Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.1, Feb. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.1.269

정보보안 투자가 침해사고에 미치는 영향에 대한 실증분석 : 정보보안 교육 서비스 투자를 중심으로

이 한 솔,† 채 상 미‡
이화여자대학교 경영대학 경영학부

An Empirical Study of Relationship between Information Security Investment and Information Security Incidents : A Focus on Information Security Training, Awareness and Education Service Sector

Hansol Lee,† Sangmi Chai‡
Ewha womans' university, Ewha school of Business

요 약

정보화 사회에서 핵심 가치로 평가받고 있는 자원은 정보 그 자체이다. 이런 이유로 기업의 가치 있는 정보를 노리는 시도가 많아지며 정보보안 사고가 급증하고 있다. 기업에서는 정보보안 사고를 예방하기 위해 다양한 정보보안 부문에 투자하고 있으나, 어떤 부문에 대한 투자가 정보보안 사고를 감소시키는 데에 직접적으로 기여하는지는 잘 알지 못한 채 투자하고 있다. 기업의 대표적인 정보보안 투자 부문인 제품뿐만 아니라 대표적인 정보보안 서비스 사업으로 각광받고 있는 정보보안 교육 및 훈련, 보안관제 서비스, 그리고 취약점 분석의 투자 효용을 알아보기 위해 본 연구를 진행하였다. 한국 인터넷 진흥원의 2014년 정보보호 실태 조사의 원자료를 이용하고, 총 정보보안 사고 건수를 종속변수로 두고 음이항분포 회귀분석을 실시한 결과 교육 서비스와 취약점 분석 서비스가 정보보안 사고를 줄이는 데에 유의미하게 기여하는 것으로 판단되었다. 이 연구는 학문적으로는 정보보안 경제학을 이론적 배경으로 하여 정보보안 투자 부문의 실제 효용을 파악한 연구이며, 실증적으로는 조직에서 한정된 자원을 정보보안 투자에 배분할 때 효율적인 의사결정을 하는 데에 지침을 제공할 수 있는 연구이다.

ABSTRACT

Many organizations are threatened by numerous information security attacks which are resulting in information security incidents. To prevent information security incidents, organizations invest on various information security measures like information security products, monitoring services and security training and educations. However they do not have enough knowledge about measurable utilities of information security investments. Since there is little studies empirically examining the effect of information security investments, this research aims to find out utilities of information security investment. We especially focuse on information security service investments. This study examined the data from the survey on information security for business sector which was conducted by Korean information & security agency. We utilized negative binomial regression model, which is a suitable model for over-dispersed count data. We found out that an investment on information security education and vulnerability testing have direct impact on reducing information security incidents. This research academically contributed to shed light on the utility of information security investments on reducing information security

Received(12. 22. 2017), Modified(02. 02. 2018), Accepted(02. 03. 2018)

† 주저자, 1989luna@ewhain.net
‡ 교신저자, smchai@ewha.ac.kr(Corresponding author)

incidents. This research practically contributed to providing information security investment guideline for organizations which want to reduce information security incidents efficiently.

Keywords: information security investment, information security product, information security service, security education, training, and awareness (SETA) programs, security monitoring, vulnerability testing

I. 서 론

정보화 사회에서, 정보는 우리 사회의 핵심가치로 여겨지고 있다[3]. 정보가 핵심가치로 여겨지게 되면서, 최근 기업의 가치 있는 정보를 노리고 발생하는 보안 사고가 급증하고 있다[2]. 한국인터넷진흥원의 2016년 정보보호 실태조사 결과에 따르면 기업에서는 악성 코드 공격, 스파이웨어, 랜섬웨어, 해킹, 디도스(DDoS) 등 다양한 정보 침해 사고를 경험하고 있으며, 2015년에 비해 정보 침해 사고를 당한 기업의 수는 1.3% 증가하였다 [1]. 보안 사고가 증가하는 추세에 맞추어 정보보안 예산을 편성하고 정보 보안에 투자하는 기업들이 증가하고 있다[1].

기업에서는 정보보호 수준을 향상시키기 위해 여러 방안을 사용하고 있다. 기업에서는 정보보호수준을 향상시키기 위해 정보 보호 전담조직을 설치하고 [37] 정보보호 투자를 실시한다. 기업들의 정보보호 투자 분야는 정보보안 정책 수립, 최고 정보보안 책임자 고용, 임직원에 대한 정보보호 교육 및 트레이닝 교육 실시, 모니터링 등을 포함한다[4]. 기업이 정보보안에 자원을 투입하면 정보보안 취약성이 감소하여 정보보안 사고 발생이 감소한다는 이론적 배경은 존재하지만[7], 실제로 정보보안의 세부 분야 중 어느 분야에 투자하였을 때 정보보안 사고의 확률이 가장 많이 감소하는지 밝힌 연구가 없다. 따라서 기업에서는 정보보안 에 투입할 수 있는 한정된 자원이 주어졌을 때 어디에 투자하는 것이 효율적인지 정확히 알지 못한 채 투자를 진행하고 있다[6]. 특히, 최근에는 기업에서 정보보안 컨설팅 및 보안 관제 사업 등에 대한 투자를 폭발적으로 증가시키고 있지만 [18], 기업에서는 정보보안 서비스 투자 효용을 정확히 알지 못한 채 투자를 진행하고 있어 관련 연구가 필요한 상황이다. 따라서 기업의 여러 가지 정보보안 투자 세부 항목 중 어느 곳에 투자하는 것이 가장 효율적인지를 파악하고, 이를 바탕으로 기업에게 정보보안 투자 지침을 제공하기 위한 연구가 꼭 필요한 실정이다.

