경영학 석사학위 논문

포스트 코로나 시대의 중소기업 산업정보 유출 방지를 위한 방안 연구

A Study on the Prevention of Industrial Information Leakage of Small and Medium Businesses in Post-Corona Era

울산대학교 경영대학원

경 영 학 전 공

송 재 혁

포스트 코로나 시대의 중소기업 산업정보 유출 방지를 위한 방안 연구

지 도 교 수 박 주 식

이 논문을 경영학 석사학위 논문으로 제출함

2021년 12월

울산대학교 경영대학원

경 영 학 전 공

송 재 혁

송재혁의 경영학 석사학위 논문을 인준함

심 사 위 원　김 도 일　(인)

심 사 위 원　서 용 한　(인)

심 사 위 원　박 주 식　(인)

울산대학교 경영대학원

2021년 12월

국문초록

최근 코로나19 영향으로 온라인 경제화가 가속화되면서, 기업들의 정보보안 위험은 더욱 증대하였고, 특히, 중소기업은 전문인력 부족과 예산 부족으로 2021년 7월 기준 랜섬웨어에 따른 전체 피해 건수인 97건 중 81%가 중소기업임이 규명되어 정보보호의 사각지대에 노출되고 있다. 차후 포스트 코로나 시대에 비대면 강화에 따른 온라인 기술의 고도화에 있어 혁신기술 창출이 관건이며, 혁신적이고 기업가 정신에 기반한 중소벤처기업 등의 기술성과 중심으로 대전환이 예상되는바, 본 연구는 포스트 코로나 시대 중소기업 정보보안 개선방안을 문헌 고찰과 실증연구를 병행하여 제시하였고, 연구 결과에 따른 정책적, 실무적 시사점을 함께 제시하여 정부와 중소기업 간 상호 협력적 방안을 최종 도출하고자 했다.

이러한 연구목적을 위해 본 연구는 1차적으로 문헌고찰을 하여 국내의 중소기업의 정보보안 현황을 분석하고, 2차적으로 전국 중소기업 구성원 200명을 대상으로 온라인상에서 정보보안 실태에 관한 설문을 진행하여 국내 중소기업 정보보완 실태를 규명한 뒤, 해외사례, 국내 실태를 비교, 분석하여 공통점과 차이점을 규명함으로써, 국내 사정에 맞춤화된 차후 포스트 코로나 시대 대비 중소기업 정보보안 방향성을 정립하였다. 또한 미국 산업보안의 사례를 바탕으로 제한적인 국내 산업보안에 대해 분석해 보았다.

연구결과, 차후 포스트 코로나 시대 디지털 가속화에 따라 산업보안 피해는 더욱 증가할 것을 예상할 수 있다. 비대면이 더욱 강화되는 이 시대에 있어서 팬데믹과 산업 디지털에 따른 변화 정도에 있어서 복합적이고 고도화된 사이버 공격 증가를 가장 많이 예상한 것이 이를 증명하고 있다. 또한, 차후 산업보안 사고가 발생하면 중소기업 경쟁력과 매출에 큰 영향을 미침을 알 수 있는데, 산업보안 사고 발생 시 기업 경쟁력과 매출에 미치는 영향 인식 결과는 평균 4.29점으로 매우 높음이 확인되었다. 또한, 이러한 보안인식은 직책이 높을수록 그 중요성과 심각성을 더 강하게 인식함을 확인했고, 이러한 높은 인식에도 불구하고, 기업에서 평소 산업보안 관련 지침을 실천하는 정도의 경우, 안내가 있어야 수동적으로 실천하는 경우가 약 80% 가까이 되어, 현재 능동적, 자발적으로 산업보안 규정 준수를 이행하지 못하고 있음을 확인하여 이를 개선할 관리적, 기술적, 물리적, 인적 관리 차원의 개선방안을 각각 제시했다.

본 연구는 기존 연구가 중소기업 산업보안 현황, 실태에만 주력하여 적절한 대안을 제시하지 못하는 한계에 따른 실무적 전략을 제시함에 의의가 있고, 각 차원 개선방안을 상호유기적으로 제시하여 더욱 실효성 있는 경영전략을 위한 유용한 자료가 될 것으로 기대한다.

목 차

표 목 차

제1장 서론

제1절 연구 필요성과 목적

오늘날 정보통신기술 발전은 전 세계를 통일된 네트워크로 형성했다. 이러한 발전은 기업의 업무 효율성과 생산성 증대에 크게 이바지함이 자명하다. 기업은 빅데이터, IoT 등 다양한 기술들을 활용하여 제품 개발, 프로세스 개선, 자동화 등 전반적인 혁신에 적극 활용하고 있다(홍준석, 2021).

하지만 최근 코로나19 영향으로 디지털화가 가속화되면서 중소기업의 정보보안 위험은 더욱 증가함이 규명되었다. 이에 산업보안에 대한 인식과 중요성은 더욱 커졌으나 관련 자료나 연구가 부족한 것이 현실이다.

2020년 국제 사이버범죄 비용은 1조 달러 이상이며, 정보를 훔치는 사이버 범죄로 인한 금전적 손실이 9.450억 달러임이 밝혀졌다. 약 130개 국가에서 약 1.500억 건이 넘는 보안 이벤트를 분석하면서 얻은 결과에 기반한 '엑스포스 위협 인텔리전스 인덱스 보고서(2021)'에 따르면, 코로나19 관련 업계와 기업에 대한 공격은 전년 대비 2배 이상 증가함이 규명되었고, 엑스포스가 차단한 공격 중 25%가 랜섬웨어였고, double extortion[1]을 취하는 방향으로 공격이 더욱 진화되어 가고 있음이 밝혀졌다(IBM, 2021).

따라서, 차후 코로나19를 기점으로 디지털 전환이 더욱 가속화되고, 공공과 민간 비대면 서비스가 더욱 급증하는 포스트 코로나 시대에 새로운 보안 위협이 끊임없이 추정되는 실정이며, 특히 기업 대상 해킹 수법이 더욱 고도화될 것을 감안해 철저한 보안대책이 시급한 실정임을 전자신문(2021)은 강조했다.

특히, 신희강(2021)은 국내 기업이 경험한 침해사고 중 약 60%가 랜섬웨어이며, 랜섬웨어 피해건수는 2019년 39건에서 2020년 127건으로 3배 이상 증가했는데, 2021년 7월까지 랜섬웨어 피해건수는 97건에 달하고, 이 중 79건에 해당하는 81%가 중소기업임을 강조했다. 현재 전 세계적으로 정보보호 중요성이 대두

1) double extortion(이중강탈전술): 랜섬웨어 범죄자가 데이터를 암호화해 피해자가 사용하지 못하게 한 후 돈을 강취하는데 만족하지 않고, 훔친 데이터를 직접 판매하여 또 다른 수익 창출 기회를 얻는 것(이코노미조선, 2021).

되면서 각 기업들은 점차 보안수위를 증대하고 있으나, 중소기업들은 현재 전문 인력 부족(77.9%), 예산부족(74.0%) 등에 따라 코로나19로 증폭된 산업정보 보안 강화를 진행하지 못하고 있음을 장상수(2020)는 피력했다. 이에 따라, 최소한의 안전장치마저 하지 않은 기업들이 부지기수이며, 이들은 정보보호의 사각지대에 고스란히 노출되고 있다는 것이다.

이시희(2020)는 코로나19 발발에 따라, 우리는 더 이상 코로나 이전 세상으로 돌아갈 수 없음을 피력했는데, 정치, 경제, 사회, 문화 등 전 분야가 그간 접하지 못했던 새로운 세상, 즉 포스트 코로나 시대에 진입할 것을 기술했고, 우리가 맞이할 포스트 코로나 시대의 수많은 변화 중 기존 대기업 위주의 성장에서 중소기업 중심의 성장으로 대전환이 발생하면서 혁신벤처 기업들의 중요성이 강조되고 있음을 제시했다. 포스트 코로나 시대 특성인 비대면 강화에 따른 온라인 기술에 있어 혁신기술 창출이 관건이며, 종래의 안정적이고 폭넓은 기술경영전략보다는 혁신적이고 기업가 정신에 기반한 혁신벤처 기업들의 기술성과가 더욱 중시될 것임을 추정한 것이다.

따라서, 코로나19로 인해 중소기업 정보보안이 안전 사각지대에 놓인 현 시점에서, 차후 포스트 코로나 시대에 그 중요성이 더욱 강조될 중소기업의 정보보안 개선전략과 방향성을 정립하는 작업은 매우 절실한 사안이다. 하지만, 이러한 연구 필요성에도 불구하고, 관련 선행연구를 보면, 장상수(2020)는 국내 중소기업 정보보호 지원 정책의 방향성을 포스트 코로나 시대 기준으로 논의하였고, 유일영(2020)은 중소기업의 중요정보 보호를 위한 IT 실무적 보안 강화 방안을 제시하는 등 포스트 코로나 시대 대비 중소기업 보안강화를 위한 정책적, 실무적 시사점을 각각 제시하고 있으나, 국내 중소기업의 정보보안 실태와 포스트 코로나 시대 방향성을 정립함에 있어 정작 중소기업 실무자들의 의견과 목소리를 반영하여 보다 실효성 있는 연구를 제시한 연구가 미흡하여, 더 나아가, 정책적, 실무적 시사점을 종합하여 상호 유기적 차원의 시사점을 제시하여 정책과 실무간 시너지 창출을 기대한 연구가 매우 부족하다.

따라서, 본 연구는 상기 연구 필요성과 선행연구 한계에 따라, 포스트 코로나 시대의 중소기업 정보보안 개선방안을 문헌고찰과 함께 설문지 조사를 통한 실증연구를 병행하여 현장의 의견을 더 적극 반영, 실효성 있는 개선방안을 제시하고자 하며, 연구 결과에 따른 정책적, 실무적 시사점을 함께 제시하여 정부와 중소기업간 상호 협력적 방안을 최종 도출하고자 한다.

제2절 연구범위와 방법

상기 연구목적을 성취하기 위한 본 연구 범위와 방법은 다음과 같다.

본 연구는 문헌고찰과 실증연구를 병행하여 진행할 것이다. 즉, 문헌고찰을 통해 포스트 코로나 시대 대비 중소기업 정보보안 필요성이 더욱 증대함을 확인하고, 해외 중소기업 정보보안 현황을 분석하여 상대적 강점과 이점을 각각 도출하여 분석 틀을 1차적으로 도출할 것이다. 이러한 분석틀과 정보보안 인식에 관한 선행연구들을 종합하여 코로나19에 따른 중소기업 정보보안 실태를 위한 설문을 진행, 현황, 정보보안 분야별 중요도 인식 등으로 연구도구를 구성, 전국 중소기업 구성원 200명을 대상으로 온라인상 설문작업을 진행하여, 통계결과를 도출함으로써 현재 코로나19 상황에서 국내 중소기업 정보보안 실태를 제시할 것이다. 마지막으로, 설문결과를 바탕으로 국내 사정에 적합한 차후 포스트 코로나 시대 대비 중소기업 정보보안 강화를 위해 관리적, 기술적, 물리적, 인적 보안의 개선책을 제시할 것이다.

제3절 연구문제

상기 연구 필요성과 목적, 연구 범위와 방법에 따른 본 연구문제를 제시하면 다음과 같다.

연구문제 1. 포스트 코로나 시대 대비 국내 중소기업 정보보안 실태는 어떠한가?
연구문제 2. 실태분석에 따른 중소기업 산업보안 개선을 위한 관리적, 기술적, 물리적, 인적 보안 개선책은 무엇인가?

제2장 이론적 배경

제1절 중소기업 산업보안

1. 산업보안 개념

산업보안이라는 용어는 단순히 산업과 보안의 합성어로 산업이라는 용어는 산업측면에서 보면 '사람이 생활하기 위해 하는 일' 혹은 '생산을 목적으로 하는 사업'으로 정의된다. 또한, 보안의 개념은 '범죄로부터 생명, 신체, 재산을 보호하고, 사회 안녕과 질서를 지키는 제반활동'으로 규정한다. 따라서 산업보안이란 넓은 의미에서 '범죄 행위에서 모든 경제활동을 보호하는 일체의 노력'이다. 쉽게 말해서, '범죄로부터 산업을 보호하는 활동'이며, 구체적인 내용으로는 유, 무형의 자산 모두를 지키는 자산보호(asset protection)와 피해를 막는 손실방지(loss prevention)활동을 의미한다(전승준, 2014).

국내에서 지금까지도 사전적 의미와 학술적으로 정의되진 않았으나, 세계적으로 산업보안 중요성이 강조되면서 비교적 최근에 보편화되고 주목을 받았다. 국가정보원에서 2013년 10월 산업기밀보안센터가 설립되면서 산업보안 중요성이 더욱 강조되면서 용어에 관한 정의, 개념이 일반에 알려지기 시작했고, 2016년 산업기술의 유출방지 및 보호에 관한 법률 제정에 따라 동법의 제18조와 제20조 등에 산업보안, 산업기술, 영업비밀 등 법률용어로서 구체화되었다(이호준, 2020).

산업분야의 전반적, 일반적인 활동을 범죄로부터 보호하는 의미로 파악하지 않고 단순히 산업기술 유출방지에 국한하는 협의적 의미로 파악하기도 한다. 국가정보대학원이 편찬한 '산업보안실무'에서는 산업보안을 '산업활동에 유용한 기술상, 경영상의 모든 정보나 문서, 인원, 시설, 자재 등을 산업스파이 혹은 경쟁관계에 있는 기업은 물론이고, 특정한 관계가 없는 자에게 누설, 침해당하지 않도록 보호, 관리하기 위한 대응방안이나 활동'으로 규정한다.

특히, 기업차원의 산업보안은 기업 혹은 연구소 등이 자체 보유하는 신기술, 원천기술, 경영상의 기밀 혹은 대외비 정보 및 이와 연관한 문서, 시설, 인원,

정보 등을 경쟁업체, 국가의 산업스파이 등과 같은 위해요소로부터 산업기술, 기업기밀을 보호하는 일체의 활동을 의미한다(이창무, 2011).

따라서, 본 연구는 산업보안을 기업이 정보, 산업기술, 핵심시설물 및 장비, 전문 기술인력 등의 기술적 차원과 영업비밀 등 경영상의 비밀을 경쟁업체 혹은 국가의 산업스파이 등으로부터 보호, 관리하는 대응방안으로 정의하고자 한다.

2. 중소기업 산업보안

2018년 기준 중소벤처기업부가 발표한 우리나라 기업 현황을 보면, 소상공인을 포함한 중소기업은 6,638,694개, 대기업은 5,062개로서, 전체 기업 중 소상공인을 포함한 중소기업 비중은 99.92%를 이루고 있어, 우리나라 기업에서 중소기업이 차지하는 비중은 절대적이라고 할 수 있다(이상범, 2021).

<표 1> 우리나라 기업 현황

	전체	소기업		중기업	**중소기업**	대기업
		소상공인	소상공인 제외			
기업수	6,643,756 (100.0)	6,199,980 (93.3)	340,885 (5.1)	6,540,865 (98.5)	97,829 (1.5)	**6,638,694 (99.9)**	5,062 (0.1)
종사자수	20,591,641 (100.0)	8,969,291 (43.6)	4,278,394 (20.8)	13,247,685 (64.3)	3,856,253 (18.7)	**17,103,938 (83.1)**	3,487,703 (16.9)
매출액	54,911,068 (100.0)	9,210,477 (16.8)	5,652,257 (10.3)	14,862,734 (27.1)	11,766,096 (21.4)	**26,628,830 (48.5)**	28,282,238 (51.5)

※출처 : 이상범. (2021). 중소기업의 산업기술보호 방안 : 경찰 수사요원 활용을 중심으로. 석사학위 논문. 단국대학교 대학원.

이와 별도로 국내 기업에서 산업기술이 유출되어 경찰이 수사를 통해 검거한 수치를 보면, 산업기술보호에 있어 중소기업이 대기업 대비 산업기술 유출범죄에 대해 효과적으로 대응하지 못하고 있음을 보여주는데, 2010~2020년까지 11년간 경찰이 수사하여 검거한 산업기술보호 사건 통계를 보면, 전체 1,182건 중

대기업 피해 건은 144건으로 12.2%인 반면, 중소기업 피해 사건 검거는 1,038건으로 87.8%를 차지하여 전체 기업 중 중소기업이 차지하는 비중 99.92%에서 단지 12,12% 떨어지는 수치로 대기업에 비해 중소기업은 거의 보안사고에 효과적으로 대응하지 못하는 현실을 보여준다.

<표 2> 피해기업별 산업기술보호 사건 피의자 검거 현황

구분	계	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
중소기업	1,038	34	78	122	79	91	82	98	128	106	104	116
대기업	144	6	6	18	18	20	16	16	12	11	11	13
중소기업 피해율	87.6	85.0	92.9	87.1	81.4	82.0	83.7	86.0	91.4	90.6	90.4	89.9

※출처 : 경기남부경찰청. (2020). 산업기술보호수사 통계자료.

이러한 조사 결과에서 보듯이 중소기업은 대기업에 비해 기술보호 역량이 부족한 실정이고, 그만큼 기술유출에 취약한 환경을 가지고 있다. 중소기업 기술유출사고가 발생하는 주된 원인에 관한 조사 결과를 보면 보안관리 감독체계 미흡이 가장 큰 요인으로 파악되었고, 임직원들의 보안인식 부족과 보안관련 기술, 인력 등에 대한 투자 미흡이 그 다음 순이었다. 이러한 결과는 중소기업이 대기업에 비해 기술유출에 관한 경각심이 부족하거나 안이한 대처를 하고 있음을 의미하고, 손실에 대한 고려 없이 비용, 예산 등을 이유로 보안업무에 투자를 하지 않고 있음을 의미한다. 또한, 내부자를 통한 기술 유출도 많은데, 이 이유도 기업이 직원 대상으로 보안교육에 대한 투자가 미흡한 현실을 반영한다.

<표 3> 중소기업의 산업기술유출 사고 주요 원인(단위: %)

연도별	보안관리 감독미흡	보안관련 투자미흡	임직원 보안의식 부족	임직원 금전적 이익추구	회사에 처우불만	보안전임 담당자 부재	회사 운영난 등 감원	기타
2017년	46.5	11.6	23.5	5.1	3.1	3.8	3.0	1.5
2016년	45.8	26.5	43.1	20.2	11.9	6.9	21.0	0.0
2015년	47.9	26.0	36.7	14.4	15.4	14.8	7.8	1.0

※출처 : 중소벤처기업부. (2018). 2017년 중소기업 기술보호수준 실태조사.

따라서, 본 연구는 이러한 결과에 따라, 중소기업의 산업보안을 창출하는 주원인으로, 보안관리 차원인 보안대응, 보안관련 투자와 연관된 보안기술, 교육, 산업정보 보안 중요성 등에 관한 보안의식으로 구성하고자 한다.

제2절 코로나19와 산업보안 이슈

코로나19에 따른 비대면 업무환경 확대, 디지털 전환 가속, 데이터 산업 활성화에 따라 산업보안에 대한 위협이 더욱 증가할 것임을 행정안전부(2021)는 강조했다. 삼성SDS(2021)도 지난해 국내외에서 발생한 보안이슈와 현장의 여러사례를 분석하여 '2021년 사이버보안 7대 이슈'를 제시했다. 이에는 비대면 환경을 노린 위협 증가, 랜섬웨어 고도화, AI를 통한 해킹 지능화, 산업설비에 대한 위협 본격화, 민감한 데이터 보호 중요성 증대, 클라우드 대상 공격 증가 등이 선정되었다.

특히, 원격근무는 가장 약한 고리(Weakest Link)[2]로 파악된다. 코로나19에 따라, 일반기업에서도 원격근무가 확대될 것인데, 보완이 취약한 가정용 네트워크와 단말기를 통한 정보 해킹 시도가 증가하는 실정이다. 직원들의 스마트폰, PC에 대한 공격은 물론이고, 메신저, 영상회의 등 업무지원 시스템을 통한 정보유출 방지는 기업 보안의 최우선 과제로 지목된다.

또한, 글로벌 해킹 트랜드를 주도하는 랜섬웨어는 종래 불특정 다수에 대한 공격에서 점차 기업 등 특정 목표를 겨냥한 표적형으로 고도화되는 실정이다. 최근 다양한 변종 출현과 함께 랜섬웨어를 서비스형으로 판매하는 사례도 발생하는 등 위협강도가 더욱 증가하고 있다.

