디지털산업정보학회 논문지 제12권 제2호-2016년 6월
http://dx.doi.org/10.17662/ksdim.2016.12.2.073

기밀정보 유출 경험을 가진 기업들의 정보사고 대응역량 강화에 관한 연구

정 병 호*

The Correspondence Competence of Information Accident by Firms Experienced in Confidential Information Leak

Jung Byoungho

〈Abstract〉

The purpose of this study is to examine a security investment for firms experienced in confidential information leak. Information security is an apparatus for protection of secret information. The competence of information security is a competitiveness to avoid information leakage in changing business environment. The type of information security is divided into administrative security, technical security and physical security. It is necessary to improve the incident correspondence competence through information security investment of the three types. Therefore, the investment of information security is to enhance information-asset protection of firms. To reinforce accident response competence, an organization discussed an establishment, security technology development, expand investment and legal system of the security system.

I have studied empirically targeting the only information leak of firms. This data is a technical security competence and technology leakage situation of firms happened in 2010. During recovery of the DDos virus damage on countries, company and individual, the collected data signify a reality of information security. The data also identify a security competence of firms worrying information security management. According to the study, the continuous investment of information security has a high competence of accident correspondence. In addition, the most of security accidents showed a copy and stealing of paper and computer files. Firm on appropriate security investment is an accident correspondence competence higher than no security investment regardless of a large, small and medium-sized, and venture firm. Furthermore, the rational security investment should choose the three security type consideration for firm size.

Key Words : Security Accident, Correspondence Competence, Confidential Information Leak, Information Security

* 한국외국어대학교 경영정보학과 박사

Ⅰ. 서론

기업들의 정보기술(Information Technology) 투자는 정보 역량을 강화하여 제품과 서비스를 차별화 시키는데 목적이 있다. 그리고 정보기술 역할이 기업 경영 환경의 불확실성을 어느 정도 해소시켜주면서 더욱 중요해지고 있는 시점이다[1]. 최근에는 기업들은 빅데이터 기술을 통해 외부에서 생성되는 최신 정보를 확보할 수 있게 되었으며 기업 내부에 있는 데이터와 결합하여 고객(소비자)의 행동을 사전에 파악하여 더 나은 서비스를 제공하고자 노력하고 있다[2]. 이렇듯, 정보기술의 이용은 기업에게 필수적인 요소가 되었고, 기업은 정보기술 관리를 매우 중요시 여겨야 되는 시점이 되었다.

한편, 기업들이 정보기술을 집중 투자하고 있지만 정보를 감독하고 유출을 방지할 수 있는 관리방안에 대해서는 미흡하다고 할 수 있다[3]. 2000년대 들어와 기업들의 정보시스템의 투자에 대한 관심이 높은 반면에 정보관리의 중요성은 상대적으로 낮아 시스템 간의 정보 불일치가 발생하고 있으며, 해킹과 비인가 접근을 방지하기 위한 방화벽 설치 등이 미흡하게 되면서 정보의 누수 현상이 나타나고 있다[4]. 특히, 2009년도부터 온라인으로 디도스(DDos) 공격이 무차별로 나타나면서 기업들은 대응방안을 마련하지 못하였고, 경영 손실이 발생하였다. 이를 계기로 기업들은 정보보안의 중요성을 인식하는 계기가 되었지만[5], 끈임 없는 사이버 공격과 인적자원의 정보 유출로 인하여 산업 기밀 유출이 비일비재하게 나타나고 있는 실정이다[6].

특히, 정보시스템의 운영 없이는 기업 활동이 불가능한 시대에서 산업기밀의 유출은 언론을 통해서 자주 보도되고 있다. 기존 정보보안 연구[5]에서도 최신 정보시스템이 기업의 경쟁력을 제공하고 있지만 이를 체계적으로 관리할 수 있는 인적자원과 시스템 준수는 미흡한 실정이라고 지적하였다. 이는 시스템 해킹뿐만 아니라 내부 인적자원들의 보안인식이 낮게 되면서 기업의 기밀정보가 외부로 손쉽게 유출되고 있는 현상이다[7]. 이제는 기업들이 보유하고 있는 정보를 자산으로서 인식전환과 함께 이를 체계적으로 관리할 역량 보유가 중요해졌다[8]. 즉, 기업들의 정보보안 투자가 선택사항이 아니라 필수사항으로 인식전환이 필요하다는 것이다[9]. 그럼에도 불구하고 2009년도 디도스(DDos) 바이러스부터 최근 램섬웨어(ransom ware) 바이러스까지 나타나면서 정보 해킹이 증대되는 상황이고 여러 기업들의 정보 누출 피해가 다시금 나타나고 있다.

따라서 본 연구에서는 기존 2013년 정보보안 연구[5]에서 다루지 못하였던 기밀정보 유출 경험을 가진 기업만을 다시 재조사하려 한다. 기존 정보 피해 기업들이 어떤 보안 요소를 중요시 여기는지를 실증적 연구를 하고자 한다. 이는 과거의 정보누출 피해기업을 다시금 실증 연구하여 최근의 바이러스 피해 기업에 대한 방안을 상기시키는데 목적이 있다. 이에 정보보안을 투자를 체계적으로 하고 있는 기업과 그렇지 않는 기업 간의 비교를 통해서 투자 역량을 차이를 살펴보고, 정보보안 투자의 중요성을 강조할 것이다. 마지막으로, 정보사고 대응역량 강화를 위한 방안을 제시하고자 한다.

Ⅱ. 관련연구

2.1 정보보안과 사회기술시스템 이론

정보보안은 기업에서 보호되어야 할 정보를 안전하게 관리하기 위한 장치이며, 여기서 정보는 활용 가능한 데이터를 가공하여 특정 목적에 사용하고 분석되는 자료를 말한다[10]. 그리고 보안은 조직에서 요구하는

사항에 따라 조직 자산을 외부의 위협으로부터 안전하게 관리하는 것을 의미한다[11]. 이러한 정보보안 활동은 조직 내부의 사람과 관련되어 있어, 기업은 정보 보호를 위한 제도와 절차를 중요시해야 된다[12, 13].

