情 報 保 護 學 會 誌
第19卷 第1號, 2009. 2

우리나라 중소기업의 정보 보호 역량 강화를 위한 교육 훈련 현황과 문제점

문 현 정*

요 약

오늘날 기업 활동 전반에 걸쳐 네트워크 및 정보시스템에 대한 의존도가 높아지고 있는 추세에 따라 이를 대상으로 한 정보 보안 침해 역시 증가하고 있다. 우리나라의 산업 구조상 중소기업은 전체 사업체수를 기준으로 99%이상을 차지하고 있으며 특히 소기업 및 소상공인은 전체의 96%이상을 차지하고 있다. 중소기업은 그 규모의 특성상 상대적으로 정보 보안 위협에 취약함이 지적되고 있으며 이들의 보안 역량 강화는 안전한 디지털 경제 환경을 조성하기 위한 핵심 과제로 떠오르고 있다. 그 중요성에 대한 인식을 기반으로 중소기업의 특성에 맞는 정보 보안 교육 훈련이 절실히 요구되고 있다. 본 논문에서는 우리나라 중소기업 및 정보 보안 관련 주무 기관인 중소기업청, 국가정보원등과 더불어 민간 정보기술(IT) 교육 훈련 기관들에서 실시되고 있는 중소기업을 위한 정보 보안 교육 훈련의 현황을 살펴보고 문제점을 파악하고자 한다.

Ⅰ. 서 론

인터넷은 인간 생활에 실로 막대한 편리와 진화를 가져다주었다. 네트워크상의 보이지 않는 수많은 거리와 상점에서는 종이인형부터 첨단 전투기 장비에 이르기까지 전 세계의 거의 모든 상품들이 진열대에 오르고 거래되고 있다[1].

우리나라 전체 사업체 수를 기준으로 중소기업(SME: Small and Medium-sized Enterprises)[1]이 차지하는 비율은 99%에 달한다[2]. 이는 중소기업의 기업 경쟁력이 전체 산업 경쟁력과 직결되어 있다는 것을 의미한다.

따라서 중소기업의 기업 정보화와 e-비즈니스 활성화 그리고 이와 더불어 중소기업의 보안 역량강화는 글로벌 디지털 경제 사회에서 기업 및 국가 경쟁력 측면에서 매우 중요한 이슈로 떠오르고 있다.

중소기업의 적극적인 정보 보안 역량 강화를 위하여 이미 미국, 유럽 등 선진국에서는 국가적 차원에서 활발한 지원 노력이 이루어지고 있다. 유럽연합(European Union)내 ENISA(European Network and Information Security Agency)는 최근 보고서를 통하여 유럽연합 전체의 안전한 네트워크 환경 구축을 위한 정보 보안의 핵심 대상을 가정 내 개인 사용자(home-user)와 중소기업으로 규정하였다[3].

위 대상들은 인터넷을 비롯한 정보 네트워크의 대부분을 구성하고 있는 주체들 임에도 불구하고 대기업 및 공공기관들과 비교하여 상대적으로 큰 보안 취약성을 보이는 특징이 있다. 실제로 해킹(hacking)과 네트워크 공격 등의 대상이 되며 종종 대규모 네트워크 테러의 거점으로 희생되고 있으며 그 피해 규모는 기업 활동과 사회 안전에 충분히 위협적 수준에 이르렀다[3][4][5].

가까운 예로 지난 2008년 2월에 발생한 옥션의 개인정보 유출 사건은 일개 기업의 보안사고 수준을 넘어서 우리나라 국민 4분의1에 달하는 개인정보가 무방비로 길거리에 나뒹굴게 되는 결과를 낳았다. 더욱 심각한 것

* 숙명여자대학교 (moonhj@sm.ac.kr)

1) 중소기업에 대한 정의는 나라마다 조금씩 다르지만 일반적으로 종사자 규모와 자본금 또는 매출액 규모를 기준으로 분류하고 있다. 우리나라 『중소기업기본법』에 의하면 업종별로 종사자 규모 기준 50~300명 미만인 기업을 중소기업으로 규정하며 이를 세분화 하여 업종별로 상시근로자수 50인 혹은 10인 미만의 기업을 소기업이라 하고 나머지를 중기업으로 나누고 있다. 또한 『소기업 및 소상공인 지원을 위한 특별조치법』에 의하여 업종별로 상시 근로자수가 10인 혹은 5인 미만의 기업은 소상공인으로 분류한다.

은 이러한 정보보안 침해 사고의 심각성에 대한 인식이 저조하고 이에 대한 기민한 후속조치가 제대로 이루어지지 않고 있다는 점이다.

