KOSDI
ISSN : 1976-2208 (Print)
ISSN : 2671-5287 (On-line)
www.sodi.or.kr

Journal of the Society of Disaster Information
Vol. 17, No. 2, pp. 375-390, June 2021
https://doi.org/10.15683/kosdi.2021.6.30.375

Original Article

개인정보유출 사고 방지를 위한 중소기업의 사이버 위험관리

Cyber Risk Management of SMEs to Prevent Personal Information Leakage Accidents

소병기[1] · 정종수[2]*
Byoung-Ki So[1], Chong-Soo Cheung[2]*

[1]Doctor's Course, Department of Disaster and Safety Management, Soongsil University, Seoul, Republic of Korea
[2]Professor, Department of Disaster and Safety Management, Soongsil University, Seoul, Republic of Korea

*Corresponding author: Chong-Soo Cheung, isobcm@gmail.com

ABSTRACT

Purpose: Most of cybersecurity breaches occur in SMEs. As the existing cybersecurity framework and certification system are mainly focused on financial and large companies, it is difficult for SMEs to utilize it due to lack of cybersecurity budget and manpower. So it is necessary to come up with measures to allow SMEs to voluntarily manage cyber risks. **Method:** After reviewing Cybersecurity market, cybersecurity items of financial institutions, cybersecurity framework comparison and cybersecurity incidents reported in the media, the criticality of cybersecurity items was analyzed through AHP analysis. And cybersecurity items of non-life insurers were also investigated and made a comparison between them. **Result:** Cyber risk management methods for SMEs were proposed for 20 major causes of cyber accidents. **Conclusion:** We hope that the cybersecurity risk assessment measures of SMEs in Korea will help them assess their risks when they sign up for cyber insurance, and that cyber risk assessment also needs to be linked to ERM standardization .

Keywords: Risk Management, Cyber Security, Personal Information Leakage, Cyber Insurance

요 약

연구목적: 사이버보안 침해사고의 대부분은 중소기업에서 발생하고 있는데, 기존 사이버보안 프레임워크(Framework)와 인증체계 등은 주로 금융권이나 대기업에 초점이 맞추어져 있어 정보보안 예산과 인력이 부족한 중소기업이 활용하기에는 어려움이 많아 중소기업이 자율적으로 사이버위험관리를 할 수 있는 방안을 마련할 필요가 있다. **연구방법:** 사이버보안 시장, 금융기관 사이버보안 항목, 사이버보안 프레임워크 비교, 언론에 보도된 사이버보안사고 등을 통해 사이버보안에 중요한 항목을 도출하고 이를 AHP 분석을 통하여 그 중요도를 분석하고, 손해보험사의 사이버보안 항목을 조사·비교 하였다. **연구결과:** 주요한 사이버사고 원인 20가지에 대한 중소기업의 사이버위험관리 방안을 제시하였다. **결론:** 본 연구에서 도출된 국내 중소기업의 사이버보안 위험평가방안이 향후 중소기업이 사이버보험 가입 시 그 기업의 위험평가에 도움이 되길 바라고 사이버 위험평가도 ERM 규격화의 한 부분에 포함되기를 희망해 본다.

핵심용어: 위험관리, 사이버보안, 개인정보유출, 사이버보험

Received | 20 May, 2021
Revised | 23 June, 2021
Accepted | 25 June, 2021

서 론

정보통신망 발달에 따라 사이버보안 위협이 크게 증가하고 있고 2001년 미국 911 테러이후 공포자극을 위한 민간인을 상대로한 테러가 급증하는데(Oh, 2019)반해, 정부의 재난대응 체계는 주로 대형재난에 초점이 맞춰져 있고 피해규모가 작은 사회재난에 대해서는 상대적으로 적절히 관리되지 못한 상황이라고 하고(Kim et al., 2016) 한편 인터넷 자체가 기술적으로도 쉽게 침해받을 수 있게 디자인되어 있다는 점과(Spinello, 2003; Lee, 2006) 해킹 등을 통해 금전적 이득을 취할 수 있기 때문이다.

최근 발생하는 사이버보안 침해사고의 대부분은 중소기업에서 발생하고 있는데, Symantec(2018)에 따르면, 2016년에 발생한 모든 사이버공격이나 사이버 침탈의 60%가 중소기업(종사자수 251~500명)을 목표로 하고 있으며, 중소기업 중 68%가 사이버보안을 확신할 수 있는 시스템적인 접근이 없고, 사이버공격을 받은 중소기업 중 60%가 회복하지 못하거나 6개월 이내에 회사 문을 닫게 된다고 한다. 이는 중소기업이 대기업보다 사이버보안 침해사고 발생 시 회복할 수 있는 능력이 매우 부족하기 때문이다. 특히 사이버 보안사고로 인한 손해를 보상받을 수 있는 사이버보험을 대기업은 약 40% 정도 가입하고 있는데 반해, 중소기업은 3% 미만이 가입하고 있다고 한다(AON, 2016).

이와 같이 중소기업은 사이버위험에 직접적으로 노출되어 있음에도 사이버보안에 대한 인력이나 시설투자를 적극적으로 하기 어려운 측면이 있다. 또한 조직이 네트워크에서 악의적인 공격을 식별하는데 걸리는 평균시간은 229일 정도라고 하며(NASSTAR, 2019), 그에 따라 사이버보안은 예방이 최선인데, 사이버공격의 약 80% 정도는 가장 기본적인 위험관리를 통해서 방지할 수 있다는 주장도 있고(NASSTAR, 2019), 사이버 위협에 대응하기 위해서는 현재의 사이버 위협요인과 그에 따른 사이버보안 능력을 평가하고, 부족한 부분을 보완해야 한다. 이러한 일련의 사이버보안 과정을 사이버보안 프레임워크라고 하며, 기밀성(confidentiality), 무결성(integrity), 가용성(availability) 등 3요소 또는 인증성(authenticity), 이용성(usability)을 포함한 5요소를 고려하여 지금까지 많은 연구가 진행되어 오고 있다(Kim, 1997). 사이버보안 국제인증인 ISO 27000(27001/27002/27005/27017/27018) 제도와 우리나라의 ISMS와 ISMS-P 인증도 이러한 사이버보안 프레임워크에 기반을 두고 있다.

우리나라는 「전자금융거래법」과 전자금융감독규정을 통해 사이버보안 관리강화를 추진하였는데, 이는 금융기관에 초점이 맞추어져 있고, 「정보통신망법」에 의한 ISMS나 ISMS-P 의무대상은 정보통신서비스 부문 전년도 매출액 100억원 이상, 전년도 직전 3개월간 일평균 이용자수 100만명 이상으로 매우 제한적이어서 2020. 6월 기준 ISMS 유효인증건수는 453건에 불과한 실정이다. 또한 ISO 27001(v.2013)은 14개 중분류와 114개 세부항목, ISMS(v.2019)는 80개, ISMS-P(v.2019)는 102개의 세부항목으로 구성되어 있어 중소기업이 활용하기에는 평가항목이 너무 많고, 외부 컨설팅사의 자문이 불가피하다. 일반 중소기업이 금융기관이나 대기업과 같이 사이버보안 투자나 망분리를 하기 어려운 상황이고, 평균 1천만원 수준의 비용이 수반되는 ISMS 인증도 받기 어려운 상황이기 때문에, 사이버보안에 대한 기본적이고 실질적이면서 다른 차원의 보안 강화를 할 수 있는 관점이 필요하다.

따라서 본 연구에서는 기존에 알려진 다양한 사이버보안 프레임워크와 사이버보안 사고 중 언론에 알려진 개인정보유출 사고를 기반으로 중소기업에 적합한 사이버보안 위험평가 항목을 AHP 도출하고, 보험적 시각을 고려하여 사이버보안 위험관리 방안을 제안하고자 한다.