한편, 사회기술시스템은 기술 중심의 시스템과 사회적 시스템과의 상호작용을 강조하고 있다[14]. 사회적 시스템은 사람, 환경 구조에 초점을 두고 있으며 기술 시스템은 직무와 기술 구조에 초점을 두고 있다[15]. 사회기술 시스템은 기술적 요소와 사회적 요소를 함께 반영함으로써 기업의 생산성을 향상시킬 수 있고 신기술의 유연한 수용이 가능해질 수 있다고 보고 있다[16]. 사회와 기술은 기업 경영에 영향을 제공하는 요소로서 기업들은 사회기술을 끈임 없이 탐색하고 적응할 필요가 있다[17].

특히, 사회적 시스템은 사람과 구조의 관점에서 실제 업무를 수행하는 인적자원의 커뮤니케이션, 권한, 업무 프로세스를 효과적으로 설계하여 기업의 성과를 높이고자 하는 것을 의미한다[14]. 즉, 사람의 태도와 행동과 관련되어 있는 사회적 시스템에서 보안 사고를 방지하기 위해서는 보안정책, 자산관리, 보안의 책임성을 강조할 수 있는 인적자원관리, 합리적인 조직 구조와 관료제 운영, 정기적 보안 감사의 운영이 필요하겠다[18]. 기술적 시스템은 기술과 직무에 관점에서 비즈니스나 정보보안 문제를 해결할 수 있는 방법, 도구의 사용에 대한 방법을 강조한다[19]. 즉, 조직이 요구하는 보안의 긍정적 결과를 만들기 위한 과정과 올바른 결과의 도출을 목적으로 한다. 이는 조직의 성과 문제를 개인의 역량이 아닌 조직 전체 관점에서 해결책을 제시하려는 의미를 가진다[16].

2.2 정보보안의 특징과 세 가지 유형

기업의 정보보안 투자는 기업의 정보 자산을 보호하기 위한 대응력 강화를 의미한다[20]. NIST[21]에 의하면 정보보안에서 중요시 여기는 세 가지 사항으로 기밀성, 무결성, 가용성이 있다고 한다. 기밀성은 정보 접근이 인가된 인적자원만 허가되고 비인가는 정보접근을 차단하는 것을 말한다[21, 22]. 기밀성은 접근통제의 모든 행위에 대한 근본적인 역할로서 정보의 특성에 따른 등급 관리를 우선시하게 된다. 다음으로 무결성은 정보가 가진 정확성과 완전성을 말한다[21]. 이는 비인가자에 의해 정보의 변경, 삭제, 파괴되지 않도록 관리하는 것을 우선시 한다. 마지막으로 가용성은 인가된 인적자원만 필요할 때만 적절히 해당 정보와 자산 접근의 보장을 말한다[21]. 즉, 인가된 사용자가 정보 요구 시 시간에 구애받지 않고 언제나 사용가능하게 허락되는 것을 우선시 한다.

한편, 정보보안의 유형으로는 관리적 보안, 기술적 보안, 물리적 보안으로 구분된다[23]. 우선 관리적 보안은 무형적 자산의 투자요소로서 인적자산, 정보자산, 정책 및 제도가 있으며, 기업의 중요한 통제 요소이다. 그리고 기술적, 물리적 보안의 통제를 더욱 강화시킬 수 있는 요인을 제공하기도 한다[24]. 두 번째로 기술적 보안은 정보시스템 자산과 관련되어 있으며 시스템, 네트워크, 서버, 데이터베이스의 기술을 보호하는데 집중되어 있다[19]. 즉, 정보 보호를 위한 파일 및 데이터 암호화, 시스템 접근 제어, 계정관리, 바이러스 등에서 비인가 침입 발생 방지를 위한 솔루션을 제공하는 역할을 담당한다. 마지막으로 물리적 보안은 기업의 중요시설 및 출입통제 보안을 설정하고 관리하는 것을 말한다[25]. 기업은 1차적인 보안을 강화시킬 수 있는 방안이 물리적 보안이며 CCTV나 보안-USB 사용을 통해 손쉽게 기밀 정보 누설을 방지하는 성과를 확보할 수 있다.

2.3 기밀정보 유출과 사고대응 역량

정보보안의 역량은 기업의 변화되는 환경에서 정

보보안 활동의 성과가 정보 유출을 방지할 수 있는 경쟁력이 된다[11]. 이는 보안사고의 위협 요소를 사전에 식별하고 자발적으로 통제하여 보안 사고를 미연에 방지할 수 있는 프로세스를 운영하는 것을 의미한다[7]. 하지만 보안 운영을 실시간으로 구현하더라도 기업은 재해, 과실, 고의성에 의해서 정보자산이 유출될 수 있으며, 이는 기업 경쟁력 약화를 발생시키는 결과로 초래될 수 있다[8]. 이렇듯, 기업의 성공적인 정보보안 관리를 위해서는 보안 관리의 규칙과 제도, 최고경영자의 확실한 지원이 요구된다[26]. 그리고 정보 보안을 위해 전체 조직의 틀에서 각 부서별로 책임과 권한, 인력배치가 합리적으로 이루어져야 보안 관리가 효과적일 것이다[27]. 즉, 보안이라는 틀 안에서 조직이 더욱 효과적으로 운영이 중요하다.

특히, 정보시스템 발전이 지속될수록 정보를 활용한 비즈니스 기회와 이익을 탐색/창출할 수 있지만 정보관리가 미흡할 경우 기업의 손실을 더욱 높아지게 된다[28]. 이에 기업들은 관리적, 기술적, 물리적 보안을 강화하여 기업의 사고 대응역량을 향상시킬 수 있는 기반을 마련할 필요가 있다. 이를 위해 사고대응 역량 강화를 위해서 조직의 보안 체계 수립, 보안시스템 구축, 보안 기술 개발 및 투자 확대, 법제도 마련과 교육훈련이 심도 있게 논의되어야 한다[29]. 기업은 보안 사고가 발생했을 시 상황별 대응시나리오를 구축하고 이를 행동으로 옮길 수 있는 실행력이 필요하다[21].