우리나라 중소기업의 정보 보안 역량을 강화하기 위한 목적으로 중소기업청, 국가정보원 뿐만 아니라 민간 정보 기술(IT) 교육기관에서도 중소기업을 위한 교육 훈련 프로그램을 마련하여 중소기업 종사자와 사업주들의 참여를 유도하고 있다.

그러나 정보 보안 전문가 양성을 목적으로 하는 취업 대비 훈련으로서의 기존 대학 전공 과정 중심의 교육 훈련 모델과 달리 중소기업의 특성을 고려한 차별화된 정보 보안 교육 모델에 대한 연구는 미흡한 수준이다.

본 논문에서는 우리나라 중소기업의 정보 보안 역량 강화 모델 수립을 위하여 중소기업을 위한 정보 보안 교육 훈련의 현황과 문제점을 살펴보고자 한다.

Ⅱ. 배경 및 관련 연구

2.1 중소기업 정보화와 정보 보안 취약성

2007년 통계청이 발표한 '2006사업체기초통계조사' 결과에 의하면 우리나라의 전체 사업체 중 99%이상이 중소기업이며. 특히 소기업과 소상공인의 비율은 전체 사업체수 기준으로 약 96%에 달하고 있다[표 1] [표 2]. 또한 우리나라 전체 근로자의 약 80%이상이 중소기업에 몸담고 있으며 전체 중소기업의 60% 이상이 대기업에 납품을 주력으로 하는 대·중소기업간 협업 관계에 있는 것으로 나타났다[6]. 이는 우리나라 산업 및 경제 구조에 있어서 그 근간이 중소기업에 있음을 의미한다.

일반적으로 중소기업 정보화는 중소기업이 자사의 업무프로세스 처리에 정보기술을 효과적으로 활용하는

〔표 1〕 우리나라 산업 종사자규모별 사업체수 및 종사자 수 (통계청 2006 사업체기초통계조사)[2]

(명, %, 개)

산업별 / 사업체규모*		전산업	농업및 임업	어업	광업	제조업	전기가스 수도	운송업	건설업	도소매업
전체종사자수		15,435,766	25,708	6,021	18,466	3,435,491	67,418	879,553	845,339	2,468,173
소상공인	종사자수	5,383,826	1,528	359	4,474	839,241	1,062	406,563	238,433	1,405,727
	비율	34.88	5.94	5.96	24.23	24.43	1.58	46.22	28.21	56.95
소기업	종사자수	2,813,953	2,913	375	7,776	1,051,355	1,657	146,987	312,806	352,221
	비율	18.23	11.33	6.23	42.11	30.60	2.46	16.71	37.00	14.27
중기업	종사자수	4,161,981	20,387	5,287	2,137	858,032	49,415	262,491	195,797	536,506
	비율	26.96	79.30	87.81	11.57	24.98	73.30	29.84	23.16	21.74
대기업	종사자수	3,076,006	880	0	4,079	686,863	15,284	63,512	98,303	173,719
	비율	19.93	3.42	0.00	22.09	19.99	22.67	7.22	11.63	7.04
전체사업체수		3,226,569	1,864	370	1,839	340,724	1,551	343,598	90,486	865,358
소상공인	사업체수	2,787,773	618	194	1,413	278,246	394	333,812	71,469	781,088
	비율	86.40	33.15	52.43	76.84	81.66	25.40	97.15	78.98	90.26
소기업	사업체수	284,634	444	53	397	53,255	249	7,285	16,883	56,456
	비율	8.82	23.82	14.32	21.59	15.63	16.05	2.12	18.66	6.52
중기업	사업체수	138,943	801	123	24	8,565	889	2,392	1,983	26,964
	비율	4.31	42.97	33.24	1.31	2.51	57.32	0.70	2.19	3.12
대기업	사업체수	15,219	1	0	5	658	19	109	151	850
	비율	0.47	0.05	0.00	0.27	0.19	1.23	0.03	0.17	0.10

*통계청 『2006 사업체기초통계조사』 결과를 『중소기업기본법 시행령 별표1』의 근로자수 기준으로 소상공인/소기업/중기업/대기업 규모를 분석하였으므로 실제 통계적 기준과 법률적 기준에 차이가 있을 수 있음.

