논문 18-43-10-26 The Journal of Korean Institute of Communications and Information Sciences '18-10 Vol.43 No.10
https://doi.org/10.7840/kics.2018.43.10.1741

한국형 스마트 팩토리 확산을 위한 사이버보안 위험관리 방안

이 송 하◆, 전 효 정*, 김 태 성°

A Study on Cyber Security Risk Management for Diffusion of Korean Smart Factories

Song-ha Lee◆, Hyo-Jung Jun*, Tae-Sung Kim°

요 약

농업, 제조업 등과 같은 전통적인 산업영역에 첨단 ICT 기술이 접목되고 네트워크로 연결되기 시작하면서 사이버 보안은 더 이상 IT기반 기업에게만 국한된 고민거리가 아니다. 특히 우리나라는 중소기업의 경쟁력 강화를 위해 IoT 등의 첨단 기술이 도입된 스마트 팩토리를 2025년까지 전국 3만 곳에 구축하는 것을 목표로 하고 있다. 스마트 팩토리 도입에 있어서 사이버보안은 필수사항이지만, 전통산업 내의 주요 플레이어들은 영세 또는 중소기업이기 때문에 사이버보안을 위한 예산 및 인력의 적극적인 투입이 어려워 체계적인 보안관리를 기대할 수 없다. 이에 본 연구에서는 스마트 팩토리를 도입하는 국내 중소기업들이 보안투자를 통한 보안체계를 구축하기에는 상당히 오랜 시간이 소요될 수 있음을 감안하여, 보안 장비 및 시스템 도입에 비해 비교적 적은 비용을 통해 단시간 내에 위험을 관리할 수 있는 대안으로서 사이버보험 도입의 필요성과 그 방안에 대해 논의해보고자 한다.

Key Words : Smart Factory, Cybersecurity Investment, Risk Management, Cyber Insurance, Risk Transfer

ABSTRACT

As traditional industries such as agriculture and manufacturing have been combined with advanced ICT technology and networking, cyber security is no longer a concern confined to IT-based businesses. Currently, the Korea government plans to build smart factories in 30,000 locations nationwide by 2025 to raise competitiveness of small- and medium-sized companies (SMEs) through an initiative called "Spreading and Diffusion of Smart Factories." Cybersecurity is essential to the introduction of smart factories. Nevertheless the system investment and response capabilities of SMEs in cyber security are very weak. Also, there is a limit in that some guidelines only deal with industrial security in the smart factory. In this study, cyber insurance is suggested as a risk transfer alternative for small- and medium-sized manufacturers who may be suffering from a lack of cyber security capability.

※ 이 논문은 2015년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2015S1A5A2A01009763)
◆ First Author : (ORCID:0000-0001-7354-7742)Department of Management Information Systems and Cybersecurity Economics Research Institute, Chungbuk National University, lsh914@naver.com, 학생회원
° Corresponding Author : (ORCID:0000-0002-6260-4972)Department of Management Information Systems and Cybersecurity Economics Research Institute, Chungbuk National University, kimts@chungbuk.ac.kr, 종신회원
* (ORCID:000-0003-2465-5266)Chungbuk National University, phdhyo@naver.com, 정회원
논문번호 : 201807-214-0-SE, Received July 16, 2018; Revised August 10, 2018; Accepted September 21, 2018

Ⅰ. 서 론

모든 시스템이 네트워크로 연결되면서 사이버공간이 새로운 국면을 맞이하고 있다. 정보보호 위협이 증가함에 따라 갈수록 보안위협을 검출하거나 숨겨진 취약점을 찾을 수 있는 고수준의 인력에 대한 구인난은 더욱 심화되고 있지만 대기업에 비해 상대적으로 임금경쟁력이 약한 중소기업 및 정부・공공기관 등은 숙련된 인력채용에 많은 어려움을 겪고 있다[32]. 4차 산업혁명 시대를 맞이하여 CEO의 우려사항 중 하나로 사이버보안(Cyber Security Risks)이 지목되고 있지만[28], 일반적인 중소기업은 이에 대응할 만한 여력이 없다. 전 산업의 지능정보화가 빠른 속도로 확산되면서 중소기업 대상의 사이버 공격과 이의 피해사례 역시 증가하는 추세이지만 중소기업은 사이버위협을 인지조차 못하거나 예산과 인력 부족으로 대책마련 및 실행에 미온적이다. 기술유출 피해업체의 예상 피해액은 연평균 약 50조 원에 달하는 상황이며 이는 2014년 기준 국내 GDP의 약 3%에 해당하는 수치이며 중소기업 약 4,700여 개의 1년 매출액에 해당하는 규모이다[41]. 더욱이 규모가 작은 중소기업일수록 정보보호 관리체계 구축이 미비할 수밖에 없다. 일례로 2017년 기준 상시 종사자수 50인 미만 기업의 정보보호 정책 수립률은 21%이지만 50인 이상 기업은 75%이며, 정보보호 전담 조직 운영 비율도 50인 미만 기업은 14%인데 반해 50인 이상 기업은 73%이다. 또한 50인 미만 기업의 38%만이 정보보호 교육을 시행하고 있는데 반해 50인 이상 기업은 87%가 정보보호 교육을 시행하고 있다[24].

정부는 2025년까지 대략 3만여 개의 국내 제조 분야 공장들을 스마트 공장으로 전환하기 위해 스마트 팩토리 보급・확산사업을 추진 중에 있다. 그러나 보급 단계에서의 관심과 지원만큼 사후관리 단계에서의 지원이 중요하며, 사이버보안 차원에서의 위험관리는 사후관리의 핵심이라 할 수 있다. 더욱이 스마트 팩토리 보급・확산이 스마트 팩토리 공급업체를 중심으로 이루어지고 있기 때문에 유지보수도 공급업체에 의존할 수밖에 없다. 따라서 중소기업 스스로가 사후관리 체계를 구축하고 위험 관리를 해 나갈 수 있어야 진정한 스마트 팩토리 확산 및 고도화가 가능할 것이다.