Ⅲ. 연구방법론

3.1 가설설정

본 연구는 한국중소기업청에서 실시한 2010년 기술보안 역량 및 기술유출 실태조사표를 기초로 하였으며 설문 문항은 국제 보안 표준규격인 ISO/ICE 27001을 바탕으로 설계되었다[30]. 이 조사는 국내 기업을 대상으로 표본 조사되었으며 조사 기간은 2010년 10월 4일 ~ 2010년 11월 29일까지 진행되었다. 총 수집된 표본 수는 벤처, 중소, 대기업을 포함하여 1,500개이다. 하지만 본 연구에서는 정보유출 피해를 경험한 기업만을 대상으로 하였기 때문에 전체 중에서 95개의 피해경험 기업만을 추출하여 연구하였다. 이는 일반적인 정보보안의 투자를 살펴보기 보다는 정보유출 피해 기업들이 정보보안 투자 유형 중 어디에 더욱 중요성을 인지하고, 필요로 하는지를 확인하는데 집중하기 위해서이다.

특히, 2010년 기술보안 역량 및 기술유출 실태 자료는 국가, 기업, 개인의 DDos 피해가 발생 후 복구하는 시점에서 조사된 자료로서 중요한 의미를 가진다고 할 수 있다. 즉, 본 데이터는 기업들이 정보보안에 대한 대책을 고민하고 관리 운영을 고찰하던 시점의 자료로서 기업의 운영 역량에 관한 내용이 내포되어 있다고 볼 수 있다.

따라서 본 연구는 정보 유출 경험을 가진 기업들을 대상으로 정보유출 사고 대응역량으로 기업규모별로 관리적 보안, 기술적 보안, 물리적 보안 중 어느 유형을 더욱 중요시 여겨야 하는지 확인하고자 한다.

특히, 기업들의 정보보안 투자에 대한 관심이 저조하면서 기업들의 정보 유출 사고는 의도치 않게 나타나곤 한다[31]. 그 예로 정보시스템에 접속 시 상급자의 아이디를 도용하여 비인가 접근을 통해 기밀정보를 파악하고, 타 기업 또는 개인 상대방과의 업무 교류 시에 활용되고 있다는 것이다[22]. 즉, 기업 내부에서 정보의 무분별한 공유를 방지하고자 정보보안 투자가 실시하게 되었고, 정보보안이 강화되면서 정보의 오남용이 줄어들게 되었다. 이러한 내용을 토대로 살펴보았을 때 기업들의 정보보안 투자 여부에 따라서 정보보안 사고 대응역량 차이가 있을 것이다. 즉,

정보보안 투자를 지속적으로 진행하는 기업이 그렇지 않는 기업보다 정보유출 사고 시에 대응역량이 높을 것이라고 보는 것이다. 이러한 내용을 토대로 가설을 설정하였다.

가설 1: 정보보안 투자 유무에 따라 정보 유출 사고 대응역량은 차이가 있을 것이다.

또한, 기업규모에 따라서 투자하는 기업과 그렇지 않는 기업 간의 차이가 있는지도 확인하고자 한다. 인적자원 관리 역량이 높은 대기업일지라도 정보보안 투자를 실시한 기업과 그렇지 않은 기업 간에는 정보보안 사고 대응역량의 차이가 있을 것이다. 이는 대기업, 중소기업, 벤처기업 구분 없이 정보보안 투자를 하지 않는 기업의 경우 정보보안 투자를 한 기업보다 사고 대응 역량이 약할 것으로 보인다. 즉, 기업 규모에 상관없이 정보보안 투자가 미흡한 기업은 투자를 지속적으로 이행하고 있는 기업에 비해 사고 대응역량이 낮다고 할 수 있다. 이러한 내용을 토대로 가설을 설정하였다.

가설 2: 기업 규모별로 정보보안 투자를 진행하고 있는 기업이 투자하고 있지 않는 기업보다 정보사고 대응역량이 높을 것이다.

그리고 기업규모별로 정보보안 사고로 인한 기밀정보 유출 시 대응에 필요한 보안 역량이 다르다고 할 수 있다. 정보보안 선도 투자 기업이 대기업일지라도 기업 규모와 사업에 따라서 정보보안 투자 요소가 다를 수 있다는 것이다. 이는 기업 규모의 차이는 사업의 규모, 인적자원의 규모, 운영 역량의 차이가 있다는 것을 의미한다. 이전 연구에서도 합리적인 정

<표 1> 변수의 조작적 정의와 주요 측정 도구

요인	조작적 정의	측정항목		관련 문헌
관리적 보안	기업의 정보유출 사고를 방지할 수 있는 정책 및 운영 관리 수준	MGT1	보안관리 규정 보유	[10, 12, 13, 20, 21, 29]
		MGT2	기업의 보안정책, 지침, 절차 등 임직원들 공지	
		MGT3	정보자산의 정기적 분류	
		MGT4	신규 입사자의 보안서약서 징구	
		MGT5	퇴사자에 대해 회사 자산의 유출방지 보안서약서 징구	
기술적 보안	기업의 정보 유출 사고 방지를 위한 IT기술 관리 수준	ITM1	통신망에 대한 보안점검 실시	[19, 20, 21, 25, 28]
		ITM2	서버 및 DB현황에 대한 보안점검	
		ITM3	바이러스 침입, 해킹, 내부로부터 정보유출 방지	
		ITM4	내부 주요 정보 및 소프트웨어 백업 관리	
		ITM5	지식관리시스템, 전자결재시스템의 관리	
		ITM6	외부로의 전자문서 발송에 대한 통제시스템	
물리적 보안	기업의 정보 유출 사고 방지를 위한 중요시설 관리 수준	PHY1	기업 내 외부인 출입절차 존재	[20, 21, 25, 29]
		PHY2	기업 내 중요시설 출입통제시스템 설치 및 운영	
		PHY3	외부인 식별을 위한 임직원 사원증 패용 의무	
		PHY4	건물 출입구 및 중요시설 CCTV 등 감시 장치 설치	
정보보안 사고 대응역량	기업 정보 유출 시 기업의 대응 역량	PER1	기술유출 및 침해사고의 대응방안	[3, 9, 10, 20, 21, 29]
		PER2	기술유출 방지 관련 주요 법규 인지	
		PER3	스마트폰 보안사고 대응방안	

보기술 투자가 아닌 모방에 의한 투자는 실제로 투자 효과를 가질 수 없다는 연구 결과도 있었다[32]. 이에 기업들은 자신들의 기업 규모에 맞는 합리적인 정보보안 투자가 필요하게 된다. 즉, 기업 규모에 따라서 정보보안을 투자해야 해야 하는 유형이 다르게 나타날 것이라고 본다. 이러한 내용을 토대로 가설을 설정하였다.

