성과가 높아지는지에 대해 조직단위의 행동에 대한 설명을 연구 범위로 설정하였다.

연구모형의 각 변수를 측정하기 위한 설문항목들은 (1)강한 부정 에서부터 (7)강한 긍정에 걸친 7점 리커트 (7-point Likert scale)의 항목으로 측정하였다. 각 설문항목은 일차적으로 기존연구를 통해 개발하여, 본 연구의 목적에 적합하게 수정 및 보완을 하였다. 또한, 현재 정보시스템 보안활동을 실행 중인 국내 기업 종사자를 대상으로 면접을 통해 설문항목을 재정립 한 후, 경영정보분야 대학교수 및 대학원생들을 대상으로 내용타당성(content validity)을 검정하여 설문항목의 타당성을 높였다. 각 변수에 대한 조작적 정의와 관련연구는 〈표 1〉에서 보여주고 있다.

최종 개발된 설문지는 대한상공회의소에서 발행한 2011년도 매출액 기준 상위 1,000대 기업들 대상뿐 아니라 코스피와 코스닥에 등록 된 기업, 또한 한국외국인기업협회에 등록된 기업을 대상으로 무작위로 설문을 실시하였다. 총 3,000부의 설문지가 이메일, 전화, 직접방문 및 우편을 통한 다차원적인 방법을 사용하여 배포되어 이 중 총 319부(회수율 10.6%)를 회수하였다. 하지만 응답이 불성실한 11부를 제외한 308부를 최종 분석에 사용하였다. 응답자의 성별, 직위 등에 대한 응답자의 특성은 〈표 2〉에서 보여주고 있다. 다음으로 산업분류, 매출액

〈표 1〉 연구변수에 대한 조작적 정의 및 관련연구

연구변수	조작적 정의	관련연구
조직의무	조직 내 보안에 대한 책임 및 중요성을 인식하는 정도	Herath and Rao(2009b)
보안위반경험	보안위반으로 인한 문제 및 위험의 직·간접 경험의 정도	Rhee et al.(2009) Li et al.(2010)
업무이점	보안행동의 실천으로 얻을 수 있는 상대적인 업무의 이익 정도	Guo et al.(2011)
조직규범	조직 내 동료 및 상사의 보안관련 행동 및 인식의 정도	Guo et al.(2011)
처벌강도	조직 내 보안위반 시 가중되는 정책적 처벌에 대한 인식 정도	Siponen and Vance(2010)
보안위협	조직 내 보안 정책 및 규칙의 위반으로 발생되는 보안 위험에 대한 인식 정도	Liang and Xue(2010)
규제권자 압력	동종 산업 내 감독기구(정부기관 및 규제기관)의 보안관리 및 위반사항에 대한 압력 및 규제의 정도	Hsu et al.(2012)
비고의적 보안위반 인식	비고의적 보안위반의 부정적 영향 및 심각성을 인식하는 정도	D'Arcy et al.(2009)
비고의적 보안위반 통제	비고의적 보안위반 행동의 억제 및 수정의 정도	Zhang et al.(2009)
보안성과	조직이 비고의적 보안위반 통제를 통해 얻을 수 있는 재무적(영리추구)/비재무적(만족, 효율성) 성과의 정도	Kotulic and Clark(2004)

〈표 2〉 응답자의 특성

분류		빈도	응답비율(%)
성별	남자	243	78.9%
	여자	65	21.1%
연령	20-29세	29	9.4%
	30-39세	95	30.8%
	40-49세	101	32.8%
	50세 이상	83	26.9%
최종학력	고졸	31	10.1%
	대졸	142	46.1%
	대학원(재)	58	18.8%
	대학원졸	77	25.0%
응답자 직위	이사급 이상	97	31.5%
	부장/차장	109	35.4%
	과장/대리	89	28.9%
	사원	13	4.2%
합계		308	100%

등에 대한 조직특성은 〈표 3〉에 제시하였다.

응답에 참여한 조직의 산업분야를 살펴보면, 금융/보험(41.2%), 전자·전기/정보통신(25.6%), 물류/유통/서비스(20.1%) 순으로 많았다. 현재 실행되고 있는 보안위반 정책으로는 경영진 견책(60.4%)이 큰 비중을 차지하는 것으로 나타났다. 이는 곧 설문에 참여한 대부분의 기업들이 비고의적 실수에 대해 어느 정도의 패널티를 가하지만 심각한 수준은 아니라는 것을 알 수 있다. 또한, 보안 관리를 위한 활동으로는 바이러스 백신 및 방화벽 프로그램 설치(80.5%), 데이터 손실 방비 및 백업 시스템(59.1%), 보안침입 탐지 시스템(57.5%)의 순으로 나타났다.

4.2 측정모형의 적합도 검정

측정도구의 신뢰성과 타당성 검정에 앞서 수집된 데이터의 특성이 측정모형의 특성과 어느 정도 일치하는지를 검정하기 위해 AMOS 19.0을 사용하여 적합도 검정을 실시하였다. 초기측정모형의 적합도 검정은 연구모형에서 제시하는 10개의 잠재변수를 측정하기 위한 총 43개의 항목으로 실시하였다. 적합도 검정의 판단 기준은 기존의 사회과학 연구에서 일반적으로 가장 많이 사용하는 증분적합지수(IFI), 기초부합지수(GFI), 수정된 기초부합지수(AGFI), 비교부합지수(CFI), 상대적 카이스퀘어(X^2/df), 표준적합지수(RMSEA)를 사용하였다. 초기측정모형의 적합도를 검정한 결과 CFI와 RMSEA 지수가 기존연구에서 제시하는 권장치 이하로 나와 적합도에 문제가 있는 것으로 나타났다.