AI기술 발전은 보안 영역을 크게 변화시키고 있는데, AI학습을 통해 대량의 해킹공격 성공률을 높이고, 딥페이크 등을 통한 정보 왜곡, 조작 위험성이 더욱 증대했다. 이를 방어하기 위해선 AI기반 멀티미디어 위변조 검출 및 자동탐지, 분석 기술이 발전하면서 AI기반 공격, 방어 전선이 확장되는 추세이다.

산업설비 보안의 중요성도 커지고 있다. 지능형 시스템을 갖춘 스마트팩토리가 증대하고, 사물인터넷, 5G 도입 등으로 네트워크 연결이 확장되면서 생산설비,

2) A chain is only as strong as its weakest link에서 유래한 용어로, 기업에게는 다양한 이해관계자가 있고 이 관계 속에서도 강한 고리, 약한 고리가 있는데, 가장 약한 고리를 보완해야만 기업 중심을 잡을 수 있다는 것(국민권익위원회, 2017)

제조공정에 대한 보안위협도 증가하고 있다. 지난해 해외에서 발생한 자동차, 석유 기업 대상 사이버공격은 정보시스템(IT)을 넘어 운영기술(OT)과 산업제어시스템(ICS) 보안 중요성을 각인시킨 사례로 평가된다.

데이터보호는 데이터산업 활성화를 위한 필수조건으로 정착했다. 국내에서도 데이터 3법 개정과 마이데이터 사업 확장에 따라, 데이터를 보호하기 위한 다양한 기술과 솔루션이 등장 중이다. 데이터산업 성공을 위해서는 종래 정보 암호화뿐 아니라 개인정보의 안전한 유통, 활용을 위한 비식별화 및 프라이버시 보호 기술이 필수적이다.

클라우드는 철저한 보안 체계 정립이 필요하다. 최근 클라우드 시스템의 단순 사고가 대규모 접속 장애 및 정보유출로 연결되고, 클라우드 시스템만 전문적으로 공격하는 사례도 증가하고 있다. 따라서 보안 설정 및 접속관리는 물론 인프라, 플랫폼, 소프트웨어 등 서비스별 보완체계 확립이 시급하다.

이러한 이슈들에 따라, 본 연구는 중소기업 산업보안 유형을 데이터 유출, 해킹, 랜섬웨어, 바이러스 감염, 핵심 시설물 피해, 기술인력 유출, 영업비밀 유출 등으로 상정하고자 한다.

제3절 선행연구 분석과 본 연구의 차별성

노민선, 이삼열(2010)은 중소기업의 산업보안 역량에 대한 영향요인 평가 연구를 진행했다. 실증분석 결과, 기업규모와 특허출원실적이 중소기업 산업보안 역량 수준에 통계적으로 유의미한 영향력을 가짐을 도출했고, 업종, 기술유출경험, 기술수출 실적, 국가연구개발 참여여부 등은 통계적 유의성이 없음을 확인했다. 이러한 결과에 따라, 연구자는 정부 차원에서 우선적으로 중소기업 지원범위의 구체화와 함께 기술유출경험에 있는 중소기업 대상 컨설팅 강화, 국가연구개발사업 참여기업에 대한 보안교육 강화 등을 통해 이러한 요인들이 산업보안 역량수준으로 연결되도록 해야 함을 강조했다.

이민형(2013)은 지역 중소기업의 성장동력 활성화 방안을 산업보안을 중심으로 검토했다. 이러한 연구목적을 위해 산업기술 유출방지를 위한 산업보안 활동들 중 AHP 기법을 통해 지역 중소기업에서 우선적으로 실시해야 할 중요도 높은 보안통제 활동을 분석했는데, 1단계 상위변수의 상대적 중요도에 있어 가장 높

은 것이 관리적 보안이며, 2단계 하위변수에 있어 물리적 보안 영역에서는 비인가자 중요시설 접근 통제, 관리적 보안에서는 보안감사가 가장 중요함을 확인했고, 기술적 보안 영역에서는 네트워크 보안의 중요성이 강조되었다.

박향미, 유지연(2015)는 중소기업 산업보안 강화를 위한 한국과 미국의 관리체계 비교, 분석연구를 진행했다. 연구자는 중소기업 피해가 증가하고 있고, 이들 기업들은 핵심기술을 대기업만큼 다량 보유할 수 없으므로 그 피해가 더 심각함을 제시하면서, 우리나라와 미국의 지침서를 비교, 분석하여 보안항목에 우선 적용할 항목을 구분하고, 전체차원의 항목을 도입하여 개별적인 보안항목을 응집함으로써 중소기업의 보안적용에 대한 부담을 줄여야 함을 제시했다.

전창욱, 유진호(2017)는 중소기업에서 산업보안을 위한 디지털포렌식 활용방안 연구를 이미징 처리시간 비교분석을 중심으로 진행했다. 정보보호 담당, 겸임 인력이 없는 다수 중소기업들은 디지털 포렌식 이미징 시간이 지연되면 담당업무를 진행하기 힘들고 외부 업체를 통해 진행하는 비용도 크기 때문에, 최대한 짧은 시간에 디지털포렌식 이미징 처리를 하여 자체적인 Hash값 획득을 통해 검증하는 것이 시간, 비용절감을 위한 핵심 방안임을 제시했다.

중소기업 산업보안과 연관된 다수 연구가 진행되어 중소기업이 갖는 상대적 열세 환경에서 효과적인 산업보안 활동을 할 방안과 전략을 제시하고 있으나, 본 연구가 주목하는 포스트 코로나 시대 대비 비대면환경이 확장되는 환경에서 중소기업 산업보안의 이상적인 방향성을 제시하는 연구가 매우 미흡하다. 이에 본 연구는 이러한 선행연구 동향과 한계에 따라, 비대면이 확장되어 산업보안 중요성이 더욱 강화되는 시점 대비 중소기업 산업보안의 이상적 방향성과 실무적 전략을 제시하고자 한다.

제3장 중소기업 산업보안 실태 분석

제1절 산업보안의 개념화에 대한 분석과 시사점

산업보안에 대한 개념 정의가 정립되지 못하기 때문에 발생하는 문제점이 심각함을 이창무(2017)는 강조했다. 즉, 산업보안 영역을 지나치게 협소, 제한하거나 아니면 산업보안과 연관이 없는 다른 영역으로 정의하면 연구 방향 자체에 오류가 생긴다는 것이다.

지난 2000년 이후 2016년까지 학술지 게재 논문 중 산업보안이 포함된 논문은 대략 47편인데, 이중 산업보안 개념을 정확하게 인지하고 이러한 개념에 입각해 분석을 시도한 연구는 거의 찾아보기 어렵다. 국가정보원(1999)은 '산업보안실무' 교재를 통해 산업보안을 '산업활동에 유용한 기술상, 경영상의 모든 정보나 인원, 문서, 시설, 자재 등을 산업스파이나 경쟁관계에 있는 기업은 물론이고 특정 관계가 없는 자에게 침해, 누설당하지 않도록 보호, 관리하기 위한 대응방안이나 활동'으로 규정했다. 이러한 국가정보원도 국가안보를 위해 존재하는 기관으로 산업기술 보호 역시 해외로 유출되는 경우에만 주력할 뿐이다. 거의 대부분 기업, 조직에서 행해지는 산업보안과는 거리가 멀며, 국제적으로 통용되는 보편화된 개념과도 상이하다.

이러한 산업보안 개념에 대한 일반적 오류는 산업보안 개념을 지극히 제한적으로 국한함에 있다. 산업보안을 산업기술보호 개념으로 한정하여 개념화하는 것이 대표적이다. 이는 개념화에 있어 포괄성을 위반하는 것이며, 일반화 오류에 해당한다. 산업보안을 논문 제목으로 설정한 전체 47편 연구 가운데 산업기술에 초점을 둔 연구가 무려 37편이다. 무려 79%로, 10편 가운데 8편 가량이 산업보안을 기술적 보호에 국한하여 결과를 도출했다.

<표 4> 산업보안 제목 설정 연구의 주제별 분류

주제	건수
산업기술보호	37
정보보호	4
기타	6
합계	47

※출처: 이창무. (2017). 산업보안 개념의 비판적 고찰. 한국경호경비학회지, 285-304.

하지만 표 5의 미국 산업보안 영역 분류 및 주요 내용에서 보듯이 산업보안 영역과 분야는 매우 다양하며, 그럼에도 불구하고 국내에서는 산업보안 연구에 있어 산업기술보호와 정보보호를 제외하고는 거의 다루지 않는 실정이다. 이로 인해, 자금 횡령, 사업 연속성 관리(BCP)[3], 컴플라이언스와 같은 산업보안의 중요한 주제에 대한 연구는 찾아볼 수 없다는 것이다.

<표 5> 미국 산업보안 영역 분류 및 주요내용

영역	주요 내용
National Security (국가 안보)	Border Security(국경 보안)
	Government Agencies(정부 기관)
	Policy & Regulation(정책 및 규제)
	Terrorism(테러리즘)
Physical Security (물리 보안)	Architecture & Engineering(설계 및 공학)
	Employee Management(직원 관리)
	Fraud/White Collar Crime(부정/화이트칼라 범죄)
	Guard Force Management(경비원 관리)
	Intrusion & Access Control(침입 및 출입 통제)
	Investigations(조사)
	Perimeter Protection(외곽 보호)
	Supply Chain(공급망)
	Surveillance(감시)

3) 사업 연속성(BC: Business Continuity)라는 개념은 위험관리(Risk Management) 영역에서 발생한 것으로, 위험관리를 통해 조직에 영향을 미칠 수 있는 Risk를 식별하고, 발생 가능성을 줄이거나, Risk가 발현되었을 때 피해 규모를 최소화하기 위한 대응절차를 마련하는 것(Deloitte, 2017).

CyberSecurity (사이버 보안)	Cloud Security(클라우드 보안) Cybercrime(사이버 범죄) Defenses(국방) Mobile Security(모바일 보안) Social Engineering(사회공학)
Strategic Security (전략기획 보안)	Enterprise Risk Management(기업 위험관리) Resilience(복원력) CSO/Leadership(CSO/리더십) Legal Issues(법적 이슈) Public/Private Partnerships(공공/민간 협력)
Security by Industry (산업별 보안)	Construction(건설) Education(교육) Emergency Services(응급 서비스) Financial Activities(금융) Government(정부) Healthcare(보건) Information(정보) Leisure and Hospitality(여가 및 관광) Manufacturing(제조업) Museums and Cultural Properties(미술관 및 문화시설) Natural Resources and Mining(천연자원 및 광업) Pharmaceutical(제약) Security, Professional, and Business Services(보안, 전문가 및 기업 서비스) Transportation(교통) Utilities(유틸리티) Wholesale and Retail Trade(도매 및 소매 유통)

※출처: 'Security Management' 홈페이지(https://sm.asisonline.org)

상기 미국의 산업보안 영역 분류 및 주요 내용을 보면, 안보정책 등에 해당하는 국가안보, 침입 및 출입 통제 등에 해당하는 물리보안, 사이버, 클라우드 범죄에 해당하는 사이버 보안은 물론 기업 위기관리, 복원력, 리더십에 해당하는 전략기획 보안 그리고 산업별 보안으로 산업보안 개념을 폭넓게 규정함을 알 수 있다.

따라서 본 연구는 일차적으로 국내 중소기업 산업보안 실태분석을 함에 있어

서는 국내에서 통용되는 데이터 유출, 해킹, 랜섬웨어, 바이러스 감염, 핵심 시설물 피해, 기술인력 유출, 영업비밀 유출 등으로 상정하여 기술적, 물리적 차원을 분석하고, 포스트 코로나 시대 개선방안을 위한 관리적 시사점을 제시함에 있어서는 미국의 이러한 분류방법을 감안하여, 관리적, 기술적, 물리적, 인력차원을 경영전략적 차원에서 조망하여 중소기업 산업보안 방향성을 제시하고자 한다.

제2절 포스트 코로나 시대 국내 중소기업 산업보안 실태

1. 연구 대상

연구 대상자의 일반적 사항을 살펴보면 <표 6>과 같이 전체 응답자는 140명이었고, 일반적 사항에 따른 분포는 다음과 같다.

성별로는 남자는 75명(53.6%), 여자는 65명(46.4%)이었고, 연령별로는 20대는 20명(14.3%), 30대는 45명(32.1%), 40대는 53명(37.9%), 50대는 15명(10.7%), 60대 이상은 7명(5.0%)이었다.

학력별로는 고졸 이하는 9명(6.4%), 전문대졸은 7명(5.0%), 4년제졸은 116명(82.9%), 대학원 재학은 7명(5.0%), 박사급은 1명(0.7%)이었고, 직급별로는 평사원은 56명(40.0%), 과장급은 55명(39.3%), 부장급은 25명(17.9%), 이사급은 3명(2.1%), 경영진은 1명(0.7%)이었다.

근무기간별로는 1년 이하는 10명(7.1%), 1-3년은 25명(17.9%), 4-6년은 30명(21.4%), 7-9년은 22명(15.7%), 10년 이상은 53명(37.9%)이었고, 재택근무 여부별로는 하고 있음은 43명(30.7%), 하고 있지 않음은 97명(69.3%)이었다.

하루 평균 디지털 미디어 사용 시간별로는 1시간 미만은 5명(3.6%), 1-3시간은 25명(17.9%), 3-5시간은 58명(41.4%), 5-7시간은 32명(22.9%), 8시간은 이상은 20명(14.3%)이었다.

산업군별로는 건설은 8명(5.7%), 화학은 4명(2.9%), 전기/전자는 51명(36.4%), 자동차는 11명(7.9%), 금융은 2명(1.4%), 의료는 4명(2.9%), 교육은 6명(4.3%), 화장품은 3명(2.1%), 통신업은 46명(32.9%), 기타는 5명(3.6%)이었고, 기업규모별로는 50명 미만은 45명(32.1%), 50-100명은 34명(24.3%), 100-200명은 21명

(15.0%), 200-300명은 13명(9.3%), 300명 이상은 27명(19.3%)이었다.

<표 6> 연구 대상자의 일반적 사항

N=140

특성	구분	N	%	특성	구분	N	%
성별	남자	75	53.6	재택근무 여부	예	43	30.7
	여자	65	46.4		아니오	97	69.3
연령	20대	20	14.3	하루 평균 디지털 미디어 사용 시간	1시간 미만	5	3.6
	30대	45	32.1		1-3시간	25	17.9
	40대	53	37.9		3-5시간	58	41.4
	50대	15	10.7		5-7시간	32	22.9
	60대 이상	7	5.0		8시간 이상	20	14.3
학력	고졸 이하	9	6.4	산업군	건설	8	5.7
	전문대졸	7	5.0		화학	4	2.9
	4년제졸	116	82.9		전기/전자	51	36.4
	대학원 재학	7	5.0		자동차	11	7.9
	박사급	1	0.7		금융	2	1.4
직급	평사원	56	40.0		의료	4	2.9
	과장급	55	39.3		교육	6	4.3
	부장급	25	17.9		화장품	3	2.1
	이사급	3	2.1		통신업	46	32.9
	경영진	1	0.7		기타	5	3.6
근무기간	1년 이하	10	7.1	기업규모	50명 미만	45	32.1
	1-3년	25	17.9		50-100명	34	24.3
	4-6년	30	21.4		100-200명	21	15.0
	7-9년	22	15.7		200-300명	13	9.3
	10년 이상	53	37.9		300명 이상	27	19.3

2. 자료 처리 방법

본 연구는 산업보안에 대한 인식 실태에 대한 연구로서 통계 프로그램 SPSS 27.0을 사용하여 자료를 분석하였다.

첫째, 연구 대상자의 일반적 사항을 알아보기 위하여 빈도분석을 실시하여 빈도와 백분율(%)을 산출하였다. 둘째, 연구 대상자의 일반적 특성에 따른 산업보

안 인식도, 산업보안 중요성, 개인정보 유출 및 산업보안 사고, 산업보안의 대응, 산업보안 교육 이수 및 보안의식 차이를 알아보기 위하여 명목척도일 경우에는 χ^2-검증에 의한 교차분석과 다중응답분석을 실시하였고, 등간척도일 경우에는 독립 t-test와 일원변량분석(ANOVA)을 실시하였다. 셋째, 모든 검증 방법들의 통계적 유의수준은 α=0.05, 0.01, 0.001에서 검증하였다.

3. 분석결과

(1) 산업보안 인식도

1) 산업보안 내 세부 영역에 대한 인지도

① 산업보안 내 세부 영역에 대한 인지도

산업보안 내 세부 영역에 대한 인지도는 <표 7-1>과 같다.

산업보안 내 세부 영역에 대한 인지도는 평균이 3.79~3.99로 모두 약간 알고 있었고, 영역별로는 전문 정보보안의 의미(M=3.99)에 대한 인지도가 가장 높았고, 다음으로 산업기술보호의 의미(M=3.95), 전문 기술인력 유출의 의미(M=3.94), 영업비밀 유출 및 산업스파이의 의미(M=3.92) 순으로 높았다.

<표 7-1> 산업보안 내 세부 영역에 대한 인지도

영역	N	M[1)]	SD
정보보안의 의미	140	3.99	0.80
산업기술보호의 의미	140	3.95	0.80
핵심 시설물 및 장비 보안의 의미	140	3.79	1.01
전문 기술인력 유출의 의미	140	3.94	0.95
영업비밀 유출 및 산업스파이의 의미	140	3.92	0.91

[1)] Likert 5점 척도: 1=전혀 모름, 3=보통, 5=잘 알고 있음

강민기, 박찬수(2020)의 전문가 델파이기법을 활용한 한국 산업보안 생태계 인식 조사연구에 따른 결과는 다음과 같다.

<표 7-2> 산업보안 이슈 인식에 대한 각 집단별 조사결과

구분	전체	산업기술 보유기업	보안 전문기업	대학	연구자	언론	정부 지원기관
퇴직인력 등 내부자에 의한 유출	36.4	45.5	12.5	50	20	40	50
M&A등 자본에 의한 기술유출	23..6	9.1	25.5	25	50	20	16.7
스마트 제조환경과 네트워크 보안	21.8	36.4	12.5	12.5	30	20	16.7
악의적 해킹에 대한 사이버보안	9.1	0	25.5	0	0	20	8.3
개인 정보보호	5.5	0	25.5	0	0	0	8.3
기타	3.6	9.1	0	12.5	0	0	0

※출처: 강민기, 박찬수(2020) 전문가 델파이기법을 활용한 한국 산업보안 생태계 인식 조사연구.

이 연구 결과에 따르면, 본 연구가 주목하는 산업기업 구성원들의 산업보안 인식의 경우, 내부자에 의한 유출이 45.5%로 가장 심각한 산업보안 위협임을 인식하였고, 스마트 제조환경과 네트워크 보안이 그 다음으로 36.4% 그리고 M&A 등 자본에 의한 기술유출, 기타 등으로 순으로 집계됨을 확인할 수 있다.

본 연구에는 전문보안의 의미, 산업기술보호의 의미 인식이 가장 높았는데, 상기 연구 통계치와 이를 접목하면, 기업 구성원이 익숙하게 인지하는 전문보안과 산업기술보호 보안을 위협하는 가장 큰 원인들이 곧 내부자에 의한 유출과

스마트 제조환경에 따른 네트워킹에 따른 유출 등임을 알 수 있다.

② 직급에 따른 산업보안 내 세부 영역에 대한 인지도

직급에 따른 산업보안 내 세부 영역에 대한 인지도는 <표 7-3>과 같다. 산업보안 내 세부 영역 모두에서 통계적으로 유의한 차이가 있었다.

정보보안의 의미는 평사원(M=3.77), 과장급(M=4.05), 부장급 이상(M=4.28)으로 통계적으로 유의한 차이가 있었고($p<.05$), 사후 검정인 Duncan test를 실시한 결과, 부장급 이상이 평사원보다 인지도가 더 높은 것으로 나타났다.

산업기술보호의 의미는 평사원(M=3.61), 과장급(M=4.15), 부장급 이상(M=4.24)으로 통계적으로 유의한 차이가 있었고($p<.001$), 사후검정인 Duncan test를 실시한 결과, 과장급/부장급 이상이 평사원보다 인지도가 더 높은 것으로 나타났다.

핵심 시설물 및 장비 보안의 의미는 평사원(M=3.34), 과장급(M=4.13), 부장급 이상(M=4.03)으로 통계적으로 유의한 차이가 있었고($p<.001$), 사후검정인 Duncan test를 실시한 결과, 과장급/부장급 이상이 평사원보다 인지도가 더 높은 것으로 나타났다.

전문 기술인력 유출의 의미는 평사원(M=3.55), 과장급(M=4.16), 부장급 이상(M=4.28)으로 통계적으로 유의한 차이가 있었고($p<.001$), 사후검정인 Duncan test를 실시한 결과, 과장급/부장급 이상이 평사원보다 인지도가 더 높은 것으로 나타났다.