이론적 배경

사이버보안 프레임워크

1995년 영국표준협회(BSI, British Standards Institution)에서 정보보호 관리를 위한 실무규약(Code of practice for information security management specification)인 BS 7799를 가장 먼저 개발하였고, Part1(정보보호관리 Best Practice)은 ISO/IEC 17799(정보보호관리 실무규범)을 거쳐 ISO 27002가 되었고, Part2(정보보호관리규격)은 2005년 ISO/IEC 27001(정보보안관리시스템)의 국제표준이 되었다(Korea Communications Commission & KISA, 2010; Min et al., 2006). ISO 27001의 구조는 Plan - Do - Check - Act 등 4단계로 구성되어 있는데, ISO 27001(v.2013) 인증을 받기 위해서는 ISO가 요구하는 평가 세부항목을 기반으로 조직이 정보보호관리체계를 수립하고 운영하고 있는지를 평가받아야 하며, 구체적으로 계획, 현황분석, 위험분석, 체계설계, 구현, 모니터링 단계에 대해 평가를 받아야만 한다(Son, 2014).

미국은 금융업을 중심으로 사이버보안이 가장 먼저 도입되었는데, 1996년 연방금융기관검사위원회(The Federal Financial Institutions Examination Council, FFIEC)에서는 Cybersecurity Assessment Tool인 FFIEC 전자금융 검사매뉴얼(IT Audit)을 도입한 이후, 2006년과 2016년 10년 단위로 지속적인 개정을 거쳐 IT Handbook(Information Technology Examination Handbook)을 운영하고 있다. 그리고 2014년 미국 표준위원회(National Institute of Standards and Technology, NIST)에서 NIST CSF(Cybersecurity Framework)를 발표하였고, 2017년 뉴욕주 금융청에서는 미국 주정부 최초로 금융기관에 대한 사이버보안규정인 NYCRR 500을 의무화(2017.3.1. 시행)하였다(Kim et al., 2018).

우리나라도 2002년 5월 한국인터넷진흥원(구, 한국정보보호진흥원, KISA) 주도로 정보보호관리체계(Information Security Management system, ISMS) 인증제도를 도입하였고, ISMS의 활성화 및 평가지표 보완을 위한 연구가 진행되었다(Korea Information Security Agency, 2003; Kim et al., 2012).

사이버 위험평가

사이버보안은 매우 광범위하기 때문에 다양한 사이버보안 프레임워크 연구와 다양한 사이버위험평가 방법이 제시되고 있다. 해외에서는 사이버보안 프레임워크와는 별개로 사이버보안 위험평가에 대한 연구가 많이 이루어졌는데, 영국의 경우 Oxford와 Cambridge 대학의 사이버위험연구소에서 위험평가 항목도출 연구가 많이 진행되었고, 세계적인 회계 및 컨설팅법인(Deloitte, Ernst&Young, KPMG, PwC 등)에서도 사이버위험 평가항목을 제시하고 있다. 유럽은 GDPR(2018. 5시행)과 NIS지침(2016.7)에 따라 유럽네트워크정보보호원(ENISA)에서 사이버위험 평가항목을 제시하였다. Radanliev et al.(2018)은 사물인터넷(IoT, Internet of Things) 사이버보험에서 양적평가방법 11개과 질적평가방법 5개 등 총 16개 방법론을 사용하여 위험을 평가하였다. Radanliev et al.(2019)은 FAIR, CMMI, CVSS, ISO, NIST, Octave, TARR 등 다양한 선진적 사이버보안 프레임워크를 비교분석하여 사물인터넷(IoT, Internet of Things)에 적합한 Risk Model을 도출하려고 하였다.

국내에서도 사이버 위험에 대응하기 위한 각 분야별 사이버 리스크 평가항목을 도출하는 연구가 진행되었는데, 초기에는 사이버 보안기술에 대한 연구가 주류를 이루었다. Kim et al.(2005)은 전자상거래 웹사이트의 보안평가 시 보안기술(인증기술, 암호화기술, 침입탐지 및 방지)와 보안제도 및 정책(정보보호정책, 데이터베이스 보호정책), 그리고 보안관리 및 운영(보안통제관리, 서비스관리, 조직 및 인력관리) 등 크게 3개 분야와 8개 중분류, 21개 세부항목 등을 AHP 방법론을 이용해 우선순위를 선정하였다. Min et al.(2006)은 보안관리수준 평가를 위해서는 영국 BS 7799, ISO/IEC 27001와 같은 유연성을 확

보하고, 미국 정보보안관리법(FISMA, Federal Information Security Management Act)과 같이 정부 부처가 필수적으로 수행해야 하는 필수통제항목이 필요하다고 하였다. Lee et al.(2008)은 SK텔레콤 사례를 통해 개인정보 유출위험을 평가하기 위해 개인정보 라이프사이클을 수집, 저장, 이용, 제공, 파기 등 5개의 단계로 구분하고, 보안관리자가 검토해야 하는 항목을 규정하였다. Park et al.(2008)은 Privacy-i를 개발한 경험을 통해 개인용컴퓨터(PC) 내부의 개인정보 보호를 위해 개인정보 보관 검출, 패턴추가 및 편집기능, 파일 및 메일 분석기능, 암호화 강제기능, 개인정보 삭제 강제기능, 기타 기능 등 6개의 개인정보보호시스템 요구사항을 규정하고, 이를 효과적으로 관리하기 위한 시스템 설계를 제안하였다. Kim et al.(2010)은 악성코드 동향과 악성코드가 유포되는 경로와 악성코드의 발전과정을 제시하고, 특히 SNS에서 악성코드의 위험성을 강조하였다.

인터넷망 발달에 따라 국내의 사이버보안 연구는 네트워킹 분야로 확대되었다. Kim(2009)는 전자금융사고 발생유형을 클라이언트 구간, 네트워크 구간, 시스템 구간 등 3개의 구간으로 구분하고, 클라이언트 구간에서는 악성코드와 사용자부주의, 비정상거래 오인(피싱 또는 파밍), 카드복제 등의 위험이 있고, 네트워크 구간에서는 데이터 도청 및 변조, DDoS 등의 위험이 있으며, 시스템 구간에서는 사용자정보 탈취공격, DDoS 등 공격을 통한 시스템 마비 등의 위험이 있음을 언급하였다. Cho et al.(2012)은 개인정보 유출 모니터링 시스템 설계 시, 개인정보 조회 오남용과 개인정보 과다 보유 등 여러 위험정보를 정량적으로 지수화한 핵심위험지표(KRI, Key Risk Indicator)를 측정하는 것을 통해 임계치를 설정하고 임계치 초과 시 경보를 발령함으로써 개인정보 유출이 내부직원, 인터넷서비스, 데이터베이스 등에서 유출되는 것을 최소화할 수 있다고 주장하였다.

최근에는 국내에서도 사이버보안 프레임워크에 대한 연구가 진행되었는데, ISMS 및 ISMS-P와 각분야 사이버보안의 요구사항과의 비교평가 연구가 주류를 이루고 있다. Kim et al.(2017)은 사이버레질리언스 평가지표를 위해 CERT-RMM, 세계경제포럼(WEF)의 성숙도 모델, 국제증권감독기구(CPMI-IOSCO)의 가이던스를 비교하여 10개 영역과 22개 지표를 도출하고, ISMS와 비교 시 ISMS과는 18개 지표가 중복되고 4개 지표가 차이가 있다고 하였다. Kim et al.(2018)은 미국 뉴욕주 NYCRR 500에 대해 조문별로 분석하면서 국내 「전자금융거래법」과 전자금융감독규정과 비교하였고, NYCRR500이 각 금융기관별로 모의침투 테스트, 주기적인 위험평가 등 사이버 취약성을 스스로 분석하도록 하는 것이 유용하다는 시사점을 도출하였다. Kim(2019)는 Cambride, Deloitte, ENISA, K-ISMS 등 5개의 사이버리스크 평가항목 131개를 비교하고, 3개 이상이 중첩된 24개 공통평가항목을 분류하였다. 이후 24개 공통항목을 포함하여 총 29개의 리스크 평가항목을 일반현황평가 11개와 보호대책평가 18개로 분류하였다.

중소기업 사이버 위험평가

지금까지 사이버보안에 대한 프레임워크, 레질리언스, 인증 및 보안규정 등에 대해서는 주로 금융업과 대기업을 중심으로 많은 연구가 진행되어 왔다. 미국은 FFIEC, 뉴욕주 NYCRR 500 등이 있고, 우리나라는 ISMS, ISMS-P와 「전자금융거래법」 및 동법 시행령에 따른 전자금융감독규정(Financial Services Commission, 2019)이 있으며, 국제기준으로는 ISO 27001 등이 있다. 최근 금융분야는 보안산업과의 협업을 통해 개방되고 투명한 보안성 확보방안을 마련 중이라고 하며(Jeong, 2018), 국내 주요 정보통신기반시설은 「정보통신기반보호법」 제9조에 따라 매년 취약점에 대해 분석·평가를 실시한다고 한다(Kim, 2019).