AMOS 19.0의 산출물 중 수정지수(modification indices)를 살펴본 결과 조직의무의 3번째 항목(oc3)과 처벌강도의 2번째 항목(ps2)이 적합도를

〈표 3〉 조직 특성

분류		빈도	응답비율(%)
산업분야	제조	38	12.3%
	물류/유통/서비스	62	20.1%
	금융/보험	127	41.2%
	전자 전기/정보통신	79	25.6%
	기타	2	0.6%
매출액	10억 미만	31	10.1%
	10억 - 50억 미만	12	3.9%
	50억 - 100억 미만	35	11.4%
	100억 - 500억 미만	71	23.1%
	500억 - 1,000억 미만	104	33.8%
	1,000억 이상	55	17.9%
보안위반 정책 (복수응답)	정해진 제재 없음	67	21.8%
	경영진 견책	186	60.4%
	직무 정지	59	19.2%
	직무 해임	34	11.0%
	법원 기소	29	9.4%
	기타	18	5.8%
보안활동 (복수응답)	바이러스 백신 및 방화벽프로그램 설치	248	80.5%
	보안침입 탐지 시스템	177	57.5%
	데이터 손실 방지 및 백업 시스템	182	59.1%
	암호화 및 디지털 서명 시스템	85	27.6%
	운영체제 및 DB 고급보안 SW 설치	79	25.6%
	보안 취약성 지속적 점검	34	11.0%
	보안 교육 및 훈련	29	9.4%
	보안위반에 대한 규제 강화	24	7.8%
합계		308	100%

저해하는 항목으로 나타났다. 이는 곧 이들 문항은 단일차원성에 대한 문제가 있음을 의미한다. 이 두 문항에 대한 수정지수 값은 25.49와 17.73으로 보수적인 수정지수 값인 10 이상으로 나타났으며, 이는 곧 연구모형에서 원래 측정하고자 하는 잠재변수 외에 다른 변수에도 높게 적재되는 교차 상관관계(cross-correlation)가 존재한다는 것을 의미한다. 따라서 기존연구에서 제안하는 방식으로oc3과 ps2를 제거한 후 적합도 검정을 다시 실시하였다. 재검정 결과 〈표 4〉에서 나타나듯이 적합도 검정에 사용된 모든 지수가 권장치 이상으로 나타나 수집된 데이터가 측정모형에 적합한 것으로 판단된다.

〈표 4〉 적합도 검정

모델	IFI	GFI	AGFI	CFI	X^2/df	RMSEA
초기측정모형	0.928	0.957	0.916	0.849	1.970	0.088
수정된 측정모형	0.957	0.968	0.948	0.921	1.824	0.041
권장치	≥0.9	≥0.9	≥0.8	≥0.9	≤3.0	≤0.05

4.3 측정모형의 신뢰성 및 타당성 검정

적합도 검정 후 구조모형 검정에 앞서 최종 수집된 데이터(n=308)로 측정도구의 신뢰성과 타당성 검정을 실시하였다. 신뢰성은 내적 일관성 검정의 한 방법으로 실증연구에서 일반적으로 가장 많이 사용하는 Cronbach's Alpha 계수(기준치 0.7 이상)를 사용하였다(Nunnally, 1967). 타당성은 집중타당성(convergent validity)과 판별타당성(discriminant validity) 검정으로 나눌 수 있는데 집중타당성은 AMOS 19.0을 사용한 확인적요인분석(Confirmatory Factor Analysis: CFA) 결과 중 요인값(factor loading), 합성신뢰도(composite reliability) 및 평균분산추출(Average Variance Extracted: AVE) 값을 사용하였다. 일반적으로 요인적재량은 ± 0.4 이상이면 유의한 것으로 판단되며(Barclay et al., 1995), 합성신뢰도 지수는 0.7 이상 그리고 각 잠재변수의 AVE 값이 0.5 이상이어야 집중타당성이 존재한다고 할 수 있다(Fornell and Lacker, 1981).

마지막으로 판별타당성 검정은 Fornell and Larcker(1981)가 제시한 평균분산추출(Average Variance Extracted: AVE)과 Pearson 상관관계분석 방법을 사용하였다. 판별타당성 존재 여부에 대한 검증은 각 잠재변수의 AVE의 제곱근(square root) 값이 해당 잠재변수와 다른 잠재변수간의 상관계수 값을 초과하여야 된다.

우선 신뢰성 검정 결과 Cronbach's Alpha 계수 값은 0.799에서 0.964로 나타나 권장치(0.7 이상) 이상으로 신뢰성은 확보된 것으로 판단된다. 요인값과 합성신뢰도, 그리고 AVE 값을 활용한 집중타당성 검정 결과 역시 모든 항목에서 기준값 이상으로 나타나 측정항목에 대한 집중타당성 문제는 없는 것으로 나타났다. 마지막으로 AVE 제곱근 값과 Pearson의 상관계수를 활용한 판별타당성 검정 결과 모든 잠재변수의 AVE 값의 제곱근이 종과 횡의 상관계수값 보다 높이 나타나 판별타당성 역시 문제가 없는 것으로 나타났다. 이와 같은 측정모형에 대한 검정 결과는 모든 설문문항의 내적 일관성과 타당성을 통계적으로 증명하고 있다. 〈표 5〉와 〈표 6〉은 측정모형에 대한 신뢰성과 타당성 검정 결과를 보여주고 있다.