우리나라의 스마트 팩토리 보안정책은 사실상 아직 없다. 산업통상자원부, 중소벤처기업부, 특허청 등을 중심으로 산업기밀 유출방지 등을 위한 법을 통해 예방 중심으로 추진되어 오고 있으며, 특허청은 중소・중견기업을 대상으로 지식재산권 소송보험을 지원하고 있다. 국가정보원, 경찰청 등은 산업기밀보호센터를 운영 중이며 산업기술 유출범죄 수사 및 징벌적 손해배상제도를 운영하고 있다. 과학기술정보통신부는 2014년 처음 IoT 정보보호 로드맵을 발표한 이후 해마다 시행계획을 마련하여 공개하고 있으며, 2017년 한국인터넷진흥원은 스마트공장 중요정보 유출방지 가이드를 발표한 바 있다[25]. 이렇듯 대부분의 정책이 기술유출방지 즉 산업보안 측면에서만 시행되고 있다.

스마트 공장 보급・확산 사업의 성공적인 마무리와 성공적인 스마트 제조공정 구축을 위해서는 사이버보안 위험관리를 위한 중소기업의 적극적인 노력과 정부의 지원과의 콜라보가 필수적이다. 그러나 주체는 중소기업이고 기반은 지능정보기술과의 융합이며 대상은 산업정보 및 산업시설인 스마트 팩토리 보안정책의 개발을 위해서는 다부처간의 협의와 이해가 필요하기 때문에 당장 가시적인 지원정책 도출까지는 상당한 시일이 걸릴 수 있다.

본 연구에서는 정부의 지원으로 점진적으로 스마트 팩토리로 이행해 나가는 과정에서 예산과 인력의 한계로 정보보호 관리체계의 구현까지 상당한 시일이 소요될 수밖에 없는 국내 중소기업을 위한 위험관리 방안의 하나로서 사이버보험의 필요성에 대한 중소기업의 인식을 조사・분석해 보고자 한다. 또한 정부의 스마트 팩토리 사이버보안을 위한 지원정책의 일환으로서 사이버보험 도입의 필요성과 방안에 대해 논의해 보고자 한다.

Ⅱ. 문헌연구

2.1 사이버보험

사이버보험은 각 보험사 혹은 연구자에 따라서 다양한 용어로 불리고 있다. 사이버 배상책임 보험(Cyber Liability Insurance), 사이버보안(보증) 보험(Cyber Security Insurance), 사이버 리스크 보험(Cyber Risk Insurance), 디지털 리스크 보험(Digital Risk Insurance), 사이버 및 프라이버시 보험(Cyber and Privacy Insurance) 등이 대표적이며, 최근에는 사이버보험(Cyber Insurance)을 대중적으로 사용하는 추세이다[44].

사이버보험은 사이버 리스크의 전가(Cyber Risk Transfer)를 통해 기업손실을 보전하고 경영안전성을 높이는 최소한의 방어수단이다<Table 1>.

ENISA(2012)[8]는 사이버보험을 사이버보안과 관련된 당사자 및 제3자 리스크를 보장하는 보험으로, Böhme and Schwartz(2010)[39]는 사이버보험을 네트

표 1. 일반적인 리스크 관리 방안[26]
Table 1. Risk Management Methods

	Descriptions
Acceptance	Accepting current risks and taking the potential cost of losses
Mitigation	Implementing measures to reduce risk
Transfer	Transfer or allocate potential costs to third parties, such as insurance or outsourcing
Avoidance	Abandonment without performing a risky process or business

워크 및 컴퓨터 관련 재정적 위험을 제3자에게 이전하는 것으로 설명하였다. Lee et al. (2017)[44]은 컴퓨터나 네트워크 등 사이버보안과 관련된 사고로부터 발생한 당사자 및 제3자의 유·무형 자산의 손실을 보장하는 보험 상품의 포괄적인 개념으로 정의하였다.

La(2003)[13]는 전자상거래 상에서 발생하는 소비자의 피해구제 방안으로 전자상거래 보험을 적극 활용해야 한다고 주장하였다. 더불어 보험업계의 다양한 보험 상품 개발 및 담보 범위의 표준화가 필요하며, 이를 위해 정부 차원의 정책적인 대책이 필요하다고 하였다. Shin(2005)[12]은 전자상거래 환경 속에서 무역기업이 신규 위험에 대비하여 방화벽, 안티 바이러스와 같은 기술적인 장치와 제도적인 장치로써 보험을 활용하는 것이 필요하다고 하였다. Hong(2013)[20]은 전자상거래 보험을 통해 비교적 적은 보험료로 고액의 손해배상책임과 소송비용을 해결함으로써 전자상거래 사업자의 적극적이고 왕성한 활동을 할 수 있다고 하였다. 이에 정부 차원에서 전자상거래 사업자의 책임위험 분산 및 책임이행을 확보하여 소비자를 보호하기 위해 보험 가입을 적극적으로 유도하고, 보험업계에서 다양한 상품을 개발해야 한다고 주장하였다. 그러나 상기 연구들은 사이버보험을 전자상거래 보험으로 한정하고, 손해배상 부분에 초점을 맞추고 있다는 한계가 있다. Kim and Lim(2014)[21]은 금융거래에 있어서 개인정보유출에 따른 소비자의 손실을 분석하고, 손해를 최소화하기 위한 방법으로 보험을 활용할 수 있다고 주장하였다. 그러나, 보험의 활용범위를 금융 분야의 개인정보보호 분야에 한정했다는 점에서 한계가 있다. 정보보호의 관점에서, Kwon and Kim(2009)[18]은 효율적인 정보보호 위험관리를 위해 기술적 한계를 보완하고 위협 발생가능성의 불확실성을 상쇄할 수 있는 정보보안 관련 보험 상품에 투자하는 전략의 필요성을 제시하였다. 또한 정보보호 위험관리에 대한 인식을 제고하고 투자전략에 보험을 고려한 연구가 필요하다고 주장하였다.