가설 3: 정보투자 세 가지 유형에서 기업 규모별로 투자에 필요한 유형이 모두 차이가 있을 것이다.

3.2 조작적 정의 및 변수 설정

본 연구는 정보 유출 경험을 가진 기업들에 있어 중요시 여겨야 하는 정보보안 유형을 검정하는데 있다. 이에 기존 문헌을 토대로 보안의 유형을 3가지로서 관리적 보안, 기술적 보안, 물리적 보안으로 구분하였다[23].

관리적 보안은 기업이 가지고 있는 무형적인 투자 요소이다. 관리적 보안은 보안규정, 자산관리, 인적자원관리가 포함되어 있다[13, 21]. 여기서 보안 규정은 1급, 2급, 대외비와 같은 관리 규정과 기업 내부의 보안 정책, 지침, 절차와 같은 프로세스를 임직원들이 공유하고 관리하는지를 말한다. 자산관리는 조직 내부에서 정보 자산을 정기적으로 분류하고 이를 통해 보관, 폐기를 체계적으로 이행하고 있는지를 말한다. 인적자원관리는 신규 입사자에게 기업 내부의 기밀정보를 누출하지 못하도록 보안서약서를 징구하고 교육훈련을 하는 것을 의미한다. 또한, 퇴사자에 대해서 회사 자산의 유출방지 보안서약서를 징구하는 내용도 포함된다. 이러한 정보보안을 위한 제도 설정 및 정책, 인적자원 관리를 관리적 보안으로 조작적 정의를 하였다.

기술적 보안은 기업이 소유하고 있는 정보시스템의 보안 관리를 의미한다[21, 25]. 통신망에 대한 정기적 보안점검 실시, 서버 및 DB 현황에 대한 보안 점검, 바이러스 침입/해킹/내부로부터 정보 유출, 내부 주요 정보 및 소프트웨어 백업 관리, 지식관리시스템/전자결제시스템 정기적 관리, 외부로의 전자문서 발송에 대한 통제 시스템 등이 기술적 보안에 해당된다. 이러한 전반적 IT 관리를 기술적 보안으로 조작적 정의를 하였다.

물리적 보안은 기업 내부 시설과 출입 보안 등의 보안 설정 관리를 의미한다[19, 21]. 기업 내 외부인 출입 절차, 기업 중요시설 출입통제시스템 설치 및 운영, 외부인 식별을 위한 임직원 사원증 패용 의무, 건물 출입구 및 중요시설 CCTV 설치 및 운영 등이 물리적 보안에 해당된다. 즉, 시설물 관리와 외부 출입관리에 관한 전반적 사항을 물리적 보안으로 조작적 정의를 하였다.

정보보안 사고 대응역량은 기술 유출 및 침해사고의 대응역량 보유, 기술유출 방지 관련 법규 인지, 스마트폰 보안사고 대응역량 등이 있다[20, 21]. 이를 토대로 정보보안 사고 대응역량으로 조작적 정의를 하였다.

Ⅳ. 연구결과

4.1 표본의 특성

정보유출 경험이 있는 기업을 대상으로 표본 특성을 확인하고자 한다. 이에 빈도 분석을 토대로 <표 2>에 결과를 제시하였다.

표본의 특성을 살펴보면 대기업이 9개(9.5%), 중소기업이 45개(48.4%), 벤처기업이 40개(42.1%)로 나타났다. 그리고 산업 유형별로 살펴보면 기계소재 분야가 다른 분야에 비해 35(36.8%)로 가장 높게 나타났다. 지역별로는 경기가 41(43.2%)로 가장 높게 차지하

<표 2> 표본의 특성

구분		빈도수	구성비율(%)
기업 규모	대기업	9	9.5
	중소기업	46	48.4
	벤처기업	40	42.1
산업 유형	기계소재	35	36.8
	전기전자	18	18.9
	정보통신	10	10.5
	화학섬유	16	16.8
	기타	16	16.8
지역	서울	26	27.4
	경기	41	43.2
	충청	9	9.5
	영남	17	17.9
	기타	2	2.1
기밀정보 유출횟수	1회	60	63.2
	2회	20	21.1
	3회	12	12.6
	5회	3	3.2

였고 다음으로 서울이 26(27.4%)로 두 번째로 높게 나타났다. 기밀정보 유출 횟수 경험은 1회(63.2%)가 가장 높게 나타났으며 세 개 기업은 5회 유출 경험을 가졌다고 응답 결과로 나타났다.

4.2 신뢰성 및 타당성 분석

본 연구의 신뢰성을 검정하기 위해 Cronbach's α 계수를 사용하였다. 신뢰성은 측정 도구가 측정 대상을 일관성 있게 측정하는 정도를 의미한다. 일반적으로 신뢰성 검정은 일반적인 연구에서 계수 값이 0.6 이상이면 측정 도수의 신뢰성에 문제가 없는 것으로 보고 있으며 0.8 이상이면 신뢰성이 높다고 판단한다[33]. 이에 <표 3>에 나타난 바와 같이 정보보안 사고 대응역량의 변수가 0.636 이며 나머지 변수는 이보다 높게 나타났다.

그리고 분석 표본의 타당성을 검정하기 위해 요인분석을 실시하였다. 요인분석은 주성분 분석을 실시한 후 요인 적재량을 단순화시키기 위해 직각 회전 방식인 베리맥스 방식을 적용하였다. 요인 적재치는 각 변수와 요인 간의 상관관계가 0.5 이상인 경우를 유의한 것을 판단한다[13]. 그리고 표본자료의 적합성을 나타내는 KMO (Kaiser-Meyer-Olkin) 검정은 요인분석을 위해 변수 간 상관관계가 어느 정도 존재하고 있는가를 검정하는 것으로 0.5 이상이면 요인분석에서 적합하다고 보고 있다[33]. 이에 관리적 보안, 기술적 보안, 물리적 보안의 KMO의 값은 0.821(p=0.000)로 나타났다. 정보 유출사고 대응역량의 KMO의 값은 0.643(p=0.000)으로 나타났다. 각 변수의 공통성이 0.4이하이면 낮다고 판정하여 요인분석에서 제외하게 되어 있으나 본 연구에서는 제외대상에 해당되는 변수는 없었다.