4.4 구조모형 분석

측정모형에 대한 타당성 검정 후 수집된 데이터로 연구모형에서 제시한 변수들 간의 인과관계를 검정하기 위해 구조방정식(Structural Equation Modeling: SEM) 접근방법을 사용하였다. 구조모형분석을 통해 구조모형에 대한 적합도와 연구모형의 변수들 간의 영향 관계를 규명 할 뿐 아니라 내생변수에 대한 결정계수(R^2)에 대해서도 알 수 있다. 첫째, 구조모형의 적합도 검정 결과는 측정모형의 적합도 검정에서 사용한 지수들을 사용하였으며, 결

〈표 5〉 측정변수의 신뢰성 및 타당성 분석 결과

변수	항목	요인값	C.R	Cronbach's Alpha	합성신뢰도	AVE
조직의무 (OC)	oc1	0.778	-	0.865	0.841	0.638
	oc2	0.803	16.842			
	oc4	0.814	19.200			
보안위반경험 (ESV)	esv1	0.820	-	0.799	0.879	0.646
	esv2	0.768	14.783			
	esv3	0.835	13.258			
	esv4	0.790	17.410			
업무이점 (RJ)	rj1	0.816	-	0.816	0.893	0.677
	rj2	0.820	16.524			
	rj3	0.882	15.450			
	rj4	0.769	15.867			
조직규범 (WN)	wn1	0.748	-	0.889	0.892	0.674
	wn2	0.892	18.100			
	wn3	0.837	16.367			
	wn4	0.800	18.692			
처벌강도 (PS)	ps1	0.858	-	0.820	0.862	0.676
	ps3	0.763	14.127			
	ps4	0.842	15.230			
보안위협 (PT)	pt1	0.741	-	0.824	0.846	0.580
	pt2	0.766	15.227			
	pt3	0.720	13.269			
	pt4	0.816	16.220			
규제권자 압력 (RP)	pri1	0.914	-	0.914	0.929	0.765
	pri2	0.840	19.570			
	pri3	0.864	16.372			
	pri4	0.879	16.774			
비고의적 보안위반 인식 (ANMSV)	anmsv1	0.863	-	0.863	0.911	0.673
	anmsv2	0.857	16.743			
	anmsv3	0.790	15.800			
	anmsv4	0.869	15.721			
	anmsv5	0.710	13.842			
비고의적 보안위반 통제 (CNMSV)	cnmsv1	0.850	-	0.942	0.927	0.719
	cnmsv2	0.934	16.947			
	cnmsv3	0.891	18.673			
	cnmsv4	0.826	18.540			
	cnmsv5	0.723	15.887			
보안성과 (EBS)	ebs1	0.800	-	0.964	0.935	0.742
	ebs2	0.894	17.413			
	ebs3	0.838	19.635			
	ebs4	0.925	15.410			
	ebs5	0.845	17.543			

주) "-": 분석시 "1"로 고정함.

〈표 6〉 잠재변수의 판별타당성 분석결과

변수	1	2	3	4	5	6	7	8	9	10
1. 조직의무	**.798**									
2. 보안위반경험	.315	**.804**								
3. 업무이점	.210	.322	**.823**							
4. 조직규범	.300	.483	.241	**.821**						
5. 처벌강도	.254	.370	.300	.329	**.822**					
6. 보안위협	.216	.258	.210	.380	.517	**.762**				
7. 규제권자 압력	.224	.307	.275	.328	.393	.215	**.875**			
8. 비고의적 보안위반 인식	.197	.200	.348	.455	.360	.268	.317	**.820**		
9. 비고의적 보안위반 통제	.205	.314	.269	.203	.322	.369	.435	.255	**.848**	
10. 보안성과	.256	.253	.498	.276	.242	.227	.348	.296	.358	**.862**

주) 진하게 표시된 대각선 AVE의 제곱근 값임.

과는 IFI = 0.981, GFI = 0.954, AGFI = 0.920, CFI = 0.968, 상대적 카이스퀘어(X^2/df) =1.629, RMSEA=0.029로 나타나 연구가설의 검정에는 별무리가 없을 것으로 판단되었다.

두 번째 구조방정식 분석을 통해 얻을 수 있는 결과는 경로계수(β)이다. 이는 두 변수간의 인과관계의 정보를 나타낸다(Wixom and Watson, 2001). 분석 결과를 살펴보면, 첫째, 자발적 동기요인의 세 변수, 조직의무(β=0.325, t=4.572)와 보안위반경험(β=0.496, t=8.827)은 유의수준 0.01에서, 그리고 업무이점(β=0.257, t=3.895)은 유의수준 0.05에서 지지되었다. 따라서 가설 1, 가설 2, 가설 3은 채택되었다. 이러한 결과는 종업원의 보안에 대한 기본적, 일반적 실수를 일깨우기 위해서는 조직에 대한 그들의 태도와 주관적 평가결과가 중요한 역할을 한다는 것을 의미한다. 둘째, 비자발적 동기요인의 보안위협을 제외한 조직규범(β=0.364, t=4.925)과 처벌강도(β=0.470, t=6.970)는 유의수준 0.05와 0.01에서 지지되었다. 따라서 가설 4와 가설 5는 채택되었지만, 가설 6은 기각되었다. 이는 곧 보안이 가지는 위험성의 인식으로 인해서는 비고의적 보안위반에 대한 행동의 수정이 이루어지지 않는 반면, 비고의적 보안위반은 조직 내부의 일정수준의 정책적 노력과 상호작용의 결과로 인해 통제될 수 있다는 것을 의미한다. 셋째, 규제권자 압력의 조절효과에 대한 가설 7a(β=0.413, t=5.623), 가설 7b(β=0.398, t=6.840), 가설 7c(β=0.459, t=9.128)는 모두 유의수준 0.01에서 채택되었다. 이는 곧 조직은 외부에 의한 사회적·정치적 압력으로부터의 규제화에 의해 실제 보안위반 관리는 더 강화될 수 있다는 것을 의미한다. 넷째, 비고의적 보안위반 인식 및 통제, 성과 변수들 간의 인과관계를 살펴보면, 인식과 통제(β=0.527, t=8.942), 그리고 인식과 성과(β=0.375, t=4.830)는 각각 유의수준 0.01과 0.05에서 지지되었으며, 통제와 성과(β=0.492, t=6.319)는 유의수준 0.01에서 지지되었다. 따라서 가설 8a, 가설 8b, 가설 9는 채택되었다. 이는 곧 비고의적 보안위반 인식이 우선될 때 행동의 수정이 이루어질 수 있고, 이러한 개선의 노력으로 인해 조직의 전반적 성과가 드러날 수 있