〔표 2〕 우리나라 산업 종사자규모별 사업체수 및 종사자 수(계속)

(명, %, 개)

산업별 / 사업체규모*		숙박음식업	통신업	금융 보험업	부동산 임대업	사업 서비스업	공공행정, 국방및 사회보장 행정	교육 서비스업	보건사회 복지업	오락문화 운동	기타공공 수리개인
전체종사자수		1,661,782	140,178	619,539	415,679	1,175,867	538,799	1,245,864	696,150	376,990	818,749
소상공인	종사자수	1,135,804	13,039	22,085	167,088	118,652	5,337	175,484	145,153	205,607	498,190
	비율	68.35	9.30	3.56	40.20	10.09	0.99	14.09	20.85	54.54	60.85
소기업	종사자수	283,143	15,041	56,564	69,284	125,987	9,339	120,985	123,007	28,337	106,176
	비율	17.04	10.73	9.13	16.67	10.71	1.73	9.71	17.67	7.52	12.97
중기업	종사자수	179,611	91,328	332,828	127,357	637,827	123,960	341,905	157,943	80,577	158,593
	비율	10.81	65.15	53.72	30.64	54.24	23.01	27.44	22.69	21.37	19.37
대기업	종사자수	63,224	20,770	208,062	51,950	293,401	400,163	607,490	270,047	62,469	55,790
	비율	3.80	14.82	33.58	12.50	24.95	74.27	48.76	38.79	16.57	6.81
전체사업체수		618,301	9,424	35,613	120,299	90,909	12,396	132,916	79,868	123,641	357,412
소상공인	사업체수	560,008	4,916	9,642	101,914	52,781	3,108	91,745	49,714	115,685	331,026
	비율	90.57	52.16	27.07	84.72	58.06	25.07	69.02	62.25	93.57	92.62
소기업	사업체수	46,921	2,375	8,052	10,683	20,071	1,249	18,879	19,885	4,600	16,897
	비율	7.59	25.20	22.61	8.88	22.08	10.08	14.20	24.90	3.72	4.73
중기업	사업체수	10,848	2,096	16,292	7,217	17,606	6,242	16,160	8,774	3,077	8,890
	비율	1.75	22.24	45.75	6.00	19.37	50.35	12.16	10.99	2.49	2.49
대기업	사업체수	524	37	1,627	485	451	1,797	6,132	1,495	279	599
	비율	0.08	0.39	4.57	0.40	0.50	14.50	4.61	1.87	0.23	0.17

정도로 정의된다[7].

중소기업은 매출, 자본, 조직, 인력, 기술력 및 경영환경면에서 기업적 특성이 다른 이유로 대기업을 중심으로 개발된 정보화 모델을 변형하여 적용시키는데 한계가 있음이 드러나 중소기업의 특성에 따른 정보화 모델에 대한 관심이 높아지고 있다[표 3][8].

기존의 중소기업 정보화 모델 연구는 대부분 중소기업 내에서 상대적으로 규모가 큰 중기업을 목적 대상으로 하고 있으며[7] 그에 반해 전체 산업체수의 86%이상을 차지하는 5인 혹은 10인 이하 종사자 규모의 소상공인과 소기업은 저소득층, 장애인등과 더불어 정보격차 취약계층으로 지목되고 있는 수준이다[9].

그러나 정보격차 해소 대책은 주로 성별, 지역, 학력, 소득 수준 등에 의한 전통적인 취약계층을 중심으로 치중되고 있어 소상공인 및 소기업의 특징을 고려한 정보격차 해소 내지는 정보화 대책은 거론되지 못하고 있다[9].

따라서 전체 중소기업의 정보화 또는 정보 보안 역량 강화를 위해서는 대다수의 소상공인 및 소기업에 대한 고려가 필수적이라고 할 수 있다.

〔표 3〕 정보화 관점에서의 중소기업의 경영적, 조직적, 환경적 특성[8][10][11]

구분	설 명
경영 측면	• 소유자와 경영자가 동일인인 경우 대부분 • 의사결정에 있어 경영자의 역할이 절대적 • 경영자가 기업 여건에 대한 상당한 지식을 보유·의사결정의 분권화가 이루어지지 않음
업무 조직적 측면	• 사업규모가 작아 업무 조직이 간단 • 한 조직이 여러 업무를 동시에 수행 • 동료들 간의 인간적인 매력과 동료애가 기업 내 협력과 생산성에 큰 영향을 미침 • 표준화된 업무의 절차나 규범이 없어 세부 업무에 대한 정의가 상세하지 않은 경우가 많음 • 조직이 체계적으로 구성되지 못해 직급에 대한 정의와 권한이 불분명 • 모든 조직이 작고 경영자와 밀접한 관계
경영 환경적 측면	• 자금, 인력, 기술 등에 한계를 가지고 있음 • 대기업과 비교하여 근로자의 급여가 적고 근무 기간이 짧고 이직률이 높음 • 주로 노동집약적인 산업에 속해 있음 • 정보수집이 경영자에 의해 수행되고 기업 내 정보 공유가 잘 이루어지지 않음 • 정보의 처리, 저장 및 활용이 미약 • 정형화된 기업경영계획과 전략이 미비

인터넷을 비롯한 정보 통신 기술의 확산과 정보화를 위한 다양한 지원에 힘입어 기업의 디지털 정보자산이 증가하고 네트워크를 통한 접근성이 높아지면서 동시에 중소기업에 대한 정보 보안 위협이 증가하고 있다. 이러한 정보 보안 위협을 그 목적과 대상 그리고 방법상의 특징에 따라 크게 두 가지 유형으로 나누어 볼 수 있다.