그러나 이러한 유용한 사이버위험 평가체계는 평가항목이 너무 많고, 검사인증비용이 발생하고, 전문인력이 필요하거나 컨설팅이 필요하기 때문에 중소기업이 활용하기에는 많은 어려움이 있다. 중소기업의 사이버위험관리를 위해서 많은 국가들이 노력하고 있는데, 미국은 2014년 NIST에서 NISTIR 7621을 통해 소규모사업장의 정보보안에 대한 지침을 제시하였고(NIST, 2016), 호주는 2017년 소기업에 대한 사이버보안 Best Practice Guide를 제시하였다(Australian Small Business and Family Enterprise Ombudsman, 2017). 그 외에도 많은 국가와 여러 대학, 연구소 등에서 중소기업들에 대한 사이버보안 가이드라인을 많이 제시하고 있다.

국내에서는 중소기업의 사이버보안을 지원하기 위해서 2010년 지식경제부에서 ISO 27001을 번역하여 중소기업에게 배포하였고(Ministry of Knowledge Economy, IO Consulting Co., Ltd., 2010), Korea Internet & Security Agency(2012, 2020)에서는 2012년 중소 IT서비스 기업을 위한 정보보호 안내서를 제작하였고, 2020년 종사자 10명 미만의 영세사업자가 활용할 수 있는 중소기업 정보보호 실무가이드(총 2권)을 제작하였다. 또한 중소기업의 사이버보안을 향상시키기 위한 많은 연구와 제안이 있었는데, Jung(2017)은 COMODO(방화벽), CASTLE(웹방화벽), COMODO Killswitch(프로세스 모니터) 등 오픈소스 프로그램을 활용해서 중소기업의 보안을 향상시키는 것을 제안하였고, Park(2020)는 중소기업의 사업연속성을 위해서 IT기반 공동재해복구센터를 운영하는 것을 제안 하였다.

그러나 이러한 중소기업에 대한 사이버보안 가이드라인도 기존에 심화되어 있는 여러 가이드라인의 축소판으로 중소기업 입장에서는 전문용어를 이해하기 어렵고, 위험평가를 스스로 하기에는 미흡한 측면이 여전히 존재한다.

연구방법

중소기업 사이버보안 위험평가 항목 선정

기존 사이버보안 프레임워크 등은 원론적으로 관리적 보호조치, 기술적 보호조치, 물리적 보호조치 등 사이버보안 전반에 걸친 내용으로 주로 금융권이나 대기업에 초점이 맞추어져 있어서 중소기업이 이를 활용하기에는 많은 어려움이 있다. 따라서 중소기업에 적합한 실효성 있는 사이버보안 체계마련이 필요하다. 그렇다고 기존의 사이버보안 프레임워크를 의도적으로 생략하거나 제외 시 사이버보안이 위험할 수 있기 때문에 해당 업종에 맞는 선별적 접근이 필요하다. 중소기업이 금융업과 같이 망분리를 하기도 곤란하며, 각종 보안장비나 보안프로그램을 설치하기도 곤란하기 때문이다. 물론 내부전산망과 인터넷망을 분리해도 고도로 지능화된 APT공격을 당하거나, 이동식 저장매체(USB 등)를 통해 악성코드가 유입될 수 있기에 주의가 필요하다(Cho et al., 2015).

중소기업에 적합한 사이버위험 평가를 위해서 사이버보안시장, 금융기관 사이버보안 항목, 사이버보안 프레임워크 비교, 언론에 보도된 사이버보안사고 등을 조사하였다. 사이버보안시장은 International Security Exhibition & Conference (2019)의 IT 보안분야 47개와 Song et al.(2018)의 연구에 있는 Gartner 16개, Technavio 10개, Markets&Markets 16개 분야를 참고하여 네트워크, 시스템보안, 콘텐츠/정보유출방지, 암호인증, 보안관리, 보안컨설팅, 유지관리, 교육/훈련, 기타 등으로 구분하였다. 금융기관 사이버보안 항목은 전자금융감독규정(Financial Services Commission, 2019) [별표2. 정보기술부문 및 정보보호 예산기준] 2-다. 정보보호시스템 분류표와 금융분야 클라우드컴퓨팅서비스 제공기준, 그리고 금융회사의 업무위수탁 관련 규정을 참고하였다. 사이버보안 프레임워크 비교는 ISO 27001(v.2013), ISMS-P(v.2019), NIST CSF(v.2018), Deloitte (2017) 등의 자료를 활용하였다. 사이버보안사고 사례는 Table 1과 같이 2006년부터 2017년까지 Wikipedia, Korea(2021),

Namu.Wiki(2021)와 언론에 알려진 주요 개인정보유출사고 30건을 활용하였다. DDoS나 랜섬웨어 공격은 세부적으로 알려지지 않기 때문에 개인정보유출사고를 사이버보안사고로 판단하였다. 사이버보안 프레임워크의 공통항목을 중심으로 사이버보안시장, 금융기관 사이버보안 항목, 언론에 보도된 사이버보안사고 등의 항목을 상호 연결하고 종합적으로 검토하여 4개 분야, 분야별 5개 항목 등 총 20개 항목을 중소기업 사이버보안 위험평가항목으로 Table 2와 같이 선정하였다.

Table 1. Lists of personal information leakage accidents

구분	사건일시	유출규모	단위	개인정보 주요 유출원인
1.1	2006~2008	6,510,000	명	직원유출. 개인정보를 텔레마케팅사에 판매 (비인가직원이 개인정보에 접근하고, USB에 저장)
1.2	2008.2, 2008.4	18,630,000	명	해킹. 이메일(악성코드)로 해커가 관리자인증정보 획득 (이메일 첨부파일 악성코드 열람)
1.3	2008	9,700,000	건	공공장소에서 무인증 무선공유기에 접속, 해커가 DB계정 접근권한 획득
1.4	2008.9	11,250,000	명	직원유출. 개인정보 엑셀파일 CD가 길거리에 버려짐
1.5	2010.3	20,000,000	건	비암호화, 로그기록 보관안함. 추후 해커검거로 유출이 밝혀짐
1.6	2011.4	1,750,000	명	해킹(퇴사직원의 ID와 PW 미삭제, 관리자PC 해킹)
1.7	2011.7	35,000,000	명	해킹. 무료프로그램 업데이트위장 악성코드
1.8	2011.8	350,000	명	해킹(개인정보 비암호화)
1.9	2011.11	13,200,000	명	해킹(백업서버와 임원PC 내 악성코드), DB접근통제의 문제
1.10	2012.3	200,000	명	개인정보이용동의 없는 활용(위치정보 등을 심부름센터 등에 판매)
1.11	2012.5	4,220,000	명	해킹(홈페이지 내 악성코드). DB암호화를 안함. 탈퇴회원정보 미파기
1.12	2012.6	1,980,000	명	직원유출(접근통제 실패)
1.13	2012.7	8,700,000	명	해킹. 대리점PC와 VPN간(데이터송수신) 암호화를 안함 대리점PC에는 방화벽이나 백신 등 보안프로그램 설치 없음
1.14	2013.4	130,000	명	직원유출
1.15	2013.5	912	명	해킹
1.16	2013.6	2,9400,000	명	해킹(웹사이트 변조, DDoS분산서비스 공격)
1.17	2013.10	>2,900,000	명	해킹(전산망침투, 클라우드 보안문제). 해외사이트(국내 유출규모 미공개)
1.18	2014.1.20	104,000,000	건	아웃소싱직원유출. 비인가USB 차단시스템이 없음. 개인정보 보유기간 초과보유
1.19	2014.3	12,000,000	명	해킹(홈페이지, 불법해킹프로그램 활용)
1.20	2014.3	20,000,000	명	정부-정비소간 비암호화 전송으로 차량번호 무단조회가능
1.21	2014.4	3,500,000	명	해킹(2011년부터 유출, 2014년 확인)
1.22	2015.3	750,000	건	공공아이핀 부정발급. 본인확인조치 미흡
1.23	2015.9	2,000,000	명	해킹. 결함있는 암호알고리즘. 열람권한조치미흡
1.24	2016.7	10,300,000	건	해킹(망분리소홀, 암호화소홀)
1.25	2017.6	36,000	명	실운영자 이메일 내 악성프로그램, 해당PC 백신미설치. 내부통제 및 보안시스템 부실
1.26	2017.7	33,000,000	건	로그기록 없음. 추후 해커검거로 유출이 밝혀짐 (보안업데이트 소홀로 보안취약점 공격으로 해킹)
1.27	2017	990,000	건	해킹(SQL인젝션 등을 통해 관리자권한 확보)
1.28	2017.9	130,000	건	해킹. 침입차단시스템 미설치 등 전반적 보안체계미흡
1.29	2017.9	420,000	명	해킹. 유지보수업체직원 PC 악성코드 감염. 해커금전요구로 밝혀짐. 수탁업체 직원에 대한 관리감독 미흡
1.30	2017.11	200,000	건	해킹. 보안체계 미흡