영업비밀 유출 및 산업스파이의 의미는 평사원(M=3.54), 과장급(M=4.09), 부장급 이상(M=4.34)으로 통계적으로 유의한 차이가 있었고($p<.001$), 사후검정인 Duncan test를 실시한 결과, 과장급/부장급 이상이 평사원보다 인지도가 더 높은 것으로 나타났다.

<표 7-3> 직급에 따른 인지도

영역	구분	N	M	SD	F	p	Duncan
정보보안의 의미	평사원(a)	56	3.77	0.83	4.444	.013*	a<c
	과장급(b)	55	4.05	0.70			
	부장급 이상(c)	29	4.28	0.80			
산업기술보호의 의미	평사원(a)	56	3.61	0.87	9.851	.000***	a<b, c
	과장급(b)	55	4.15	0.62			
	부장급 이상(c)	29	4.24	0.74			
핵심 시설물 및 장비 보안의 의미	평사원(a)	56	3.34	1.05	10.906	.000***	a<b, c
	과장급(b)	55	4.13	0.82			
	부장급 이상(c)	29	4.03	0.94			
전문 기술인력 유출의 의미	평사원(a)	56	3.55	1.06	8.863	.000***	a<b, c
	과장급(b)	55	4.16	0.71			
	부장급 이상(c)	29	4.28	0.88			
영업비밀 유출 및 산업스파이의 의미	평사원(a)	56	3.54	0.93	10.245	.000***	a<b, c
	과장급(b)	55	4.09	0.75			
	부장급 이상(c)	29	4.34	0.90			

*p<.05, ***p<.001

③ 근무기간에 따른 산업보안 내 세부 영역에 대한 인지도

근무기간에 따른 산업보안 내 세부 영역에 대한 인지도는 <표 7-4>와 같다.

산업보안 내 세부 영역 중에서 핵심 시설물 및 장비 보안의 의미에서 통계적으로 유의한 차이가 있었다.

핵심 시설물 및 장비 보안의 의미는 1년 이하(M=3.60), 1-3년(M=3.52), 4-6년(M=3.43), 7-9년(M=3.95), 10년 이상(M=4.09)으로 통계적으로 유의한 차이가 있었고(p<.05), 사후검정인 Duncan test를 실시한 결과, 10년 이상이 1-3년/4-6년보다 인지도가 더 높은 것으로 나타났다.

<표 7-4> 근무기간에 따른 인지도

영역	구분	N	M	SD	F	p	Duncan
정보보안의 의미	1년 이하	10	4.10	0.74	1.068	.375	
	1-3년	25	3.76	0.83			
	4-6년	30	3.87	0.73			
	7-9년	22	4.09	0.53			
	10년 이상	53	4.09	0.90			
산업기술보호의 의미	1년 이하	10	3.80	0.79	2.222	.070	
	1-3년	25	3.72	0.89			
	4-6년	30	3.73	0.69			
	7-9년	22	4.14	0.77			
	10년 이상	53	4.13	0.79			
핵심 시설물 및 장비 보안의 의미	1년 이하(a)	10	3.60	0.97	2.998	.021*	b, c<e
	1-3년(b)	25	3.52	1.05			
	4-6년(c)	30	3.43	1.10			
	7-9년(d)	22	3.95	0.84			
	10년 이상(e)	53	4.09	0.93			
전문 기술인력 유출의 의미	1년 이하	10	3.90	0.99	1.314	.268	
	1-3년	25	3.72	0.94			
	4-6년	30	3.73	1.01			
	7-9년	22	4.05	0.95			
	10년 이상	53	4.13	0.90			
영업비밀 유출 및 산업스파이의 의미	1년 이하	10	3.80	0.92	.658	.622	
	1-3년	25	3.76	0.88			
	4-6년	30	3.87	0.90			
	7-9년	22	3.86	0.89			
	10년 이상	53	4.08	0.96			

*p<.05

④ 재택근무 여부에 따른 산업보안 내 세부 영역에 대한 인지도

재택근무 여부에 따른 산업보안 내 세부 영역에 대한 인지도는 <표 7-5>와 같다.

산업보안 내 세부 영역 중에서 정보보안의 의미에서 통계적으로 유의한 차이가 있었다.

정보보안의 의미는 재택근무(M=4.33)가 재택근무 아님(M=3.84)보다 인지도가 더 높았으며, 통계적으로 유의한 차이가 있었다($p<.01$).

<표 7-5> 재택근무 여부에 따른 인지도

영역	구분	N	M	SD	t	p
정보보안의 의미	예	43	4.33	0.61	3.499	.001**
	아니오	97	3.84	0.83		
산업기술보호의 의미	예	43	4.12	0.63	1.650	.101
	아니오	97	3.88	0.86		
핵심 시설물 및 장비 보안의 의미	예	43	3.98	0.91	1.444	.151
	아니오	97	3.71	1.04		
전문 기술인력 유출의 의미	예	43	4.09	0.89	1.247	.214
	아니오	97	3.88	0.97		
영업비밀 유출 및 산업스파이의 의미	예	43	4.07	0.86	1.281	.202
	아니오	97	3.86	0.94		

**$p<.01$

⑤ 하루 평균 디지털 미디어 사용 시간에 따른 인지도

하루 평균 디지털 미디어 사용 시간에 따른 산업보안 내 세부 영역에 대한 인지도는 <표 7-6>과 같다.

산업보안 내 세부 영역 중에서 정보보안의 의미에서 통계적으로 유의한 차이가 있었다.

정보보안의 의미는 3시간미만(M=3.63), 3-5시간(M=4.09), 5-7시간(M=4.13), 8

시간 이상(M=4.00)으로 통계적으로 유의한 차이가 있었고(p<.05), 사후검정인 Duncan test를 실시한 결과, 3-5시간과 5-7시간이 3시간미만보다 인지도가 더 높은 것으로 나타났다.

<표 7-6> 하루 평균 디지털 미디어 사용 시간에 따른 인지도

영역	구분	N	M	SD	*F*	*p*	Duncan
정보보안의 의미	3시간 미만(a)	30	3.63	0.89	2.695	.049*	a<b, c
	3-5시간(b)	58	4.09	0.82			
	5-7시간(c)	32	4.13	0.71			
	8시간 이상(d)	20	4.00	0.56			
산업기술보호의 의미	3시간 미만	30	3.63	0.85	2.283	.082	
	3-5시간	58	4.02	0.81			
	5-7시간	32	4.13	0.75			
	8시간 이상	20	3.95	0.69			
핵심 시설물 및 장비 보안의 의미	3시간 미만	30	3.57	1.04	2.024	.113	
	3-5시간	58	3.67	1.08			
	5-7시간	32	4.06	0.84			
	8시간 이상	20	4.05	0.89			
전문 기술인력 유출의 의미	3시간 미만	30	3.97	0.93	1.232	.301	
	3-5시간	58	3.78	0.97			
	5-7시간	32	4.16	0.88			
	8시간 이상	20	4.05	1.00			
영업비밀 유출 및 산업스파이의 의미	3시간 미만	30	3.70	0.88	1.632	.185	
	3-5시간	58	3.93	0.92			
	5-7시간	32	4.19	0.78			
	8시간 이상	20	3.80	1.11			

*p<.05

⑥ 산업군에 따른 산업보안 내 세부 영역에 대한 인지도

산업군에 따른 산업보안 내 세부 영역에 대한 인지도는 <표 7-7>와 같다.

산업보안 내 세부 영역 중에서 정보보안의 의미, 산업기술보호의 의미, 핵심 시설물 및 장비 보안의 의미에서 통계적으로 유의한 차이가 있었다.

정보보안의 의미는 제조업(M=3.70), 정보통신(M=4.10), 기타(M=3.75)로 통계적으로 유의한 차이가 있었고($p<.05$), 사후검정인 Duncan test를 실시한 결과, 정보통신이 제조업/기타보다 인지도가 더 높은 것으로 나타났다.

산업기술보호의 의미는 제조업(M=3.70), 정보통신(M=4.07), 기타(M=3.65)로 통계적으로 유의한 차이가 있었고($p<.05$), 사후검정인 Duncan test를 실시한 결과, 정보통신이 제조업/기타보다 인지도가 더 높은 것으로 나타났다.

핵심 시설물 및 장비 보안의 의미는 제조업(M=3.43), 정보통신(M=3.95), 기타(M=3.45)로 통계적으로 유의한 차이가 있었고($p<.05$), 사후검정인 Duncan test를 실시한 결과, 정보통신이 제조업/기타보다 인지도가 더 높은 것으로 나타났다.

<표 7-7> 산업군에 따른 인지도

영역	구분	N	M	SD	F	p	Duncan
정보보안의 의미	제조업(a)	23	3.70	1.11	3.592	.030*	a, c<b
	정보통신(b)	97	4.10	0.65			
	기타(c)	20	3.75	0.91			
산업기술보호의 의미	제조업(a)	23	3.70	0.97	3.866	.023*	a, c<b
	정보통신(b)	97	4.07	0.71			
	기타(c)	20	3.65	0.88			
핵심 시설물 및 장비 보안의 의미	제조업(a)	23	3.43	1.04	3.929	.022*	a, c<b
	정보통신(b)	97	3.95	0.93			
	기타(c)	20	3.45	1.19			
전문 기술인력 유출의 의미	제조업	23	3.61	0.94	2.068	.130	
	정보통신	97	4.04	0.88			
	기타	20	3.85	1.23			
영업비밀 유출 및 산업스파이의 의미	제조업	23	3.57	0.99	2.125	.123	
	정보통신	97	3.99	0.88			
	기타	20	4.00	0.92			

*$p<.05$

2) 평소 산업보안에 대해 필요성을 느끼는 시기

평소 산업보안에 대해 필요성을 느끼는 시기는 <표 8>과 같이 전체적으로는 항상 중요하게 생각함이 54.3%로 가장 많았고, 다음으로 커뮤니티, 매체, 지인을 통해 간접 경험(33.6%), 직접 피해를 겪은 후(10.7%) 순으로 많았다.

직급, 근무기간, 재택근무 여부, 디지털 미디어 사용 시간, 산업군 모두에서 통계적으로 유의한 차이가 없었다.

<표 8> 평소 산업보안에 대해 필요성을 느끼는 시기

N(%)

구분		항상 중요하게 생각	직접 피해를 겪은 후	커뮤니티, 매체, 지인을 통해 간접 경험	필요하지 않음	전체	χ^2/p
직급	평사원	26(46.4)	7(12.5)	22(39.3)	1(1.8)	56(100.0)	3.508/.743
	과장급	31(56.4)	5(9.1)	18(32.7)	1(1.8)	55(100.0)	
	부장급 이상	19(65.5)	3(10.3)	7(24.1)	0(0.0)	29(100.0)	
근무기간	1년 이하	3(30.0)	2(20.0)	5(50.0)	0(0.0)	10(100.0)	12.524/.405
	1-3년	11(44.0)	2(8.0)	12(48.0)	0(0.0)	25(100.0)	
	4-6년	14(46.7)	5(16.7)	11(36.7)	0(0.0)	30(100.0)	
	7-9년	14(63.6)	1(4.5)	6(27.3)	1(4.5)	22(100.0)	
	10년 이상	34(64.2)	5(9.4)	13(24.5)	1(1.9)	53(100.0)	
재택근무 여부	예	24(55.8)	2(4.7)	16(37.2)	1(2.3)	43(100.0)	2.750/.432
	아니오	52(53.6)	13(13.4)	31(32.0)	1(1.0)	97(100.0)	
디지털 미디어 사용 시간	3시간 미만	14(46.7)	5(16.7)	10(33.3)	1(3.3)	30(100.0)	7.133/.623
	3-5시간	33(56.9)	8(13.8)	16(27.6)	1(1.7)	58(100.0)	
	5-7시간	18(56.3)	1(3.1)	13(40.6)	0(0.0)	32(100.0)	
	8시간 이상	11(55.0)	1(5.0)	8(40.0)	0(0.0)	20(100.0)	
산업군	제조업	12(52.2)	1(4.3)	9(39.1)	1(4.3)	23(100.0)	4.114/.661
	정보통신	55(56.7)	11(11.3)	30(30.9)	1(1.0)	97(100.0)	
	기타	9(45.0)	3(15.0)	8(40.0)	0(0.0)	20(100.0)	
전체		76(54.3)	15(10.7)	47(33.6)	2(1.4)	140(100.0)	

3) 기업 내 임직원들이 산업보안에 관심을 갖지 않는 이유

기업 내 임직원들이 산업보안에 관심을 갖지 않는 이유(다중응답)는 <표 9>와 같이 전체적으로는 조치를 하기 위해 많은 비용이 발생한다는 생각이 26.8%로 가장 많았고, 다음으로 보안 조치를 하기가 귀찮고 불편(24.9%), 나와 상관없는 일이라고 생각(21.9%) 순으로 많았다.

직급별로는 평사원(28.7%), 부장급 이상(28.1%)은 조치를 하기 위해 많은 비용이 발생한다는 생각이 가장 많았고, 과장급(27.1%)은 보안 조치를 하기가 귀찮고 불편이 가장 많았다.

근무기간별로는 1년 이하(35.0%), 4-6년(28.1%)은 보안 조치를 하기가 귀찮고 불편하다가 가장 많았고, 1-3년(24.4%), 7-9년(30.8%), 10년 이상(28.8%)은 조치를 하기 위해 많은 비용이 발생한다는 생각이 가장 많았다.

재택근무 여부별로는 재택근무(29.4%)는 보안 조치를 하기가 귀찮고 불편하다가 가장 많았고, 재택근무 아님(28.9%)은 조치를 하기 위해 많은 비용이 발생한다는 생각이 가장 많았다.

디지털 미디어 사용 시간별로는 3시간 미만(32.1%), 5-7시간(30.6%)은 조치를 하기 위해 많은 비용이 발생한다는 생각이 가장 많았고, 3-5시간(27.9%), 8시간 이상(27.9%)은 보안 조치를 하기가 귀찮고 불편하다가 가장 많았다.

산업군별로는 제조업(36.4%)은 조치를 하기 위해 많은 비용이 발생한다는 생각이 가장 많았고, 정보통신(25.4%)은 보안 조치를 하기가 귀찮고 불편하다가 가장 많았고, 기타는 보안 조치를 하기가 귀찮고 불편, 조치를 하기 위해 많은 비용이 발생한다는 생각이 각각 30.0%로 가장 많았다.

<표 9> 기업 내 임직원들이 산업보안에 관심을 갖지 않는 이유

N(%)

구분 (다중응답)		내용이 이해하기 어려움	보안 조치를 하기가 귀찮고 불편	조치를 해도 보안 사고는 막을 수 없다고 생각	나와 상관없는 일이라고 생각	조치를 하기 위해 많은 비용이 발생한다는 생각	기타	전체
직급	평사원	10(9.9)	22(21.8)	16(15.8)	23(22.8)	29(28.7)	1(1.0)	101(100.0)
	과장급	8(7.5)	29(27.1)	23(21.5)	20(18.7)	26(24.3)	1(0.9)	107(100.0)
	부장급 이상	4(7.0)	15(26.3)	7(12.3)	15(26.3)	16(28.1)	0(0.0)	57(100.0)
근무기간	1년 이하	1(5.0)	7(35.0)	4(20.0)	3(15.0)	5(25.0)	0(0.0)	20(100.0)
	1-3년	9(20.0)	9(20.0)	6(13.3)	9(20.0)	11(24.4)	1(2.2)	45(100.0)
	4-6년	4(7.0)	16(28.1)	11(19.3)	13(22.8)	13(22.8)	0(0.0)	57(100.0)
	7-9년	1(2.6)	9(23.1)	9(23.1)	7(17.9)	12(30.8)	1(2.6)	39(100.0)
	10년 이상	7(6.7)	25(24.0)	16(15.4)	26(25.0)	30(28.8)	0(0.0)	104(100.0)
재택근무 여부	예	7(8.2)	25(29.4)	18(21.2)	16(18.8)	19(22.4)	0(0.0)	85(100.0)
	아니오	15(8.3)	41(22.8)	28(15.6)	42(23.3)	52(28.9)	2(1.1)	180(100.0)
디지털 미디어 사용 시간	3시간 미만	2(3.6)	12(21.4)	9(16.1)	14(25.0)	18(32.1)	1(1.8)	56(100.0)
	3-5시간	9(8.7)	29(27.9)	17(16.3)	25(24.0)	24(23.1)	0(0.0)	104(100.0)
	5-7시간	7(11.3)	13(21.0)	11(17.7)	12(19.4)	19(30.6)	0(0.0)	62(100.0)
	8시간 이상	4(9.3)	12(27.9)	9(20.9)	7(16.3)	10(23.3)	1(2.3)	43(100.0)
산업군	제조업	3(6.8)	8(18.2)	4(9.1)	12(27.3)	16(36.4)	1(2.3)	44(100.0)
	정보통신	18(9.9)	46(25.4)	38(21.0)	35(19.3)	43(23.8)	1(0.6)	181(100.0)
	기타	1(2.5)	12(30.0)	4(10.0)	11(27.5)	12(30.0)	0(0.0)	40(100.0)
전체		22(8.3)	66(24.9)	46(17.4)	58(21.9)	71(26.8)	2(0.8)	265(100.0)

(2) 산업보안 중요성

1) 산업보안 영역에 대한 중요도

① 산업보안 영역에 대한 중요도

산업보안 영역에 대한 중요도는 <표 10-1>과 같다.

산업보안 영역에 대한 중요도는 평균이 4.19~4.61로 모두 매우 높은 것으로 나타났고, 영역별로는 정보 자산에 대한 보안(M=4.61)이 중요도가 가장 높았고, 다음으로 인적 자산에 대한 보안(M=4.32), 설비·시설 자산에 대한 보안(M=4.19) 순으로 높았다.

<표 10-1> 산업보안 영역에 대한 중요도

영역	N	M[1)]	SD
인적 자산에 대한 보안	140	4.32	0.65
설비·시설 자산에 대한 보안	140	4.19	0.66
정보 자산에 대한 보안	140	4.61	0.56

[1)] Likert 5점 척도: 1=전혀 그렇지 않다, 3=보통이다, 5=매우 그렇다

② 직급에 따른 산업보안 영역에 대한 중요도

직급에 따른 산업보안 영역에 대한 중요도는 <표 10-2>과 같다.

산업보안 영역 모두에서 통계적으로 유의한 차이가 없었다.

<표 10-2> 직급에 따른 중요도

영역	구분	N	M	SD	F	p	Duncan
인적 자산에 대한 보안	평사원	56	4.29	0.62	.385	.681	
	과장급	55	4.31	0.69			
	부장급 이상	29	4.41	0.63			
설비·시설 자산에 대한 보안	평사원	56	4.11	0.71	.652	.523	
	과장급	55	4.24	0.67			
	부장급 이상	29	4.24	0.58			
정보 자산에 대한 보안	평사원	56	4.54	0.60	1.542	.218	
	과장급	55	4.62	0.56			
	부장급 이상	29	4.76	0.44			

③ 근무기간에 따른 산업보안 영역에 대한 중요도

근무기간에 따른 산업보안 영역에 대한 중요도는 <표 10-3>과 같다.

산업보안 영역 모두에서 통계적으로 유의한 차이가 없었다.

<표 10-3> 근무기간에 따른 중요도

영역	구분	N	M	SD	F	p	Duncan
인적 자산에 대한 보안	1년 이하	10	4.40	0.52	.238	.916	
	1-3년	25	4.24	0.66			
	4-6년	30	4.30	0.70			
	7-9년	22	4.41	0.73			
	10년 이상	53	4.32	0.61			
설비·시설 자산에 대한 보안	1년 이하	10	3.90	0.57	2.231	.069	
	1-3년	25	4.04	0.79			
	4-6년	30	4.03	0.67			
	7-9년	22	4.27	0.70			
	10년 이상	53	4.36	0.56			
정보 자산에 대한 보안	1년 이하	10	4.30	0.67	1.236	.299	
	1-3년	25	4.64	0.49			
	4-6년	30	4.53	0.63			
	7-9년	22	4.68	0.57			
	10년 이상	53	4.68	0.51			

④ 재택근무 여부에 따른 산업보안 영역에 대한 중요도

재택근무 여부에 따른 산업보안 영역에 대한 중요도는 <표 10-4>와 같다.
산업보안 영역 모두에서 통계적으로 유의한 차이가 없었다.