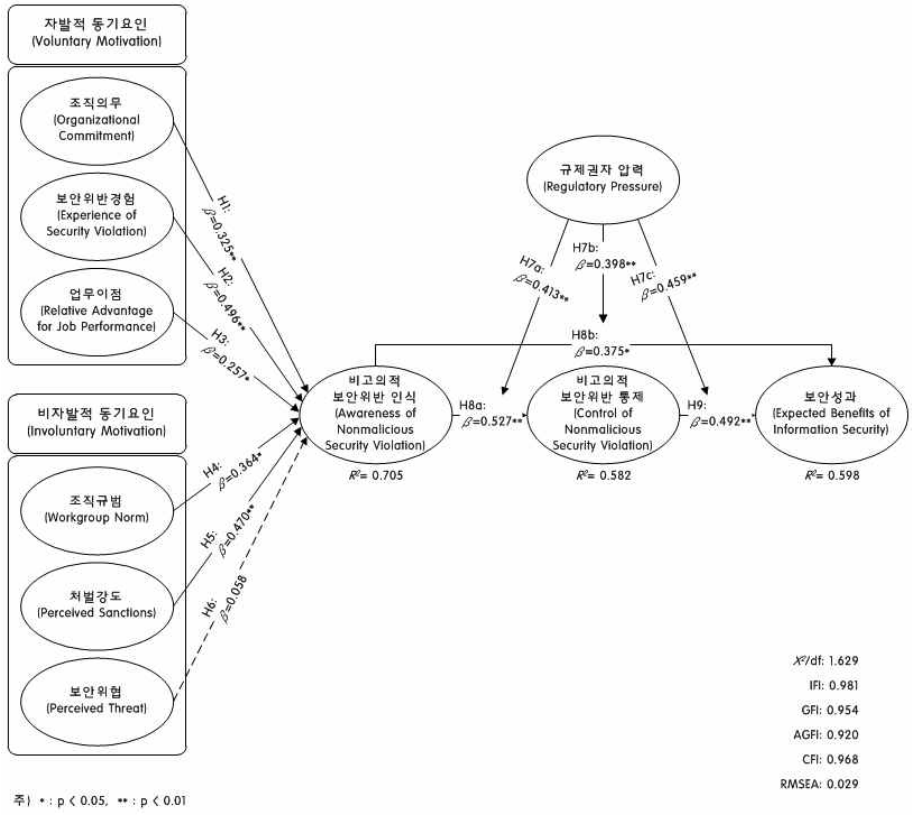
다는 것을 의미한다. 마지막으로 외생변수별 영향정도를 살펴보면, 자발적 동기요인의 보안위반경험(β=0.665)이 비고의적 보안위반 인식에 가장 큰 영향을 주는 것으로 나타났으며, 다음으로 처벌강도(β=0.470) 순으로 나타났다. 이는 곧 이전의 정보보안 및 기술관련 연구에서 제시된 보안위반경험 및 처벌강도의 중요성이 비고의적 보안위반에서도 적용될 수 있음을 알 수 있다.

구조모형 분석의 세 번째 결과는 내생변수(endogenous variable)에 대한 결정계수 즉 R^2 결과 값이다. 결정계수 R^2는 연구모형의 총 변동 중에서 회귀선 즉 외생변수(설명변수, 독립변수)들에 의해 설명되는 비율을 의미한다. 연구모형에서 제안한 조직의 자발적, 비자발적 동기의 총 6개 변수 중 보안위협을 제외한 나머지 5개 변수는 조직의 보안위반 인식이 가지고 있는 분산의 70.5%를 설명하고 있다. 즉, 조직의 보안위반 인식이 가지고 있는 정보 중 70.5%는 자발적, 비자발적 동기의 5개 변수의 변동으로 알 수 있다는 것을 의미한다. 또한, 보안위반 인식은 보안위반 통제를 표현하는 분산의 58.2%, 보안위반 통제는 보안성과의 59.8%의 분산을 설명하고 있는 것으로 나타났다. 가설검정에 대한 요약과 구조방정식 분석 결과는 〈표 7〉과 〈그림 2〉에서 보여준다.

〈표 7〉 가설검정 결과요약

가설	경로	경로계수	t-값	채택 유·무
가설1	조직의무 → 보안위반인식	0.325**	4.572	채택
가설2	보안위반경험 → 보안위반인식	0.496**	8.827	채택
가설3	업무이점 → 보안위반인식	0.257*	3.895	채택
가설4	조직규범 → 보안위반인식	0.364*	4.925	채택
가설5	처벌강도 → 보안위반인식	0.470**	6.970	채택
가설6	보안위협 → 보안위반인식	0.058	0.121	기각
가설7a	보안위반인식 → 보안위반통제 ↑ 규제권자 압력	0.413**	5.623	채택
가설7b	보안위반인식 → 보안성과 ↑ 규제권자 압력	0.398**	6.840	채택
가설7c	보안위반통제 → 보안성과 ↑ 규제권자 압력	0.459**	9.128	채택
가설8a	보안위반인식 → 보안위반통제	0.527**	8.942	채택
가설8b	보안위반인식 → 보안성과	0.375*	4.830	채택
가설9	보안위반통제 → 보안성과	0.492**	6.319	채택