Loveland(2017)[22]에 따르면 사이버보험은 2000년대 초반에는 매우 소수의 공급자에 의해 주로 제3자(3rd Party)에 대한 피해보상을 보장하였으나, 2003년 캘리포니아 주법인 보안침해에 대한 공지법(CA Security Breach Information Act)이 시행되면서 공급자가 증가하였고, 당사자 보상(1st Party)에 대한 보장도 추가되었다. 더불어 2016년에는 미국에만 약 60여 개 이상의 공급자가 존재하는 것으로 파악되며, 그 시장규모(보험료 수익)가 약 25억 달러 수준에 달하는 것으로 보인다. AON(2017)[2]은 2020년까지 미국 사이버보험의 시장규모가 약 56억 달러 규모로 성장 할 것으로 전망하였으며, AGCS(2015)[1]는 글로벌 사이버보험 시장이 2025년 까지 200억 달려 규모로 성장할 것으로 예측하였다.

국내의 경우 사이버보험 가입 기업에 대한 정보가 공개된 경우가 거의 없지만, 최근 주요 가상화폐 거래소들이 사이버보험에 가입되어 있는 것으로 공개된 바 있다. 일례로 2017년 12월 해킹으로 인한 파산신청을 한 유빗은 DB손해보험의 사이버종합보험(지급보험금 기준 30억원 규모)에, 가상화폐 거래소인 코인원은 현대해상의 뉴사이버시큐리티 보험(지급 보험금 기준 30억원 규모)에, 빗썸은 현대해상의 뉴 사이버종합보험과 흥국화재의 개인정보유출 배상책임보험에 가입(지급 보험금 기준 각 30억원 규모)되어 있었던 것으로 공개되었다[11].

2.2 위험관리

위험관리 프로세스나 방법론은 매우 다양하나, 미국에너지부(DOE)에서 제시한 위험관리 사이클은 FRAME, ASSESS, RESPOND, MONITOR 등 4단계로 구성된다[6]. FRAME 단계는 위험 기반 의사결정을 위한 제반사항들을 정의하는 단계로서 의사결정자들에게 설명 가능한 신뢰성 있는 위험구조를 시나리오에 기반하여 설정한다. ASSESS 단계는 위협(Threats), 취약점(Vulnerabilities), 영향(Impacts; 결과 또는 기회), 가능성(Likelihood) 등을 규명한다. RESPOND 단계에서는 각 위험에 대한 대응책 또는 가능한 해결책을 제시하고 각 방안들을 평가하여 구현한다. 마지막으로 MONITOR 단계에서는 위험에 대한 방안들이 제대로 구현이 되었는지, 수정사항은 없는지, 또 다른 위험은 없는지 등을 지속적으로 모니터링 한다.

위험분석은 자산의 취약점을 식별하고 존재하는 위

협을 분석하여 이들의 발생 가능성 및 위협이 미칠 수 있는 영향을 파악해서 보안 위험의 내용과 정도를 결정하는 과정이다[45]. 위험분석은 위협관리의 일부분으로서, 화재, 사고 등의 물리적 위협에 적용되어 위협의 발생가능성에 따른 잠재적인 손실을 계산한다. 위험분석을 통해 적절한 보호대책을 우선순위에 따라 효율적으로 세울 수 있으며, 과도하거나 과소의 투자를 예방하고 효율적이고 효과적인 보안을 실현할 수 있다.

일반적인 사이버보안 투자는 주로 방화벽과 같은 접근제어(사전탐지)방식과 IDS와 같은 침입탐지(사후탐지)방식이 있으며, 여러 논문들이 이런 기술적 보안대책구현에 대한 투자의 적절성, 각 대책들 간의 비용효과 분석에 대한 연구를 진행하였다[15,16]. 그러나, 보안대책들의 효과를 정량적으로 계산하고, 비용편익을 산출하기 위해서는 방대한 양의 데이터와 가정들이 필요하기 때문에 실질적으로 어려움이 존재한다. 이에 Bodin et al. (2005)[30]은 각 보안 대책들에 대한 시나리오 기반의 AHP 설문을 실시하여 정성적인 의견을 정량적으로 바꾸어 실제 기업의 CISO들이 보안투자 예산과 관련해 CFO를 효과적으로 설득 할 수 있도록 하는 복잡한 계산을 우회하는 방안을 제시하기도 하였다.

그러나 사전적 위험관리 수단을 구현한 경우에도 사이버 침해사고 발생 시 기업 평판 훼손 등의 잔여위험이 존재하기 때문에 완벽한 보안은 없으며, 사이버 보안사고의 경우 사후처리를 위해 발생하는 비용이 크기 때문에 Gordon et al.(2003)[29]는 기술적 보안대책과 더불어 보험을 고려한 위험관리 프레임워크를 제시하였다. Kumar et al.(2008)[42]는 기존의 사이버 보안 투자에 대한 연구들이 침입탐지 및 예방의 측면만 고려하고 있다고 비판하며, 사이버 침해사고에 따른 복구계획으로써 보험까지 고려한 종합 보안투자결정 모형을 제시하였다.