본 연구는 Gordon과 Loeb이 제시한 이론적 배경에 근거하여 기업이 정보보안에 투자하였을 때 정보보안 사고가 감소하며, 기업의 다양한 정보보안 투자 항목 중 어떤 항목이 가장 정보보안 사고를 감소시키는 데에 기여하는지 파악하기 위해 진행되었다. 특히, 이 연구에서는 정보보안 투자의 여러 세부 항목 중 제품 구매, 임직원에 대한 정보보안 교육 및 훈련, 취약점 분석, 모니터링이 정보보안 사고에 미치는 영향을 중심으로 탐구하고자 한다. 이를 위해 본 연구에서는 관련 연구 및 이론적 배경을 소개하고, 연구에 이용된 데이터와 방법론을 기술한 후, 분석 결과와 논의사항, 결론에 대해 서술하고자 한다.

II. 이론적 배경

2.1 정보보안 투자

Gordon 과 Loeb은 2002년 발표한 연구에서 기업의 정보보안 투자에 대한 기본 이론을 제시하였다. 그들은 한 기업의 최적의 정보보안 투자 금액은 정보보안 사고 발생으로 예상되는 총 피해 비용의 약 36.7%라고 제시한 바 있으며, 최적의 투자 금액에 도달할 때까지는 정보보안 투자를 증가시킬수록 정보보안 사고의 확률이 감소한다고 설명하였다 [7]. 이후 Gordon과 Loeb이 제시한 기본 이론을 보완하거나 수정한 연구는 많이 제시되었지만[8,9,10], 실제로 Gordon과 Loeb이 제시한 최적 투자 금액의 타당성을 확인하기 위해 진행된 실증 연구는 아직 존재하지 않는다. 대신 정보보안 사고 발생으로 인한 기업의 손실 또는 정보보안 투자로 인한 수익을 기업의 시장 가치를 이용하여 측정한 연구가 존재한다. 국내 기업의 경우 정보보안 사고가 발생할 경우 기업의 시장 가치가 하락하였다[11, 12, 13]. 미국 기업의 데이터를 이용한 같은 방식의 연구에서는 기업이 정보 보안에 투자하였음을 공시하였을 때 기업의 주식 가치가 유의미하게 상승한 것이 확인되었다[5, 14].

또한 정보보안 투자 의사결정 시 효율적인 의사결정을 내릴 수 있도록 평가 기준을 제시하고 실제로 이 평가 기준을 활용하여 실증 연구를 실시한 연구들이 존재한다. AHP 기법을 활용하여 정보보호 제품

에 대한 투자를 결정하는 모델이 제시된 바 있으며[15], 대기 확률 모형을 활용하여 해당 조직에 적합한 보안 투자 포트폴리오를 구성하는 방안을 제시한 연구가 존재한다[16].

III. 문헌 연구 및 가설 설정

3.1 정보보안 제품

정보보안 제품에 대한 투자는 많은 기업들이 정보보안 사고를 겪은 후 가장 손쉽게 투자하는 분야 중 하나이다 [31]. 2015년 기준, 국내 정보보안 시장 전체의 매출 중 77.3%를 정보보안 제품이 차지하고 있다 [18]. 정보보안 제품은 네트워크 보안, 시스템 보안, 콘텐츠/정보 유출 방지 보안, 암호/인증, 보안 관리 제품으로 세분화할 수 있다 [17]. 정보보호의 대상은 데이터 저장장치, 호스트 컴퓨터 응용 프로그램, 유선 및 무선 통신망, 라우터, PC 및 워크스테이션 등을 포함하며[20] 중요한 데이터를 보유하고 있거나 기밀로 유지해야 할 사항을 보유하고 있는 기업은 철저한 정보보안 유지를 위해 강력한 PC/서버 보안, 네트워크 보안, 스팸필터, 정보유출방지 솔루션, WEB 보안을 위한 솔루션 구축 등에 자원을 투입하여 보안을 강화하며[19], 데이터의 손실을 막기 위해 노력하고 있다. 정보보안 제품을 구입하는 기업은 정보보안 사고를 감소시키는 것을 기대하며 정보보안 제품을 구입하고 있다는 사실을 반영하고, 기업의 정보보안 제품에 대한 투자와 실제 사고와의 관계를 확인하기 위해 본 연구에서는 다음과 같은 가설을 제시한다.

H1: 정보보안 제품에 대한 투자와 정보보안 사고 횟수는 음의 상관관계를 갖는다.

3.2 정보보안 교육

한국인터넷진흥원의 정보보호 산업 분류에 따르면, 정보보안 교육 사업은 정보보안 서비스 사업에 해당한다[17]. 정보보안 교육의 목적은 담당자 및 직무에 맞게 정보보안 교육을 실시하여 조직 구성원들의 정보보안에 대한 인식을 높이고 정보보안 정책을 준수하여 정보보안 사고를 최소화 하는 데에 있으며, 기본적인 정보보호 기능 관련 교육뿐만 아니라 기업의 정보보호 정책에 대한 교육 및 홍보까지 정보보호 교육에 포함된다[19].