<표 10-4> 재택근무 여부에 따른 중요도

영역	구분	N	M	SD	*t*	*p*
인적 자산에 대한 보안	예	43	4.33	0.71	.050	.960
	아니오	97	4.32	0.62		
설비·시설 자산에 대한 보안	예	43	4.19	0.70	.004	.997
	아니오	97	4.19	0.65		
정보 자산에 대한 보안	예	43	4.65	0.53	.520	.604
	아니오	97	4.60	0.57		

⑤ 하루 평균 디지털 미디어 사용 시간에 따른 중요도

하루 평균 디지털 미디어 사용 시간에 따른 산업보안 영역에 대한 중요도는 <표 10-5>와 같다.
산업보안 영역 모두에서 통계적으로 유의한 차이가 없었다.

<표 10-5> 하루 평균 디지털 미디어 사용 시간에 따른 중요도

영역	구분	N	M	SD	*F*	*p*	Duncan
인적 자산에 대한 보안	3시간 미만	30	4.37	0.56	.166	.919	
	3-5시간	58	4.28	0.72			
	5-7시간	32	4.34	0.65			
	8시간 이상	20	4.35	0.59			
설비・시설 자산에 대한 보안	3시간 미만	30	4.13	0.73	.525	.666	
	3-5시간	58	4.22	0.59			
	5-7시간	32	4.09	0.73			
	8시간 이상	20	4.30	0.66			
정보 자산에 대한 보안	3시간 미만	30	4.63	0.56	.224	.880	
	3-5시간	58	4.57	0.57			
	5-7시간	32	4.66	0.60			
	8시간 이상	20	4.65	0.49			

⑥ 산업군에 따른 산업보안 영역에 대한 중요도

산업군에 따른 산업보안 영역에 대한 중요도는 <표 10-6>과 같다.

산업보안 영역 모두에서 통계적으로 유의한 차이가 없었다.

<표 10-6> 산업군에 따른 산업보안 중요도

영역	구분	N	M	SD	*F*	*p*	Duncan
인적 자산에 대한 보안	제조업[4]	23	4.17	0.58	2.551	.082	
	정보통신[5]	97	4.30	0.66			
	기타[6]	20	4.60	0.60			
설비・시설 자산에 대한 보안	제조업	23	4.22	0.60	.166	.848	
	정보통신	97	4.16	0.69			
	기타	20	4.25	0.64			
정보 자산에 대한 보안	제조업	23	4.65	0.57	.397	.673	
	정보통신	97	4.59	0.57			
	기타	20	4.70	0.47			

4) <표 6> 자동차, 건설, 화학, 철강업
5) <표 6> 전기/전자, 통신업
6) <표 6> 금융, 의료, 교육, 화장품

2) 산업보안을 구성원 모두가 심각성을 인지하고 실천하는 것의 중요도

산업보안을 구성원 모두가 심각성을 인지하고 실천하는 것의 중요도는 <표 11>과 같이 전체적으로는 평균이 4.36점으로 '그렇다(4점)'과 '매우 그렇다(5점)' 사이로 매우 높은 것으로 나타났다.

직급별로는 평사원(M=4.20), 과장급(M=4.47), 부장급 이상(M=4.48)으로 통계적으로 유의한 차이가 있었고($p<.05$), 사후검정인 Duncan test를 실시한 결과, 과장급/부장급 이상이 평사원보다 산업보안을 구성원 모두가 심각성을 인지하고 실천하는 것의 중요도가 더 높은 것으로 나타났다.

산업군별로는 제조업(M=4.30), 정보통신(M=4.31), 기타(M=4.70)로 통계적으로 유의한 차이가 있었고($p<.05$), 사후검정인 Duncan test를 실시한 결과, 기타가 제조업/정보통신보다 산업보안을 구성원 모두가 심각성을 인지하고 실천하는 것의 중요도가 더 높은 것으로 나타났다.

<표 11> 심각성을 인지하고 실천하는 것에 대한 중요도

구분		N	M[1)]	SD	*F/t*	*p*	Duncan
직급	평사원(a)	56	4.20	0.55	3.772	.025*	a<b, c
	과장급(b)	55	4.47	0.60			
	부장급 이상(c)	29	4.48	0.63			
근무기간	1년 이하	10	4.20	0.42	1.732	.146	
	1-3년	25	4.16	0.55			
	4-6년	30	4.30	0.65			
	7-9년	22	4.45	0.60			
	10년 이상	53	4.49	0.61			
재택근무 여부	예	43	4.44	0.55	1.015	.312	
	아니오	97	4.33	0.62			
디지털 미디어 사용 시간	3시간 미만	30	4.37	0.67	.557	.644	
	3-5시간	58	4.29	0.62			
	5-7시간	32	4.44	0.50			
	8시간 이상	20	4.45	0.60			
산업군	제조업(a)	23	4.30	0.56	3.770	.025*	a, b<c
	정보통신(b)	97	4.31	0.62			
	기타(c)	20	4.70	0.47			
전체		140	4.36	0.60			

[1)] Likert 5점 척도: 1=전혀 그렇지 않다, 3=보통이다, 5=매우 그렇다

*$p<.05$

3) 산업보안 피해 발생 시 가장 피해가 클 것이라 생각되는 산업 종류

① 전체, 직급, 근무기간

산업보안 피해 발생 시 가장 피해가 클 것이라 생각되는 산업 종류(다중응답)는 <표 12-1>와 같이 전체적으로는 전기/전자가 17.4%로 가장 많았고, 다음으로 금융(14.0%), 통신업(13.2%) 순으로 많았다.

직급별로는 평사원은 금융(17.4%), 전기/전자(16.5%), 통신업(14.3%) 순으로 많았고, 과장급은 전기/전자(17.9%), 금융(12.6%), 화학(12.2%) 순으로 많았고, 부장급 이상은 전기/전자(17.9%), 자동차(17.1%), 통신업(14.5%) 순으로 많았다.

근무기간별로는 1년 이하는 전기/전자(19.4%), 통신업(13.9%) 순으로 많았고, 1-3년은 금융(16.5%), 전기/전자(12.4%), 의료(12.4%) 순으로 많았고, 4-6년은 전기/전자(21.4%), 금융(14.3%), 화학(12.5%), 자동차(12.5%) 순으로 많았고, 7-9년은 전기/전자(16.0%), 금융(12.3%), 의료(12.3%) 순으로 많았고, 10년 이상은 전기/전자(18.3%), 통신업(17.4%), 금융(13.8%) 순으로 많았다.

<표 12-1> 산업보안 피해가 클 것이라 생각되는 산업 종류

N(%)

구분 (다중응답)	직급			근무기간					전체
	평사원	과장급	부장급 이상	1년 이하	1-3년	4-6년	7-9년	10년 이상	
전기/전자	38(16.5)	44(17.9)	21(17.9)	7(19.4)	15(12.4)	24(21.4)	17(16.0)	40(18.3)	103(17.4)
금융	40(17.4)	31(12.6)	12(10.3)	4(11.1)	20(16.5)	16(14.3)	13(12.3)	30(13.8)	83(14.0)
통신업	33(14.3)	28(11.4)	17(14.5)	5(13.9)	11(9.1)	12(10.7)	12(11.3)	38(17.4)	78(13.2)
자동차	24(10.4)	26(10.6)	20(17.1)	4(11.1)	12(9.9)	14(12.5)	11(10.4)	29(13.3)	70(11.8)
의료	23(10.0)	26(10.6)	12(10.3)	4(11.1)	15(12.4)	8(7.1)	13(12.3)	21(9.6)	61(10.3)
화학	20(8.7)	30(12.2)	9(7.7)	3(8.3)	11(9.1)	14(12.5)	9(8.5)	22(10.1)	59(9.9)
조선업	17(7.4)	18(7.3)	10(8.5)	2(5.6)	10(8.3)	10(8.9)	8(7.5)	15(6.9)	45(7.6)
철강업	11(4.8)	13(5.3)	6(5.1)	3(8.3)	9(7.4)	4(3.6)	7(6.6)	7(3.2)	30(5.1)
건설업	10(4.3)	14(5.7)	6(5.1)	1(2.8)	7(5.8)	5(4.5)	7(6.6)	10(4.6)	30(5.1)
교육	9(3.9)	8(3.3)	2(1.7)	2(5.6)	6(5.0)	4(3.6)	5(4.7)	2(0.9)	19(3.2)
화장품	5(2.2)	8(3.3)	2(1.7)	1(2.8)	5(4.1)	1(0.9)	4(3.8)	4(1.8)	15(2.5)
전체	230(100.0)	246(100.0)	117(100.0)	36(100.0)	121(100.0)	112(100.0)	106(100.0)	218(100.0)	593(100.0)

※ 전체, 직급, 근무기간

② 재택근무 여부, 디지털 미디어 사용 시간, 산업군

재택근무 여부, 디지털 미디어 사용 시간, 산업군별로 산업보안 피해 발생 시 가장 피해가 클 것이라 생각되는 산업 종류(다중응답)는 <표 12-2>과 같다.

재택근무 여부별로는 재택근무는 전기/전자(18.3%), 금융(15.4%), 자동차(13.6%) 순으로 많았고, 재택근무 아님은 전기/전자(17.0%), 통신업(13.9%), 금융(13.4%) 순으로 많았다.

디지털 미디어 사용 3시간 미만은 전기/전자(17.3%), 금융(13.5%), 통신업(13.5%) 순으로 많았고, 3-5시간은 전기/전자(20.8%), 금융(15.6%), 통신업(14.6%) 순으로 많았고, 5-7시간은 전기/전자(14.3%), 금융(12.4%), 통신업(11.2%) 순으로 많았고, 8시간 이상은 전기/전자(14.9%), 금융(13.8%), 화학(13.8%) 순으로 많았다.

산업군별로는 제조업은 전기/전자(13.3%), 자동차(13.32) 순으로 많았고, 정보통신은 전기/전자(18.5%), 금융(13.5%), 통신업(13.2%) 순으로 많았고, 기타는 전기/전자(18.6%), 금융(18.6%), 통신업(14.0%) 순으로 많았다.

<표 12-2> 산업보안 피해가 클 것이라 생각되는 산업 종류

N(%)

구분 (다중응답)	재택근무 여부		디지털 미디어 사용 시간				산업군		
	예	아니오	3시간 미만	3-5 시간	5-7 시간	8시간 이상	제조업	정보 통신	기타
건설	8(4.7)	22(5.2)	7(5.3)	8(3.8)	11(6.8)	4(4.6)	8(6.3)	17(4.5)	5(5.8)
화학	16(9.5)	43(10.1)	11(8.3)	22(10.4)	14(8.7)	12(13.8)	14(10.9)	37(9.8)	8(9.3)
전기/전자	31(18.3)	72(17.0)	23(17.3)	44(20.8)	23(14.3)	13(14.9)	17(13.3)	70(18.5)	16(18.6)
자동차	23(13.6)	47(11.1)	17(12.8)	25(11.8)	17(10.6)	11(12.6)	17(13.3)	42(11.1)	11(12.8)
금융	26(15.4)	57(13.4)	18(13.5)	33(15.6)	20(12.4)	12(13.8)	16(12.5)	51(13.5)	16(18.6)
의료	20(11.8)	41(9.7)	12(9.0)	23(10.8)	16(9.9)	10(11.5)	7(5.5)	46(12.1)	8(9.3)
교육	5(3.0)	14(3.3)	6(4.5)	4(1.9)	8(5.0)	1(1.1)	4(3.1)	14(3.7)	1(1.2)
화장품	4(2.4)	11(2.6)	4(3.0)	4(1.9)	5(3.1)	2(2.3)	5(3.9)	8(2.1)	2(2.3)
통신업	19(11.2)	59(13.9)	18(13.5)	31(14.6)	18(11.2)	11(12.6)	16(12.5)	50(13.2)	12(14.0)
철강업	7(4.1)	23(5.4)	4(3.0)	7(3.3)	14(8.7)	5(5.7)	10(7.8)	18(4.7)	2(2.3)
조선업	10(5.9)	35(8.3)	13(9.8)	11(5.2)	15(9.3)	6(6.9)	14(10.9)	26(6.9)	5(5.8)
전체	169(100.0)	424(100.0)	133(100.0)	212(100.0)	161(100.0)	87(100.0)	128(100.0)	379(100.0)	86(100.0)

※ 재택근무 여부, 디지털 미디어 사용 시간, 산업군

4) 산업보안 피해 발생 시 가장 피해가 클 것이라 생각되는 기업 규모

산업보안 피해 발생 시 가장 피해가 클 것이라 생각되는 기업 규모는 <표 12-3>와 같이 전체적으로는 대기업이 62.1%로 가장 많았고, 다음으로 중소기업(22.9%), 중견기업(11.4%) 순으로 많았다.

일반적 특성 중에서 재택근무 여부에서 통계적으로 유의한 차이가 있었다.

재택근무 여부별로는 재택근무(65.1%), 재택근무 아님(60.8%) 모두 대기업이 가장 많았으나, 중견기업의 경우에는 재택근무 아님(16.5%)이 재택근무(0.0%)보다 더 많았으며, 통계적으로 유의한 차이가 있었다($p<.05$).

<표 12-3> 산업보안 피해가 클 것이라 생각되는 기업 규모

N(%)

구분		대기업	중견 기업	중소 기업	자영 업자	기타	전체	χ^2/p
직급	평사원	36(64.3)	3(5.4)	14(25.0)	3(5.4)	0(0.0)	56(100.0)	7.368/ .498
	과장급	34(61.8)	8(14.5)	11(20.0)	1(1.8)	1(1.8)	55(100.0)	
	부장급 이상	17(58.6)	5(17.2)	7(24.1)	0(0.0)	0(0.0)	29(100.0)	
근무기간	1년 이하	3(30.0)	1(10.0)	6(60.0)	0(0.0)	0(0.0)	10(100.0)	21.871/ .147
	1-3년	14(56.0)	2(8.0)	7(28.0)	2(8.0)	0(0.0)	25(100.0)	
	4-6년	19(63.3)	5(16.7)	5(16.7)	1(3.3)	0(0.0)	30(100.0)	
	7-9년	16(72.7)	1(4.5)	3(13.6)	1(4.5)	1(4.5)	22(100.0)	
	10년 이상	35(66.0)	7(13.2)	11(20.8)	0(0.0)	0(0.0)	53(100.0)	
재택근무 여부	예	28(65.1)	0(0.0)	12(27.9)	3(7.0)	0(0.0)	43(100.0)	12.003/ .017*
	아니오	59(60.8)	16(16.5)	20(20.6)	1(1.0)	1(1.0)	97(100.0)	
디지털 미디어 사용 시간	3시간 미만	18(60.0)	2(6.7)	10(33.3)	0(0.0)	0(0.0)	30(100.0)	16.913/ .153
	3-5시간	38(65.5)	6(10.3)	12(20.7)	2(3.4)	0(0.0)	58(100.0)	
	5-7시간	19(59.4)	7(21.9)	4(12.5)	2(6.3)	0(0.0)	32(100.0)	
	8시간 이상	12(60.0)	1(5.0)	6(30.0)	0(0.0)	1(5.0)	20(100.0)	
산업군	제조업	16(69.6)	4(17.4)	3(13.0)	0(0.0)	0(0.0)	23(100.0)	8.142/ .420
	정보통신	60(61.9)	11(11.3)	23(23.7)	2(2.1)	1(1.0)	97(100.0)	
	기타	11(55.0)	1(5.0)	6(30.0)	2(10.0)	0(0.0)	20(100.0)	
전체		87(62.1)	16(11.4)	32(22.9)	4(2.9)	1(0.7)	140(100.0)	

*$p<.05$

5) 코로나19로 인한 보안의 중요성 증대에 대한 동의 정도

코로나19의 영향으로 일상의 비대면, 디지털화가 가속화되면서 이에 따른 산업보안의 중요성이 증대하고 있다는 것의 동의 정도는 <표 12-4>와 같이 전체적으로는 평균이 4.24점으로 '그렇다(4점)'과 '매우 그렇다(5점)' 사이로 매우 높은 것으로 나타났다.

직급, 근무기간, 재택근무 여부, 디지털 미디어 사용 시간, 산업군 모두에서 통계적으로 유의한 차이가 없었다.

<표 12-4> 코로나19로 인한 보안의 중요성 증대에 대한 동의 정도

구분		N	M[1)]	SD	*F*/*t*	*p*	Duncan
직급	평사원	56	4.13	0.69	2.421	.093	
	과장급	55	4.24	0.77			
	부장급 이상	29	4.48	0.63			
근무기간	1년 이하	10	4.30	0.48	1.673	.160	
	1-3년	25	4.20	0.76			
	4-6년	30	4.00	0.79			
	7-9년	22	4.50	0.67			
	10년 이상	53	4.28	0.69			
재택근무 여부	예	43	4.33	0.81	.907	.366	
	아니오	97	4.21	0.68			
디지털 미디어 사용 시간	3시간 미만	30	4.27	0.69	.232	.874	
	3-5시간	58	4.22	0.65			
	5-7시간	32	4.31	0.74			
	8시간 이상	20	4.15	0.93			
산업군	제조업	23	4.17	0.72	2.967	.055	
	정보통신	97	4.19	0.74			
	기타	20	4.60	0.50			
전체		140	4.24	0.72			

[1)] Likert 5점 척도: 1=전혀 그렇지 않다, 3=보통이다, 5=매우 그렇다

(3) 개인정보 유출 및 산업보안 사고

1) 개인정보의 침해 및 유출에 대한 직/간접 경험 여부

개인정보의 침해 및 유출에 대한 직/간접 경험 여부는 <표 13-1>과 같이 전체적으로는 경험 있음이 60.0%, 경험 없음이 40.0%로 경험 있음이 더 많은 것으로 나타났다.

일반적 특성 중에서 근무기간에서 통계적으로 유의한 차이가 있었다.

근무기간별로는 1년 이하(80.0%), 1-3년(56.0%), 7-9년(72.7%), 10년 이상(66.0%)은 경험 있음이 가장 많았고, 4-6년(63.3%)은 경험 없음이 가장 많았으며, 통계적으로 유의한 차이가 있었다($p<.05$).

<표 13-1> 개인정보의 침해 및 유출에 대한 직/간접 경험 여부

N(%)

구분		예	아니오	전체	χ^2/p
직급	평사원	33(58.9)	23(41.1)	56(100.0)	.079/ .962
	과장급	33(60.0)	22(40.0)	55(100.0)	
	부장급 이상	18(62.1)	11(37.9)	29(100.0)	
근무기간	1년 이하	8(80.0)	2(20.0)	10(100.0)	10.929/ .027*
	1-3년	14(56.0)	11(44.0)	25(100.0)	
	4-6년	11(36.7)	19(63.3)	30(100.0)	
	7-9년	16(72.7)	6(27.3)	22(100.0)	
	10년 이상	35(66.0)	18(34.0)	53(100.0)	
재택근무 여부	예	29(67.4)	14(32.6)	43(100.0)	1.432/ .231
	아니오	55(56.7)	42(43.3)	97(100.0)	
디지털 미디어 사용 시간	3시간 미만	14(46.7)	16(53.3)	30(100.0)	6.619/ .085
	3-5시간	32(55.2)	26(44.8)	58(100.0)	
	5-7시간	24(75.0)	8(25.0)	32(100.0)	
	8시간 이상	14(70.0)	6(30.0)	20(100.0)	
산업군	제조업	15(65.2)	8(34.8)	23(100.0)	.677/ .713
	정보통신	56(57.7)	41(42.3)	97(100.0)	
	기타	13(65.0)	7(35.0)	20(100.0)	
전체		84(60.0)	56(40.0)	140(100.0)	

*$p<.05$

2) 팬데믹과 산업의 디지털화에 따른 변화 정도

① 팬데믹과 산업의 디지털화에 따른 변화 정도

팬데믹과 산업의 디지털화에 따른 변화 정도는 <표 13-2>와 같다.

팬데믹과 산업의 디지털화에 따른 변화 정도는 디지털화로 복합적이고 고도화된 사이버 공격 증가(M=4.28)가 가장 높았고, 다음으로 산업의 디지털화로 인한 전문 인력의 유출과 산업스파이 증가(M=4.12), 비대면 일상생활로 인해 개인정보 유출 증가(M=4.00) 순으로 높았다.

<표 13-2> 팬데믹과 산업의 디지털화에 따른 변화 정도

영역	N	M[1)]	SD
비대면 일상생활로 인해 개인정보 유출 증가	140	4.00	0.71
재택근무로 인한 데이터 유출·해킹 피해 증가	140	3.89	0.82
디지털화로 복합적이고 고도화된 사이버 공격 증가	140	4.28	0.74
산업의 디지털화로 인한 전문 인력의 유출과 산업스파이 증가	140	4.12	0.75

[1)] Likert 5점 척도: 1=전혀 그렇지 않다, 3=보통이다, 5=매우 그렇다

② 직급에 따른 팬데믹과 산업의 디지털화에 따른 변화 정도

직급에 따른 팬데믹과 산업의 디지털화에 따른 변화 정도는 <표 13-3>과 같다.