Ⅲ. 사이버보안 위험관리 방안

3.1 스마트 팩토리의 내재된 사이버보안 위험

4차 산업혁명시대를 맞이하여 국가차원에서 중소·중견 기업의 경쟁력을 강화하고자 민관합동으로 스마트공장 추진단을 운영하고 있으며, 2014년 시범사업을 시작으로 매해 스마트공장 보급·확산사업을 실시하고 있다. 이를 통해 우리나라는 2025년까지 전국의 중소·중견기업을 대상으로 약 3만 여개의 스마트 팩토리를 구축해 나갈 예정이며, 스마트 공장 기반기술 R&D에 2020년까지 총 2,154억 원을 투입할 예정이다[33].

스마트 팩토리는 ICT 기술 도입으로 인하여 공장 제어시스템에 대한 원격제어 모니터링, 외부 네트워크와 연결 등을 필수적으로 요구하며, 기획설계, 유통판매, 생산공정 등의 업무공정별로 다양한 중요정보를 생성·저장한다[25]. 스마트 팩토리에 대한 직접적인 사이버공격 및 위협으로 인한 피해사례는 잘 알려져 있지 않다. 2014년 말 독일의 한 철강회사가 사이버

표 2. 국내 중소기업의 사이버보험 도입 현황
Table 2. Cyber Insurance Survey Result for Domestic SMEs

Questions	Total Mean (N=141)			Smart Factories (N=42)		
	Yes	No	I don't know	Yes	No	I don't know
Is information security (including cyber security) important in management activities in your organization?	71%	23%	6%	86%	12%	2%
Do you needs an insurances or deductions to minimize risk mitigation or reduction of accidents cost?	95%	4%	1%	100%	-	-
Have you ever been or have been enrolled in other insurance (including cyber insurance) or deductions?	67%	11%	22%	67%	7%	26%
Do you know about cyber insurance?	25%	57%	18%	5%	90%	5%
Have you ever been or have been enrolled in cyber insurance	4%	90%	6%	5%	90%	5%
Do you have any plans to join if you have government support (partial insurance premium, etc.) when you join cyber insurance? ※ companies being enrolled cyber insurance are excepted.	59%	11%	30%	63%	10%	27%

해킹으로 공장의 제어시스템이 파괴되어 용광로 차단 기능이 마비되면서 제시간에 멈추지 못해 엄청난 물리적 피해가 발생한 사례가 알려져 있지만[14], 상세한 피해내역이나 공격일자는 공개되지 않고 있다. 그러나 스마트 제조 이외에도 스마트 시티, 스마트 에너지, 스마트 교통, 스마트 의료, 스마트 홈 등 사물인터넷 기술이 적용되어 발전하고 있는 분야에서 사물인터넷이 갖는 근원적인 보안취약성에 대한 우려는 지속적으로 제기되고 있으며, 이를 고려한 보안설계의 필요성이 제기되고 있다[3,27,31,47]. 더욱이 스마트 팩토리에 대한 사이버공격은 스마트 팩토리 자체에 대한 물리적 피해뿐만 아니라 기업의 산업자산 전체를 위협하는 피해를 초래할 수 있다는 점에서 더 큰 문제가 있다. 현재 알려져 있는 스마트 팩토리 대상 사이버 공격의 유형으로는 서비스거부공격, 도청공격, 중간자공격, 오류데이터인젝션공격, 시간지연공격, 스푸핑공격, 부채널공격, 제로데이공격, 물리적공격 등 매우 다양하다[5,17,19,23,36].

스마트 팩토리는 다양한 기술과 환경이 통합되어 복잡도와 불확실성이 더욱 커지기 때문에 예상치 못한 문제가 발생할 가능성이 높음에도 불구하고 스마트 팩토리 위협 분석과 관련된 연구는 부족한 실정이다[7]. 특히, 기존에 독립적으로 운영되던 시스템 환경과는 달리 시스템 간 연결성을 갖게 되는 새로운 환경에 대한 적응과 위험관리가 필요함에도 불구하고, 영세한 중소기업들은 인적·물적 자원의 부족으로 이에 대한 대응능력을 확보하지 못하고 있어 그 위험은 배로 증가할 수밖에 없다.

3.2 스마트 팩토리 사이버보험

더 이상 일반기업들에게 사이버 리스크는 새로운 것이 아니지만, 스마트 팩토리 시대가 도래하면서 제조기업에게는 사이버 리스크가 그 어느 때보다 큰 의미를 지니게 되었다[48].

2017년 정보보호실태조사에 따르면 정보보호 또는 개인정보보호 조직을 보유한 사업체의 비율은 9.9%에 불과하였으며, 2016년을 기준으로 IT예산 중 정보보호 또는 개인정보보호 예산을 5%이상 편성한 사업체는 2.2%에 불과하였다[24]. 스마트 팩토리 도입에는 사이버보안이 필수임에도 불구하고, 스마트 팩토리 도입기업의 절대 다수는 중소·중견 기업으로 사이버 위협을 인지조차 못하거나 예산과 인력 부족으로 대책마련 및 실행에 미온적일 수밖에 없다. 사이버보험은 기술적 관리적 보안대책을 수립하는 것보다 비교적 적은 비용과 시간이 소요된다고 알려져 있기 때문에[29], 중소기업에게는 유용한 위험관리 수단으로 활용될 수 있다.