주) *:p〈0.05, **:p〈0.01



〈그림 2〉 구조모형 분석결과

Ⅴ. 결 론

5.1 연구결과 요약 및 시사점

본 연구는 비고의적 보안위반에 대한 사전점검의 시행을 통해 조직이 실질적인 효과를 거두기 위한 요건들과 제반 사항들을 제시함으로써 조직의 정보보안 위반관리 실천방법을 유형화하였다. 이는 이전 연구의 비판적 고찰을 통해 많은 조직들의 비고의적 보안위반에 대한 정확한 인식에 근거하기 위한 유인기재를 마련하였다. 따라서 조직 내부의 자발적(조직의무, 보안위반경험, 업무이점) 및 비자발적(조직규범, 처벌강도, 보안위협) 동기요인을 제안하고 보안위반 통제 프로세스(인식, 통제, 성과)에 미치는 영향을 검정하였다. 또한, 제도적 실효성 확보의 중요한 역할을 검정하기 위해 규제권자 압력의 조절효과를 살펴보았다. 이에 대한 본 연구의 결과를 요약하면 다음과 같다.

첫째, 자발적 동기요인의 세 변수 모두 조직의 비고의적 보안위반 인식에 긍정적인 영향을 미치는 것으로 나타났다. 이는 곧 종업원의 잠재적 불안정한

행동에 대한 경고를 위해서는 그들 행동에 대한 내부 패턴의 발견과 의식이 중요하다는 것을 알 수 있다. 즉, 세 변수에 의해 종업원 개인이 보안위반 인식에 가지는 다양한 이해관계 및 입장을 합리적으로 통합 및 조정할 수 있다는 것을 의미한다. 둘째, 비자발적 동기요인의 보안위협을 제외한 나머지 두 변수(조직규범, 처벌강도)는 조직의 비고의적 보안위반 인식에 긍정적인 영향을 미치는 것으로 나타났다. 즉, 종업원의 보안위반에 대한 규율 및 통제는 그들이 속한 조직의 태도와 조직내부 환경설정으로부터의 영향이 중요하다는 것을 의미한다. 따라서 조직 내부의 보안위반에 대한 평가지표 및 프로그램의 도입이 그들 행동에 자극을 줄 수 있다는 것을 알 수 있다. 하지만 보안위협은 비고의적 보안위반 인식에 영향을 미치지 않는 것으로 나타났다. 이는 곧 위해 요소에 대한 인식이 보안사고의 사전적인 대비나 사후적 구제 방안과는 직접적인 관련성이 없다는 것을 의미한다. 셋째, 규제권자 압력의 조절효과는 보안위반 인식, 통제, 성과들 간의 관계를 강화시켜주는 것으로 나타났다. 즉, 조직이 비고의적 보안위반에 대한 일정 행동들의 제거의 필요성을 가지지만 안정된 형태의 관리를 위한 보안체계의 강압적 제도화가 달성되지 않는다면 보안위반 관리의 현실적 적용은 구체적으로 실현되기 어렵다는 것을 의미한다. 마지막으로 보안위반통제 프로세스의 과정은 모두 그 영향이 긍정적인 것으로 나타났다. 이는 곧 비고의적 보안위반에 대한 피해방지 노력을 통해 조직 전반의 질적 향상이 가능하다는 것을 의미한다.

본 연구는 실증적 검정을 통해 비고의적 보안 위반에 대한 관리기준을 제시하였다. 이는 많은 정보보안과 관련된 연구에도 불구하고 비고의적 측면의 연구가 부진한 점을 지적하고, 종업원의 성공적인 보안관리 실행에 필요한 이론적 바탕과 실용적인 지침의 결과물을 제안하여 그 의미가 크다고 할 수 있다. 본 연구결과에 근거하여 몇 가지 기대효과 및 활용방안을 제시하면 다음과 같다. 첫째, 본 연구는 어느 조직에서나 적용 및 실행이 가능한 비고의적 보안위반 통제의 관리 기준을 이론적 연구를 시행하여 정립하였다. 즉, 아직까지 국·내외의 종업원의 부주의한 행동에 대한 사전 예방적 종업원의 경각심을 고취하기 위한 기준이 미흡한 상황에서 시의적절한 학문적 토대를 마련하고, 보안위반 관리 및 통제에 대한 개인과 조직의 행동을 설명하는 연구에 좋은 시발점이 될 수 있다.

둘째, 이전의 보안위반의 연구에서 찾아 볼 수 없었던 조직의무, 보안위반경험 등의 외생변수와 규제권자 압력의 조절효과, 그리고 보안위반 통제 과정을 나열함으로써 새로운 변수를 이론화하여 그 시사점이 크다. 이는 곧 이전 연구에서 실증적으로 검정되지 않았던 요소 및 인과관계에 대한 이론적 연구의 산물을 제시하여 논리적 틀을 마련하였다. 마지막으로 비고의적 보안위반과 관련된 변수를 측정하기 위한 새로운 측정변수를 이전 연구로부터 개발하여 타당성을 검정한다는 시사점이 있다.

아울러 실무적 시사점으로는 첫째, 비고의적 보안위반 통제 수준을 향상시키기 위한 통합적인 방법을 제공하여 많은 조직들의 실질적인 문제점에 대한 바람직한 해결책이 무엇인가에 대해 조언과 도움을 줄 수 있다. 즉, 상당수의 기업들이 보안 관리로부터 발생되는 갈등의 해결 수단으로 기술적, 물리적 도구에 의존하고 있다. 따라서 이들만으로 보안환경이 충분히 구축되었다는 오해를 상기시키고 현재의 조직차원의 보안조치는 한계가 있다는 것을 알 수 있다. 둘째, 최종 사용자의 지식 및 이해, 교육과 주의에 대한 인식전환의 출발이 어떤 과정을 통해 체계적으로 이루어질 수 있는지에 대한 정보를 제공하였

다는 시사점이 있다. 이는 곧 비고의적 보안위반의 관리지표가 모호한 현실에서 본 연구의 의미를 통해 실제 기업들의 보안 비즈니스 및 프로세스에 적용할 수 있는 기회와 동기를 제공하고, 보안의 관리 영역이 인적 요소로 확장됨에 따라 통합적 정보보안 관리에 대한 역할을 재설정할 수 있는 계기를 마련할 수 있다.