정보보안 교육에 투자하면 직원들의 정보보안 인식이 높아질 뿐만 아니라 정보 시스템을 이용하는 데에 있어 실수가 감소한다[21]. 정보보안 교육을 실시하면 조직의 구성원들은 정보보안의 중요성을 이해하며, 정보시스템을 보다 올바르게 사용할 수 있게 된다 [22]. 또한 정보보안 교육을 실시하면 조직 구성원들의 정보보안에 대한 인식이 긍정적으로 변화하며, 이는 실제 정보보안 정책 준수로 이어진다[23]. 또한 조직 구성원들의 높은 보안 의식은 높은 보안 효과로 이어진다[36]. 따라서 본 연구에서는 기업이 정보보안 교육에 투자하였을 때, 기업의 정보보안 사고가 줄어들 것이라 가정하고 다음의 가설을 제시한다.

H2: 정보보안 교육에 대한 투자와 조직의 정보보안 사고 횟수는 음의 상관관계를 갖는다.

3.3 취약점 분석

한국인터넷진흥원의 정보보호 산업 분류에 따르면, 취약점 분석 사업은 정보보안 컨설팅의 세부분야 중 하나로서 정보보안 서비스 사업에 해당한다[17]. 보안 취약점은 사이버 공격자에 의해 악용되어 기업에 치명적인 손실을 입힐 수 있으므로, 기업에서는 지속적으로 취약점을 제거하고 대비하는 것이 중요하다[24]. 취약점을 분석하기 위해서는 네트워크의 구성을 식별하고, 어플리케이션을 스캔하고 네트워크 취약성을 점검한 후 시스템의 취약성을 점검하는 과정이 필요하다[25]. 네트워크 구성 식별 단계에서는 실질적인 네트워크의 정보와 구조를 확인하며, 애플리케이션 스캔 단계에서는 네트워크에 연결된 여러 가지 시스템의 서비스 포트를 점검한다. 네트워크 취약점 점검 단계에서는 기술적인 보안 취약점과 비기술적인 보안 허점들을 식별하며 시스템 취약점 점검 단계에서는 시스템 보안 정책 설정, 구성 파일 등에 대한 취약점을 확인한다. 일련의 과정을 거쳐 확인된 취약점을 이후에 보완하는 과정이 꼭 필요하며, 정기적이고 취약점 점검으로 최신 취약점을 파악하여 사고를 예방할 수 있다[26]. 따라서 본 연구에서는 다음과 같은 가설을 제시한다.

H3: 정보보안 취약점 분석에 대한 투자와 조직의 정보보안 사고 횟수는 음의 상관관계를 갖는다.

3.4 정보 보안 관제

한국인터넷진흥원의 정보보호 산업 분류에 따르면, 정보 보안 관제 사업은 정보보안 서비스 사업에 해당한다[17]. 정보 보안 관제는 조직의 정보 자원을 보호하기 위해 보안 이벤트 및 로그를 감시하고 분석 및 대응하는 일련의 업무를 의미한다[27]. 보안 관제를 성공적으로 수행하기 위해서는 조직이 보유한 모든 시스템을 실시간으로 모니터링하고 즉각 대응할 수 있는 역량이 필요하다. 이를 위해 조직에서는 보안 관제 센터를 구축하고 운영하거나 타 기관에 보안 관제 업무를 위탁 수행한다. 주요 관제 대상은 유무선 네트워크, 웹서비스 및 데이터베이스, 엔드 포인트 및 콘텐츠이며, 기업에서는 사고가 발생하였을 때를 대비하여 백업 시스템을 마련하며, 실제 사고나 테러가 발생하였을 때에는 시스템을 복구하고, 사고를 분석하여 대책을 마련해야 한다[27]. 정보 보안 관제를 성공적으로 수행하면 신규 보안위협에도 선제적으로 대응할 수 있어 각종 보안 위협에서 조직을 보호할 수 있다 [28]. 따라서 본 연구에서는 다음과 같은 가설을 제시한다.

H4: 정보보안 관제에 대한 투자와 조직의 정보보안 사고 횟수는 음의 상관관계를 갖는다.