<표 3> 변수의 타당성 및 신뢰도 분석 결과

요인	측정항목	표준화 요인 적재량	공통성	신뢰성
관리적 보안	MGT1	.738	.699	.772
	MGT2	.657	.571	
	MGT3	.598	.493	
	MGT4	.720	.618	
	MGT5	.742	.564	
기술적 보안	ITM1	.742	.685	.838
	ITM2	.785	.737	
	ITM3	.695	.550	
	ITM4	.704	.498	
	ITM5	.653	.467	
	ITM6	.639	.480	
물리적 보안	PHY1	.605	.524	.679
	PHY2	.654	.478	
	PHY3	.745	.558	
	PHY4	.678	.488	
정보보안 사고 대응역량	PER1	.806	.650	.636
	PER2	.714	.510	
	PER3	.788	.621	

4.3 가설 검정

4.3.1 집단 간 차이 분석 결과

기업들의 정보보안 투자 유형을 장기 투자와 단기

투자, 투자 없음으로 구분하여 정보유출 사고 대응역량의 차이가 있는지를 검정하고자 One-way ANOVA를 실시하였다. ANOVA는 두 집단 이상이 종속변수에 대한 평균 차이를 검정할 때 사용하는 기법이다[33].

<표 4>를 살펴보면 정보보안 투자 없음이 49개, 단기 투자가 35개, 장기 투자가 11개 기업으로 나타났다. 장기 투자를 진행하는 기업이 저조하게 정보보안을 투자하는 기업보다 사고대응 역량이 높게 나타났다. 또한 유의확률(p=0.000)에서도 세 집단 간의 차이가 있다고 나타났다. 보안 투자가 없는 기업의 경우 평균이 1.53으로 나타났고 장기 투자하는 기업의 경우 2.13으로 나타났다. 큰 폭의 차이는 아니지만 사고대응 역량에 있어 보안 투자하지 않는 기업보다 투자하는 기업이 역량이 더 높다고 볼 수 있으며 가설 1은 채택되었다. 특히, 집단 간의 유의한 차이를 확인하기 위한 사후 검정인 Scheffe 분석을 실시한 결과, 단기 투자와 장기 투자 간의 차이는 없다고 나타났지만 정보보안 투자를 하지 않는 기업과는 차이가 있다고 나타났다. 이는 정보보안 투자가 무형적이고 가시적인 성과를 보이지 않더라도 사고 대응을 위한 예방적 차원으로서 중요성을 가진다고 할 수 있다.

<표 4> 정보보안 투자 집단 간 사고대응역량 차이 검점

변수	집단	n	평균	표준편차	F	유의확률	사후검정
사고대응역량	투자없음(A)	49	1.53	.400	9.490	.000	A<B,C
	단기투자(B)	35	1.82	.436			
	장기투자(C)	11	2.13	.744			

그리고 기업 규모별로 정보보안에 투자하지 않는 기업과 장단기 투자하는 기업으로 구분하여 이들 간의 차이가 있는지를 확인하였다. 대기업의 경우 투자하지 않는 기업은 3개, 장단기로 투자하는 기업은 6개 기업이다. 중소기업의 경우 투자하지 않는 기업의 경우 27개 기업이었고 장단기 투자하는 기업은 19개 기업이었다. 벤처기업의 경우 정보보안에 투자하지 않는 기업은 19개 기업이었으며 장단기 투자하는 기업은 21개 기업으로 나타났다.

<표 5>를 살펴보면 대기업, 중소기업, 벤처기업 모두 정보보안에 투자하는 기업이 투자하지 않는 기업보다 사고대응 역량이 높게 나타났다. 95% 유의수준에서 장단기 투자 기업과 투자하지 않는 기업 간의 역량 차이가 있다고 나타났으며 가설 2는 채택되었다. 비록 기업 정보유출을 경험하였기 때문에 큰 폭의 점수 차이가 있는 것은 아니지만 유의미한 결과가 있다고 나타났다.

<표 5> 기업규모별 정보보안 투자 유무에 따른 정보보안 사고대응역량 차이 분석

구분	평균		표준편차		t	유의확률
	투자 없음	장단기 투자	투자 없음	장단기 투자		
대기업	1.66	2.58	.288	.491	-3.514	.011
중소기업	1.51	1.76	.427	.386	-2.025	.049
벤처기업	1.52	1.83	.389	.532	-2.094	.043

4.3.2 정보보안 사고대응 역량 회귀분석

관리적 보안, 기술적 보안, 물리적 보안의 세 가지 보안 유형이 기업의 정보보안 사고 대응역량에 미치는 결과를 살펴보기 위하여 회귀분석을 실시하였다. 회귀분석 결과는 <표 6>에 나타내었다.

정보보안 사고 대응역량에 미치는 유의한 영향으로는 관리적 보안, 기술적 보안, 물리적 보안 모두 중요하다고 나타났다. 관리적 보안의 t값은 3.236(p=.002)으로 정(+)의 영향을 미치는 것으로 나타났다. 기술적 보안의 t값은 4.529(p=.000)로 정(+)의 영향을 미치는 것으로 나타났다. 물리적 보안의 t값은 3.973(p=.002)으로 정(+)의 영향을 미치는 것으로 나

타났다. 회귀식에 대한 설명력으로는 31.8%를 보이고 있다. 그리고 F값은 15.592(p=.000)으로 나타났으며 Dubin-Watson=1. 658로 잔차들 간에 상관관계가 없어 회귀모형이 적합한 것으로 나타났다.