PartnerRe and Advisen(2017)에 따르면 신규 사이버보험 시장에 대한 기여도가 높을 것으로 예상되는 산업군은 헬스케어와 전문서비스 분야와 더불어 '제조 및 공업' 분야가 꼽혔다. 일례로 전세계 시장을 대상으로 한 조사에서 제조기업의 2016년 사이버보험 가입률은 2015년 대비 2배 이상 증가하였으며, 주로 당사자 손해(1st Party)에 대한 보험에 가입한 것으로 나타난 바 있다[40].

3.3 위험전가 수단으로서의 사이버보험의 필요성

KISA(2017)[24]의 조사에 따르면, 국내 사업체의 0.6% 만이 사이버보험에 가입한 상태로 응답하여, 실질적으로 국내에서는 사이버보험 시장이 거의 형성되어 있지 못한 것으로 나타났다. 이에 본 연구에서는 국내 제조기업 및 스마트 팩토리 도입업체를 대상으로 사이버보안 위험관리의 수단으로서 사이버보험의 향후 가입의사에 대해 조사하고 이를 통해 국내 사이버보험 시장 개화를 위한 시사점을 도출해 보고자 하였다.

조사는 2018월 3월에서 5월까지 약 두 달간 국내 600여개 이상의 중소기업을 대상으로 진행되었다. 141개의 중소기업이 응답하였으며 이 중 스마트 팩토리를 도입한 기업은 42개이다. 주요 분석 결과는 <Table 2>와 같다.

전체 응답기업의 71%가 정보보호가 매우 중요한 기업 내 관리활동이라고 응답하였다. 특히 스마트 팩토리 도입기업의 경우 86%가 정보보호의 중요성에 대한 인식이 높은 것으로 나타났다. 이를 반증하듯 응답기업의 95%, 스마트 팩토리 도입기업의 경우 전체가 향후 정보보호 사고에 따르는 비용을 최소화하기 위해 사이버보험을 포함한 보안이나 공제의 도입이 필요하다고 응답하였다. 그러나, 사이버보험에 대해 알고 있다고 응답한 비율은 전체 응답기업의 25%, 스마트 팩토리 도입기업의 경우 5%에 불과해 산업보안 및 사이버보안 차원에서의 기업 내 위험관리를 위한 최소한의 장치에 대한 이해와 활동은 비교적 낮은 상태로 보인다.

현재 화재, 산업재해, 기자재 손실·도난, 기밀 유출, 지재권관리 등과 관련된 각종 보험이나 공제에 가입중이거나 가입한 적이 있다고 응답한 비율은 각각 67%로, 이미 중소기업은 보험이나 공제를 활용하여 위험을 관리한 경험을 보유하여 사이버보험에 대한 거부감이 크지 않을 것으로 예상된다.

특히, 전체 응답기업의 59%, 스마트 팩토리 도입 기업의 63%가 사이버보험에 대해 정부지원(보험료 일부 지원 등)이 있다면 바로 가입 할 의사가 있다고 응답하였다. 따라서 중소기업의 사이버 위험관리를 위한 보조수단으로서 사이버보험의 도입·확산 및 보조의 필요성이 매우 높다고 할 수 있다.

전체 응답평균과 스마트 팩토리 도입업체의 평균을 비교해보면, 스마트 팩토리 도입업체에서 정보보호의 중요도에 대한 인식과 사이버보험의 필요성, 정부지원이 있을 경우 사이버보험 도입 의사가 전체 평균에 비해 다소 높게 나타났다. 이에 스마트 팩토리를 도입·운영 중에 있는 중소기업의 정보보호 특히 사이버보안 측면에서의 위험관리에 대한 인식과 필요성이 높은 것으로 판단된다.

Ⅳ. 연구의 결론 및 시사점

4.1 연구의 결론

정보보호체계는 수많은 연결고리로 이루어져 있다. 아무리 많은 자원을 투입하더라도, 연결된 네트워크 중 한 부분에서 보안 취약성이 발생한다면 전체 시스템이 외부공격에 쉽게 침해당할 수 있다. 즉 취약고리에 의해 전체 보안 수준이 결정된다[34]. 우리나라는 중소·영세기업이 산업의 근간을 이루고 있지만, 많은 중소·영세기업이 정보보호체계 수립 및 운영에 어려움을 겪고 있으며 이로 인해 국가 전체 보안시스템의 취약고리가 될 수밖에 없다는 한계가 존재한다.

현재의 사이버보험 시장은 민간기업 그 중에서도 보유한 IT자산이나 고객 개인정보가 많은 정보통신서비스제공사업자나 대기업 위주로 형성되고 있다. 때문에 사이버보험의 세부 보장범위도 그에 맞춰지고 있는 실정이다. 사이버보험이 보다 보편적인 위험관리 방안이 될 수 있도록 하기 위해서는 중소기업 및 스마트 팩토리 도입기업에 적합한 사이버보험의 개발이 필요하다. 예산과 인력이 부족한 중소기업은 적극적으로 정보보호 투자에 나설 수는 없지만, 정보보호 위험에 대해 우려하고 있으며, 이를 관리하기 위한 보험이나 공제의 도입에 대한 필요성도 절감하고 있다.