IV. 데이터 및 연구 방법론

4.1 데이터

연구를 진행하기 위해, 한국인터넷진흥원의 2014 정보보호 실태조사 기업부문의 원자료(raw data)를 이용하였다. 연구에 이용된 원자료는 2013년 7월 1일부터 2013년 9월 30일 사이 한국인터넷진흥원에 의해 7089개 국내 기업을 대상으로 수집되었다. 본 연구에서는 설문에 응한 7089개 기업 중, 기업 정보보안 투자에 대한 설문 항목에 응답하지 않은 3개 기업을 제외하고 7086개 기업을 대상으로 분석을 실시하였다. 연구를 위해 전체 설문 항목 중 기업의 크기와 업종, 기업의 정보보안 수준을 알 수 있는 항목, 정보보안 투자에 해당하는 측정항목을 추출하였으며, 이를 Table. 1.에 정리하였다.
문 4번의 응답 항목 7번은 '정보보안 예산 편성이 없음' 항목이기 때문에 이를 0으로 재코딩하여 7점 척도로 바꾸었으며, 총 IT 예산 중 정보보안 제품 및 서비스 투자와 교육훈련 투자 비율을 구하기 위해 설문 4번 항목과 4-1번 항목을 이용하였다. 4번 항목과 4-1번 항목의 곱을 통하여 총 IT 예산 중 정보보안 제품 및 서비스 투자와 교육훈련 투자 비율을 구해 이를 각각 변수로 설정하였다. 본 설문조사에서는 정보보안 서비스 투자 중 정보보안 컨설팅과 정보보안 관제 서비스만을 정보보안 서비스로 분류하여 설문을 실시하였으며, 정보보안 교육은 따로 투자 항목으로 구성하였으며, 유지관리, 인증 서비스 사업은 서비스 산업으로 분류하지 않아 투자 비율을 정확히 추정할 수 없었다. 따라서 본 연구에서는 정보보안 서비스 사업 투자 항목에 대한 데이터를 원자료에서 다시 추출하여 연구를 진행하였다. 7086개 기업 중 정기적인 취약점 점검을 수행하는 기업을 1로 코딩하고, 그렇지 않은 기업을 0으로 재코딩 하였으며, 보안관제 사업을 수행하고 있는 기업을 1로, 그렇지 않은 기업을 0으로 재코딩하여 데이터를 정리하였다. 또한 Table 2.와 3은 Table 1에 제시된, 본 연구의 가설 4개를 검증하기 위해 추출한 주요 변수에 대한 기초 통계를 정리하여 제시한 표이다.

Table 1. Construct, survey question and scale

construct	question	scale
Information security investment	Q 4) In 2013, what percentage of the total IT budget did you invest on information security?	1) less than 1% 2) 1% to 3% 3) 3% to 5% 4) 5% to 7% 5) 7% to 10% 6) more than 10 % 7) We don't invest on information security.
Detail of Information security investment	Q 4-1) In 2013, what percentage of total information security investment did you pay on each sector of information	Product and its service Education and training : Write

	security?(If you pick 1 to 6 at Q4, then you have to answer)	down percentage of the investment
regular information security vulnerability test	Q 12) Do your organization regularly conduct vulnerability test?	1) We do regularly 2) We do irregularly 3) etc 4) We don't conduct vulnerability testing
information security management	Q 9) What kind of countermeasures does your organization utilize to maintain information security? Please draw check mark at the blank if you utilize those countermeasures.	1) We use it 2) We don't use it.
	Q 9-6) information security monitoring and control	
information security incidents	Q 19-1) If your organizations suffer information security incidents, please check on the square box that describes type of information security incidents that you suffer, severity of the incidents and frequency of the incidents.	reporting the number of information security incidents
	1. Computer virus, Worm, and Trojan attack	
	2. Hacking	
	3. DoS(Denial of Service)/DDoS(Distributed Denial of Service) attack	
	4. Adware/spyware infection	
	5. information breach	
	6. ETC	

Table 2. Statistics of investment on product and education

Variable	Investment on product and its service	Investment on education and training
Observation	7086	7086
Average	0.174	0.054
Standard deviation	0.505	0.184
Minimum	0	0
Maximum	6	3.2

Table 3. Statistics of investment on Threat assessment and monitoring

Dummy variable : Threat assessment	Frequency	Percent
We conduct it(1)	1,673	23.61
We don't conduct it(0)	5,413	76.39
Total	7086	100
Dummy variable : Monitoring	Frequency	Percent
We conduct it(1)	884	12.48
We don't conduct it (0)	6,202	87.52
Total	7086	100

분석을 진행하기 전에 통제변수로서 전체 데이터 중 기업의 특성을 나타낼 수 있는 변수를 추출하여 데이터 셋에 추가하였다. 본 연구에서는 전체 설문 중 기업의 업종과 기업 크기에 대한 항목을 추출하였다. 기업의 크기는 기업의 종사자수로 측정하였으며 7점 척도를 이용하였다. 기업의 업종은 총 13개 카테고리로 나누어져 있으나, 이를 금융업과 비 금융업으로 나누어 더미 변수를 형성하였다. 금융업은 금융감독 기관이 요구하는 강력한 가이드라인에 맞춘 정보보호 투자를 적극적으로 수행하고 있기 때문에

[29] 다른 업종과 따로 분석하였다. 또한 기업의 정보보안 수준을 나타낼 수 있는 여러 가지 특성[30] 중 공식적인 정보보안 정책 보유 여부와 정보보안 투자 증가 여부를 추출하여 더미 변수로 형성하였다. 공식적인 정보보안 정책을 보유하고 있다고 응답한 기업을 1로 코딩하고 그 외의 기업은 모두 0으로 재코딩하였으며, 기업들이 지난해에 비해 정보보안 투자를 증가시켰다고 응답한 경우를 1로 코딩하고 그 외의 경우는 모두 0으로 코딩하였다. 통제변수 설문항목은 Table 4.에서 정리하였으며, 해당 변수들에 대한 통계값은 Table 5.와 7에서 정리하였다. Table 6는 모든 변수들 간의 상관관계를 정리한 표이다.