이를 살펴보면 정보보안 유출 대응역량을 위해서는 기술적 보안을 가장 중요시 여겨야 하는 것으로 나타났다. 그리고 물리적 보안, 관리적 보안 순으로 영향력이 높게 나타났다. 이는 사회기술시스템 관점 중 기술시스템으로서 기술과 직무를 중요시하여, 기업들이 정보자산 관리를 할 필요가 있다고 판단된다.

<표 6> 정보보안 사고 대응역량의 회귀 분석 결과

요인	비표준화계수		표준화 계수	t	유의 확률
	B	표준오차			
(상수)	2.188e-17	.085			
관리적보안	**.276**	**.085**	**.276**	**3.236**	**.002**
기술적보안	**.386**	**.085**	**.386**	**4.529**	**.000**
물리적보안	**.339**	**.085**	**.339**	**3.973**	**.000**
R^2=.340 수정된 R^2=.318 F=15.592(0.000) Durbin-Watson=1.658					

다음은 기업 규모별로 정보보안의 세 가지 유형의 중요성이 서로 다르게 나타나는지를 검정하고자 한다. 이는 앞서 정보보안의 투자가 기업 규모에 상관없이 모두가 동일한 요소에 정보보안 투자를 집중하기 보다는 자신의 기업 규모와 사업의 맞추어 투자해야 할 보안 유형이 다르다는 것이다. 이에 따라 대기업, 중소기업, 벤처기업으로 집단을 구분하여 별도의 회귀분석을 실시하였다. 이에 대한 내용은 <표 7>에 나타내었다.

우선 대기업에서 정보보안 유출사고 대응역량의 회귀분석을 살펴보면 비록 샘플수가 9개로 적어 표본의 대표성이 부족할 수 있다. 하지만 기존 이정환・정병호・김병초[5]의 연구에서 대기업의 샘플이 150개였으며 이중 9개 기업의 정보유출 피해 경험을 가지고 있었다. 샘플 수는 적지만 모형의 적합성과 설명력에서 회귀 모형이 충족되어 이에 <표 7>에 대기업의 내용을 포함하였다.

<표 7> 기업규모별 정보보안 사고 대응역량의 회귀 분석 결과

구분	요인	비표준화계수		표준화 계수	t	유의확률
		B	표준 오차			
대기업	(상수)	.232	.512			
	관리적보안	**4.084**	**1.172**	**1.603**	**3.484**	**.018**
	기술적보안	.514	.456	.230	1.127	.311
	물리적보안	-1.190	.647	-.890	-1.839	.125
	R^2=.838 수정된 R^2=.741 F=8.627(0.020) Durbin-Watson=1.318					
중소기업	(상수)	-.036	.119			
	관리적보안	.125	.112	.153	1.113	.272
	기술적보안	**.190**	**.123**	**.358**	**2.594**	**.013**
	물리적보안	**.284**	**.124**	**.314**	**2.281**	**.028**
	R^2=.214 수정된 R^2=.157 F=3.803(0.017) Durbin-Watson=1.656					
벤처기업	(상수)	-.067	.127			
	관리적보안	**.314**	**.122**	**.368**	**2.571**	**.014**
	기술적보안	**.302**	**.131**	**.333**	**2.303**	**.027**
	물리적보안	.223	.129	.252	1.732	.092
	R^2=.268 수정된 R^2=.207 F=4.389(0.010) Durbin-Watson=1.696					

대기업의 내용을 살펴보면 관리적 보안이 정보보안 유출사고 대응역량으로서 중요하다고 나타났다. 관리적 보안의 t값은 3.484(p=.018)로 정(+)의 영향을 미치는 것으로 나타났다. 회귀식에 대한 설명력으로는 74.1%로 나타났으며 F값은 8.627(p=0.020), Dubin-Watson=1.318로 잔차들 간에 상관관계가 없어 회귀모형이 적합한 것으로 나타났다.

두 번째로 중소기업에서 정보보안 유출사고 대응역량의 회귀분석을 살펴보면 기술적 보안과 물리적 보안이 정보보안 유출사고 대응역량으로서 중요하다고 나타났다. 기술적 보안의 t값은 2.594(p=.013)으로 정(+)의 영향을 미치는 것으로 나타났다. 물리적 보안

의 t값은 2.281 (p=.028)로 정(+)의 영향을 미치는 것으로 나타났다. 회귀식에 대한 설명력으로는 15.7%로 나타났으며 F값은 3.803(p=0.017), Dubin-Watson=1.656으로 잔차들 간에 상관관계가 없어 회귀모형이 적합한 것으로 나타났다.

마지막으로 벤처기업에서 정보보안 유출사고 대응역량의 회귀분석을 살펴보면 기술적 보안과 관리적 보안이 정보보안 유출사고 대응역량으로서 중요하다고 나타났다. 기술적 보안의 t값은 2.303(p=.027)으로 정(+)의 영향을 미치는 것으로 나타났다. 관리적 보안의 t값은 2.571 (p=.014)로 정(+)의 영향을 미치는 것으로 나타났다. 회귀식에 대한 설명력으로는 20.7%로 나타났으며 F값은 4.389(p=0.010), Dubin-Watson=1.696으로 잔차들 간에 상관관계가 없어 회귀모형이 적합한 것으로 나타났다.

이를 통한 결과를 살펴보면 기업규모에 따라 보안 투자 유형이 달라져야 하는 것을 확인 할 수 있다. 즉, 가설 3은 채택되었으며, 기업 규모에 따라서 집중 투자해야 할 보안 유형을 합리적으로 판단할 필요가 있겠다.

4.3.3 기업 기밀정보 유출 수단 우선순위 분석

기업규모별로 기밀정보가 어떤 수단에 의해 유출되었는지를 살펴보았다. 기밀유출 수단 유형은 복수응답으로 체크 받았다. 이에 대한 내용은 <표 8>에 나타내었다.

분석 내용을 확인해보면 복사, 절취가 기업 규모와 상관없이 가장 많이 정보유출 수단으로 작용되었다는 것을 알 수 있다. 대기업이 5건, 중소기업이 17건, 벤처기업이 23건으로 복사, 절취로 인한 정보 유출의 피해가 있었다고 응답하였다. 그 다음으로는 핵심인력 스카우트에 의한 기밀 정보가 유출되었다고 중소기업이 11건, 벤처기업이 16건으로 응답하였다. 세 번째로는 email, 합작사업과 공동연구 순으로 대기업이 2건, 중소기업이 9건, 벤처기업이 9건으로 정보 유출 수단으로 작용되었다고 나타났다.