팬데믹과 산업의 디지털화에 따른 변화 중에서 디지털화로 복합적이고 고도화된 사이버 공격 증가에서 통계적으로 유의한 차이가 있었다.

디지털화로 복합적이고 고도화된 사이버 공격 증가는 평사원(M=4.34), 과장급

(M=4.09), 부장급 이상(M=4.52)으로 통계적으로 유의한 차이가 있었고(p<.05), 사후검정인 Duncan test를 실시한 결과, 부장급 이상이 과장급보다 디지털화로 복합적이고 고도화된 사이버 공격이 더 증가할 것이라고 생각하는 것으로 나타났다.

<표 13-3> 직급에 따른 변화 정도

영역	구분	N	M	SD	*F*	*p*	Duncan
비대면 일상생활로 인해 개인정보 유출 증가	평사원	56	4.00	0.63	1.907	.152	
	과장급	55	3.89	0.81			
	부장급 이상	29	4.21	0.62			
재택근무로 인한 데이터 유출・해킹 피해 증가	평사원	56	3.86	0.77	.078	.925	
	과장급	55	3.89	0.85			
	부장급 이상	29	3.93	0.88			
디지털화로 복합적이고 고도화된 사이버 공격 증가	평사원(a)	56	4.34	0.64	3.594	.030*	b<c
	과장급(b)	55	4.09	0.82			
	부장급 이상(c)	29	4.52	0.69			
산업의 디지털화로 인한 전문 인력의 유출과 산업스파이 증가	평사원	56	4.09	0.67	.085	.919	
	과장급	55	4.15	0.87			
	부장급 이상	29	4.14	0.69			

*p<.05

③ 근무기간에 따른 팬데믹과 산업의 디지털화에 따른 변화 정도

근무기간에 따른 팬데믹과 산업의 디지털화에 따른 변화 정도는 <표 13-4>와 같다.

팬데믹과 산업의 디지털화에 따른 변화 모두에서 통계적으로 유의한 차이가 없었다.

<표 13-4> 근무기간에 따른 변화 정도

영역	구분	N	M	SD	*F*	*p*	Duncan
비대면 일상생활로 인해 개인정보 유출 증가	1년 이하	10	3.90	0.57	.247	.911	
	1-3년	25	3.92	0.86			
	4-6년	30	3.97	0.76			
	7-9년	22	4.05	0.65			
	10년 이상	53	4.06	0.66			
재택근무로 인한 데이터 유출・해킹 피해 증가	1년 이하	10	3.80	0.92	.468	.759	
	1-3년	25	3.76	0.83			
	4-6년	30	3.80	0.92			
	7-9년	22	4.00	0.62			
	10년 이상	53	3.96	0.83			
디지털화로 복합적이고 고도화된 사이버 공격 증가	1년 이하	10	4.30	0.48	1.093	.363	
	1-3년	25	4.08	0.91			
	4-6년	30	4.17	0.79			
	7-9년	22	4.32	0.65			
	10년 이상	53	4.42	0.69			
산업의 디지털화로 인한 전문 인력의 유출과 산업스파이 증가	1년 이하	10	4.30	0.67	.715	.583	
	1-3년	25	4.04	0.89			
	4-6년	30	4.00	0.83			
	7-9년	22	4.05	0.65			
	10년 이상	53	4.23	0.70			

④ 재택근무 여부 따른 팬데믹과 산업의 디지털화에 따른 변화 정도

재택근무 여부에 따른 팬데믹과 산업의 디지털화에 따른 변화 정도는 <표 13-5>와 같다.

팬데믹과 산업의 디지털화에 따른 변화 모두에서 통계적으로 유의한 차이가 없었다.

<표 13-5> 재택근무 여부에 따른 변화 정도

영역	구분	N	M	SD	t	p
비대면 일상생활로 인해 개인정보 유출 증가	예	43	4.07	0.86	.773	.441
	아니오	97	3.97	0.64		
재택근무로 인한 데이터 유출・해킹 피해 증가	예	43	3.93	0.88	.425	.672
	아니오	97	3.87	0.80		
디지털화로 복합적이고 고도화된 사이버 공격 증가	예	43	4.28	0.88	.005	.996
	아니오	97	4.28	0.67		
산업의 디지털화로 인한 전문 인력의 유출과 산업스파이 증가	예	43	4.19	0.79	.674	.501
	아니오	97	4.09	0.74		

⑤ 하루 평균 디지털 미디어 사용 시간에 따른 변화 정도

하루 평균 디지털 미디어 사용 시간에 따른 팬데믹과 산업의 디지털화에 따른 변화 정도는 <표 13-6>과 같다.

팬데믹과 산업의 디지털화에 따른 변화 모두에서 통계적으로 유의한 차이가 없었다.

<표 13-6> 하루 평균 디지털 미디어 사용 시간에 따른 변화 정도

영역	구분	N	M	SD	F	p	Duncan
비대면 일상생활로 인해 개인정보 유출 증가	3시간 미만	30	3.97	0.76	1.950	.125	
	3-5시간	58	3.86	0.71			
	5-7시간	32	4.13	0.61			
	8시간 이상	20	4.25	0.72			
재택근무로 인한 데이터 유출·해킹 피해 증가	3시간 미만	30	3.90	0.84	.869	.459	
	3-5시간	58	3.83	0.80			
	5-7시간	32	3.81	0.86			
	8시간 이상	20	4.15	0.81			
디지털화로 복합적이고 고도화된 사이버 공격 증가	3시간 미만	30	4.10	0.96	.816	.487	
	3-5시간	58	4.31	0.65			
	5-7시간	32	4.31	0.69			
	8시간 이상	20	4.40	0.68			
산업의 디지털화로 인한 전문 인력의 유출과 산업스파이 증가	3시간 미만	30	4.10	0.92	1.781	.154	
	3-5시간	58	3.98	0.71			
	5-7시간	32	4.22	0.71			
	8시간 이상	20	4.40	0.60			

⑥ 산업군에 따른 팬데믹과 산업의 디지털화에 따른 변화 정도

산업군에 따른 팬데믹과 산업의 디지털화에 따른 변화 정도는 <표 13-7>와 같다.

팬데믹과 산업의 디지털화에 따른 변화 모두에서 통계적으로 유의한 차이가 없었다.

<표 13-7> 산업군에 따른 변화 정도

영역	구분	N	M	SD	*F*	*p*	Duncan
비대면 일상생활로 인해 개인정보 유출 증가	제조업	23	3.83	0.72	.996	.372	
	정보통신	97	4.05	0.65			
	기타	20	3.95	0.94			
재택근무로 인한 데이터 유출・해킹 피해 증가	제조업	23	3.87	0.81	.007	.993	
	정보통신	97	3.89	0.78			
	기타	20	3.90	1.07			
디지털화로 복합적이고 고도화된 사이버 공격 증가	제조업	23	4.39	0.58	.386	.681	
	정보통신	97	4.27	0.77			
	기타	20	4.20	0.77			
산업의 디지털화로 인한 전문 인력의 유출과 산업스파이 증가	제조업	23	4.04	0.77	.416	.660	
	정보통신	97	4.11	0.75			
	기타	20	4.25	0.79			

3) 기업에서 산업보안 사고 발생 여부

기업에서 산업보안 사고 발생 여부는 <표 14>와 같이 전체적으로는 발생한 적이 있음이 21.4%, 발생한 적이 없음이 78.6%로 대체로 없는 것으로 나타났다.

일반적 특성 중에서 재택근무 여부에서 통계적으로 유의한 차이가 있었다.

재택근무 여부 별로는 재택근무는 발생한 적 있음(44.2%)과 발생한 적 없음(55.8%)이 비슷했고, 재택근무 아님은 발생한 적 없음(88.7%)이 가장 많았으며, 통계적으로 유의한 차이가 있었다($p<.001$).

<표 14> 기업에서 산업보안 사고 발생 여부

N(%)

구분		예	아니오	전체	χ^2/p
직급	평사원	8(14.3)	48(85.7)	56(100.0)	3.624/ .163
	과장급	16(29.1)	39(70.9)	55(100.0)	
	부장급 이상	6(20.7)	23(79.3)	29(100.0)	
근무기간	1년 이하	1(10.0)	9(90.0)	10(100.0)	7.555/ .109
	1-3년	2(8.0)	23(92.0)	25(100.0)	
	4-6년	5(16.7)	25(83.3)	30(100.0)	
	7-9년	8(36.4)	14(63.6)	22(100.0)	
	10년 이상	14(26.4)	39(73.6)	53(100.0)	
재택근무 여부	예	19(44.2)	24(55.8)	43(100.0)	19.090/ .000***
	아니오	11(11.3)	86(88.7)	97(100.0)	
디지털 미디어 사용 시간	3시간 미만	2(6.7)	28(93.3)	30(100.0)	4.954/ .175
	3-5시간	15(25.9)	43(74.1)	58(100.0)	
	5-7시간	8(25.0)	24(75.0)	32(100.0)	
	8시간 이상	5(25.0)	15(75.0)	20(100.0)	
산업군	제조업	2(8.7)	21(91.3)	23(100.0)	5.431/ .066
	정보통신	26(26.8)	71(73.2)	97(100.0)	
	기타	2(10.0)	18(90.0)	20(100.0)	
전체		30(21.4)	110(78.6)	140(100.0)	

***p<.001

4) 피해를 경험한 기업의 산업정보 피해 유형

피해를 경험한 기업의 산업정보 피해 유형(다중응답)은 <표 15>와 같이 데이터 유출・해킹과 바이러스・랜섬웨어 감염이 각각 28.8%로 가장 많았고, 다음으로 기술 인력 유출이 26.9%로 많았다

<표 15> 피해를 경험한 기업의 산업정보 피해 유형

구분(다중응답)	N	%
데이터 유출・해킹	15	28.8
바이러스・랜섬웨어 감염	15	28.8
핵심 시설물 피해	3	5.8
기술 인력 유출	14	26.9
영업비밀 침해	5	9.6
전체	52	100.0

5) 산업보안 사고가 기업의 경쟁력과 매출에 미치는 영향

산업보안 사고 발생 시 기업의 경쟁력과 매출에 미치는 영향은 <표 16>와 같이 전체적으로는 평균이 4.29점으로 '그렇다(4점)'과 '매우 그렇다(5점)' 사이로 매우 높은 것으로 나타났다.

직급, 근무기간, 재택근무 여부, 디지털 미디어 사용 시간, 산업군 모두에서 통계적으로 유의한 차이가 없었다.

<표 16> 산업보안 사고가 기업의 경쟁력과 매출에 미치는 영향

구분		N	M[1)]	SD	*F*/*t*	*p*	Duncan
직급	평사원	56	4.18	0.64	1.514	.224	
	과장급	55	4.31	0.81			
	부장급 이상	29	4.45	0.51			
근무기간	1년 이하	10	4.00	0.67	1.038	.390	
	1-3년	25	4.12	0.93			
	4-6년	30	4.37	0.72			
	7-9년	22	4.36	0.49			
	10년 이상	53	4.34	0.62			
재택근무 여부	예	43	4.19	0.82	-1.136	.258	
	아니오	97	4.33	0.62			
디지털 미디어 사용 시간	3시간 미만	30	4.17	0.83	1.152	.331	
	3-5시간	58	4.22	0.62			
	5-7시간	32	4.41	0.61			
	8시간 이상	20	4.45	0.76			
산업군	제조업	23	4.39	0.50	1.186	.309	
	정보통신	97	4.23	0.73			
	기타	20	4.45	0.69			
전체		140	4.29	0.69			

[1)] Likert 5점 척도: 1=전혀 그렇지 않다, 3=보통이다, 5=매우 그렇다

4. 산업보안의 대응

(1) 산업정보 피해 유형 중 보완대책 마련이 가장 시급한 것

산업정보 피해 유형 중 보완대책 마련이 가장 시급한 것은 <표 17>과 같이 전체적으로는 데이터 유출・해킹이 42.9%로 가장 많았고, 다음으로 바이러스・랜섬웨어 감염(23.6%), 기술 인력 유출(22.9%) 순으로 많았다.

직급, 근무기간, 재택근무 여부, 디지털 미디어 사용 시간, 산업군 모두에서 통계적으로 유의한 차이가 없었다.

<표 17> 산업정보 피해 유형 중 보완대책 마련이 가장 시급한 항목

N(%)

구분		데이터 유출・해킹	바이러스・랜섬웨어 감염	핵심 시설물 피해	기술 인력 유출	영업 비밀 침해	전체	χ^2/p
직급	평사원	24(42.9)	11(19.6)	4(7.1)	12(21.4)	5(8.9)	56(100.0)	5.347/.720
	과장급	23(41.8)	15(27.3)	3(5.5)	13(23.6)	1(1.8)	55(100.0)	
	부장급 이상	13(44.8)	7(24.1)	0(0.0)	7(24.1)	2(6.9)	29(100.0)	
근무기간	1년 이하	3(30.0)	2(20.0)	1(10.0)	3(30.0)	1(10.0)	10(100.0)	13.405/.643
	1-3년	12(48.0)	3(12.0)	3(12.0)	6(24.0)	1(4.0)	25(100.0)	
	4-6년	11(36.7)	8(26.7)	0(0.0)	8(26.7)	3(10.0)	30(100.0)	
	7-9년	13(59.1)	5(22.7)	0(0.0)	4(18.2)	0(0.0)	22(100.0)	
	10년 이상	21(39.6)	15(28.3)	3(5.7)	11(20.8)	3(5.7)	53(100.0)	
재택근무 여부	예	22(51.2)	13(30.2)	1(2.3)	7(16.3)	0(0.0)	43(100.0)	7.776/.100
	아니오	38(39.2)	20(20.6)	6(6.2)	25(25.8)	8(8.2)	97(100.0)	
디지털 미디어 사용 시간	3시간 미만	12(40.0)	5(16.7)	1(3.3)	8(26.7)	4(13.3)	30(100.0)	19.659/.074
	3-5시간	27(46.6)	13(22.4)	3(5.2)	13(22.4)	2(3.4)	58(100.0)	
	5-7시간	9(28.1)	12(37.5)	0(0.0)	9(28.1)	2(6.3)	32(100.0)	
	8시간 이상	12(60.0)	3(15.0)	3(15.0)	2(10.0)	0(0.0)	20(100.0)	
산업군	제조업	8(34.8)	4(17.4)	2(8.7)	7(30.4)	2(8.7)	23(100.0)	7.269/.508
	정보통신	41(42.3)	27(27.8)	5(5.2)	19(19.6)	5(5.2)	97(100.0)	
	기타	11(55.0)	2(10.0)	0(0.0)	6(30.0)	1(5.0)	20(100.0)	
전체		60(42.9)	33(23.6)	7(5.0)	32(22.9)	8(5.7)	140(100.0)	

(2) 우리 기업의 보안 조직구성 별도 운영 여부

우리 기업의 보안 조직구성 별도 운영 여부는 <표 18>과 같이 전체적으로는 별로도 운영하고 있음이 40.7%, 별도로 운영하고 있지 않음이 47.1%, 모름이 12.1%로 나타났다.

직급, 근무기간, 재택근무 여부, 디지털 미디어 사용 시간, 산업군 모두에서 통계적으로 유의한 차이가 있었다.

직급별로는 평사원(46.4%), 부장급 이상(55.2%)은 별도로 운영하고 있지 않음이 가장 많았고, 과장급(52.7%)은 별도로 운영하고 있음이 가장 많았으며, 통계적으로 유의한 차이가 있었다($p<.01$).

근무기간별로는 1년 이하는 별도로 운영하고 있음과 별도로 운영하고 있지 않음이 각각 40.0%로 가장 많았고, 1-3년(48.0%), 4-6년(56.7%)은 별도로 운영하고 있지 않음이 가장 많았고, 7-9년(59.1%)은 별도로 운영하고 있음이 가장 많았고, 10년 이상은 별도로 운영하고 있음과 별도로 운영하고 있지 않음이 각각 45.3%로 가장 많았으며, 통계적으로 유의한 차이가 있었다($p<.05$).

재택근무 여부별로는 재택근무(69.8%)는 별도로 운영하고 있음이 가장 많았고, 재택근무 아님(57.7%)은 별도로 운영하고 있지 않음이 가장 많았으며, 통계적으로 유의한 차이가 있었다($p<.001$).

디지털 미디어 사용 시간별로는 3시간 미만(50.0%), 8시간 이상(50.0%)은 별도로 운영하고 있지 않음이 가장 많았고, 3-5시간은 별도로 운영하고 있음과 별도로 운영하고 있지 않음이 각각 44.8%로 가장 많았고, 5-7시간(53.1%)은 별도로 운영하고 있음이 가장 많았으며, 통계적으로 유의한 차이가 있었다($p<.05$).

산업군별로는 제조업(69.6%), 기타(75.0%)는 별도로 운영하고 있지 않음이 가장 많았고, 정보통신(54.6%)은 별도로 운영하고 있음이 가장 많았으며, 통계적으로 유의한 차이가 있었다($p<.001$).

<표 18> 우리 기업의 보안 조직구성 별도 운영 여부

N(%)

구분		예	아니오	모름	전체	χ^2/p
직급	평사원	17(30.4)	26(46.4)	13(23.2)	56(100.0)	13.614/ .009**
	과장급	29(52.7)	24(43.6)	2(3.6)	55(100.0)	
	부장급 이상	11(37.9)	16(55.2)	2(6.9)	29(100.0)	
근무기간	1년 이하	4(40.0)	4(40.0)	2(20.0)	10(100.0)	18.122/ .020*
	1-3년	5(20.0)	12(48.0)	8(32.0)	25(100.0)	
	4-6년	11(36.7)	17(56.7)	2(6.7)	30(100.0)	
	7-9년	13(59.1)	9(40.9)	0(0.0)	22(100.0)	
	10년 이상	24(45.3)	24(45.3)	5(9.4)	53(100.0)	
재택근무 여부	예	30(69.8)	10(23.3)	3(7.0)	43(100.0)	21.742/ .000***
	아니오	27(27.8)	56(57.7)	14(14.4)	97(100.0)	
디지털 미디어 사용 시간	3시간 미만	7(23.3)	15(50.0)	8(26.7)	30(100.0)	13.377/ .037*
	3-5시간	26(44.8)	26(44.8)	6(10.3)	58(100.0)	
	5-7시간	17(53.1)	15(46.9)	0(0.0)	32(100.0)	
	8시간 이상	7(35.0)	10(50.0)	3(15.0)	20(100.0)	
산업군	제조업	1(4.3)	16(69.6)	6(26.1)	23(100.0)	28.015/ .000***
	정보통신	53(54.6)	35(36.1)	9(9.3)	97(100.0)	
	기타	3(15.0)	15(75.0)	2(10.0)	20(100.0)	
전체		57(40.7)	66(47.1)	17(12.1)	140(100.0)	

*p<.05, **p<.01, ***p<.001

(3) 우리 기업이 산업보안 피해 대응이 잘 되고 있는 정도

우리 기업이 산업보안 피해 대응이 잘 되고 있는 정도는 <표 19>과 같이 전체적으로는 평균이 2.97점으로 '보통이다(3점)' 정도로 나타났다.

재택근무 여부 별로는 재택근무(M=3.28)가 재택근무 아님(M=2.84)보다 우리 기업의 산업보안 피해 대응이 더 잘 되고 있다고 생각하였으며, 통계적으로 유의한 차이가 있었다(p<.01).

산업군별로는 제조업(M=2.65), 정보통신(M=3.16), 기타(M=2.40)로 통계적으로 유의한 차이가 있었고(p<.001), 사후검정인 Duncan test를 실시한 결과, 정보통신

이 제조업/기타보다 우리 기업의 산업보안 피해 대응이 더 잘 되고 있다고 생각하는 것으로 나타났다.