스마트 팩토리 도입의 주역이 될 중소기업은 보호의 대상이 비교적 명확하고 규모가 작아 자산식별이 용이하다는 장점이 있어 최고경영자의 관심과 정부의 독려가 있다면 사이버보험을 통해 매우 탄탄한 위험관리 체계를 구축할 수 있을 것이다. 따라서 우선 스마트 팩토리를 도입할 계획이 있거나 현재 운영 중인 중소기업을 대상으로 발생할 수 있는 사이버 침해사고 정보공유체계를 확립하고 사이버보험 가입을 의무화하여 보다 빠르게 사이버보안을 위한 안전망을 구축하는 것이 필요하다. 또한 주문자 방식(order made)의 보험상품을 제공하고 공동구매 형식으로 사이버보험을 운영한다면 활성화 저해요인의 일부가 해소될 수 있을 것이다. 공동구매 보험은 소비자가 보험판매 및 운영 단계에 참여하여 보험료 할인이 가능하여[10], 사이버보험 가입에 따르는 금전적인 부담을 경감 할 수 있다.

4.2 연구의 시사점

사이버보험은 피보험자가 보유한 리스크를 제3자(보험사)에게 전가하는 위험관리 방안이다. 사이버보험으로 보장받을 수 있는 리스크는 크게 피보험자가 받는 리스크(당사자 리스크; 1st Party)와 피보험자가 받은 리스크로 인해 제 3자가 받는 리스크(제 3자 리스크; 3rd party)로 구분된다. Biener et al.(2015)[4]은 사이버보험 계약자의 일반적인 당사자 리스크의 보장범위를 위기관리, 조업중단, 데이터자산 보호, 사이버 강탈 등으로 제시하였으며, 제 3자 리스크의 보장범위는 개인정보보호 관련 배상책임, 네트워크 보안 배상책임, 지적재산권 및 미디어 유출로 정리하였으며, 각 보장범위에 따른 보장손실은 <Table 3>과 같다.

OECD(2017)[37], OECD(2018)[38], RMS(2016)[39,43] 등의 연구를 종합하면 당사자 리스크는 데이터 및 자산손실, 과징금 및 과태료, 사이버 강탈, 금융절도 및 금융사기, 사업중단, 평판하락, 변호사선임, 규제 및 법적 방어비용, 사고대응(위기관리), 물리적 자산손실, 지적재산권 도난 등으로 분류되며, 제 3자 리스크의 경우 정보유출로 인한 정신적 피해, 정보유출로 인한 신체적 상해 및 죽음, 적합한 기술 제공 실패에 대한 배상, 제조물 배상책임, 우발적 사업중단, 네트워크 보안실패에 따른 배상, 미디어배상, 정보 및 네트워크 서비스에 대한 전문인 배상 등으로 분류된다. 더불어 개인정보 유출 및 환경복구는 당사자 리스크 및 제 3자 리스크 모두에 포함되는 것으로 정리된다.

Financial Security Institute(2017)[9]은 당사자 리스크에 대한 보장범위로 위기관리, 정보자산관리, 운영장애, 사이버강탈, 신원도용, 임원법적책임 등을 제시하였으며, 제3자 리스크에 대한 보장범위로는 사생활 배상책임, 네트워크보안배상책임, 클라우드 컴퓨팅 등을 제시하였다.

Lee et al. (2017)[44]는 사이버보험의 보장범위를 크게 개인정보유출비용, 사업 손실에 따른 비용, 사고대응비용, 배상책임비용, 법적비용, 자산손실에 따른

표 3. 사이버 보험의 커버리지
Table 3. Cyber Insurance Coverage and Sustained Loss

Coverage	Sustained Loss
Personal Information Protection Liability	· Legal liability (defense costs, litigation costs, etc.) · Crisis control · Credit monitoring (costs related to credit monitoring, fraud monitoring, etc.)
Network security liability	· Data recovery costs (data and software recovery or deployment) · Legal costs
Intellectual property rights and media outflow	· Legal liability
Crisis management	· Professional service costs to restore reputation · Notification and monitoring costs for stakeholders
Shut Down	· System return costs · Profit loss · Guaranteed for data recovery costs
Data assets Protection	· Data recovery or replacement costs · Intellectual property restoration or replacement costs
Cyber robbery	· Extortion payment cost · The cost of avoiding robbery · Ransom costs

비용으로 분류하였다. 더불어 개인정보유출의 세부 보장범위는 정신적·물질적 위자료, 정보유출통지 비용, 신용정보 모니터링 서비스 등으로 정의하였다. 또한 사업손실의 세부 보장범위는 자사사업중단 및 제3자 사업중단, 배상책임의 세부 보장범위는 지적재산권 도용, 제3자 네트워크 피해, 임원배상책임, 정보·네트워크 배상책임, 제조물 배상책임으로 분류하였다. 법적 비용의 세부 보장범위는 과징금 및 과태료, 규제 및 법적 방어, 변호사 선임비용, 자산손실의 세부 보장범위로는 랜섬웨어 및 강탈, 데이터 및 SW 손실, 물리적 자산 손실, 환경복구, 지적재산권 도난, 평판하락, 금융절도 및 금융사기로 분류하였다. Kim(2017)[47]은 국외와 국내에서 제공하고 있는 단일 사이버보험의 세부 보장범위를 비교 분석한 결과, 국외의 단일 사이버보험 상품이 국내보다 다양한 보장사항을 보유하고 있는 것으로 나타났다.

사이버보험은 기본적으로 보험사와의 계약을 통해 자사에 보안침해가 발생했을 경우 사후비용 및 복구비용을 담보하고 리스크를 경감하기 위한 수단으로 활용된다. 이에 사이버 리스크에 대한 사후적 대비책으로 볼 수 있으나 일면 사전적 위험관리 기능도 가지고 있다. 사이버보험은 기본적으로 보험사와의 계약을 통해 자사에 보안침해가 발생했을 경우 사후비용 및 복구비용을 담보하고 리스크를 경감하기 위한 수단으로 활용된다. 이에 사이버 리스크에 대한 사후적 대비책으로 볼 수 있으나 일면 사전적 위험관리 기능도 가지고 있다. 예를 들어 사이버보험 가입을 위한 보험사의 언더라이팅(보험 가입 심사) 과정에서 자사가 가진 리스크에 대한 이해도를 높일 수 있는데, 보험계약 인수과정에서 보험회사는 계약자의 리스크 관리정도와 실행정도를 측정하고 이를 보험계약 내용에 반영하기 때문이다[35,44].