Table 2. 20 Risk assessment Items for SME's cyber security

4개 분야	T2.Q1. 사이버보안 정책, 인력, 조직	T2.Q2. 사이버 위험관리 차단, 보안장치	T2.Q3. 사이버보안 개인정보 관리	T2.Q4. 사이버보안 개인PC 보안설정
각 분야별 5개 항목 (총20개)	(2.1) 정보보호사규 (보안지침 등)	(2.6) 보안지역설정 (시건장치)	(2.11) 개인정보암호화 (암호화 프로그램)	(2.16) 부적절OS (윈도우XP 등)
	(2.2) 정보보호조직	(2.7) 직원신분증 착용 (외부인 통제)	(2.12) 개인정보 암호화전송	(2.17) 백신 미설치
	(2.3) 정보보호책임자 임명	(2.8) 방화벽 등 보안장치	(2.13) 개인정보접근제한 (비인가자)	(2.18) PC 방화벽 미설정
	(2.4) 정보보호 교육	(2.9) ID, PW 강화 (OTP 등 2중 보안)	(2.14) 휴대용저장 제한 (USB 저장 불가)	(2.19) 키보드 보안프로그램 미설치
	(2.5) 개인정보유출 시 대응절차	(2.10) 로그기록 보관	(2.15) 기간만료 폐기	(2.20) 보안업데이트 미흡

따라서 연구방법 프로세스는 4단계로 Fig. 1과 같다.

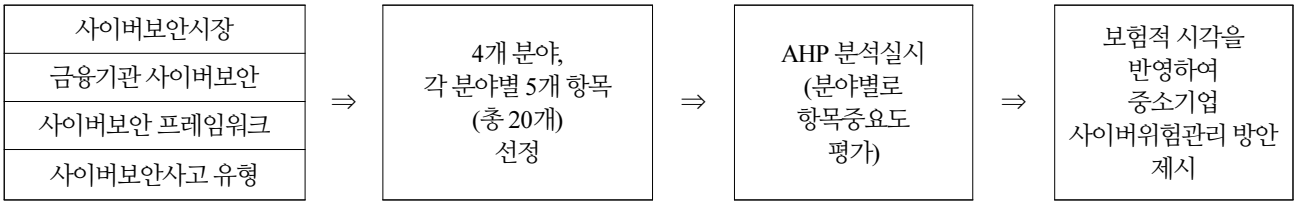

Fig. 1. Flow of research method

AHP을 통한 분야별 중요도 분석

4개 분야에서 각 분야별 5개 항목의 중요도를 판단하기 위하여 계층적 의사결정 방법론인 AHP(Analytic Hierarchy Process) 방법론을 통해 중요도를 평가하였다. 분석 대상으로는 사이버보안, 위험관리, 경영관리, 재난관리 분야 전문가 40명으로 "사이버사고에 기반한 중소기업 사이버위험관리 방안" 설문지를 통해 4개의 분야별로 각 분야별 5개의 항목의 중요도를 조사하였다. 평가항목별 배점은 Table 3과 같이 1~9점으로 하였고, 동등한 경우 배점을 1로 하였다. 4개 분야별 중요도 우선순위는 조사하지 않았다.

Table 3. Score of AHP assessment item

	← (2.1)가 더 중요함								동등	(2.2)가 더 중요함 →								
평가항목 <표2> T2.Q1. (2.1)	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	평가항목 <표2> T2.Q1. (2.2)
	절대중요		매우중요		중요		약간중요		같음		약간중요		중요		매우중요		절대중요	

AHP는 전문가들의 주관적 평가에 따라 결정되므로, 인간의 추론에 있어서 편이(bias)와 오류(error)는 불가피하게 발생할 수 밖에 없는 한계점이 있고 사고의 일관성이 부족할 수 있는데, 통상 일관성 비율(CR, consistency ratio)이 0.1(10%) 이하면 사고의 일관성이 인정된다고 한다(Yoon, 1990). 따라서 Table 2의 4개 분야내 5개 항목간 우선순위 설문조사 40건 중 CR값이 0.1(10%)이내인 것은 T1.Q1 25명, T1.Q2 24명, T1.Q3 24명, T1.Q4 33명이었는데, T1.Q1~T1.Q4 모두 CR 값이 0.1(10%) 이내인 22건을 분석에 활용하였다. 22건 중 10건은 국내 IT분야 대기업 보안회사에 소속된 전문가들의 의견이었다. 평가항목이 5개로 n=5를 적용하였고, RI는 n=5일 때의 계수 1.12를 적용하였다. AHP 분석석방법은 Kinosita et al. (2012)을 참고하여 적용하였다.

$$CI = (\lambda max - n) / (n - 1),\ CR = CI / RI \text{ (Random Index)}$$

보험적 시각을 고려한 위험평가 방법

선진국은 사이버보험을 통해 사이버보안을 강화시키고 있다. 보험은 1차적으로 우연한 사고 발생에 따른 손실을 보상하는 금융제도지만, 2차적으로 보험에 가입한 계약자들의 위험 정도에 따른 보험료 할인할증 제도를 갖추고 있어서 사고를 예방하거나 손실을 줄이는 순기능이 있기 때문이다(Korea Insurance Development Institute, 2015).

보험은 주로 기술적인 요인보다는 기술적 요인에 의해 나타나는 현상을 통해 위험을 관리한다. 보험에서는 사이버보안 사고의 발생사례와 피해정도 등 경험사례가 가장 중요하다. 보험시각적 관점에서 사이버보안은 (i)보험사고가 발생하지 않거나 (ii)보험사고가 발생해도 최소한의 범위로 피해를 최소화하는 것이다. 전자는 방화벽이 뚫린 해킹이 발생했다고 하더라도 지적재산권이나 개인정보 등 정보자산이 유출되지 않고, 물리적 보안장비 등에 피해가 발생하지 않는 것을 말하며. 후자는 피해가 발생 시 큰 피해가 발생하지 않거나, 피해를 최소화할 수 있는 방법이 있는 것이다.

보험적 시각에서 중소기업 대상 사이버보안은 첨단장비나 첨단소프트웨어의 구입보다 기본을 얼마나 충실히 지키고 있는지와 기존에 잘 알려진 사이버 해킹사례에 대한 대비책의 존재 여부이다. 사이버 해킹은 어디서든 발생이 가능한 만큼, 불가피하게 발생한 피해를 보상하는 것이 보험이기 때문에 보험사는 보험사고가 언제든지 발생할 수 있다는 것을 전제로 위험관리나 위험평가를 실시한다.

「정보통신망법」에 따른 개인정보유출 배상책임 의무화로 국내 손해보험사는 개인정보유출배상책임보험 또는 사이버보험을 판매하고 있는데, 보험사는 계약자가 얼만큼 위험한지 여부를 판단하는 방법으로 계약자로부터 설문조사를 받고 있다. Table 4는 2019년 기준 각 손해보험사에서 사이버보험을 인수하기 위해 계약자로부터 설문조사 항목을 비교한 것이다.