<표 19> 우리 기업이 산업보안 피해 대응이 잘 되고 있는 정도

구분		N	M[1)]	SD	*F*/*t*	*p*	Duncan
직급	평사원	56	2.95	0.98	.756	.472	
	과장급	55	3.07	0.74			
	부장급 이상	29	2.83	0.97			
근무기간	1년 이하	10	2.80	1.03	1.229	.302	
	1-3년	25	2.68	0.95			
	4-6년	30	2.93	0.87			
	7-9년	22	3.14	0.89			
	10년 이상	53	3.09	0.84			
재택근무 여부	예	43	3.28	0.77	2.792	.006**	
	아니오	97	2.84	0.91			
디지털 미디어 사용 시간	3시간 미만	30	2.93	1.01	.961	.413	
	3-5시간	58	3.09	0.84			
	5-7시간	32	2.97	0.93			
	8시간 이상	20	2.70	0.73			
산업군	제조업(a)	23	2.65	0.88	8.798	.000***	a, c<b
	정보통신(b)	97	3.16	0.81			
	기타(c)	20	2.40	0.94			
전체		140	2.97	0.89			

[1)] Likert 5점 척도: 1=전혀 그렇지 않다, 3=보통이다, 5=매우 그렇다

**p<.01, ***p<.001

(4) 귀 기업에서 평소 산업보안 관련 지침을 실천하는 정도

귀 기업에서 평소 산업보안 관련 지침을 실천하는 정도는 <표 20>과 같이 전체적으로는 관련 안내가 있으면 확인 후 실천이 45.0%로 가장 많았고, 다음으로 관련 안내가 있으면 일부 선택 실천이 36.4%로 많았다.

직급, 근무기간, 재택근무 여부, 디지털 미디어 사용 시간, 산업군 모두에서 통계적으로 유의한 차이가 없었다.

<표 20> 귀 기업에서 평소 산업보안 관련 지침을 실천하는 정도

N(%)

구분		전혀 안 함	상황에 따라 다르며, 안내가 있어도 무시	관련 안내가 있으면 일부 선택 실천	관련 안내가 있으면 확인 후 실천	스스로 항상 신경 쓰면서 적극 실천	전체	χ^2/p
직급	평사원	5(8.9)	2(3.6)	22(39.3)	22(39.3)	5(8.9)	56(100.0)	4.038/ .854
	과장급	1(1.8)	1(1.8)	20(36.4)	27(49.1)	6(10.9)	55(100.0)	
	부장급 이상	2(6.9)	1(3.4)	9(31.0)	14(48.3)	3(10.3)	29(100.0)	
근무기간	1년 이하	0(0.0)	0(0.0)	3(30.0)	6(60.0)	1(10.0)	10(100.0)	25.120/ .068
	1-3년	2(8.0)	0(0.0)	11(44.0)	11(44.0)	1(4.0)	25(100.0)	
	4-6년	1(3.3)	4(13.3)	13(43.3)	12(40.0)	0(0.0)	30(100.0)	
	7-9년	2(9.1)	0(0.0)	6(27.3)	10(45.5)	4(18.2)	22(100.0)	
	10년 이상	3(5.7)	0(0.0)	18(34.0)	24(45.3)	8(15.1)	53(100.0)	
재택근무 여부	예	1(2.3)	0(0.0)	12(27.9)	25(58.1)	5(11.6)	43(100.0)	6.803/ .147
	아니오	7(7.2)	4(4.1)	39(40.2)	38(39.2)	9(9.3)	97(100.0)	
디지털 미디어 사용 시간	3시간 미만	3(10.0)	1(3.3)	10(33.3)	13(43.3)	3(10.0)	30(100.0)	8.277/ .763
	3-5시간	3(5.2)	1(1.7)	23(39.7)	28(48.3)	3(5.2)	58(100.0)	
	5-7시간	1(3.1)	2(6.3)	9(28.1)	15(46.9)	5(15.6)	32(100.0)	
	8시간 이상	1(5.0)	0(0.0)	9(45.0)	7(35.0)	3(15.0)	20(100.0)	
산업군	제조업	2(8.7)	0(0.0)	10(43.5)	10(43.5)	1(4.3)	23(100.0)	9.690/ .287
	정보통신	4(4.1)	3(3.1)	32(33.0)	49(50.5)	9(9.3)	97(100.0)	
	기타	2(10.0)	1(5.0)	9(45.0)	4(20.0)	4(20.0)	20(100.0)	
전체		8(5.7)	4(2.9)	51(36.4)	63(45.0)	14(10.0)	140(100.0)	

(5) 중소기업이 가진 산업보안 활동의 애로사항

중소기업이 가진 산업보안 활동의 애로사항(다중응답)은 <표 21>과 같이 전체적으로는 전문 인력 부족(24.0%), 예산(22.2%), 전문적 보호기술 부재(21.0%) 순으로 많았다.

직급별로는 평사원(25.6%), 과장급(22.5%)은 전문 인력 부족이 가장 많았고, 부장급 이상(27.3%)은 예산이 가장 많았다.

근무기간별로는 1년 이하는 전문 인력 부족, 전문적 보호기술 부재, 예산이 각각 23.8%로 가장 많았고, 1-3년(23.5%)은 전문적 보호기술 부재가 가장 많았고, 4-6년(26.0%), 7-9년(22.2%), 10년 이상(24.6%)은 전문 인력 부족이 가장 많았다.

재택근무 여부별로는 재택근무(27.8%)는 전문 인력 부족이 가장 많았고, 재택근무 아님은 전문 인력 부족, 예산이 각각 22.5%로 가장 많았다.

디지털 미디어 사용 시간별로는 3시간 미만(26.6%)은 임직원의 관심 및 이해부족이 가장 많았고, 3-5시간(25.4%), 8시간 이상(24.6%)은 전문 인력 부족이 가장 많았고, 5-7시간(24.4%)은 예산이 가장 많았다.

산업군별로는 제조업(25.0%)은 전문적 보호기술 부재가 가장 많았고, 정보통신(25.5%)은 전문 인력 부족이 가장 많았고, 기타(26.4%)는 임직원의 관심 및 이해부족이 가장 많았다.

<표 21> 중소기업이 가진 산업보안 활동의 애로사항

N(%)

구분 (다중응답)		전문 인력 부족	전문적 보호기술 부재	예산	법적, 제도적 장치 미흡	임직원의 관심 및 이해부족	전체
직급	평사원	32(25.6)	27(21.6)	25(20.0)	18(14.4)	23(18.4)	125(100.0)
	과장급	32(22.5)	31(21.8)	31(21.8)	22(15.5)	26(18.3)	142(100.0)
	부장급 이상	16(24.2)	12(18.2)	18(27.3)	8(12.1)	12(18.2)	66(100.0)
근무기간	1년 이하	5(23.8)	5(23.8)	5(23.8)	3(14.3)	3(14.3)	21(100.0)
	1-3년	11(21.6)	12(23.5)	11(21.6)	7(13.7)	10(19.6)	51(100.0)
	4-6년	19(26.0)	15(20.5)	17(23.3)	11(15.1)	11(15.1)	73(100.0)
	7-9년	12(22.2)	10(18.5)	10(18.5)	11(20.4)	11(20.4)	54(100.0)
	10년 이상	33(24.6)	28(20.9)	31(23.1)	16(11.9)	26(19.4)	134(100.0)
재택근무 여부	예	27(27.8)	19(19.6)	21(21.6)	15(15.5)	15(15.5)	97(100.0)
	아니오	53(22.5)	51(21.6)	53(22.5)	33(14.0)	46(19.5)	236(100.0)
디지털 미디어 사용 시간	3시간 미만	14(21.9)	14(21.9)	11(17.2)	8(12.5)	17(26.6)	64(100.0)
	3-5시간	33(25.4)	28(21.5)	32(24.6)	20(15.4)	17(13.1)	130(100.0)
	5-7시간	19(23.2)	15(18.3)	20(24.4)	13(15.9)	15(18.3)	82(100.0)
	8시간 이상	14(24.6)	13(22.8)	11(19.3)	7(12.3)	12(21.1)	57(100.0)
산업군	제조업	14(21.9)	16(25.0)	13(20.3)	8(12.5)	13(20.3)	64(100.0)
	정보통신	55(25.5)	43(19.9)	49(22.7)	35(16.2)	34(15.7)	216(100.0)
	기타	11(20.8)	11(20.8)	12(22.6)	5(9.4)	14(26.4)	53(100.0)
전체		80(24.0)	70(21.0)	74(22.2)	48(14.4)	61(18.3)	333(100.0)

5. 산업보안 교육 이수 및 보안의식

(1) 산업보안 교육 이수 경험

산업보안 교육 이수 경험은 <표 22>와 같이 전체적으로는 있음이 57.1%, 없음이 42.9%로 나타났다.

일반적 특성 중에서 재택근무 여부, 산업군에서 통계적으로 유의한 차이가 있었다.

재택근무 여부 별로는 재택근무(79.1%)는 경험 있음이 가장 많았고, 재택근무 아님(52.6%)은 경험 없음이 가장 많았으며, 통계적으로 유의한 차이가 있었다 ($p<.001$).

산업군별로는 제조업(73.9%), 기타(60.0%)는 경험 없음이 가장 많았고, 정보통신(68.0%)은 경험 있음이 가장 많았으며, 통계적으로 유의한 차이가 있었다 ($p<.001$).

<표 22> 산업보안 교육 이수 경험

N(%)

구분		예	아니오	전체	χ^2/p
직급	평사원	31(55.4)	25(44.6)	56(100.0)	3.420/ .181
	과장급	36(65.5)	19(34.5)	55(100.0)	
	부장급 이상	13(44.8)	16(55.2)	29(100.0)	
근무기간	1년 이하	4(40.0)	6(60.0)	10(100.0)	2.745/ .601
	1-3년	13(52.0)	12(48.0)	25(100.0)	
	4-6년	16(53.3)	14(46.7)	30(100.0)	
	7-9년	13(59.1)	9(40.9)	22(100.0)	
	10년 이상	34(64.2)	19(35.8)	53(100.0)	
재택근무 여부	예	34(79.1)	9(20.9)	43(100.0)	12.184/ .000***
	아니오	46(47.4)	51(52.6)	97(100.0)	
디지털 미디어 사용 시간	3시간 미만	13(43.3)	17(56.7)	30(100.0)	3.267/ .352
	3-5시간	34(58.6)	24(41.4)	58(100.0)	
	5-7시간	20(62.5)	12(37.5)	32(100.0)	
	8시간 이상	13(65.0)	7(35.0)	20(100.0)	
산업군	제조업	6(26.1)	17(73.9)	23(100.0)	16.162/ .000***
	정보통신	66(68.0)	31(32.0)	97(100.0)	
	기타	8(40.0)	12(60.0)	20(100.0)	
전체		80(57.1)	60(42.9)	140(100.0)	

*** $p<.001$

(2) 산업보안 교육을 받은 방식

산업보안 교육을 받은 방식은 <표 23>와 같이 사이버 교육이 41명(51.3%)으로 가장 많았고, 다음으로 자체 교육 18명(22.5%), 외부 전문 기관 위탁 교육 17명(21.3%) 순으로 많았다.

<표 23> 산업보안 교육을 받은 방식

구분	N	%
사이버 교육	41	51.3
자체 교육	18	22.5
외부 전문 기관 위탁 교육	17	21.3
현장 교육	4	5.0
전체	80	100.0

(3) 우리 기업에서의 산업보안 교육 의무 여부

우리 기업에서의 산업보안 교육 의무 여부는 <표 24>와 같이 전체적으로는 의무적으로 받아야 함이 66.4%, 그렇지 않음이 33.6%로 나타났다.

일반적 특성 중에서 산업군에서 통계적으로 유의한 차이가 있었다.

산업군별로는 제조업(60.9%)은 의무적으로 받지 않음이 가장 많았고, 정보통신(74.2%), 기타(60.0%)는 의무적으로 받아야 함이 가장 많았으며, 통계적으로 유의한 차이가 있었다($p<.01$).

<표 24> 우리 기업에서의 산업보안 교육 의무 여부

N(%)

구분		예	아니오	전체	χ^2/p
직급	평사원	35(62.5)	21(37.5)	56(100.0)	.871/ .647
	과장급	37(67.3)	18(32.7)	55(100.0)	
	부장급 이상	21(72.4)	8(27.6)	29(100.0)	
근무기간	1년 이하	4(40.0)	6(60.0)	10(100.0)	6.912/ .141
	1-3년	14(56.0)	11(44.0)	25(100.0)	
	4-6년	24(80.0)	6(20.0)	30(100.0)	
	7-9년	15(68.2)	7(31.8)	22(100.0)	
	10년 이상	36(67.9)	17(32.1)	53(100.0)	
재택근무 여부	예	31(72.1)	12(27.9)	43(100.0)	.893/ .345
	아니오	62(63.9)	35(36.1)	97(100.0)	
디지털 미디어 사용 시간	3시간 미만	16(53.3)	14(46.7)	30(100.0)	3.014/ .389
	3-5시간	40(69.0)	18(31.0)	58(100.0)	
	5-7시간	23(71.9)	9(28.1)	32(100.0)	
	8시간 이상	14(70.0)	6(30.0)	20(100.0)	
산업군	제조업	9(39.1)	14(60.9)	23(100.0)	10.701/ .005**
	정보통신	72(74.2)	25(25.8)	97(100.0)	
	기타	12(60.0)	8(40.0)	20(100.0)	
전체		93(66.4)	47(33.6)	140(100.0)	

** $p<.01$

(4) 우리 기업이 보안 교육을 주기적으로 시행하는 정도

우리 기업이 산업보안과 관련된 보안 교육을 주기적으로 시행하는 정도는 <표 25>와 같이 전체적으로는 평균이 3.09점으로 '보통이다(3점)' 정도로 나타났다.

재택근무 여부 별로는 재택근무(M=3.53)가 재택근무 아님(M=2.89)보다 산업보안과 관련된 보안 교육을 더 주기적으로 시행한다고 하였으며, 통계적으로 유의한 차이가 있었다(p<.01).

산업군별로는 제조업(M=2.30), 정보통신(M=3.41), 기타(M=2.40)로 통계적으로

유의한 차이가 있었고(p<.001), 사후검정인 Duncan test를 실시한 결과, 정보통신이 제조업/기타보다 산업보안과 관련된 보안 교육을 더 주기적으로 시행한다고 하였다.

<표 25> 우리 기업이 보안 교육을 주기적으로 시행하는 정도

구분		N	M[1)]	SD	*F/t*	*p*	Duncan
직급	평사원	56	2.88	1.11	1.995	.140	
	과장급	55	3.25	0.95			
	부장급 이상	29	3.17	1.04			
근무기간	1년 이하	10	2.40	0.97	1.852	.122	
	1-3년	25	2.84	1.03			
	4-6년	30	3.23	0.94			
	7-9년	22	3.18	1.01			
	10년 이상	53	3.21	1.10			
재택근무 여부	예	43	3.53	0.98	3.533	.001**	
	아니오	97	2.89	1.01			
디지털 미디어 사용 시간	3시간 미만	30	2.87	1.11	.860	.464	
	3-5시간	58	3.17	1.06			
	5-7시간	32	3.22	0.83			
	8시간 이상	20	2.95	1.19			
산업군	제조업(a)	23	2.30	0.88	19.757	.000***	a, c<b
	정보통신(b)	97	3.41	0.88			
	기타(c)	20	2.40	1.19			
전체		140	3.09	1.04			

[1)] Likert 5점 척도: 1=전혀 그렇지 않다, 3=보통이다, 5=매우 그렇다
**p<.01, ***p<.001

(5) 본인의 평상시 산업보안 관리 정도

본인이 평상시 산업보안에 관심을 가지고 보안 관리를 잘하고 있다고 생각하는 정도는 <표 26>와 같이 전체적으로는 평균이 3.21점으로 '보통이다(3점)'보다 조금 높은 것으로 나타났다.

재택근무 여부 별로는 재택근무(M=3.49)가 재택근무 아님(M=3.08)보다 평상시 산업보안에 관심을 가지고 보안 관리를 더 잘하고 있다고 생각하였으며, 통

계적으로 유의한 차이가 있었다(p<.05).

산업군별로는 제조업(M=2.70), 정보통신(M=3.45), 기타(M=2.60)로 통계적으로 유의한 차이가 있었고(p<.001), 사후검정인 Duncan test를 실시한 결과, 정보통신이 제조업/기타보다 평상시 산업보안에 관심을 가지고 보안 관리를 더 잘하고 있다고 생각하는 것으로 나타났다.

<표 26> 본인의 평상시 산업보안 관리 정도

구분		N	M[1)]	SD	*F/t*	*p*	Duncan
직급	평사원	56	3.07	0.99	3.030	.052	
	과장급	55	3.44	0.76			
	부장급 이상	29	3.03	0.91			
근무기간	1년 이하	10	2.90	0.88	.942	.442	
	1-3년	25	3.12	0.93			
	4-6년	30	3.17	0.79			
	7-9년	22	3.50	0.96			
	10년 이상	53	3.21	0.93			
재택근무 여부	예	43	3.49	0.88	2.503	.013*	
	아니오	97	3.08	0.89			
디지털 미디어 사용 시간	3시간 미만	30	3.00	0.98	.860	.464	
	3-5시간	58	3.26	0.93			
	5-7시간	32	3.34	0.87			
	8시간 이상	20	3.15	0.75			
산업군	제조업(a)	23	2.70	0.82	14.095	.000***	a, c<b
	정보통신(b)	97	3.45	0.74			
	기타(c)	20	2.60	1.19			
전체		140	3.21	0.90			

[1)] Likert 5점 척도: 1=전혀 그렇지 않다, 3=보통이다, 5=매우 그렇다

*p<.05, ***p<.001

(6) 귀 기업에서 산업보안 관련 직무(겸직) 여부

귀 기업에서 산업보안 관련 직무(겸직) 여부는 <표 27>과 같이 전체적으로는 직무(겸직)를 하고 있음은 25.0%, 하고 있지 않음은 75.0%로 대체로 하고 있지 않은 것으로 나타났다.

일반적 특성 중에서 재택근무 여부, 산업군에서 통계적으로 유의한 차이가 있었다.

재택근무 여부 별로는 재택근무는 직무(겸직)를 하고 있음(41.9%)과 하고 있지 않음(58.1%)이 비슷했고, 재택근무 아님(82.5%)은 하고 있지 않음이 가장 많았으며, 통계적으로 유의한 차이가 있었다($p<.01$).

산업군별로는 직무(겸직)를 하고 있음의 경우 정보통신(30.9%)이 제조업(8.7%), 기타(15.0%)보다 더 많았으며, 통계적으로 유의한 차이가 있었다($p<.05$).

<표 27> 귀 기업에서 산업보안 관련 직무(겸직) 여부

N(%)

구분		예	아니오	전체	χ^2/p
직급	평사원	11(19.6)	45(80.4)	56(100.0)	1.452/ .484
	과장급	16(29.1)	39(70.9)	55(100.0)	
	부장급 이상	8(27.6)	21(72.4)	29(100.0)	
근무기간	1년 이하	1(10.0)	9(90.0)	10(100.0)	4.148/ .386
	1-3년	6(24.0)	19(76.0)	25(100.0)	
	4-6년	10(33.3)	20(66.7)	30(100.0)	
	7-9년	3(13.6)	19(86.4)	22(100.0)	
	10년 이상	15(28.3)	38(71.7)	53(100.0)	
재택근무 여부	예	18(41.9)	25(58.1)	43(100.0)	9.409/ .002**
	아니오	17(17.5)	80(82.5)	97(100.0)	
디지털 미디어 사용 시간	3시간 미만	6(20.0)	24(80.0)	30(100.0)	2.190/ .534
	3-5시간	14(24.1)	44(75.9)	58(100.0)	
	5-7시간	11(34.4)	21(65.6)	32(100.0)	
	8시간 이상	4(20.0)	16(80.0)	20(100.0)	
산업군	제조업	2(8.7)	21(91.3)	23(100.0)	6.145/ .046*
	정보통신	30(30.9)	67(69.1)	97(100.0)	
	기타	3(15.0)	17(85.0)	20(100.0)	
전체		35(25.0)	105(75.0)	140(100.0)	

*$p<.05$, **$p<.01$

제3절 보안 개선방안

상기 결과를 종합하면, 차후 포스트 코로나 시대 디지털 가속화에 따라 산업보안 피해는 더욱 증가할 것을 예상할 수 있다. 비대면이 더욱 강화되는 이 시대에 있어서 팬데믹과 산업 디지털에 따른 변화 정도에 있어서 복합적이고 고도화된 사이버 공격 증가를 가장 많이 예상한 것이 이를 증명하고 있다. 또한, 차후 산업보안 사고가 발생하면 중소기업 경쟁력과 매출에 큰 영향을 미침을 알 수 있는데, 산업보안 사고 발생 시 기업경쟁력과 매출에 미치는 영향 인식 결과는 평균 4.29점으로 매우 높음이 확인되었다.

또한, 이러한 보안인식은 직책이 높을수록 그 중요성과 심각성을 더 강하게 인식함을 확인했고, 이러한 높은 인식에도 불구하고, 기업에서 평소 산업보안 관련 지침을 실천하는 정도의 경우, 안내가 있어야 수동적으로 실천하는 경우가 약 80% 가까이 되어, 현재 능동적, 자발적으로 산업보안 규정 준수를 이행하지 못하고 있음을 확인했다. 이러한 결과를 토대로, 차후 포스트 코로나 시대에 중소기업 산업보안 강화를 위한 개선방안을 제시하면 다음과 같다.