따라서 자구적인 위험평가 및 관리에 대한 역량과 예산이 부족한 중소기업은 사이버보험의 가입을 통해 비교적 적은 비용으로 기업의 위험수준을 평가· 및 관리 받을 수 있다는 점에서 매우 유용한 위험관리 수단으로 활용 가능 할 것이다.

향후 연구에서는 사이버보안에 대해 상대적으로 투자여력이 낮은 중소기업 및 정부・공공기관의 실제 사이버 침해사고 사례를 수집·분석하고, 현재 시판되고 있는 사이버보험을 활용하여 피해를 경감한 사례를 비교함으로써, 중소기업 등 상대적 취약계층을 대상으로 한 사이버보험의 보급의 필요성에 대한 공감대를 형성해 나가고자 한다. 또한 지속적인 문헌연구와 사례연구를 통해 급변하는 신규 사이버보안 리스크를 보장범위에 추가해 나가면서 연구를 확대해 나가고자 한다.

References

[1] AGCS, *A Guide to Cyber Risk: Managing The Impact of Increasing Interconnectivity,* Allianz Global Corporate & Specialty SE, 2015.

[2] AON, *2017 Global Cyber Risk Transfer*

Comparison Report, 2017.

[3] A. R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," *IEEE 2015 52nd Design Automation Conf. (DAC)*, pp. 1-6, San Francisco, CA, U.S.A., 2015.

[4] C. Biener, M. Eling, and J. H Wirfs, "Insurability of Cyber Risk: An Empirical Analysis," *The Geneva Papers on Risk and Insurance-Issues and Practice*, vol. 40, no. 1, pp. 131-158, Jan. 2015.

[5] Deloitte, "Industry 4.0 and cybersecurity: Managing risk in an age of connected production," *Deloitte University Press*, pp. 1-24, Jan. 2018.

[6] DOE, *Electricity Subsector Cybersecurity Risk Management Process*, DOE, 2012.

[7] E. J. Park and S. J. Kim, "Derivation of security requirements of smart factory based on STRIDE threat modeling," *J. KIISC*, vol. 27, no. 6, pp. 1467-1482, Dec. 2017.

[8] ENISA, *Incentives and Barriers of the Cyber Insurance Market in Europe*, ENISA, 2012.

[9] Financial Security Institute, *Domestic and Overseas Insurance Market due to Cyber Risk*, Financial Security Institute, 2017.

[10] G. D. Kim, "Analysis of effect of P2P insurance introduction," *KIRI Weekly*, vol. 418, pp. 1-10, Mad. 2017a.

[11] G. H. Jung, "I heard that cyber insurance was the currency exchange ⋯ Where is the reward?" *Market Economy News*, Feb. 2018.

[12] G. H. Shin, "A study on the market status and issues of e-Commerce insurance," *Int. Commerce and Inf. Rev.*, vol. 7, no. 3, pp. 27-51, Sep. 2005.

[13] G. W. La, "A study on the insurance system for the improvement electronic commerce," *The J. Korea Res. Soc. for Customer*, vol. 4, no. 1, pp. 199-224, Feb. 2003.

[14] G. Y. Moon, "Why stuxnet, ducu, and dragonplay are more scary?" *Boan News*, Nov. 2015.

[15] H. Cavusoglu, B. Mishra, and S. Raghunathan, "A model for evaluating IT security Investments," *Commun. of the ACM*, vol. 47, no. 7, pp. 87-92, Jul. 2004.

[16] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The value of intrusion detection systems in information technology security architecture," *Inf. Syst. Res.*, vol. 16, no. 1, pp. 28-46, Mar. 2005.

[17] H. Jin and C. Y. Jung, "Convergence-based smart factory security threats and response trends," *J. Korea Convergence Soc.*, vol. 8, no. 11, pp. 29-35, Nov. 2017.

[18] H. Kwon and T. S. Kim, "A note on information security risk management using insurance," *Korean Academic Soc. of Business Administration Symp.*, pp. 1-3, Aug. 2009.

[19] H. S. Kang, J. Y. Lee, S. Choi, H. Kim, J. H. Park, J. Y. Son, B. H. Kim, and S. D. Noh, "Smart manufacturing: Past research, present findings, and future directions," *Int. J. Precision Eng. Manufacturing-Green Technol.*, vol. 3, no. 1, pp. 111-128, Jan. 2016.

[20] J. H. Hong, "Legal issues of insurance on liability from electronic commerce," *Dong-A Law Rev.*, vol. 59, pp. 325-359, May 2013.

[21] J. H. Kim and J. I. Lim, "Composition and policy direction of compensation insurance against customer information infringements in financial transactions," *The J. Soc. e-Business Stud.*, vol. 19, no. 3, pp. 1-21, Aug. 2014.

[22] J. Loveland, "Cyber-insurance - I do not think that word means what you think it mean," *RSA Conf. 2017*, San Francisco, U.S.A., Feb. 2017.

[23] J. T. Kim, "Analyses of countermeasure of vulnerability and device security on internet of things," *Asia-pacific J. Multimedia Serv. Convergent with Art, Humanities, and Sociol.*, vol. 7, no. 10, pp. 817-826, Oct. 2017.