<표 8> 정보유출 수단의 우선순위 분석

구분	대기업	중소기업	벤처기업
복사, 절취	5	17	23
e-mail	2	9	9
시찰 및 견학	2	2	3
전화, Fax 도청	0	2	2
핵심인력 스카우트	0	11	16
합작사업, 공동연구	0	8	7
관계자 매수	2	2	7
컴퓨터해킹	1	1	0

Ⅴ. 결론

5.1 연구결론

본 연구의 출발점은 기업의 기밀정보 유출을 경험한 기업들의 정보보안 대응에 미치는 보안 유형을 살펴보고, 정보보안 투자의 중요성을 강조하고자 시작하였다. 대다수의 기업들이 최근에 이르러 정보보안의 실패가 기업의 자산의 손실과 경쟁력을 크게 약화시킨다는 사례를 언론이나 동종 산업에서 인지하기 시작하였다. 따라서 정보보안 사고의 경험을 가진 기업들의 보안의 실패를 탐지하고 이에 따른 사고 예방을 위한 관리적, 기술적, 물리적 보안 역량을 마련할 필요가 있다. 또한, 정보보안 사고를 사전에 방지하고 보안 투자를 집중적으로 실행하고 있는 기업들이 더 나은 대응역량이 있다는 것을 실증 분석을 통해서 강조하였다. 연구 결과에서도 보안사고 및 기밀정보 유출을 방지하기 위해서 기업 규모와 상관없이 투자의 중요성이 필요하다고 밝혀졌다. 이러한 실증연구의

결과를 요약하면 다음과 같다.

첫째, 기업규모별로 정보보안을 투자하는 기업과 그렇지 않는 기업 간의 정보보안 사고 대응력의 차이를 확인하였을 때 정보보안을 투자한 기업이 그렇지 않는 기업보다 보안 역량이 강화된다고 나타났다. 이는 관리적, 기술적, 물리적 보안 투자가 보안 사고를 예방하고 대응하는데 도움이 된다고 볼 수 있는 결과이다.

둘째, 정보보안 사고 대응역량에 있어 관리적 보안, 기술적 보안, 물리적 보안의 투자가 모두 중요하다고 나타났다. 세 가지 보안 유형의 투자가 모두 유의한 결과로 나타났으며 이 중 기밀 유출을 경험한 기업들은 정보보안을 강화에 집중해야 할 부분으로서 기술적 보안이 제일 필요하다고 확인되었다. 기밀정보가 IT 기술로 유출되는데 기인한 결과라고 볼 수 있으며 자료의 복사, 이동과 함께 해킹과 로그를 추적할 수 있는 기술적 역량이 필요하다는 결과이다.

마지막으로, 기업 규모별로 정보보안 사고 대응역량에 필요한 보안 유형이 다르다고 나타났다. 세 가지 정보보안 유형이 모두 중요하지만 기업규모별로 중점을 두고 투자해야 할 보안 유형이 다르다는 것이다. 대기업의 경우 관리적 보안을 중요시해야 한다면 중소기업의 경우 기술적, 물리적 보안을 중요시하고, 벤처기업은 기술적, 관리적 보안에 집중 투자해야 된다는 결과가 나타났다. 이는 선도 기업의 보안 투자에 집중도 필요하지만 기업 규모와 사업관리를 위한 보안투자 유형을 선택할 필요가 있다는 것을 밝혀냈다.

5.2 연구의의

본 연구의 이론적 시사점으로는 고전의 사회기술시스템 이론 관점을 정보보안과 결합하여 비즈니스에서 정보보안의 중요성을 강조할 수 있었다. 비즈니스는 인적자원과 조직, IT시스템의 결합에 의해서 환경 변화에 대처해 나아간다. 이에 변화되는 환경에서 변화되는 정보를 올바르게 이해하고, 기업 내부의 핵심정보를 체계적이고 합리적으로 관리할 능력이 요구된다. 따라서 기업은 사회기술시스템 이론처럼 구조, 사람, 기술, 직무를 정보보안을 결합하여 이해할 필요가 있겠다. 사회기술시스템 이론은 정보기술을 활용하는 모든 기업에 해당되는 요소로서 기술과 직무, 구조와 사람을 정적인 관점, 동적인 관점 모두에서 판단하여 기업에 적용할 필요가 있겠다.

다음으로 본 연구의 실무적 시사점으로는 정보 유출을 경험한 기업일수록 기술적 보안에 초점을 두어 정보보안 투자를 진행할 필요가 있겠다. 이를 위해서는 우선적으로 정보 유출의 재 발생되는 위험 요소를 방지하기 위해서는 인적자원들이 활용하는 IT의 체계적 관리 방안을 마련할 필요가 있다. 마지막으로 정보 누출의 피해를 최소화하기 위해서 기업의 보안 제도적 장치를 구축하고 인적자원의 정보 보안 교육을 정기적으로 운영할 필요가 있겠다.

5.3 향후 연구 방향

본 연구는 2010년 한국중소기업청에서 실시한 2010년 기술보안 역량 및 기술유출 실태조사표를 기초로 하였으며 국가 데이터를 토대로 실증연구를 하였다. 이에 연구자가 직접 가공한 1차 데이터가 아닌 2차 데이터로서 의미가 있다. 하지만 2011~2016년까지 기술유출 피해 기업의 조사가 진행되지 않아 정보누출 피해 규모에 대한 데이터가 존재하지 못해 과거와 현재를 비교하지 못하였다. 이에 향후 연구에는 2010년도 정보 피해와 비교할 수 있는 데이터를 확보하여 기업에서 중요시 여겨야 할 보안 유형이 무엇인지 확인할 필요가 있다.

또한, 본 연구에서는 정보보안의 중요성에 있어서

세 가지 유형 중 기술보안이 중요하다는 당연한 결과가 나타났다. 이는 예상되는 결과이지만 이를 실천하고 매년 정보기술 보안 업데이트를 정기적으로 하지 않는 기업들에게 재차 상기시키는데 목적이 있었다. 이에 당연한 결과물을 기본적 자세에서 중요성을 인지시키는데 본 연구는 기여점이 있다고 판단된다.