또한, 조직들의 보안관리 체계구축에 대한 이견을 좁힐 뿐 아니라 설득력을 얻고, 기업의 생산성 향상 및 사회적 책임 강화를 위해서는 내부의 노력과 사회 및 제도적 투자와 압력이 필요하다는 점도 본 연구를 통해 시사한다. 만약 기업들이 그들 환경에 도출된 지표를 활용한다면 상당부분의 가치 평가에 유용한 효과를 제시하고 기존의 역기능들을 최소화할 수 있다는 것도 알 수 있다. 본 연구는 국내 기업환경에서 비고의적 보안위반 관리를 위해 국내 환경에 적합한 요인들을 결합한 정형화된 모형을 개발하고 검정된 진단도구를 제시함으로 그 의의가 더욱 크다고 할 수 있다.

5.2 연구의 한계점 및 향후 연구방향

하지만 본 연구에서도 여느 사회과학의 연구와 마찬가지로 몇 가지 한계점을 내포한다. 첫째, 이전의 비고의적 보안위반에 대한 연구의 시도는 상당히 제한되어 왔다. 이는 곧 보안위반에 대한 선행연구의 미비함으로 인해 구체적인 참고자료를 통한 조직관리 현상을 설명하기에는 많은 제약이 뒤따른다. 따라서 본 연구에 사용된 변수 및 측정항목에 대한 타당성 검정이 지속적으로 개선 및 개발될 필요가 있다. 즉, 본 연구에서 사용된 측정도구는 하나의 시안으로 연구변수의 조작화(operationalization)에 보다 엄격한 개념타당성과 신뢰성 검정을 추가적 연구를 통해 확보할 필요가 있다. 둘째, 본 연구에서 제안한 이론적 모델에서 포함하는 요인 이외에 실제 조직 사례에 적용되기 위한 실무적 관점에서의 비고의적 보안위반에 의미 있는 요소들의 이론화와 실증적 분석이 더 필요하다.

셋째, 비고의적 보안위반 인식 및 통제의 과정을 측정하는 개념은 보다 세분화된 프로세스를 적용시켜 연구할 필요성이 있다. 이는 곧 한정된 변수에 의존할 수 있다는 한계가 있기 때문이다. 또한, 본 연구에서 제안한 규제권자 압력 외의 관리 과정을 효과적으로 설계하기 위한 상관관계를 증감시키는 변수의 타당성 검정이 필요하다. 마지막으로 한정된 자료의 보편성 및 일반성을 확보하기 위해서는 설문조사의 표본에 대해 다양한 조직의 특성과 참여를 포함시킬 필요가 있다. 즉, 향후 연구에서는 기업들의 비고의적 보안위반 통제에 대한 인식제고를 위해 단편적 범위를 탈피한 개발과 적용이 필요하다는 것을 의미한다. 따라서 현실적인 비고의적 보안위반 관리에 대한 파급효과를 기대하고 제한요인들을 설명하기 위해서는 보다 심층적인 관점에서의 정량적, 정성적 분석이 더욱 필요하다.

참고문헌

Anderson, D. L. and R. Agarwal(2010), "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly*, 34(3), 613-643.

Appari, A. and M. E. Johnson(2009), "HIPAA Compliance: An Institutional Theory Perspective," *AMCIS 2009 Proceedings*.

Baker, W. H. and L. Wallace(2007), "Is Information Security Under Control?," *IEEE Security & Privacy*, 5(1), 36-44.

Banerjee, D., T. P. Cronan, and T. W. Jones (1998), "Modeling IT Ethics: A Study in Situational Ethics," *MIS Quarterly*, 22(1), 31-60.

Barclay, D., R. Thompson, and 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.

Basu, V., E. Hartono, A. L. Lederer, and V. Sethi (2002), "The Impact of Organizational Commitment, Senior Management Involvement, and Team Involvement on Strategic Information Systems Planning," *Information & Management*, 39(6), 513-524.

Besnard, D. and B. Arief(2004), "Computer Security Impaired by Legitimate Users," *Computers & Security*, 23(3), 253-264.

Boss, S. R., L. J. Kirsch, I. Angermmeier, R. A. Shingler, and 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.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat(2010), "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, 34(3), 523-548.

Compeau, D. R. and C. A. Higgins(1995), "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly*, 19(2), 189-211.

D'Arcy, J., A. Hovav, and 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.

Dhillon, G. and J. Backhouse(2000), "Information Systems Security Management in the New Millennium," *Communications of the ACM*, 43(7), 125-128.

DiMaggio, P. J. and W. W. Powell(1983), "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review*, 48 (2), 147-160.

Fornell, C. and D. Larcker(1981), "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, 18(1), 39-50.

Gosain, S.(2004), "Enterprise Information Systems as Objects and Carriers of Institutional Forces: The New Iron Cage?," *Journal of the Association of Information Systems*, 5(4), 151-182.

Guo, K. H., Y. Yuan, N. P. Archer, and C. E. Connelly(2011), "Understanding Nomnalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems*, 28(2), 203-236.

Gupta, A. and R. Hammond(2005), "Information Systems Security Issues and Decisions for Small Business: An Empirical Examination," *Information Management & Computer Security*, 13(4), 297 - 310.

Harrington, S. J.(1996), "The Effects of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Inten-

tions," *MIS Quarterly*, 20(3), 257 - 278.

Herath, T. and H. R. Rao(2009a), "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems*, 47(2), 154-165.