[24] KISA, *2017 Survey on Information Security (Enterprise)*, KISA, Dec. 2017a.

[25] KISA, *Important Information Leakage Prevention Guide for Smart Factory*, KISA, Mar. 2017b.

[26] KISA, *Information Security Risk Management Guide*, KISA, Nov. 2004.

[27] KPMG, “Industrial 4.0 and manufacturing innovation: Introduction of smart factories and changing manufacturing paradigm,” *Insight*, KPMG, vol. 55, Dec. 2017.

[28] KPMG, *Now or Never: 2016 Global CEO Outlook*, KPMG, Jun. 2016.

[29] L. A. Gordon, M. P. Loeb, and T. Sohail, “A framework for using insurance for Cyber-Risk management,” *Commun. of the ACM*, vol. 46, no. 3, pp. 81-85, Mar. 2003.

[30] L. D. Bodin, L. A. Gordon, and M. P. Loeb, “Evaluating information security investments using the analytic hierarchy process,” *Commun. of the ACM*, vol. 48, no. 2, pp. 78-83, Fab. 2005.

[31] M. Hermann, T. Pentek, and B. Otto, “Design principles for industrie 4.0 scenarios,” *IEEE 2016 49th HICSS*, pp. 3928-3937, Hawaii, U.S.A., Jan. 2016.

[32] M. C. Libicki, D. Senty, and J. Pollak, *Hackers Wanted : An Examination of the Cybersecurity Labor Market*, Rand Corporation, Feb. 2014.

[33] MOTIE, *Smart Manufacturing Innovation Vision 2025*, MOTIE, 2017.

[34] M. S. Ahn, S. J. Park, and B. H. Meng, “A study on the establishment direction of electronic government information protection system,” *Korea Inf. Secur. and Cryptol. Rev.*, vol. 13, no. 3, pp. 1-14, Jun. 2003.

[35] MunichRe and Beazley, “Munich Re, Beazley Partner to Provide Enhanced Cover for Large Cyber Risks,” *Insurance J.*, Apr. 2017.

[36] N. Tuptuk and S. Hailes, “Security of smart manufacturing systems,” *J. Manufacturing Syst.*, vol. 47, pp. 93-106, Apr. 2018.

[37] OECD, *Enhancing the role of insurance in cyber risk management*, OECD, 2017.

[38] OECD, *The cyber insurance market: Responding to a risk with few boundaries*, OECD, 2018.

[39] R. Böhme and G. Schwartz, “Modeling cyber-insurance: Towards a unifying framework,” in *WEIS*, Harvard, U.S.A., Jun. 2016.

[40] PartnerRe and Advisen, *2017 Survey of Cyber Insurance Market Trends*, PartnerRe and Advisen, 2017.

[41] Presidential Council on Intellectual Property, *Measures for Strengthening Technology Protection Capabilities of SMEs*, 2016.

[42] R. L. Kumar, S. Park, and C. Subramaniam, “Understanding the value of countermeasure portfolios in information systems security,” *J. Management Inf. Syst.*, vol. 25, no. 2, pp. 241-280, 2008.

[43] RMS, *Managing Cyber Insurance Accumulation*, Risk Management Solutions and Inc. 2016.

[44] S. H. Lee, H. J. Jun, and T. S. Kim, “Risk management requirements for cyber insurance,” *J. KIISC*, vol. 27, no. 5, pp. 1233-1245, Oct. 2017.

[45] S. S. Jang, T. H. Cho, S. H. Shin, and D. C. Shin, *Establishment and Utilization of Information Security Management System*, SangNeung Publishing, Jun. 2015.

[46] Symantec, *Smarter security for manufacturing in the industry 4.0 era: Industry 4.0 cyber resilience for the manufacturing of the future*, Symantec Corporation, 2017.

[47] T. S. Kim, “Information security risk management using cyber insurance,” *General Insurance*, General Insurance Association of Korea, vol. 11, pp. 8-20, Nov. 2017.

[48] W. René, L. Tyler, H. Ramsey, and R. C. Hajj, *Cybersecurity in the Age of Smart Manufacturing*(2018), Retrieved Aug., 5, 2018. from https://deloitte.wsj.com/cio/2018/02/27/cybersecurity-in-the-age-of-smart-manufacturing/

이 송 하 (Song-ha Lee)

2015년 2월 : 충북대학교 경영정보학과 학사
2017년 2월 : 충북대학교 경영정보학과 석사
2017년 3월~현재 : 충북대학교 경영정보학과 박사과정

<관심분야> 정보보호 교육 및 인력, 정보보호정책, 보안경제성, 개인정보보호

전 효 정 (Hyo-Jung Jun)

2001년 2월 : 충북대학교 경영정보학과 학사
2003년 8월 : 충북대학교 경영정보학과 석사
2003년 9월~2007년 5월 : 한국전자통신연구원 사업기획팀 기술원
2014년 2월 : 충북대학교 경영정보학과 박사

<관심분야> 정보보호정책, 정보보호인력, 정보자원관리, 보안경제성

김 태 성 (Tae-Sung Kim)

1997년 2월 : KAIST 산업경영학과 박사
1997년 2월~2000년 8월 : 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2000년 9월~현재 : 충북대학교 경영정보학과 교수, 보안경제연구소장, 보안컨설팅연계전공 주임교수, 일반대학원 정보보호경영전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가위원, 행정자치부 전자정부 민관협력포럼 자문위원, 국방부 사이버보안 자문위원, KISA ISMS/PIMS 인증위원회위원, 한국전력 정보보안 자문위원, 보안GRC리더스포럼 공동의장

<관심분야> 정보통신과 정보보호 분야의 정책 및 경영 의사결정