1. 관리적 보안

비록 산업보안에 대한 인식은 높으나 이를 적극 실천하지 못하고 있고, 직책이 높을수록 산업보안 인식, 중요성 자각 정도가 더 강하여, 전반적인 실무를 담당하는 평사원의 산업보안 인식이 매우 저조함을 확인했다. 따라서 차후 중소기업에서는 차후 포스트 코로나 시대에 예상되는 복합적이고 고도화된 사이버 공격의 개념, 유형, 대응방법에 대한 기업차원 매뉴얼을 구축하여 이를 배포하고, 정기적인 교육을 의무화함으로써, 산업보안 피해에 가장 약한 실무담당의 평사원 대상으로 보안의식과 대응 역량을 증대해야 한다.

또한, 산업보안 교육 이수 경험 분석 결과, 교육 경험이 있음이 과반수를 넘음에도 불구하고, 교육 방식은 현장에서 생생한 실제 환경에 기반한 실습 위주의 교육이 아닌 사이버 교육 형태가 51.3%로 가장 높았다. 따라서 차후 중소기업은 온라인 교육과 함께 오프라인 교육을 적합하게 접목하여 각 사원들의 보안

역량을 증대하기 위한 보안 대응 실습에 중점을 두고 보안교육을 전개할 필요가 있다.

또한, 산업보안 겸직 여부 분석결과, 겸직을 하고 있지 않음이 75%로 높은 비중을 보였다. 따라서 상기 교육 과정에서 각 직무 특성에 적합한 보안 대응 교육을 맞춤화하여 제공하고, 이를 직무분야에 포함시켜 각 부서의 직원들이 그들 직무를 안전한 환경에서 전개할 수 있도록 해야 할 것이다.

2. 기술적 보안

차후 포스트 코로나 시대에 가장 높게 예상되는 산업 보안 공격 형태는 복합적이고 고도화된 사이버 공격임을 확인했다. 또한, 산업보안 피해 유형 분석 결과, 데이터 유출과 해킹, 바이러스, 랜섬웨어 감염 비중이 가장 높았다. 따라서 조직원 관리와 교육에 따른 보안 역량 강화로 대응함도 중요하지만, 1차적으로 이러한 공격에 대응할 수 있는 중소기업의 기술적 보완이 선행되어야 한다. 따라서 차후 중소기업은 현재 가장 문제시되는 데이터 유출과 해킹, 바이러스, 랜섬웨어 차단을 위한 네트워킹 보안에 역점을 두고 보안 프로그램을 구축하되, 차후 이러한 공격 형태가 더욱 고도화되고 복합적인 형태로 진화할 것을 감안하여, 지금까지 검증된 바이러스, 랜섬웨어는 물론 차후 개발될 수 있는 유형들을 정확하게 추정하여 더욱 견고한 예방용 보안 프로그램을 구성할 필요가 있다.

또한, 각 부서에 따른 직무의 성격과 형태가 상이함을 감안하여 각 부서 특성에 맞춤화된 보안 프로그램을 구성해야 한다. 한 예로, 마케팅 부서의 경우 외부 거래처와 네트워킹 작업 등이 더 활발할 것이 예상되므로, 이 부서에서는 특히 네트워킹 보안에 상대적 비중을 두고 프로그램을 선별적으로 구성한다면 그 높은 보안 효과를 기대할 수 있다.

3. 물리적 보안

비록 본 연구에서 물리적 보안에 대한 직접적인 통계 결과는 없으나, 물리적

보안이란, 물리적으로 발생이 가능한 위협으로부터 조직의 자산을 보호하기 위해 의지와 욕구를 실체화 해 유지하는 것을 말하며 사람이나 시설물 또는 정보 보호를 위해 물리적, 시스템적인 통제방법으로 취약성과 리스크를 분석하여 허가 받지 않은 인원 및 차량을 통제하고 무단 침입 및 화재감지, 주요 인원, 자산의 보호 등에 대한 대응을 의미하므로, 상기에서 제시한 기업 보안프로그램을 구축하는 연구실이나 부서에 갖는 자산을 절도, 파괴 등 물리적 위협으로 보호해야 함은 1차적으로 전제되어야 할 핵심적 사안임이 자명하다.

따라서, 각 중소기업 업체는 그들의 보안체계를 구성함에 있어 수반되는 연구실, 보안부서에 대한 엄격한 물리적 보안이 필요하며, 기술인력 유출 비중도 상대적으로 높음을 감안할 때, 각 연구소에서 근무하는 기술인력에 대한 예방적 보안도 필요하다.

이를 위하여, 중소기업은 상황별 통제 매뉴얼을 구축하고 보안대책을 수립한다. 먼저 기술인력들에 대한 보안교육, 윤리 교육을 정기적으로 진행하고, 계약사항에 별첨을 마련하여 이들로 인한 기술이 유출될 경우 피해보상 등 규정을 엄격하게 신설하여 물리적 보안을 견고하게 구성할 필요가 있다. 또한, 연구소와 기업의 중요시설은 보호구역으로 정의하고, 권한이 없는 자의 접근을 통제한다. 그리고 주요 시스템에 별도의 접근 권한을 부여하고 이중의 보안 장치를 설치하여 물리적, 환경적 위협이 없도록 철저한 관리가 필요하다.

3. 인적 보안

차후 포스트 코로나 시대에 예상되는 디지털화에 따른 변화에 있어, 전문인력 유출이 2번째로 비중이 높았으며, 실제 발생한 보안사고 유형 분석 결과도 기술인력 유출은 2번째로 높았다. 따라서 중소기업이 상기 관리적, 기술적, 물리적 보안을 성공적으로 성취하기 위해선 이러한 보안을 담당하는 기술인력에 대한 효과적인 관리가 필요하다. 또한 외부 인력에 대해서도 자체적인 매뉴얼을 구축하여 지속적이고 철저한 보안 관리가 필요하다.

외부 인력 보안에 대한 방안은 <표 28>과 같다.

<표 28> 외부 인력 보안 방안

항목	내용
신원 확인 및 보안서약서 징구	◦ 외부 인력을 활용하여 업무를 수행할 경우 반드시 신원 확인을 거쳐야 하고 보안서약서를 징구하고 이를 준수하도록 해야 한다.
정보시스템에 대한 접근권한 제한	◦ 정보시스템에 접근하는 경우 외부 인력에게 할당된 별도의 계정을 부여하여 사용토록 하고 계정별 접근권한을 부여하여 제한한다. ◦ 정보보안 담당관은 외부 인력의 정보시스템 접근기록 등 작업이력을 자료관리 대장을 기록 및 관리 하며 주기적으로 보관 실태를 확인 한다.
보안 위해물품 소지여부 점검	◦ 정보보안담당관은 외부 인력의 출입 시 보안 위해물품 소지여부를 점검하여야 한다. ◦ 무작위 점검을 실시하거나 점검 도구를 도입하고 자동 소거가 가능한 시스템을 활용할 수 있다.
담당자 입회	◦ 외부 인력은 정보보안 담당관의 입회하에 정해진 장소와 지정된 단말기에서 정보시스템을 사용하도록 통제해야 한다.

상기 표와 같이 기술 인력의 보안 기술과 정보에 대한 접근 권한을 제한하고, 이들의 물품 소지 여부를 수시로 점검하며, 이들에게 맞춤화된 보안 서약서 작성 등의 대안도 중요하지만, 기술 인력이 자사에 애사심을 가지고 몰입함으로써 자발적, 능동적으로 조직 발전을 위해 보안을 철저하게 준수하는 태도가 선행되어야 함은 자명하다. 상기 표에서 제시된 비교적 강압적 방법은 조직지원인식을 저하할 우려가 있으므로, 기술 인력에 대한 처우를 보장하고, 이들의 성과에 따른 상대적 인센티브 지급, 성과에 따른 정당한 승진 기회 등을 명확하게 함께 제공함과 동시에 상기 표에서 제시된 방법을 상호 협의하에 구성원 설득을 전제로 진행한다면 기술 인력 유출의 가능성을 최소화함에 일조할 수 있을 것이다.

제4장 결론

제1절 연구의 요약

최근 코로나19 영향으로 온라인 경제화가 가속화되면서, 기업 정보보안 위험은 더욱 증대하였고, 특히 국내 기업이 경험한 침해사고 건수는 2019년 39건에서 2020년 127건으로 증가했는데, 이 중 79건에 해당하는 81%가 중소기업임이 규명되어 이들이 정보보호 사각지대에 고스란히 노출되어 있음을 확인했다. 차후 포스트 코로나 시대에는 기존 대기업 위주 성장에서 혁신벤처 기업들 중요성이 강조되어 중소기업 중심 성장이 예견되어 이들 기업의 산업보호 개선방안이 절실한 시점인바, 본 연구는 국내 중소기업 직원들 200명 대상으로 온라인상에서 설문 작업을 진행, 실태조사를 함으로써 포스트 코로나 시대 중소기업 정보보호 개선방안을 제시하고자 했다. 이러한 연구목적을 위해, 선행연구를 검토하여 국내의 산업보안 개념에 따른 구분은 데이터 유출, 해킹, 랜섬웨어, 바이러스 감염, 핵심 시설물 피해, 기술인력 유출, 영업비밀 유출 등으로 상정하여 기술적, 물리적 차원임을 확인했으나, 이러한 개념정리는 너무 협소하여 지나친 일반화의 오류를 범함이 확인되어 미국 사례를 참고하여 개선방안을 제시함에 있어 산업보안 개념을 정책적, 기술적, 물리적, 경영 전략기획 보안 차원으로 확장해야 함을 확인했다.

온라인상에서 실태조사 분석을 실시했고, SPSS 27.0 프로그램을 통해 분석하여, 산업보안 인식도, 산업보안 중요성, 개인정보 유출 및 산업보안 사고, 산업보안 대응, 산업보안 교육이수 및 보안의식 차이를 분석했다. 연구결과를 요약하면 다음과 같다.

산업보안 내 세부영역 인지도는 평균이 3.79~3.99로 모두 약간 알고 있었고, 영역별로는 전문 정보보안의 의미(M=3.99)에 대한 인지도가 가장 높았고, 다음으로 산업기술보호의 의미(M=3.95), 전문 기술인력 유출의 의미(M=3.94), 영업비밀 유출 및 산업스파이의 의미(M=3.92) 순으로 높았다. 또한, 강민기, 박찬수(2020) 연구에서 산업보안 이슈 인식 조사를 검토한 결과, 산업기술을 갖춘 기업 구성원들의 인식 경우, 내부자에 의한 유출, 스마트 제조환경과 네트워크 보

안 등이 가장 높음을 확인하여, 전문보안과 산업기술보호를 인지함에 있어 이를 위협하는 가장 큰 요인에 대한 인식은 곧 내부자 유출과 스마트 제조환경에 따른 네트워킹임을 확인했다. 또한, 이러한 산업보안에 대한 인지도는 직급이 높을수록 인지도가 더 큼을 확인했다. 더 나아가, 재택근무를 하는 구성원이 그렇지 않은 구성원보다 정보보안 의미를 더 높게 인식하였고, 하루 평균 디지털 미디어를 사용하는 시간이 길수록 정보보안 의미를 더 높게 인식했다. 산업군에 따른 인지도를 분석한 결과, 정보보안 의미 등 전반적 인식은 제조업, 정보통신업 등이 상대적으로 높은 인지도를 보였다.

평소 산업보안에 대한 필요성을 느끼는 시기는 전체적으로는 항상 중요하게 생각함이 54.3%로 가장 많았고, 다음으로 커뮤니티, 매체, 지인을 통해 간접 경험(33.6%), 직접 피해를 겪은 후(10.7%) 순으로 많았다. 하지만, 직급, 근무기간, 재택근무 여부, 디지털 이용 시간, 산업군에 따른 유의한 차이는 없었다.

한편, 기업 내 임직원들이 산업보안에 관심을 갖지 않도록 하는 이유의 경우, 조치를 하기 위해 많은 비용이 발생한다는 생각이 26.8%로 가장 많았고, 다음으로 보안 조치를 하기가 귀찮고 불편(24.9%), 나와 상관없는 일이라고 생각(21.9%) 순으로 많았다.

또한, 산업보안 중요성을 분석한 결과, 산업보안 영역에 대한 중요도는 평균이 4.19~4.61로 모두 매우 높은 것으로 나타났고, 영역별로는 정보 자산에 대한 보안(M=4.61)이 중요도가 가장 높았고, 다음으로 인적 자산에 대한 보안(M=4.32), 설비・시설 자산에 대한 보안(M=4.19) 순으로 높았다. 산업보안 영역 중요도에서 있어 직급, 근무기간, 재택근무 여부, 하루 평균 디지털 미디어 이용 시간, 산업군 등에 따른 유의한 차이는 없었다.

한편, 산업보안을 구성원 모두가 심각성을 인지하고 실천하는 것의 중요도 경우, 전체적으로는 평균이 4.36점으로 '그렇다(4점)'과 '매우 그렇다(5점)' 사이로 매우 높은 것이 규명되었고, 직급이 높을수록, 제조업, 정보통신업인 경우 더 인식도가 높았다.

산업보안 피해 발생 시 가장 피해가 클 것이라고 생산되는 산업군을 분석한 결과, 전기/전자가 17.4%로 가장 많았고, 다음으로 금융(14.0%), 통신업(13.2%) 순이었고, 산업보안 피해 발생 시 가장 피해가 클 것이라고 생각되는 기업 규모는 대기업이 62.1%로 가장 많았고, 다음으로 중소기업(22.9%), 중견기업(11.4%) 순임이 규명되었다.

한편, 코로나19 영향으로 일상 비대면, 디지털화 가속으로 이에 따른 산업보안 중요성이 증대함에 동의하는 정도의 경우, 전체적으로는 평균이 4.24점으로 '그렇다(4점)'와 '매우 그렇다(5점)' 사이로 매우 높은 것이 밝혀졌으나, 직급, 근무기간, 재택근무 여부, 디지털 이용시간, 산업군에 따른 유의한 차이는 없었다.
개인정보 침해 및 유출에 대한 직, 간접적 경험 여부 분석 결과, 경험 있음이 60.0%, 경험 없음이 40.0%로 경험 있음이 더 많은 것으로 나타났고, 1년 이하의 근무기간 집단이 가장 높았다.

팬데믹과 산업의 디지털화에 따른 변화 정도에 있어서, 복합적이고 고도화된 사이버 공격 증가(M=4.28)가 가장 높았고, 다음으로 산업의 디지털화로 인한 전문 인력의 유출과 산업스파이 증가(M=4.12), 비대면 일상생활로 인해 개인정보 유출 증가(M=4.00) 순으로 규명되었고, 직급이 높아질수록 복합적이고 고도화된 사이버 공격 증가 비중이 더 높았다.

또한, 기업에서 산업보안 사고 발생 여부에 있어 발생한 적이 있음이 21.4%, 발생한 적이 없음이 78.6%로 대체로 없는 것으로 밝혀졌고, 재택근무를 할수록 더 높은 발생한 적 있음이 큰 비중을 가지는 것을 확인했다. 또한, 산업정보 피해 유형은 데이터 유출・해킹과 바이러스・랜섬웨어 감염이 각각 28.8%로 가장 많았고, 다음으로 기술 인력 유출이 26.9%로 많았다. 이러한 산업보안 사고 발생 시 기업 경쟁력과 매출에 미치는 영향은 전체적으로는 평균이 4.29점으로 '그렇다(4점)'와 '매우 그렇다(5점)' 사이로 매우 높은 것이 밝혀졌으나, 직급, 근무기간, 재택근무 여부, 디지털 미디어 이용시간, 산업군에서 유의한 차이가 없었다.

이러한 산업정보 피해 유형 중 보완대책이 가장 시급한 것은 데이터 유출・해킹이 42.9%로 가장 많았고, 다음으로 바이러스・랜섬웨어 감염(23.6%), 기술 인력 유출(22.9%) 순이었고, 직급, 근무기간, 재택근무 여부, 디지털 미디어 이용시간, 산업군에 따른 유의한 차이는 없었다. 또한, 보안 조직구성 별도 운영여부의 경우, 별로도 운영하고 있음이 40.7%, 별도로 운영하고 있지 않음이 47.1%, 모름이 12.1%로 나타났고, 직급별, 근무기간별, 재택근무 별, 디지털 미디어 이용시간별로 유의한 차이가 있었다.

결과적으로, 기업이 산업보안 피해 대응이 잘되는 정도를 분석한 결과, 5점 만점에 평균이 2.97점으로 '보통이다(3점) 정도임을 규명했다. 재택근무를 할수록, 제조업, 정보통신 분야일수록 우리 기업의 산업보안 피해 대응이 더 잘되고 있

다고 생각했다. 또한, 기업에서 평소 산업보안 관련 지침을 실천하는 정도의 경우, 관련 안내가 있으면 확인 후 실천이 45.0%로 가장 많았고, 다음으로 관련 안내가 있으면 일부 선택 실천이 36.4%로 많았고, 직급, 근무기간, 재택근무, 디지털 미디어 사용시간, 산업군에 따른 차이는 없었다.

본 연구가 주목하는 중소기업이 갖는 산업보안 애로사항의 경우, 전문 인력 부족(24.0%), 예산(22.2%), 전문적 보호기술 부재(21.0%) 순으로 응답했고, 직급별, 근무기간별, 재택근부별, 디지털 이용 시간별, 산업군별 유의한 차이가 있었다.

산업보안 교육 이수 경험의 경우, 있음이 57.1%, 없음이 42.9%로 나타났고, 재택근무를 할수록 높았으며, 제조업 등은 경험 없음이 가장 많았고, 정보통신분야가 가장 높음이 확인되었다. 이러한 교육을 받는 방식은 사이버 교육이 41명(51.3%)으로 가장 많았고, 다음으로 자체 교육 18명(22.5%), 외부 전문 기관 위탁 교육 17명(21.3%) 순이었다. 또한, 이러한 교육은 의무적으로 받아야 함이 66.4%, 그렇지 않음이 33.6%으로 밝혀졌고, 산업군에서 제조업은 의무적으로 받지 않음이, 정보통신 경우 의무적으로 받아야 함이 가장 높았다. 보안교육을 주기적으로 시행하는 정도는 전체적으로는 평균이 3.09점으로 '보통이다(3점)' 정도였고, 재택근무일수록, 제조업, 정보통신분야일수록 더 주기적으로 시행함을 확인했다.

본인이 이러한 산업보안에 관심을 가지고 보안관리를 잘한다는 생각 정도는 평균 3.21로 보통 수준이었고, 재택근무일수록, 제조업, 정보통신 분야일수록 더 보안 관리를 잘한다고 인지했다.

한편, 산업보안 겸직 여부의 경우, 직무(겸직)를 하고 있음은 25.0%, 하고 있지 않음은 75.0%로 대체로 하고 있지 않음을 확인했고, 재택근무일수록, 정보통신, 제조업 분야일수록 겸직 비중이 높았다.

이러한 결과에 따라, 본 연구는 관리적, 기술적, 물리적, 인적 보안 관리 차원 개선방안을 경영 전략적 관점에서 각각 제시하였고, 이를 간략하게 정리하면 다음과 같다.

첫째, 관리적 차원의 개선을 위하여 차후 포스트 코로나 시대에 예상되는 복합적, 고도화된 사이버 공격 증가 예상에 따른 이 유형의 개념, 유형, 대응방법에 대한 기업차원 매뉴얼을 구축, 배포하고, 이를 교재로 하여 정기적 교육을 진행하여 실무에 주력하는 평사원의 보안의식과 대응역량을 증대할 것과 실습 위주의 교육을 강화, 각 직무 특성에 맞춤화된 보안대응 교육을 제공할 것을 제시했

다.

둘째, 기술적 보안의 경우, 현재 데이터 유출, 해킹, 바이러스, 랜섬웨어 감염 비중이 가장 높으므로, 이에 주력한 보안 프로그램을 구성하되, 차후 포스트 코로나 시대 복합적, 고도화된 사이버 공격 증가를 반영하여 지금까지 검증된 것은 물론 차후 개발될 수 있는 바이러스 유형들을 추정하여 견고한 예방용 프로그램 형태로 구성할 것과 각 부서 직무가 상이함으로 각 부처 특성에 맞춤화된 프로그램 개발을 제안했다.