Table 4. Insurance company' checklists for cyber insurance

구분		보험사	A_1	A_2	B	C	D_1	D_2	E	F	G	H
회사 개요	1.1	연간매출액	∨	∨	∨	∨	∨	∨	∨	∨	∨	∨
	1.2	홈페이지 여부										∨
	1.3	보유 개인정보수	∨	∨	∨	∨	∨	∨	∨	∨	∨	∨
	1.4	개인정보 세부항목		∨						∨	∨	∨
	1.5	업종구분	∨	∨	∨	∨		∨	∨		∨	∨

Table 4. Insurance company' checklists for cyber insurance (Continue)

구분		보험사	A_1	A_2	B	C	D_1	D_2	E	F	G	H
정보관리체계	2.1	정보시스템운영방식(직접, 위탁)			∨							
	2.2	정보관리 사규		∨				∨		∨		∨
	2.3	개인정보보호 책임자					∨	∨	∨		∨	∨
	2.4	정보보호 교육 및 연간교육횟수			∨	∨	∨	∨	∨		∨	∨
	2.5	정보관리 모니터링		∨						∨		
	2.6	개인정보취급절차 매뉴얼		∨	∨		∨	∨		∨		∨
	2.7	개인정보 누출 시 대응절차		∨	∨	∨	∨	∨	∨	∨	∨	∨
위수탁	3.1	개인정보 수탁여부		∨						∨		∨
	3.2	개인정보 공유여부		∨						∨		∨
	3.3	개인정보 위탁여부		∨						∨		∨
	3.4	개인정보 위탁업체 선정기준		∨						∨		
	3.5	위탁계약서상 의무사항 적시		∨		∨	∨	∨		∨		∨
정보보호 및 보안	4.1	신분증착용의무, 외부자출입금지		∨		∨	∨	∨		∨		
	4.2	서버접근 ID, PW		∨	∨		∨	∨		∨		∨
	4.3	서버관리자 OTP 적용			∨							
	4.4	서버접근 PW 주기적 변경		∨								
	4.5	퇴직자 접근차단		∨	∨					∨		∨
	4.6	외부자보안관리(외주IT직원 등)			∨							
	4.7	방화벽	∨	∨	∨					∨		∨
	4.8	방화벽 테스트		∨								
	4.9	모의해킹 테스트			∨		∨	∨				∨
	4.10	백신프로그램		∨			∨	∨		∨		∨
	4.11	정보보호 소프트웨어 사용여부			∨	∨	∨	∨				∨
	4.12	개인정보서버 로그기록보관		∨		∨	∨	∨		∨		∨
	4.13	개인정보보관 물리적차단(시건)		∨						∨		∨
	4.14	노트북 비밀번호 설정		∨								
	4.15	노트북 등 모바일기기 반출입통제			∨							
	4.16	휴대용저장장치 사용통제			∨							
	4.17	개인정보 송수신 시 암호화		∨			∨	∨		∨		
	4.18	개인정보 적정 폐기		∨						∨		∨
	4.19	정보보안 인증	∨	∨	∨	∨				∨	∨	∨
	4.20	개인정보DB암호화	∨	∨	∨	∨	∨	∨			∨	
	4.21	DB암호화 개인정보 항목		∨								
	4.22	DB암호화 솔루션명		∨								
	4.23	DB암호화 CC/K4 인증		∨								
	4.24	DB암호화 공인된 알고리즘		∨								
	4.25	망분리	∨	∨	∨	∨	∨	∨			∨	
	4.26	데이터 백업									∨	

Table 4. Insurance company' checklists for cyber insurance (Continue)

구분		보험사	A_1	A_2	B	C	D_1	D_2	E	F	G	H
보험 조건	5.1	보험가입이력	∨	∨								∨
	5.2	법규위반 이력				∨	∨	∨			∨	
	5.3	개인정보유출이력	∨	∨	∨		∨	∨		∨	∨	∨
	5.4	유출이력 세부사항		∨	∨					∨	∨	∨
	5.5	5년 내 전사시스템 개발		∨								
	5.6	시스템 개발 시 보안점검			∨							

(출처 : 국내 주요 손해보험사 8개사(A_1과 A_2는 동일보험사로 기업규모별 차등조사)의 사이버보험 가입 설문조사 자료)

분석결과

AHP를 통한 중소기업 사이버보안 중요인자 우선순위 도출

AHP 방법론은 계층적 분석방법으로 다단계 분석방법에 활용할 수 있으나, 본 연구에서는 4개 분야별 중요도는 별도로 조사하지 않고, 4개의 분야에서 각 분야별 5개 평가항목별로 중요한 우선순위를 조사하였다. 이유는 4개의 분야 모두 중요하다고 판단했기 때문이다.

설문지 40건 중 CR 0.1(10%) 이하인 22건에 대한 평균값을 분석하였다. 22건 중 12건은 경영관리, 재난관리 전문가들(표본A)이었고, 10건은 사이버보안 전문가들(표본B)이었다.

사이버보안 정책, 인력, 조직 측면에서 가장 중요한 것(Fig. 2)에 대해 표본A(n=12)는 정보보호조직(25.7%) > 정보보호책임자 임명(21.6%) > 정보보호사규(20.7%) > 정보보호 교육(18.6%) > 개인정보유출 시 대응절차(13.5%) 순이었다. 사이버보안 전문가들인 표본B(n=10)의 판단은 정보보호사규(32.1%) > 정보보호조직(28.6%) > 정보보호책임자 임명(23.9%) > 개인정보유출 시 대응절차(8.0%) > 정보보호 교육(7.3%) 순이었다. 중요한 항목 3가지는 공통적으로 정보보호사규, 정보보호 조직, 정보보호책임자 임명이었다. 상대적으로 정보보호교육의 비율이 낮은 것은 교육이 효과적이지 못한 현실이라 생각되며, 정보유출 시 대응절차는 이미 정보유출이 되었기 때문에 낮은 것으로 판단된다.

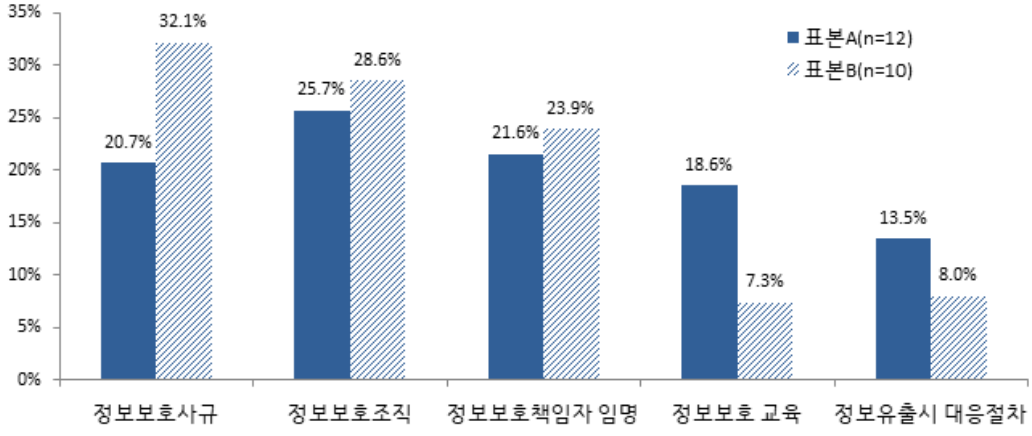

Fig. 2. Results of criticality assessment in terms of cybersecurity policy & leadership

사이버 위험관리의 차단, 보안장치 측면에서 가장 중요한 것(Fig. 3)에 대해 표본A는 방화벽 등 보안장치(40.5%) >ID, PW 강화(30.3%) > 보안지역설정(12.3%) > 로그기록 보관(9.5%) > 직원신분증 착용(7.5%) 순이었다. 표본B는 방화벽 등 보안장치(35.0%) > ID, PW 강화(25.2%) > 보안지역 설정(15.7%) > 직원신분증 착용(12.8%) > 로그기록 보관(11.2%) 순이었다. 중요한 항목 3가지는 공통적으로 방화벽 등 보안장치와 ID, PW 강화, 보안지역 설정이었다. 비록 방화벽은 해킹의 일부분만 방어함에도 여전히 여전히 네크워크/웹 방화벽은 유용하고, 통상적으로 패스워드 글자 하나가 늘어나게 되면 보안수준은 2~10배 정도 증가한다고 알려져 있어(Yang, 2019), 중소기업이 큰 비용없이 유용하게 사이버보안을 강화할 수 있을 것이라 판단한다.