참고문헌

[1] 정병호・김병초, “중소기업의 IT 투자에 따른 정보품질과 프로세스 개선에 관한 연구,” 중소기업연구, 제36권, 제4호, 2014b, pp. 47-71.

[2] 정병호・권태형, “소셜 미디어는 캐즘(Chasm)과 구매 가치에 얼마나 영향을 미치는가? 채택 집단 간 정보력 및 신뢰도 효과,” 한국IT서비스학회지, 제13권, 제1호, 2014, pp. 221-251.

[3] Nosworthy, Julie D., “Implementing Information Security In The 21 st Century—Do You Have the Balancing Factors?,” Computers & security, Vol. 19, No. 4, 2000, pp. 337-347.

[4] Stoneburner, G., Goguen, A., & Feringa, “A. Risk Management Guide for Information Technology Systems (Special Publication 800-30),” Gaithersburg, MD: National Institute of Standards and Technology, 2002.

[5] 이정환・정병호・김병초, “기업 보안 유형에 따른 보안사고 대응역량: 사회기술시스템 이론 관점에서,” 한국IT서비스학회지, 제12권, 제1호, 2013, pp. 289-208.

[6] Kotulic, Andrew G., and Jan Guynes Clark., “Why there aren’t more information security research studies,” Information & Management, Vol. 41 No. 5, 2004, pp. 597-607.

[7] Ifinedo Princely., “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory,” Computers & Security, Vol. 31, No. 1, 2012, pp. 83-95.

[8] Anderson, Evan E., and Joobin Choobineh., Enterprise information security strategies, Computers & Security, Vol. 27, No. 1, 2008, pp. 22-29.

[9] 최재영, “IT 투자 정당화 요인에 관한 연구,” 디지털정보산업학회지, 제11권, 제4호, 2015, pp. 177-187.

[10] Mattord, Herbert, and Michael Whitman., “Regulatory Compliance in Information Technology and Information Security,” AMCIS 2007 Proceedings, 2007.

[11] Merkow, Mark S., and Jim Breithaupt., Information security: Principles and practices. Pearson Education, 2014.

[12] 신현조・이경복・박태형, “인적 및 직무특성과 보안교육 이수율 및 사이버테러 대응과의 연관성 분석,” 디지털산업정보학회지, 제10권, 제4호, 2014, pp. 97-107.

[13] Fred, C., “Managing network security – Part 5: Risk management or risk analysis,” Network Security, Vol. 1997, No, 4, 1997, pp 15-19.

[14] Clegg, Chris W., Sociotechnical principles for system design, Applied ergonomics, Vol. 31, No. 5, 2000, pp. 463-477.

[15] Heller, Frank., Socio-technology and the environ -ment, Human Relations, Vol. 50, No. 5, 1997, pp. 605-624.

[16] Seni, Dan Alexander., The sociotechnology of

sociotechnical systems: Elements of a theory of plans, Studies on Mario Bunge's Treatise, 1990, pp. 431-454.

[17] Trist, E., "The evolution of socio-technical systems," a conceptual framework and an action research program, Occasional paper, 1981.

[18] Guo, Ken H., Security-related behavior in using information systems in the workplace: A review and synthesis, Computers & Security, Vol. 32, 2013, pp. 242-251.

[19] Yeh, Quey-Jen, and Arthur Jung-Ting Chang., "Threats and countermeasures for information system security: A cross-industry study," Information & Management, Vol. 44, No. 5, 2007, pp. 480-491.

[20] Vacca, John R., Computer and information security handboo,. Newnes, 2012.

[21] NIST, Information Security Handbook: A Guide for Managers, 2006.

[22] Pugh, Derek S., and David J. Hickson., Writers on organizations, Penguin UK, 2007.

[23] Baskerville, Richard, and Mikko Siponen., An information security meta-policy for emergent organizations, Logistics Information Management, Vol. 15.5, No. 6, 2002, pp. 337-346.

[24] Hsu, Jack Shih-Chieh, et al., "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness, Information Systems Research," Vol. 26, No. 2, 2015, pp. 282-300.

[25] Von Solms, Basie, Corporate governance and information security, Computers & Security, Vol. 20, No. 3, 2001, pp. 215-218.

[26] Hu, Qing, et al., "Managing employee compliance with information security policies: the critical role of top management and organizational culture," Decision Sciences, Vol. 43, No. 4, 2012, pp. 615-660.

[27] Ifinedo, Princely., "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," Information & Management, Vol. 51, No. 1, 2014, pp. 69-79.

[28] Post, Gerald, and Albert Kagan, "Management tradeoffs in anti-virus strategies," Information & Management, Vol. 37, No. 1, 2000, pp. 13-24.

[29] Whitman, Michael, and Herbert Mattord., Management of information security, Nelson Education, 2013.

[30] 중소기업청, "보안 컨설턴트용 실무가이드북," 중소기업기술정보진흥원, 2007.

[31] Vance, Anthony, Mikko Siponen, and Seppo Pahnila., "Motivating IS security compliance: insights from habit and protection motivation theory," Information & Management, Vol. 49, No. 3, 2012, pp. 190-198.

[32] 정병호・김병초, "IT 프로젝트 모방 투자 유형에 따른 성과 차이 연구," 한국IT서비스학회지, 제11권, 제3호, 2012, pp. 205-225.

[33] Hair, Joseph F., Multivariate data analysis, 2010.

■ 저자소개 ■

정 병 호
Jung Byoungho

2015년 9월~현재
한국외국어대학교 경영학 박사
2011년 3월 한국외국어대학교 경영정보학과
(경영학 석사)
2009년 3월 한국외국어대학교 경영정보학과
(경영학 학사)

관심분야 : IT투자, 정보보안, 정보윤리,
사물인터넷, 빅데이터
E-mail : jung. hmis@gmail.com

논문접수일: 2016년 6월 1일
수 정 일: 2016년 6월 10일
게재확정일: 2016년 6월 17일