Table 4. Survey question and scale for control variable

Construct	Question	Scale
Firm size	How many employees does your organization have?	1) 1~4 2) 5~9 3) 10~40 4)50 ~249 5)250~499 6)500~999 7) more than 1000
Category of Business	Category of Business	1)Agriculture, Forestry and Fishery 2)manufacture 3)Construction 4)Wholesale 5)Transportation 6)Hospitality 7)Publishing, media, broadcasting and information service 8) finance and insurance 9) real estate and leasing 10)Professional, scientific and technical activities 11) Business facilities management and business support services; rental and leasing activities 12)Membership organizations, repair and other personal services 13) ETC
Information security policy	Q1) Does your organization have information security policy as an official document?	1) We have information security policy as an official document. 2) We don't have the policy yet, we are now establishing information security policy. 3) We don't have information security policy document, but we have some rules to handle information security. 4)We don't have any kind of rules or information security policy.
Increase or decrease of information security investment	Q 4-2) In 2013, did your investment on information security increase or decrease, compared to 2012 ?	1) Increased 2) Decreased 3) No change

Table 5. Statistics of control dummy variables

Dummy variable : Finance industry	Frequency	Percent
Finance(1)	423	5.97
Non-Finance(0)	6663	94.03
Total	7086	100
Dummy variable : Possession of information security policy	Frequency	Percent
We possess it(1)	1700	23.99
We don't possess it (0)	5386	76.01
Total	7086	100
Dummy variable : Increase of information security investment	Frequency	Percent
Increased(1)	448	6.32
Not increased(0)	6638	93.68
Total	7086	100

4.2 연구방법론

본 연구에서는 설문에 참여한 총 7089개 기업 중, 정보보안 투자에 대해 응답하지 않은 3개 기업을 제외한 7086개 기업의 관측치를 이용하였다. 7086개 기업 중 가장 많은 정보보안 사고를 겪은 기업은 총 1008회의 사고를 겪었다. Table 8.은 종속변수인 사고 횟수의 분포를 나타내는 표이다. 종속변수인 정보 보안 사고의 횟수가 가산자료(countable data) 형태이기 때문에, 본 연구에서는 가산자료모형을 이용하였다[32]. 본 연구에서는 여러 가지 가산 자료 모형 중에서도 음이항 회귀 분석 모형(negative binomial regression model)을 이용하여 분석을 진행하였다. 이는 종속 변수인 정보 보안 사고의 횟수에서 분산이 평균보다 매우 큰 과대산포(Overdispersion) 현상이 발생하기 때문에 음이항 회귀 분석 방법을 이용하는 것이 더 적합하기 때문이다[33].

Table 7. Statistics of firm size

Variable	The number of employees
Observation	7086
Average	2.588
Standard deviation	1.514
Minimum	1
Maximum	7

Table 6. Correlation of each variable

	Dummy :Finance	Dummy: Information security policy	Dummy: Increase of investment	Firm size	Product and its service	Education &training	Vulnerability testing	Monitoring
Dummy :Finance	1.0000							
Dummy: Information security policy	-0.0704	1.0000						
Dummy: Increase of investment	-0.0582	0.5084	1.0000					
Firm size	-0.0779	0.4352	0.4551	1.0000				
Product and its service	-0.0587	0.4558	0.9085	0.4360	1.0000			
Education &training	-0.0349	0.3876	0.7428	0.3070	0.4358	1.0000		
Vulnerability testing	-0.0643	0.5413	0.4240	0.3503	0.3804	0.3198	1.0000	
Monitoring	-0.0519	0.4430	0.4351	0.3226	0.4025	0.2942	0.4066	1.0000

Table 8. Frequency of information security incidents

The number of incidents	Frequency	Percentage	Accumulated rate
0	6836	96.47	96.47
1	91	1.28	97.76
2	62	0.87	98.63
3	34	0.48	99.11
4	6	0.08	99.20
5	6	0.08	99.28
6	4	0.06	99.34
8	2	0.03	99.36
9	12	0.17	99.53
10	5	0.07	99.60
11	3	0.04	99.65
12	1	0.01	99.66
13	1	0.01	99.68
14	3	0.04	99.72
15	1	0.01	99.73
16	3	0.04	99.77
18	2	0.03	99.80
19	3	0.04	99.84
20	1	0.01	99.86
24	2	0.03	99.89
28	2	0.03	99.92
30	1	0.01	99.93
104	2	0.03	99.96
125	1	0.01	99.97
218	1	0.01	99.99
1008	1	0.01	100.00

V. 결과 및 논의

5.1 결과

Table 9.는 음이항 회귀분석 결과를 요약한 표이다. 분석 결과 4개의 가설 중 가설 2와 3이 채택되었다. 즉, 기업에서 조직 구성원에 대한 교육 훈련비에 더 많은 자원을 투입할수록 기업의 정보보안 사고가 감소한다. 또한 기업에서 정기적인 취약점 분석을 실시할수록 기업의 정보보안 사고가 감소한다.

이는 취약점을 발견하고 제거하기 위한 취약점 분석이나 조직 구성원들의 정보보안 행동을 증진시킬 수 있는 정보보안 교육에 투자하는 것이 정보보안 사고를 줄이는 데에 효과적이라는 사실을 의미한다. 또한, 정보보호 제품 및 서비스 투자와 모니터링 서비스의 경우 정보보안 사고와 통계적으로 유의한 양적 상관관계가 있다는 것이 확인되었다.

Table. 9. Result of negative binomial regression analysis

Variable	Negative binomial regression coefficient
Dummy :Finance	-3.266***
Firm size	0.002
Dummy: Policy	-0.599***
Dummy: Increase of investment	0.873*
Product and its service	0.534***
Education & training	-1.541**
Vulnerability testing	-1.042***
Monitoring	0.819**
Consistant	-2.204***
Alpha	71.345
Observations	7086

Table 10.은 7086개 기업 중 사고를 경험한 250개 기업만을 대상으로 음이항 회귀분석을 실시한 결과를 제시한 표이다. 전체 기업을 대상으로 실시한 분석 결과와 동일하게 가설 2와 3이 채택되었다. 또한, 전체 기업을 대상으로 한 분석 결과와는 달리 정보보호 제품 투자만 정보보안 사고와 통계적으로 유의한 양적 상관관계가 있다는 것이 확인되었다.