Herath, T. and H. R. Rao(2009b), "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems*, 18(2), 106-125.

Hong, K. S., Y. P. Chi, L. R. Chao, and J. H. Tang (2006), "An Empirical Study of Information Security Policy on Information Security Elevation in Taiwan," *Information Management & Computer Security*, 14(2), 104-115.

Hsu, C. W.(2009), "Frame Misalignment: Interpreting the Implementation of Information Systems Security Certification in and Organization," *European Journal of Information Systems*, 18(2), 140-150.

Hsu, C., J. N. Lee, and D. W. Straub(2012), "Institutional Influences on Information Systems Security Innovations," *Information Systems Research*, 23(1), 1-22.

Hu, Q., P. Hart, and D. Cooke(2007), "The Role of External and Internal Influences on Information Systems Security- A Neo-Institutional Perspective," *The Journal of Strategic Information Systems*, 16(2), 153-172.

Ifinedo, P.(2012), "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security*, 31(1), 83-95.

Johnston, A. C. and M. Warkentin(2010), "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly*, 34(3), 549 - 566.

Kankanhalli, A., H. H. Teo, B. C. Y. Tan, and K. K. Wei(2003), "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management*, 23(2), 139-154.

Karahanna, E., D. W. Straub, and N. L. Chervany (1999), "Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs," *MIS Quarterly*, 23(2), 183-213.

Karyda, M., E. Kiountouzis, and S. Kokolakis (2005), "Information Systems Security Policies: A Contextual Perspective," *Computers & Security*, 24(3), 246-260.

Khalifa, M. and R. M. Davison(2006), "SME Adoption of IT: The Case of Electronic Trading Systems," *IEEE Transactions on Engineering Management*, 53(2), 275-284.

Knapp, K. J., T. E. Marshall, R. K. Rainer, and F. N. Ford(2006), "Information Security: Management's Effect on Culture and Policy," *Information Management & Computer Security*, 14(1), 24-36.

Kotulic, A. G. and J. G. Clark(2004), "Why There aren't More Information Security Research Studies," *Information & Management*, 41 (5), 597-607.

Lee, Y. and 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.

Lee, S. M., S. G. Lee, and S. Yoo(2004), "An Inte-

grative Model of Computer Abuse Based on Social Control and General Deterrence Theories," *Information & Management*, 41 (6), 707-718.

Leonard, L. N. K. and T. P. Cronan(2001), "Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences," *Journal of the Association for Information Systems*, 1(1), 1-31.

Li, H., J. Zhang, and R. Sarathy(2010), "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory," *Decision Support Systems*, 48(4), 635-645.

Liang, H., N. Saraf, Q. Hu, and Y. Xue(2007), "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management," *MIS Quarterly*, 31(1), 59-87.

Liang, H. and Y. Xue(2009), "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly*, 33(1), 71-90.

Liang, H. and Y. Xue(2010), "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems*, 11(7), 394-413.

Marakas, G. M., M. Y. Yi, and R. D. Johnson (1998), "The Multilevel and Multifaceted Characteristics of Computer Self-Efficacy," *Information Systems Research*, 9(2), 126-163.

Myyry, L., M. Siponen, S. Pahnila, T. Vartiainen, and A. Vance(2009), "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems*, 18(2), 126 - 139.

Mowday, R.(1998), "Reflections on the Study and Relevance of Organizational Commitment," *Human Resources Management Review*, 8(4), 387-401.

Nelms, J. E.(2011), "Predicting Threats on Electronic Health Record Systems," SAIS 2011 Proceedings.

Newman, M. and R. Sabherwal(1996), "Determinants of Commitment to Information Systems Development: A Longitudinal Investigation," *MIS Quarterly*, 20(1), 23-54.

Ng, B. Y., A. Kankanhalli, and Y. C. Xu(2009), "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems*, 46(4), 815-825.

Nunnally, J. C.(1967), *Psychometric Theory*, New York: McGraw-Hill.

Post, G. V. and A. Kagan(2007), "Evaluating Information Security Tradeoff: Restricting Access can Interfere with User Tasks," *Computers & Security*, 26(3), 229 - 237.

Pososky, D.(2002), "A Field Study of Computer Self-Efficacy Beliefs as an Outcome of Training: The Role of Computer Playfulness, Computer Knowledge, and Performance during Training," *Computers in Human Behavior*, 18(3), 241-255.

Ransbotham, S. and S. Mitra(2009), "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research*, 20(1), 121-139.

Rhee, H. S., C. Kim, and Y. U. Ryu(2009), "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior," *Computers & Security*,

28(8), 816 - 826.

Scott, W. R.(1987), "The Adolescence of Institutional Theory," *Administrative Science Quarterly*, 32(4), 493-511.

Siponen, M. and A. Vance(2010), "Neutralzation: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly*, 34(3), 487-502.

Spears, J. L. and H. Barki(2010), "User Participation in Information Systems Security Risk Management," *MIS Quarterly*, 34(3), 503-522.

Stanton, J. M., K. Stam, I. Guzman, and C. Caldera(2003), "Examining the Linkages Between Organizational Commitment and Information Security," *In IEEE Systems, Man, and Cybernetics Conference Washington DC*, USA.

Stanton, J. M, K. R. Stam, P. Mastrangelo, and J. Jolton(2005), "Analysis of End User Security Behavior," *Computers & Security*, 24(2), 124-133.

Straub, D. W.(1990), "Effective IS Security: An Empirical Study," *Information Systems Research*, 1(3), 255-276.

Straub, D. W., M. Boudreau, and D. Gefen(2004), "Validation Guidelines for IS Positivist Research," *Communications of the Association for Information Systems*, 13(24), 380-427.

Straub, D. W. and R. W. Collins(1990), "Key Information Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy," *MIS Quarterly*, 14(2), 143-156.