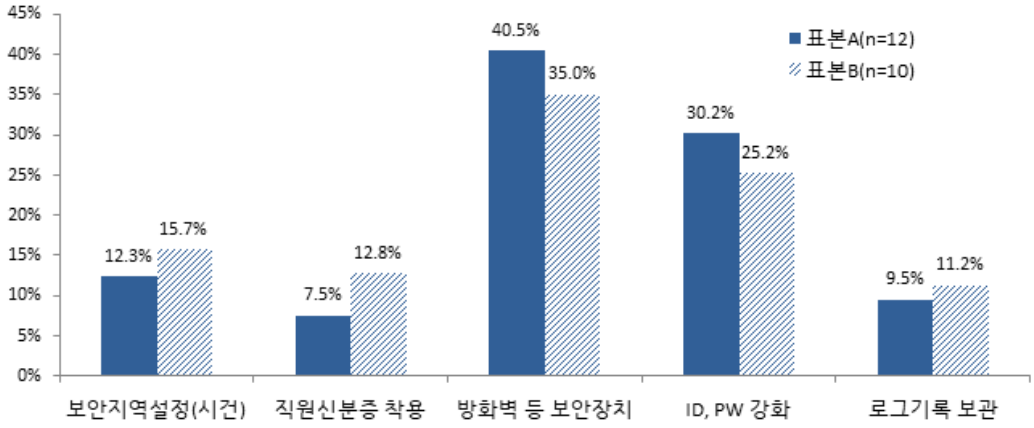

Fig. 3. Results of criticality assessment in terms of cyber risk management(Block & Secured device)

사이버보안 개인정보관리에서 가장 중요한 것(Fig. 4)에 대해 표본A는 개인정보암호화(41.2%) > 개인정보 암호화전송(22.0%) > 개인정보접근제한(16.5%) > 휴대용저장 제한(10.3%) > 기간만료 폐기(10.0%) 순이었다. 표본B는 개인정보암호화(34.1%) > 개인정보접근제한(27.8%) > 개인정보암호화전송(16.2%) > 휴대용저장 제한(11.4%) > 기간만료 폐기(10.5%) 순이었다. 중요한 항목 3가지는 공통적으로 개인정보암호화와 개인정보접근제한, 개인정보 암호화전송이다. 비록 해킹이 되었더라도 개인정보가 암호화되어 있으면 큰 피해가 발생하지 않는 만큼, 개인정보 암호화는 반드시 필요하다. 암호화를 하였으나 결함이 있어 해킹된 사례도 있는데, 암호화 체계는 정부에서 인가받은 암호화체계를 사용해야 하며, 유효인증기간이 지난 암호화체계는 매우 위험하다.

사이버보안 개인PC 보안설정에서 가장 중요한 것(Fig. 5)에 대해 표본A는 백신미설치(27.8%) > PC 방화벽 미설정(26.3%) > 보안업데이트 미흡(17.9%) > 키보드보안프로그램 미설치(17.3%) > 부적절OS(10.7%) 순이었다. 표본B는 부적절OS(39.9%) > 백신미설치(23.8%) > 보안업데이트 미흡(19.6) > PC방화벽 미설정(10.7%) > 키보드 보안프로그램 미설치(6.0%) 순이었다. 가장 중요한 3가지 요인으로는 부적절OS, 백신미설치, 보안업데이트 미흡이다. 특히 사이버보안 전문가들인 표본B는 부적절OS(윈도우XP 등)와 보안업데이트를 가장 중요하다고 판단했는데, 이는 기본적인 운영체제의 취약점을 통해 공격이 될 경우, 다른 여러 보안프로그램의 역할도 크게 제약받는다는 것을 매우 잘 알고 있기 때문으로 판단된다.

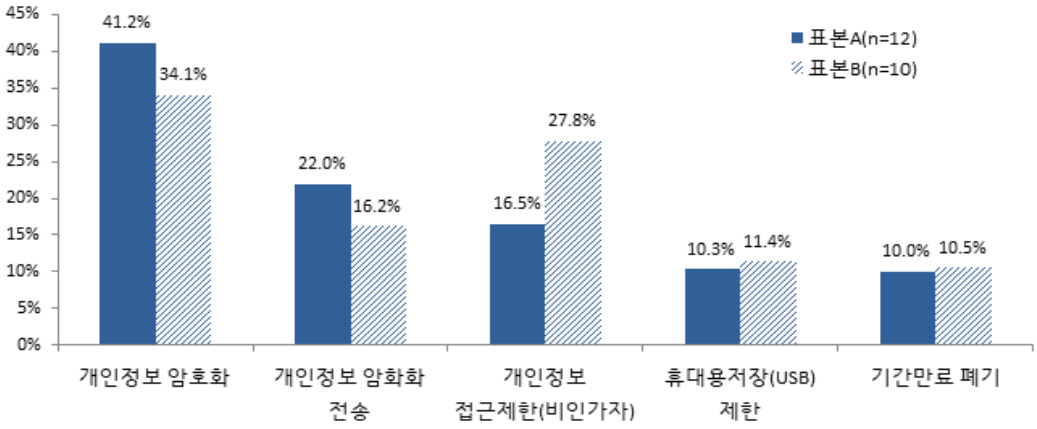

Fig. 4. Results of criticality assessment in terms of cybersecurity on privacy management

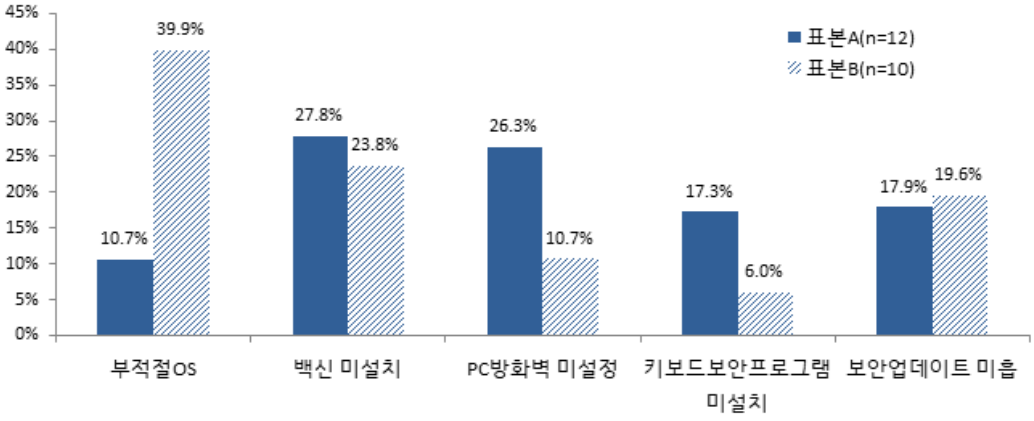

Fig. 5. Results of criticality assessment in terms of personal pc cybersecurity setting

보험적 시각을 통한 사이버위험관리 방안 제시

최소율의 법칙(Law of Minimum)은 n개의 나무기둥으로 만들어진 물통에서 어느 한 개의 나무기둥의 높이가 낮을 경우, 가장 낮은 나무기둥 높이에 따라 물통의 높이가 결정되는 원리를 말한다. 이는 보안에서도 동일하게 적용될 수 있다. 즉, 가장 취약한 부분으로 인해 사이버보안이 위협받을 수 있다는 의미이다.

개인정보유출배상책임 측면에서 살펴보면, (중소)기업의 사이버보안에서 가장 중요한 것은 해커의 표적이 되지 않도록 하는 것이 가장 중요하다. 인터넷을 사용하지 않거나 개인정보를 보유하지 않는 것이 가장 좋지만, 이는 현실적으로 어렵기 때문에 쉽게 해킹되지 않도록 하는 것이 중요하며, 개인정보를 최소한으로 보유하여 해킹으로 인한 피해를 최소화하는 방안을 사전에 마련하는 것이 필요해 보인다.

보험적 시각을 고려하여 주요한 사이버사고 원인 20가지에 대한 중소기업의 사이버위험관리 방안을 Table 5와 같이 제시하였다. 사이버위험관리 방안에는 20개 항목 중에서 특히 중요하다고 선별된 12가지 항목(Fig. 2~5)과 개인정보유출배상책임보험 가입 시 조사하는 보험사의 조사항목(Table 4) 중 일부가 포함되어 있다.