Table. 10. Result of negative binomial regression analysis with organizations which suffered information security incidents

Variable	Negative binomial regression coefficient
Dummy :Finance	-1.63
Firm size	-0.059
Dummy: Policy	1.413***
Dummy: Increase of investment	0.462
Product and its service	0.285***
Education & training	-1.39***
Vulnerability testing	-0.941***
Monitoring	0.166
Consistant	1.832***
Alpha	1.659
Observations	250

5.2 논의

본 연구 결과 기업 구성원들의 정보보안 의식 및 배경지식을 제고할 수 있는 교육 훈련에 대한 투자, 기업의 정보보안 취약점을 파악하고 대비책을 강구하기 위한 목적으로 실시하는 취약점 분석에 대한 투자

가 실질적으로 정보보안 사고를 줄이는 데에 기여한다는 사실을 확인하였다. 추가로 실시한 침해사고의 발생을 명확히 인지하고 있는 기업만을 대상으로 분석 결과도 교육 훈련과 취약점 분석에 대한 투자가 기업의 정보보안 사고를 줄이는 데에 기여한다는 사실을 지지한다. 따라서 기업에서는 기존의 정보보안 제품 및 서비스 투자, 모니터링과 같은 투자에서 기업의 정보보안 사고를 감소시키는 데에 실질적으로 기여하는 취약점 분석이나 교육에 대한 투자에 보다 자원을 집중하는 것이 중요할 것이다. 특히 직원들에 대한 정보보호 교육이 정보보안 관련 사고를 줄이는 데에 효율적일 수 있다. 정보보호 교육은 정보 보안의 중요성을 강조하는 방향으로 진행되며[38], 정보보호 교육을 실시하면 조직 구성원들이 조직의 정보자산을 보호하는 일을 더욱 중요하게 여기게 되고, 조직 구성원들의 정보보안 의식이 상승한다[39]. 정보보안 의식이 상승한 조직 구성원들은 정보보안 정책을 더욱 잘 준수하게 되어[40] 조직 구성원들에 의한 정보보안 사고가 감소할 수 있다.

전체 기업과 사고를 경험한 250개 기업만을 대상으로 음이항 회귀분석을 실시한 결과, 모두 공통으로 정보보호 제품 투자가 정보보안 사고와 통계적으로 유의한 양적 상관관계가 있다는 사실이 확인되었다. 또한 Table 5.의 상관분석 결과에 의하면 정보보안 제품에 대한 투자와 정보보안 투자 증가 더미는 0.9085의 높은 상관관계를 갖고 있음이 확인되었다. 이는 정보보호 제품에 대한 투자 증가가 정보보안 사고를 줄이는 데에 기여하지 못한다는 뜻이 아니라, 한국 기업들이 사고가 발생한 이후 제품을 적극적으로 도입하여 추가적인 정보보안 사고에 대한 가능성을 줄이려고 노력하는 현황과 관련이 있다고 해석할 수 있다[34]. 또한, 분석 결과 단순히 공식적인 정보보안 정책을 만들고, 정보보안 투자를 증진시키는 것만으로는 기업의 정보보안 사고를 줄일 수 없음을 확인하였다. 정보보안 정책은 조직 구성원들에게 경각심을 주는 역할을 수행하는데, 이러한 정보보안 정책의 성숙도를 보다 높여 경각심을 더 불어넣고 정책을 준수하게 만들기 위해서는 조직 전체에서 정보보호 정책에 대한 지원이 필요하기 때문이다[35]. 여러 업종 중에서도 금융업에서 정보 보안 관련 사고가 유의미하게 적게 발생하는 것이 확인되었는데, 이는 금융업에 특별히 적용되는 금융 감독 기관의 엄격한 규제와 가이드라인이 정보보안 사고를 막는 데에 유의미한 영향을 미친다는 사실을 의미한다[29]. 따라서 정보 보안 관련 사고를 줄이기 위해서는 기업에 보다 엄격한 규제와 가이드라인을 제시하는 것이 효과적일 수 있다.

VI. 결 론

본 연구는 정보보안 투자의 여러 세부 분야 중 어떤 부문에 대한 투자가 가장 정보보안 사고를 줄이는 데에 효율적인지를 파악하기 위해 실시되었다. 7086개 기업 데이터를 이용한 분석 결과, 본 연구는 직원들에 대한 교육 및 훈련 비용 지출과 취약점 분석이 기업의 정보보안 사고를 줄이고 예방하는 데에 기여한다는 사실을 확인하였다.

이 연구는 학문적으로는 세분화된 정보보안 투자 중 어떤 분야가 가장 정보보안 사고를 줄이는 데에 기여하는지를 실증적으로 분석하여 검증하였다는 데에 의의가 있다. 즉, 기업에서 정보보안에 투입할 수 있는 한정된 자원이 존재할 때, 어느 부분에 자원을 투입하는 것이 가장 효율적인 선택이 될 수 있는지를 확인한 연구이다. 본 연구는 정보보안 사고를 예방하거나 줄이기 위해, 가장 취약한 지점 중 하나로 여겨지는 조직 구성원의 정보보안 인식을 증진시키는 것과 조직이 보유한 실질적인 정보보안 취약점을 찾아내고 방비하는 것이 가장 경제적인 선택이 될 수 있음을 확인하였다.