Straub, D. W. and R. J. Welke(1998), "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, 22(4), 441-469.

Teo, H. H., K. K. Wei, and I. Benbasat(2003), "Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective," *MIS Quarterly*, 27(1), 19-49.

Wixom, B. and H. Watson(2001), "An Empirical Investigation of the Factors Affecting Data Warehousing Success", *MIS Quarterly*, 21(2), 17-41.

Workman, M., W. H. Bommer, and D. Straub(2008), "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior*, 24(6), 2799-2816.

Zhang, J., X. Luo, S. Akkaladevi, and J. Ziegelmayer(2009), "Improving Multiple-Password Recall: An Empirical Study," *European Journal of Information Systems*, 18(2), 165-176.

Zhang, J., B. J. Reithel, and H. Li(2009), "Impact of Perceived Technical Protection on Security Behaviors," *Information Management & Computer Security*, 17(4), 330-340.

An Empirical Study on Factors Influencing the Awareness of Nonmalicious Security Violation and the Moderating Effects of Regulatory Pressure

Sanghyun Kim* · Geuna Kim**

Abstract

Today, many enterprises perceive the risk of information security as a big obstacle in the process of advancement into knowledge information society. In other words, modern companies enjoy various benefits from information, but at the same time they are exposed to various dysfunctions and risks (e.g., cyber terror, the leakage of personal information and important assets, etc.) by external sources. Failures in security of companies' resources may bring social and financial damages, which may lead to the extinction of the company. In particular, incidents related with information security more frequently results from internal factors, and consequently internal risks are perceived as fatal to organizations. Most of security related incidents are caused by insufficient vigilance on employees, such as lack of loyalty of employees, moral hazard and non-intentional misuse and mistakes, and the absence of the development of detailed indexes.

Thus, issues related to end-users' behaviors regarding of security have attracted much interest for researchers to explain the successful management of security. No matter what security system is in place, there are potential and incidental possibilities that end users can make a mistake. Moreover, even if end-users have no intention to violate security policies at organization, their mistakes are evaluated as crucial factors in the dimension of loss of information and information related security incidents. Even small and trivial mistakes in security related matters would result in a big and fatal consequency for a organization.

* Associate Professor, School of Business Administration, Kyungbook National University
** Doctoral Candidate, School of Business Administration, Kyungbook National University

However, even with this reality, researches related to information security management has been inconsistent and scant. Prior studies only focus on conventional security, including physical and technical security design and construction, investment effects and decision making for information system security, development and standardization of information security indexes, role and maturity of information security policies, and information security and risk management. Therefore, there is a need to carry out a series of appropriate control means for nonmalicious violation of information security within organizations.

In this regard, this study was conducted as a part of attempts for identifying the motivation to manage nonmalicious security violation of organizations and for proposing a possible answer for the following research question: "What makes an organization increase awareness of nonmalicious security violation, and what are the processes of information security management (ISM)?" In addition, this study suggested the role of regulatory influence on the processes of information security management. Particularly, this study focuses on the impacts of voluntary motivation and involuntary motivation of an organization as main categories on awareness of nonmalicious security violation that influences control of nonmalicious security violation and excepted benefits of information security. Voluntary motivation includes organizational commitment, experience of security violation, and relative advantage for job performance while involuntary motivation includes workgroup norm, perceived sanctions, and perceived threat. Furthermore, this study is meaningful in that it is differentiated from other studies through the empirical verification of how the regulatory pressure makes effects on awareness of nonmalicious security violation, control and performance. Thus, the following hypotheses were tested:

Hypothesis 1: Organizational Commitment will have a positive effect on Awareness of Nonmalicious Security Violation

Hypothesis 2: Experience of Security Violation will have a positive effect on Awareness of Nonmalicious Security Violation

Hypothesis 3: Relative Advantage for Job Performance will have a positive effect on Awareness of Nonmalicious Security Violation

Hypothesis 4: Workgroup Norm will have a positive effect on Awareness of Nonmalicious Security Violation

Hypothesis 5: Perceived Sanctions will have a positive effect on Awareness of Nonmalicious Security Violation

Hypothesis 6: Perceived Threat will have a positive effect on Awareness of Nonmalicious Security Violation

Hypothesis 7a: Regulatory Pressure moderates the relationship between Awareness of Nonmalicious Security Violation and Control of Nonmalicious Security Violation

Hypothesis 7b: Regulatory Pressure moderates the relationship between Awareness of Nonmalicious Security Violation and Expected Benefits of Information Security

Hypothesis 7c: Regulatory Pressure moderates the relationship between Control of Nonmalicious Security Violation and Expected Benefits of Information Security

Hypothesis 8a: Awareness of Nonmalicious Security Violation will have a positive effect on Control of Nonmalicious Security Violation

Hypothesis 8b: Awareness of Nonmalicious Security Violation will have a positive effect on Expected Benefits of Information Security

Hypothesis 9: Control of Nonmalicious Security Violation will have a positive effect on Expected Benefits of Information Security

To induce the research results, 319 responses were collected from employees of domestic companies which were operating information system security activities. Structural Equation Modeling(SEM) approach was used to verify both measurement and structural model. The results showed that all constructs in voluntary and involuntary motivation with exception of perceived threat, had a significant effect on awareness of nonmalicious security violation, which then had a significant effect on control of nonmalicious security violation and excepted benefits of information security. In addition, the moderating effect of regulatory pressure was indicated to have significant influence upon the process of controlling the nonmalicious security violation. The implications of the findings suggest the theoretical and practical implication for minimizing a losses in the mistake-based aspect of security incident through monitoring and diagnosis on security violation.

Key words: Nonmalicious Security Violation, Voluntary/Involuntary Motivation, Regulatory Pressure, Information Security