Table 5. Major risk factors for personal information leakage and risk management method for SMEs

구분	주요 사고원인	위험관리방안	관련근거		
			Table1	Table2	Table3
1	정보보호 인식 미흡 및 정보보호담당자 부재	<정보보호사규, 정보보호책임자 임명, 정보보호 조직 구성> 정보보호에 대한 회사 경영진의 강력한 의지표명이 필요		2.1~ 2.3	2.1~ 2.3
2	관리자인가 해킹	<관리자인가(ID) 및 비밀번호(PW) 관리 강화> 관리자암호 수시변경, 최소 10자 이상 크랙이 어려운 암호나 이중암호체계(기존+추가(보안토큰 등)) 출고 시와 동일한 ID/PW또는 Admin/Admin은 무방비 해킹	1.27	2.9	4.2~ 4.4
3	개인정보 비암호화	<개인정보 및 중요 정보자산 암호화> 인증받은 암호화 프로그램 사용, 엑셀(상용프로그램) 암호화 저장, 보안취약 압축프로그램(rar 등) 사용금지	1.5	2.11	4.20~ 4.24
4	부적절 운영체계(OS) 해킹	<적절한 컴퓨터 운영체제(OS)> 업데이트 종료된 운영체계 사용금지, 주기적 OS 업데이트, 정품인증 크랙(crack) 프로그램은 대부분 악성코드(랜섬웨어)		2.16	4.11
5	백신 미설치	<백신프로그램 설치> 백신프로그램 설치, 매일 업데이트, 최소 1주단위 정밀점검	1.13 1.25	2.17	4.10
6	방화벽 미설치/미적용	<방화벽 설정> Windows 방화벽 설정, 네트워크/시스템/PC 방화벽 설정	1.13	2.8 2.18	4.7
7	악성코드로 컴퓨터 해킹	<악성코드 예방> 업데이트파일, 경품, 청첩장, 무료프로그램 등으로 위장한 악성코드로 확인이 불가능한 첨부파일 열기 금지 및 파일확장자 확인 한글은 자동업데이트로 첨부파일 업데이트는 악성코드파일임	1.25		
8	백도어 프로그램 사용	<프리웨어나 쉐어웨어 사용 자제> 실시간 광고가 있는 프리웨어나 쉐어웨어 사용자제, 가급적 정품사용	1.7		2.11
9	직원 유출	<모바일저장장치 사용제한 및 퇴직자 접근차단> 비인가 직원의 PC 내 개인정보 유무확인 후 삭제, 모바일 저장장치(USB, CD 등) 사용제한, 개인정보 접근권한 부여, DRM프로그램 사용. 퇴직자 접근차단 등	1.1, 1.4 1.6, 1.12 1.18	2.13 2.14	4.5
10	보안업데이트 관리 미흡	<보안업데이트 설정> 윈도우즈 및 기타 사용프로그램의 주기적/긴급 업데이트 필요. 대부분 프로그램은 자동업데이트로 한글 첨부파일 업데이트는 악성코드임	1.20	2.20	2.11
11	홈페이지 웹쉘 감염	<홈페이지/서버 업로드제한> 파일업로드 기능 삭제·최소화, 웹쉘의 주기적 검사 (WHISTL활용)	1.11		4.12
12	서버보안 미흡	<안전한 클라우드서비스 사용> 신뢰할 수 있는 클라우드서비스 업체 활용	1.17		
13	보안인식 및 투자미흡	<사이버보안 교육> 직원교육강화 및 보안전문업체에 점검의뢰&서버의뢰		2.4	2.4
14	개인정보 보관/관리 미흡	<개인정보 접근제한> 서버나 PC의 보안이 미흡한 회사들은 인터넷 미연결된 컴퓨터에서 저장, 활용 시 보안USB사용. 보유기간이 만료되거나 활용이 끝난 개인정보는 반드시 삭제	1.11, 1.18	2.15	4.18
15	아웃소싱 개인정보 유출	<개인정보 암호화전송> 외부업체 위수탁 시 계약서 내 정보보안의무 필수기재, 외부업체와 개인정보 공유 시 암호화 후 전송 및 관리강화	1.20 1.29	2.12	4.6 4.17
16	무인증 무선공유기로 해킹	<무선공유기 보안설정> 무인증 무선공유기(WiFi등) 사용금지, 회사 내 무선공유기 암호설정	1.3		
17	보안점검 미실시	<보안업체의 보안점검> 중소기업은 사이버보안 자체진단능력이 부족하여, 외주 보안업체 점검으로 사이버위험평가 및 보안능력 향상 필요			4.8~9, 4.19
18	키보드 해킹 발생	<무료 보안프로그램 설치> ID, PW 입력 등에 대한 키보드해킹사례가 많아 키보드보안 필요. 금융기관, 공공기관에서 무료 키보드 보안프로그램 설치가능	1.25	2.19	
19	중요 정보자산 복구불능	<데이터 백업> 기업의 중요한 정보자산의 보관 소홀로, 랜섬웨어로 사이버강탈 시 복구 불능. 기업연속성 측면에서 중요 정보자산 백업 실시			4.26
20	정보누출 시 대응미숙	<정보누출 시 대응절차 마련> 해킹공격이 의심되거나 해킹발생을 인지하였을 때 대응매뉴얼에 따른 신속한 대처로 추가 피해를 예방		2.5	2.7

결 론

중소기업 사이버위험평가는 기존 사이버보안 프레임워크를 그대로 적용할 수 없고, 그렇다고 기존 사이버보안 프레임워크를 배제하고 중소기업에 적합한 새로운 사이버보안 프레임워크를 만드는 것은 많은 시간과 노력이 필요하기 때문에 더더욱 곤란하다. 가장 좋은 방법은 기존에 알려진 사이버공격 패턴이나 수법 등을 사전에 대비하는 것인데, 사이버보안 사고는 자료공개가 매우 제한되어 있어 한계가 존재한다.

사이버보안 시장, 금융기관 사이버보안 항목, 사이버보안 프레임워크 비교, 언론에 보도된 사이버보안사고 등을 통해 사이버보안에 중요한 4가지 분야와 각분야 별 5가지 항목 등 총 20개 항목을 도출하였다.

중소기업에 대한 사이버보안 강화방안으로 (1) 정보보호 사규/책임자/조직 구성, (2) 관리자 인가 및 비밀번호(password) 관리, (3) 개인정보 및 중요정보자산 암호화, (4) 적절한 컴퓨터 운영체계(OS), (5) 백신프로그램 설치, (6) 방화벽 설정, (7) 악성코드 예방, (8) 프리웨어나 쉐어웨어 사용자제, (9) 모바일저장장치 사용제한 및 퇴직자 접근차단, (10) 보안업데이트 설정, (11) 홈페이지/서버 업로드 제한, (12) 안전한 클라우드서비스 사용, (13) 사이버보안 교육, (14) 개인정보 접근제한, (15) 개인정보 암호화전송, (16) 무선공유기 보안 설정, (17) 보안업체의 보안점검, (18)무료 보안프로그램의 설치, (19) 데이터 백업, (20) 정보누출 시 대응절차 마련을 제시하였다.

미국은 전 세계 사이버보안 시장의 절반 이상을 점유하고 있고, 사이버보험은 85~90% 정도를 점유하고 있다. 미국은 사이버보험이 사이버보안을 지원하고 협력하는 구조로 되어 있으며, 보험사가 정부기관 및 보안업계와 협업하여 위험평가 방안을 도출하고 있고, 위험평가를 통해 보험료를 부과하는 체제를 갖추고 있는데, 우리나라도 미국의 사례와 같이 발전해 나갈 필요가 있다.

본 연구에서 도출된 국내 중소기업의 사이버보안 위험평가방안이 향후 중소기업이 사이버보험 가입 시 그 기업의 위험평가에 활용할 수 있다. 또한 기업의 리스크 관리 활성화를 위한 ERM 규격화에 보험이 연계될 필요성 있는데(Lee, 2017), 사이버 위험평가도 ERM 규격화의 한 부분에 포함되는 토대를 제공하고자 한다.

Acknowledgement

본 연구는 행정안전부의 재난안전 분야 전문 인력 양성사업을 통해 지원받아 수행된 연구의 결과이며, 이에 감사드립니다.