본 연구는 실무적으로는 기업이 정보보안 투자 항목에 대한 우선순위를 제시한다. 기업에서는 한정된 자원이 배정된 상태에서 정보보안 사고를 최대한 예방하기 위해 자원을 집중해서 투입해야 할 분야를 선택해야 한다. 이 연구의 결과는 기업에서 한정된 자원을 정보보안에 투입하여 정보보안 사고를 최대한 줄이고자 할 때에는 직원들에 대한 교육 및 훈련과 취약점 분석에 자원을 투입하는 것이 효율적일 수 있음을 시사한다. 또한 본 연구는 기업에게 구체적인 정보보안 투자 지침을 제시한다는 실무적인 공헌도를 가진다.

본 연구는 다음과 같은 한계점을 가지고 있다. 본 연구는 한국 기업만을 대상으로 실시한 설문조사 데이터를 바탕으로 진행되었다. 따라서 본 연구 결과를 다른 국가의 상황에 일반화하여 적용하기에는 어려움이 따른다. 또한 본 연구에 사용된 데이터는 준정부기관에서 수집하고 가공하여 제공한 것으로서 연구자들이 연구에 필요한 데이터를 추가로 수집하거나 업데이트하기에는 한계가 따른다. 추후에는 국가 간 비

교 연구를 통하여 국가 별 상황에 따른 정보보안 투자 종목의 정보보안 사고 감소에 대한 효율성을 확인하고 비교할 필요가 있으며, 이를 위해 연구자들이 직접 정보보안 투자와 사고 관련 데이터를 수집하여 바탕으로 보다 심도 있는 연구를 진행할 예정이다.

References

[1] Jung-Ho Lee. "Firms' "Ransomware accidents has increased 11 times," Hankyung health, Jan. 2017. http://health.hankyung.com/article/2017012359241 (Retrieved from November 7th, 2017)

[2] Yu-ji Lee. "The size of information security incidents damage is increaing- Top managements' strong support and insurance subscription help firms to reduce damage amount," Digital daily. Jun. 2015. http://www.ddaily.co.kr/news/article.html?no=131217 (Retrieved from November 18, 2017)

[3] Seung-pil Choi. "Information society and its enemy," Korea times, Oct. 2017.http://www.hankookilbo.com/v/b36ad2295d3545659ed8f3b91cd43b9c (Retrived from November 7, 2017)

[4] PwC. Turnaround and transformation in cybersecurity: Retail and consumer, PwC, 2016

[5] K.Campbell, L. A. Gordon, M. P. Loeb & L. Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," Journal of Computer Security, vol.11, no.3, pp. 431-448. Jul. 2003.

[6] Tae-Hyung Kim. "Information security budget management② - 5 factors tha t firms must consider to invest on inf ormation security," Boan news. Sep. 2 015. http://www.boannews.com/media/view.asp?idx=47639 (Retrieved from November 7, 2017)

[7] L. A. Gordon and M. P. Loeb, "The economics of information security investment," ACM Transactions on Information and System Security (TISSEC), vol.5, no.4, pp. 438-457. Nov.2002.

[8] K. Hausken, "Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability," Information Systems Frontiers, vol.8, no.5, pp. 338-349. Dec.2006.

[9] C. D. Huang, Q. Hu, and R. S. Behara, "An economic analysis of the optimal information security investment in the case of a risk-averse firm," International Journal of Production Economics, vol.114, no.2, pp. 793-804. Aug. 2008.

[10] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model," Journal of Information Security, vol.6, no.1, pp. 24-30. Oct. 2015.

[11] Young-Ok Kwon and Byung-Do Kim, "The Effect of Information Security Breach and Security Investment Announcement on the Market Value of Korean Firms," Information Systems Review, 9(1), pp. 105-120. Apr. 2007.

[12] Anat Hovav and Jin-Young Han, "The Impact of Security Breach Announcements on the Stock Value of Companies in South Korea," The Journal of internet electronic commerce research, 13(3), pp. 43-67. Sep. 2013.

[13] Il-Yoo Hong, Jae-Hoon Lee, and

Sung-Min Kang, "The Effect of Official Announcement about Information Security Breach on Corporate Stock Value in the Market," Entrue Journal of Information Technology, 14(2), pp. 33-56. Aug. 2015.

[14] S. Chai, M. Kim, and H. R. Rao, "Firms' information security investment decisions: Stock market evidence of investors' behavior," Decision Support Systems, vol.50, no. 4, pp. 651-661. Mar. 2011.

[15] Hee-Kyung Kong, Hyo-Jung Jun and Tae-Sung Kim. "A Study on Information Security Investment by the Analytic Hierarchy Process," Journal of Information Technology Applications & Management, 15(1), pp. 139-152, Mar. 2008.

[16] Won-Seok Yang, Tae-Sung Kim and Hyun-Min Park. "Probabilistic Modeling for Evaluation of Information Security Investment Portfolios," Journal of the Korean Operations Research and Management Science Society, 34(3), pp.155-163. Sep. 2009.