셋째, 물리적 보안의 경우, 상기에서 제시한 기업 보안 프로그램을 구성하는 연구실, 부서에 대한 절도, 파괴 등 물리적 위협으로 보호하기 위해 각 연구소에서 근무하는 기술적 인력에 대한 보안 교육, 윤리 교육은 물론 계약사항에 별첨을 마련하여 입사, 퇴사자의 보안서약서를 작성하고, 피해보상 등 엄정한 규정을 통해 물리적 보안을 전개해야 함을 강조했다.

마지막으로, 인적 보안의 경우, 상기에서 제시한 강제적 보안도 중요하지만 기술 인력이 자사에 애착을 갖고 몰입을 유도함으로 자발적, 능동적으로 조직 발전을 위해 보안을 준수하는 태도 형성을 위해 기술 인력에 대한 처우를 보장, 성과에 대한 상대적 인센티브, 성과에 따른 정당한 승진 기회를 제공하여 기술 인력 가능성을 최소화함에 일조해야 함을 제안했다. 또한 산업보안은 임직원 모두가 선택이 아닌 필수적인 사항임을 인식하고 함께 노력해야 함을 강조한다.

제2절 연구의 의의

본 연구는 차후 포스트 코로나 시대에 그 비중과 중요성이 더욱 강조되는 중소기업 보안실태를 면밀하게 조사하고, 기존 연구들이 실태, 현황에만 주력하여 적절하고 실효성 있는 개선방안이 미흡한 이 시점에, 설문조사에 근거한 관리적, 기술적, 물리적, 인력 관리 차원의 경영전략을 제시함으로써 중소기업의 경쟁력을 확보하고 보안 강화에 기여함에 그 의의가 있다.

또한, 각 차원의 개선방안을 개별적으로 제시하지 않고, 상호유기적으로 제시함으로써 경영 차원에서 더 이해하기 쉽고, 수행하기 용이한 방향성을 제시함에 차별성에 있다.

제3절 연구의 한계 및 차후 연구방향

첫째, 본 연구가 비록 중소기업에 한정하여 산업보안 실태를 조사했으나, 산업 분야별 실태 결과를 도출하진 못했다. 따라서 차후 관련 연구는 분야별로 산업 보안 실태를 비교, 분석하여 각 산업별 맞춤화된 관리적 시사점을 제시한다면 더 유용한 연구결과를 기대할 수 있다.

둘째, 본 연구는 산업보안 실태를 분석함에 있어 중소기업 직원들의 인식수준을 기준으로 분석하여 중소기업에게 객관적으로 필요한 산업보안 요인들과 차이가 있을 수 있다. 따라서 차후 관련 연구는 객관적 요인을 제시하고, 중소기업 조직원 인식과 차이를 규명함으로써 관리적 시사점을 제시한다면 더 설득력 있는 연구 결과를 기대할 수 있다.

끝으로, 비록 본 연구가 코로나19 상황에서의 산업보안 인식을 통해 차후 포스트 코로나 시대 인식을 함께 검토하여 이 시기에 적합한 산업보안 방향성을 제시하고 있으나, 코로나19 이전의 산업보안 인식과 현재 인식 간 비교분석을 통한 변화 양상 추이는 충분히 검토하지 못하고 있다. 따라서, 차후 연구는 코로나19 이전 산업보안의 전반적 인식을 분석하여 본 연구 결과와 비교, 대조함으로써 변화 양상을 명확히 규명하고, 이에 기반한 중소기업을 위한 산업보안 전략을 구축한다면 좋을 것이다. 더 나아가, 더욱 발전된 디지털화에 따른 패러다임 변화를 함께 검토하여 차후 포스트 코로나 시대의 산업보안 방향을 제시한다면 더 유용한 연구 결과를 기대할 수 있다.

참고문헌

1. 국내문헌

김태형, (2019), “중소기업 산업기술유출방지 강화방안에 대한 연구”, 석사학위 논문, 동국대학교 대학원.

이상범, (2021), “중소기업의 산업기술보호 방안 : 경찰 수사요원 활용을 중심으로”, 석사학위 논문, 단국대학교 대학원.

전승준, (2014), “산업기술 보호를 위한 기업의 보안수준 강화 연구”, 석사학위 논문, 한국산업기술대학교 대학원.

홍준석, (2021), “중소기업 임직원의 정보보안 정책 준수에 미치는 주요 인자 연구 : 구조방정식 모형을 이용하여”, 박사학위 논문, 서울과학기술대학교 대학원.

이호준, (2020), “중소기업 산업보안 수준 개선에 관한 연구”, 석사학위 논문, 동아대학교 대학원.

전창욱 · 유진호, (2017), “중소기업에서 산업보안을 위한 디지털포렌식 활용방안 연구 : 이미징 처리시간 비교분석을 중심으로”, 한국산업보안연구, 6(2), 169-193.

이민형, (2013), “지역 중소기업의 성장동력 활성화 방안 : 산업보안을 중심으로”, 한국지방자치연구, 15(2), 141-159.

노민선 · 이삼열, (2010). “중소기업의 산업보안 역량에 대한 영향요인 평가”, 한국행정학보, 44(3), 239-259.

김건희 · 박준석 · 정성배, (2018). “중소기업 산업기술보호활동이 산업보안정책 준수의지에 미치는 영향 : 보안인식의 매개효과를 중심으로”, 한국산업보안연구, 8(1), 75-111.

박향미 · 유지연, (2015). “중소기업 산업보안 강화를 위한 한국과 미국의 관리체계 비교・분석 연구”, 한국사회안전학회지, 10(2), 119-140.

유일영, (2020), “중소기업의 중요정보 보호를 위한 보안 강화 방안”, 한국 IT 서비스학회 학술대회 논문집, 526-541.

김문선 · 전대성 · 남경현 · 김규로 · 한찬명, (2013), “산업보안 역량 수준평가 및 개선방안”, 품질경영학회지, 41권 4호, 649-657.

이상희 · 이주락, (2017), “물리보안의 정의에 관한 연구 : 위험평가이론을 중심으로, 한국산업보안연구, 7(2), 33-52.

박태형 · 임채홍 · 이기오 · 임종인, (2013), ”중소기업 산업보안 강화를 위한 지방정부의 역할 분석연구 : 경기도 사례에 대한 실증분석을 중심으로“, 한국디지털정책학회.

전자신문, (2021), [보안칼럼]'포스트 코로나' 시대 보안, 기업·개인·정부 삼각편대로.

강민지 · 박찬수, (2020), ”전문가 델파이기법을 활용한 한국 산업보안 생태계 인식 조사연구“, 융합보안논문지, 20(3), 89-97.

황윤희 · 정호준 · 유진호, (2015), ”다면평가제도의 산업보안 분야에 대한 활용방안과 효과성 분석“, 한국산업보안연구, 5권 2호, 117-140.

이시희, (2020), ”포스트 코로나19 중소기업 경영전략“, K DEVELOPEDIA.

이창무, (2012), “산업보안론”, 박영사.

이창무, (2017), “산업보안 개념의 비판적 고찰”, 한국경호경비학회지, 285-304.

장상수, (2020), “국내 중소기업 정보보호 지원 정책 개선 방안에 관한 연구”, 융합정보논문지 (구 중소기업융합학회논문지), 10(11), 332-339.

장상수, (2020), “국내외 중소기업 정보보호 지원 정책 분석 및 개선 검토”, KISA REPORT.

중소벤처기업부, (2018), “2017년 중소기업 기술보호수준 실태조사”.

중소벤처기업부, (2013), “중소기업 기술보호 매뉴얼”.

한국과학기술정보연구원(편), (2015), 미래창조과학부.

한국산업보안연구학회 홈페이지, http://www.kais.or.kr/.

한국학술지인용색인 홈페이지, https://www.kci.go.kr/.

행정안전부, (2021), “제2차 전자정부 기본계획(2021년~2025년)”.

경기남부경찰청, (2020), “산업기술보호수사 통계자료”.

국가정보원, (1999), “산업보안실무”.

국민권익위원회, (2017), “약한 고리 이론”.

신희강, (2021), “전세계 랜섬웨어 피해액 22兆, 국내 보안 빨간불”, 뉴데일리경제.

Deloitte, (2017), “사업연속성계획의 의미와 오해”.

IBM, (2021), “2021 엑스포스 위협 인텔리전스 인덱스 보고서”, IBM 시큐리티

연례 보고서.

삼성 SDS, (2021), “2021년 사이버보안 7대 트렌드 선정”, SAMSUNG SDS

2. 해외문헌

Jansen, C., & Jeschke, S, (2018), “Mitigating risks of digitalization through managed industrial security services”, Ai & Society, 33(2), 163-173.

Lee, C. M, (2014), “The strategic measures for the industrial security of small and medium business”, The Scientific World Journal, 2014.

Lv, Z., Chen, D., Lou, R., & Song, H, (2020), “Industrial security solution for virtual reality”, IEEE Internet of Things Journal, 8(8), 6273-6281.

Mitchell, V. W, (1990), “Industrial risk reduction in the purchase of microcomputers by small businesses”, European Journal of Marketing, 24(5), 7-19.

Security Management homepage, (https://sm.asisonline.org).

부록

설 문 지

본 설문은 산업보안에 관한 설문입니다. 문항에 대한 정답은 없으며 귀하께서 알고 있거나 생각하시는 대로 솔직하게 응답해 주시면 감사하겠습니다.

※**산업보안**은 범죄행위로부터 모든 경제활동을 보호하는 제반 노력"이라고 합니다. 구체적으로 유·무형의 모든 산업자산을 불법행위로부터 지키는 자산보호(asset protection)와 피해를 막는 손실방지(loss prevention) 활동을 의미한다.

■ 다음은 산업보안의 인식도에 대한 질문입니다.

1. 귀하는 산업보안이라는 용어와 개념을 알고 계십니까?

①예 **(2번부터 응답)** ②아니오 **(26번 인적사항부터 응답)**

2. 다음은 산업보안 내 세부 영역에 대한 인지도에 관한 질문입니다. 해당하는 곳에 표기해주시기 바랍니다.

산업보안 관련 지식	전혀 모른다	거의 알지 못한다	보통이다	약간 알고 있다	잘 알고 있다
1) 산업보안 중 정보보안의 의미에 대해					
2) 산업보안 중 산업기술보호의 의미에 대해					
3) 산업보안 중 핵심 시설물 및 장비 보안의 의미에 대해					
4) 산업보안 중 전문 기술인력 유출의 의미에 대해					
5) 산업보안 중 영업비밀 유출 및 산업스파이에 대해					

3. 귀하는 평소 산업보안에 대해 필요성을 느낄 때는 언제입니까?

①항상 중요하게 생각 ②직접 피해를 겪은 후 ③커뮤니티, 매체, 지인을 통해 간접 경험 ④필요하지 않음 ⑤기타( )

4. 기업내 임직원들이 산업보안에 관심을 갖지 않도록 하는 이유는 무엇이라고 생각하십니까? (복수 선택 가능)

①내용이 이해하기 어려움 ②보안 조치를 하기가 귀찮고 불편 ③조치를 해도 보안 사고는 막을 수 없다고 생각 ④나와 상관없는 일이라고 생각 ⑤조치를 하기위해 많은 비용이 발생한다는 생각 ⑥기타( )

■ 다음은 산업보안의 중요성에 대한 질문입니다.

5. 다음은 산업보안 영역에 대한 중요도에 관한 질문입니다. 해당하는 곳에 표기 해주시기 바랍니다.

산업보안의 중요성	전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
1) 인적 자산에 대한 보안이 중요하다.					
2) 설비∘ 시설 자산에 대한 보안이 중요하다.					
3) 정보 자산에 대한 보안이 중요하다.					

6. 나는 산업보안을 개인부터 경영자까지 구성원 모두가 심각성을 인식하고 실천하는게 중요하다고 생각한다.

①전혀 그렇지 않다 ②그렇지 않다 ③보통이다 ④그렇다 ⑤매우 그렇다

7. 산업보안 피해가 발생했을 경우 피해가 클 것이라 생각되는 산업 종류는 무엇입니까?

(복수 선택 가능)

①건설 ②화학 ③전기, 전자 ④자동차 ⑤금융 ⑥의료 ⑦교육 ⑧화장품 ⑨통신업 ⑩철강업

⑪조선업 ⑫기타( )

8. 산업보안 피해가 발생했을 경우 피해가 가장 클 것이라 생각되는 기업 규모는

무엇입니까?

①대기업 ②중견기업 ③중소기업 ④자영업자 ⑤기타(　　)

9. 귀하는 코로나19의 영향으로 일상의 비대면, 디지털화가 가속화되면서 이에 따른 산업보안의 중요성이 증대하고 있는다는 것에 동의하십니까?

①전혀 그렇지 않다 ②그렇지 않다 ③보통이다 ④그렇다 ⑤매우 그렇다

■ 다음은 산업보안의 개인정보 유출 및 보안 사고에 대한 질문입니다.

10. 나는 개인정보의 침해 및 유출을 경험하거나 본 적이 있다.

①예　②아니오

11. 다음은 팬데믹과 산업의 디지털화에 따른 변화에 관한 것입니다. 귀하의 생각과 일치하는 곳에 표기해주시기 바랍니다.

개인정보 유출 및 산업보안 사고	전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
1) 비대면 일상 생활로 인해 개인정보 유출이 증가할 것이다.					
2) 재택근무가 데이터 유출◦해킹 피해를 키울 것이다.					
3) 디지털화로 복합적이고 고도화된 사이버 공격이 증가할 것이다.					
4) 산업의 디지털화로 인해 전문인력의 유출과 산업 스파이가 늘어날 것이다.					

12. 귀하가 속한 기업에서 산업보안 사고가 발생했던 적이 있다.

①예**(13번부터 응답)** ②아니오**(14번부터 응답)**

13. 귀하가 경험한 기업의 산업정보 피해 유형은 무엇입니까? (복수 선택 가능)
①데이터 유출◦해킹 ②바이러스◦랜섬웨어 감염 ③핵심 시설물 피해 ④기술 인력 유출
⑤영업비밀 침해 ⑥기타( )

14. 산업보안 사고 발생시 기업의 경쟁력과 매출에 영향을 끼친다고 생각한다.
①전혀 그렇지 않다 ②그렇지 않다 ③보통이다 ④그렇다 ⑤매우 그렇다

■ 다음은 산업보안의 대응에 대한 질문입니다.

15. 산업정보 피해 유형 중에서 보완대책 마련이 시급하다고 생각하는 순서대로 나열하시오. ①데이터 유출◦해킹 ②바이러스◦랜섬웨어 감염 ③핵심 시설물 피해 ④기술 인력 유출
⑤영업비밀 침해 ⑥기타( )

16. 우리 기업은 보안 조직을 구성하여 별도로 운영하고 있다.
①예 ②아니요 ③모른다.

17. 우리 기업은 산업보안 피해 대응이 잘 되고 있다고 생각한다.
①전혀 그렇지 않다 ②그렇지 않다 ③보통이다 ④그렇다 ⑤매우 그렇다
18. 귀하는 귀하가 속한 기업에서 평소 산업보안 관련 지침을 어느 정도 자주 실천하십니까?
-항목 추가 했습니다.
①전혀 안 함 ②상황에 따라 다르며, 안내가 있어도 무시 ③관련 안내가 있으면 일부 선택 실천 ④관련 안내가 있으면 확인 후 실천 ⑤스스로 항상 신경 쓰면서 적극 실천

19. 중소기업이 가진 산업보안 활동의 애로사항은 무엇이라고 생각하십니까?(복수 선택 가능)
①전문인력 부족 ②전문적보호기술 부재 ③예산 ④법적, 제도적 장치미흡 ⑤임직원의 관심 및 이해부족 ⑥기타( )

■ 다음은 산업보안의 교육 이수 및 보안의식에 대한 질문입니다.

20. 나는 산업보안 교육을 받아본 적이 있다.
①예 **(21번부터 응답)** ②아니오 **(22번부터 응답)**

21. 귀하는 어떤 방식으로 산업보안 교육을 받으셨습니까?
①사이버 교육 ②자체 교육 ③외부 전문 기관 위탁 교육 ④현장 교육 ⑤기타(
)

22. 우리 기업에서는 산업보안 교육을 의무적으로 받아야 한다.
①예 ②아니오

23. 우리 기업은 산업보안과 관련된 보안 교육을 주기적으로 시행한다.
①전혀 그렇지 않다 ②그렇지 않다 ③보통이다 ④그렇다 ⑤매우 그렇다

24. 나는 평상시 산업보안에 관심을 가지고 보안관리를 잘하고 있다고 생각한다.
①전혀 그렇지 않다 ②그렇지 않다 ③보통이다 ④그렇다 ⑤매우 그렇다

25. 귀하가 속한 기업에서 산업보안 관련 직무(겸직)를 하고 있습니까?
①예 ②아니오

■ 다음은 인적 사항에 대한 문항입니다.

26. 귀하의 성별은?
①남자 ②여자

27. 귀하의 연령은?
①20대 ②30대 ③40대 ④50대 ⑤60대 이상

28. 귀하의 학력은?

①고졸 이하 ②전문대졸 ③4년제 졸 ④대학원 재학 ⑤박사급

29. 직장내 귀하의 직급은 어떻게 되십니까?

①평사원 ②과장급 ③부장급 ④이사급 ⑤경영진

30. 귀하의 (이전, 현재) 직장 근무기간은 어떻게 되십니까?

①1년 이하 ②1-3년 ③4-6년 ④7-9년 ⑤10년 이상

31. 귀하는 현재 재택근무를 하고 있습니까?

①예 ②아니오

32. 귀하의 하루 평균 디지털 미디어 사용은 시간은?

①1시간 미만 ②1~3시간 ③3~5시간 ④5~7시간 ⑤8시간 이상

33. 귀하가 종사하는 기업이 속해 있는 산업군은 무엇입니까?

①건설 ②화학 ③전기, 전자 ④자동차 ⑤금융 ⑥의료 ⑦교육 ⑧화장품 ⑨통신업 ⑩철강업

⑪조선업 ⑫기타( )

34. 귀하가 종사하는 기업의 규모는 어떠합니까?

①50명 미만 ②50-100명 ③100-200명 ④200-300명 ⑤300명 이상

※설문에 응해 주시어 대단히 감사합니다※

ABSTRACT

A Study on the Prevention of Industrial Information Leakage of Small and Medium Businesses in Post-Corona Era

Song, Jae Hyeok
Department of Business Administration
The Graduate School of Ulsan University

As the online economy accelerates due to the recent COVID-19 impact, the information security risks of companies have increased even more. In particular, 81% of the 97 cases of ransomware damage as of July 2021 due to lack of professional manpower and insufficient budget has been identified as a small and medium-sized enterprise, and is exposed to a blind spot in information protection.

In the future post-corona era, the creation of innovative technology is the key to the advancement of online technology due to the reinforcement of non-face-to-face, and a major shift is expected to be focused on the technological achievements of small and medium-sized venture companies based on innovative and entrepreneurial spirit.

In this study, literature review and empirical research were conducted to suggest ways to improve information security of small and medium-sized enterprise in the post-corona era and by presenting both policy and practical implications according to the research results, it was attempted to finally derive a plan for mutual cooperation between the government and small and medium-sized enterprises.

For this research purpose, this study primarily analyzes the information security status of domestic SMEs by reviewing the literature,

Second, by conducting an online survey on information security status for 200 members of SMEs across the country to find out the status of information supplementation for domestic SMEs, by comparing and analyzing overseas cases and domestic conditions to identify commonalities and differences, We have established the direction of information security for small and medium-sized enterprises (SMEs) in preparation for the post-corona era tailored to the circumstances.

In addition, based on the case of US industrial security, we analyzed the limited domestic industrial security.

As a result of the study, it can be expected that industrial security damage will further increase in the future as digital acceleration in the post-corona era. In this era where non-face-to-face is getting more prevalent the increase in complex and sophisticated cyber attacks in terms of the degree of change due to the pandemic and industrial digital is proving this.

In addition, it can be seen that if an industrial security incident occurs in the future, it has a great effect on the competitiveness and sales of SMEs.

The result of recognition of the impact on corporate competitiveness and sales in the event of an industrial security incident was confirmed to be very high with an average of 4.29 points.

In addition, it was confirmed that the higher the position, the stronger the recognition of the importance and severity of this security awareness, and despite this high awareness, in the case of the extent to which companies usually practice industrial security-related guidelines.. In about 80% of cases, it was confirmed that they must be guided and were not actively and voluntarily complying with industrial security regulations.

Management, technical, physical, and manpower-level improvement measures to improve this issue were presented respectively.

This study is meaningful in presenting practical strategies according to the limitations of existing studies that cannot present appropriate alternatives by focusing only on the status and actual conditions of industrial security for SMEs.

It is expected that it will be a useful material for more effective management strategies by presenting improvement plans in each dimension organically.