References

[1] AON (2016). Cyber, the Fast Moving Target. (http://www.aon.com/attachments/risk-services/cyber/2016-Captive-Cyber-Survey-Interactive.pdf)

[2] Australian Small Business and Family Enterprise Ombudsman (2017) Cybersecurity: The Small Business Best Practice Guide (https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-cyber-security-research-report.pdf)

[3] Cho, B.-J., Yun, J.-H., Lee, K.-H. (2015). “Study of effectiveness for the network separation policy of financial companies.” Journal of The Korea Institute of Information Security & Cryptology, Vol. 25, No. 1, pp. 181-195.

[4] Cho, S.-K., Jun, M.-S. (2012). “Privacy leakage monitoring system design for privacy protection.” Journal of The Korea Institute of Information Security & Cryptology, Vol. 22, No. 1, pp. 99-106.

[5] Deloitte (2017). Cybersecurity and the Role of Internal Audit.

[6] Financial Services Commission (2019). Regulation of Supervision on Electronic Financial.

[7] International Security Exhibition & Conference (2019). Exhibition items for participation in the International Security Exhibition(Cybersecurity Field). (https://www.seconexpo.com/2019/kor/exhibit/sub02.asp)

[8] Jeong, Y.-C. (2018). "Finance industry and cybersecurity policy." Journal of Financial Regulation and Supervision, Vol. 5, No. 2, pp. 89-122.

[9] Jung, H.-C. (2017). A Study on Security Technology for Enhancing Security of Small and Medium Enterprises by using Open Source. Master Thesis, Soongsil University.

[10] Kim, D.-C., Kim, I.-S. (2018). "A study on cybersecurity regulation for financial sector: Policy suggestion based on New York's cybersecurity regulation(23 NYCRR 500)." Journal of Society for e-Business Studies, Vol. 23, No. 4, pp. 87-107.

[11] Kim, H.-W., Lee, K.-S., Kim, S.-H. (2005). "Website security evaluation for electronic commerce." Joint Spring Conference between The Korean Operations Research and Management Science Society/Korean Institute of Industrial Engineers, Chungbuk University, pp. 340-347.

[12] Kim, J-G., Lee, D-S., Cho, J-Y., Han, S-G., Kim, T-H. (2016). "Introduction of perpcetion on ICT to respond social disaster." Journal of The Korea Society of Disaster Inforrmation, Vol. 12, No. 3, pp. 249-260.

[13] Kim, J.-H., Cho, J.-H. (2010). "Security threats in cyber environments." Journal of The Korea Institute of Information Security & Cryptology, Vol. 20, No. 4, pp. 11-20.

[14] Kim, K.-C., Kim, S.-J. (2012). "Evaluation criteria for Korean smart grid based on K-ISMS." Journal of The Korea Institute of Information Security & Cryptology, Vol. 22, No. 6, pp. 1375-1391.

[15] Kim, K.-R. (2019). A Study on the Cyber Risk Item Disclosure for Cyber Insurance Subsidiary. Master Thesis, Sangmyung University.

[16] Kim, K.-Y. (1997). "Risk management and crisis management: Disaster recovery for information system." Journal of Risk Management, pp. 291-315.

[17] Kim, S.-H. (2019). A Study on the Improvement of Vulnerability Checklist for Enhanced PC Security. Master Thesis, Konkuk University.

[18] Kim, S.-J., Kim, J.-D. (2017). "A study on developing assessment indicators for cyber resilience." Journal of Digital Convergence, Vol. 15, No. 8, pp.137-144.

[19] Kim, S.-Y. (2009). Korea Financial Telecommunications & Clearings Institute, Payment, Clearance and Information Technology, Vol. 38, pp. 34-62.

[20] Kinosita, E., Ooya, T. (Kwon, J.-H., Trans.) (2012) Strategic Decision Making Techniques, AHP. Cheongram Press, Seoul, Korea.

[21] Korea Communications Commission & KISA (2010). Guide for Information Security Management System.

[22] Korea Information Security Agency (2003). A Study on the Development of Certification System for Information Protection Management System.

[23] Korea Internet & Security Agency (2012). Information Security Guide for Small and Medium IT Service Companies(III), Information Security management for working-level officials.

[24] Korea Internet & Security Agency (2020). Small and Medium Business Information Protection Practice Guide(1/2, 2/2).

[25] Korea Insurance Development Institute (2015). A Study on Introduction of Government Reinsurance System in Environment Impairment liability Insurance. Research & Service Report by Minister of Environment.

[26] Lee, K.-H. (2017). “A study on ERM standardization and insurance linkage scheme to promote corporate risk management.” The Journal of Risk Management, Vol. 28, No. 3, pp. 43-79.

[27] Lee, K.-H., Yoon, J.-D. (2008). “A study on the measurement methods and cases of personal information leakage risk in private enterprises.” Journal of The Korea Institute of Information Security & Cryptology, Vol. 18, No. 3, pp. 92-100.

[28] Lee, K.-S. (2006). “The problem and policy alternatives for cyber security in the networking age.” Journal of Korea Association for Regional Information Society, Vol. 9, No. 1, pp. 109-128.

[29] Min, B.-G., Lee, D.-H. (2006). “Research of improvement and system of the information security management evaluation.” Journal of Convergence Security, Vol. 6, No. 4, pp. 101-112.

[30] Ministry of Knowledge Economy, IO Consulting Co., Ltd. (2010). Detailed Security Control Implementation Guidelines for Technology Protection for SMEs.

[31] Namu.Wiki (2021). (https://namu.wiki/w/개인정보%20유출사태)

[32] NASSTAR (2019). Cyber Security for SMEs: A Practical Guide to Protection Your Business. (https://www.nasstar.com/hubfs/Marketing-Material/white%20paper%20-%20cyber%20security.pdf)

[33] NIST (2016). NISTIR 7621, Small Business Information Security: The Fundamentals. (https://doi.org/10.6028/NIST.IR.7621r1)

[34] NIST CSF (2018). Framework for Improving Critical Infrastructure Cybersecurity.

[35] Oh, H.-G. (2019). “Countermeasure of Unmanned Aerial Vehicle(UAV) against terrorist’s attacks in South Korea for the public crowded places.” Journal of The Korea Society of Disaster Inforrmation, Vol. 12, No. 1, pp. 49-66.

[36] Park, J.-T. (2020). A Study on the Establishment of IT-based Joint Disaster Recovery Center for Business Continuity Management System of Small and Medium Business. Ph.D. Dissertation, Hansei University.

[37] Park, J.-H., Cho, N.-W., Lee, K.-H., Choi, I.-H. (2008). “ Development of Security System on Personal Information in custody internally in Corporates.” Journal of The Korea Institute of Information Security & Cryptology, Vol. 18, No. 6, pp.28-34.

[38] Radanliev, P., De Roure, D., Nurse, J.R.C., Nicolescu, R., Huth, M., Cannady, S., Montalvo, R.M. (2019). Cyber Security Framework for the Internet-of-Things in Industry 4.0, University of Oxford, UK. (doi: 10.20944/preprints 201903.0111.v1)

[39] Radanliev, P., De Roure, D., Cannady, S., Montalvo, R.M., Nicolescu, R., Huth, M. (2018). “Analysing IoT cyber risk for estimating IoT cyber insurance.” IET Conference Proceeding. (doi: 10.1049/cp.2018.0003)

[40] Son, S.-S. (2014). The Study on the Improved Assessment Methodology for Information Security Level Using ISO 27001. Master Thesis, Sungkyunkwan University.

[41] Song, E.-J., Bae, B.-H., Oh, N.-H. (2018). “A comparative analysis on the calculation method of domestic and foreign information security market.” Institute for Information & Communications Technology Promotion, Weekly ICT Trends, Vol. 1860, pp. 17-26.

[42] Spinello, R. (2003). “Cyberethics: Morality and law in cyberspace.” 2th Edition. Jones and Bartlett Learning, LLC., Jones and Bartlett Publishers, Inc, USA.

[43] Symantec (2018). Cybersecurity for SMEs, a lightweight cybersecurity framework for thorough protection. (https://www.smesec.eu/doc/SMESEC_Flyer_A5_V2_2018-05-03_Singlepages.pdf)

[44] Wikipedia, Korea (2021). (https://ko.wikipedia.org/wiki/대한민국의_정보_보안_사고_목록)

[45] Yang, D.-I. (2019). Introduction to Information Security(3rd E.). Hanbit Academy, Seoul, Korea.

[46] Yoon, J.-G. (1990). “Application of AHP and its limitation.” Management & Economics review, Vol. 7, pp. 75-92.