[17] Korea Internet & security agency, Survey for Information Security Industry in Korea, Korea Internet & security agency, pp.1-345, Dec. 2014.

[18] Se-ah Min. "Korean information security market has growing - its total size is expected to grow 3,844.9 billion won until 2020," Boan news, May. 2017. http://www.boannews.com/media/view.asp?idx=54571 (Retrieved from November 10, 2017)

[19] Hangbae Chang, Jun-Taek Lee, Sanghoon Kim. Industrial information security management, Beobmoonsa, Jul. 2013.

[20] Seongmong Lee. Information systems security, Infodream, Oct. 2013.

[21] M. E. Thomson and R. von Solms, "Information Security Awareness: Educating Your Users Effectively," Information Management & Computer Security, vol.6, no.4, pp. 167-173. 1998.

[22] J. D'Arcy, A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research, vol.20, no.1, pp. 79-98. Mar. 2009.

[23] M. Siponen, S. Pahnila, and M. A. Mahmood, "Compliance with information security policies: An empirical investigation," Computer, vol.43, no.2, Feb. 2010.

[24] Jung-Ae Kim. "Vulnerabilities found to be target of cyber war make information security professionals be nervous," Boan news, Sep. 2017. http://www.boannews.com/media/view.asp?idx=57015. (Retrieved from November 17, 2017)

[25] Jung-Ho Eom, Seong-Su Choi, and Tai-Myoung Chung, "introduction of cyber warfare : attack and security techniques," Hongrung publishing company, Feb. 2012.

[26] Hye-Kwon Shin. "Information security incidents prevention : Finding vulnerabilities is important," ET news, Jul. 2013. http://www.etnews.com/20130719 0248 (Retrieved from November 17, 2017)

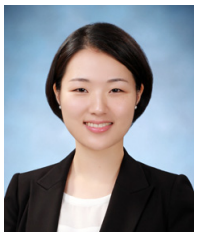
[27] Sungjin Ahn, Kyung-Ho Lee, and Won-Hyung Park. "Security monitoring and control," Ehan media, Apr. 2014.

[28] Samsung SDS. "Samsung SDS consulting - Information security monitoring and level diagnosis," Samsung SDS, 2016.

[29] Deloitte Anjin. "Risk management in

Financial industry : Focusing on protection of information asset," Deloitte Anjin, Apr.2014.
〔30〕 Deloitte Anjin. "Cyber risk assessment," Deloitte Anjin, 2016.
〔31〕 Department for Business, Innovation and Skills, "2015 Information Security Breaches Survey," HM Government, 2015.
〔32〕 M. Creel and J. Loomis, "Theoretical and empirical advantages of truncated count data estimators for analysis of deer hunting in California," American Journal of Agricultural Economics, vol.72, pp.434 - 441, May. 1990.
〔33〕 D.R. Cox, "Some remarks on overdispersion," Biometrika, vol.70, pp.269 - 274, Apr.1983.
〔34〕 Kwan-kyu Park "If there is another in formation security breach, it will dest roy our organization : organizations are now improving their information s ecurity," Korea times. Jul. 2014. http://www.hankookilbo.com/v/1e8cc0b887d54ad4b7b76ec5bd4e7fa1. (Retreived fr om December 7, 2017)
〔35〕 Myeonggil Choi, Won-Joo Hwang and Myoung-Soo Kim, "An Empirical Study on Factors Affecting the Maturity of Information Security Policy," Journal of The Korea Institute of Information Security and Cryptology, 18(3), pp. 131-142. Jun. 2008.
〔36〕 Jongki Kim, & Dayeon Kang. "The Effects of Security Policies, Security Awareness and Individual Characteristics on Password Security Effectiveness," Journal of The Korea Institute of Information Security and Cryptology, 18(4), pp.123-133. Aug. 2008.
〔37〕 Dong-Keun Choi, Mi-sun Song, Jong In Im and Kyung-Ho Lee, "Study the role of information security personnel have on an organization's information security level," Journal of The Korea Institute of Information Security and Cryptology, 25(1), pp.197-209, Feb. 2015.
〔38〕 Whitman, M. E. "Enemy at the Gate: Threats to Information Security," Communications of the ACM. 46(8), pp. 91-95. Aug. 2003.
〔39〕 M. Wilson and J. Hash, "Building an Information Technology Security Awareness and Training Program," NIST Special Publication (800), p. 50. Oct. 2003.
〔40〕 B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," MIS Quarterly, vol.34, no.3, pp. 523-548. Sep. 2010.

〈저 자 소 개〉



이 한 솔 (Hansol Lee) 학생회원
이화여자대학교에서 학사 학위를 취득하였으며, 현재 이화여자대학교 일반대학원 경영학과 석사 과정에 재학 중이다. 현재는 개인정보보호, 정보 보안, 프라이버시 관련 연구를 진행 중이다.

채 상 미(Sangmi Chai) 정회원
현재 이화여자대학교 경영대학 부교수로 재직 중이다. 이화여자대학교에서 학사, 서울대학교에서 경영학 석사 학위를 취득하였으며 미국 The state university of New York at Buffalo에서 경영학으로 박사 학위를 취득하였다. 주요 연구 분야는 정보기술과 인간 행동에 관한 주요 이슈, IT와 조직 및 전략, 정보보안과 조직, 그리고 최근에는 빅데이터 분석 기술을 활용한 연구를 진행 중이다.