우선, 사이버 테러로 분류 되는 단순 침입, 사용자 도용, 파일 삭제·변경, 자료 유출, 폭탄·스팸메일, DOS공격 등의 해킹과 바이러스·웜 공격 등의 보안 위협이다[12]. 이러한 위협은 주로 네트워크를 통한 외부로 부터의 무작위적 침투 및 공격을 특징으로 한다. 전 세계적인 인터넷 기술의 확산과 익명성 등에 힘입어 이러한 위협은 지역 및 국가 경계를 넘어 더욱 심각해지고 있다.

다른 하나는 내·외부 관계자에 의한 조직적이고 계획적인 기업 정보에 대한 복사·절취로서 일반적으로 우리가 알고 있는 산업 스파이에 의한 기업 기밀 유출 위협 등이 이에 속한다[13].

최근 국가정보원 산업기밀보호센터에 의하면 2003년부터 2007년 까지 산업 스파이에 의한 기업의 핵심 기술 유출 사건이 지속적으로 증가하고 있으며 산업 전반으로 확산되는 추세를 보이는 것으로 나타났다. 또한 2007년 중소기업기술정보진흥원이 실시한 '중소기업 산업기밀관리실태조사'에 의하면 조사대상 기업 중 17.8%가 최근 3년간 산업기밀의 외부 유출로 피해를 입었으며 기업 규모가 작을수록 기밀 유출 비율이 높으며 그 피해 규모가 특히 소기업의 규모를 감안한다면 기업 활동에 치명적인 수준인 것으로 나타났다.

중소기업 정보 보안에 있어서 중소기업은 그 규모와 성격에 따라 일반 사용자 보안과 기업 보안의 성격을 동시에 고려해야 한다.

정보 보안과 같은 고도의 전문성을 요하는 정보 업무를 전담하는 조직 또는 인력을 설치 운영하지 못하는 것은 전체 중소기업이 안고 있는 취약성이지만 특히나 소상공인 및 소기업의 경우 경영자 1인이 대부분의 정보 업무를 수행하므로 정보 이용자 유형으로 보면 개인 사용자와 유사한 면이 있다[9]. 상대적으로 큰 중기업의 경우 보안 컨설팅 지원 정책의 수혜로 보안 체계 확립 또는 보안 업무의 아웃소싱 등을 통하여 기업 보안 활동을 수행할 수 있으나, 소상공인 및 소기업의 경우 인적 규모 면에서 거의 1인 체제의 기업 보안 활동이 요구된다.

따라서 중소기업의 정보 보안 역량 강화를 위한 교육 및 훈련은 대상과 내용면에서 위 두 가지 관점에 대한 균형적 고려가 필요하다.

2.2 중소기업을 위한 정보 보안 역량 강화 관련 해외 사례

이미 미국, 유럽의 선진국들에서는 국가적 차원에서 중소기업의 보안에 대한 지원정책과 연구들이 확대되고 있다. 중소기업은 금전적·인적 자원의 한계성으로 기업 내 보안 전담 인력이나 부서를 운영할 수 없고, 보안 HW/SW의 구매와 지속적인 업데이트를 하지 못하는 등의 보안 취약성을 가지고 있으며 특히 보안에 대한 인식 부족이 가장 큰 장애요인으로 지적되고 있다[3][4][14].

2.2.1 미국

미국 중소기업청(U.S. SBA: U.S. Small Business Administration)은 1953년 설립된 이래 중소기업을 미 경제 발전과 고용 창출의 원동력이며 기회(opportunity)의 수단으로 인식하고 관련 정책과 각종 사업을 전담하고 있다. 미국 중소기업청과 NIST(National Institute of Standards and Technology)는 FBI(Federal Bureau of Investigation)와 공동으로 중소기업을 위한 보안 훈련 워크숍(Small Business Corner Computer Security Workshop)을 계획하여 미전역에 걸쳐 시행하고 있으며 후속 사업으로 중소기업 보안 전문 강사 양성을 위한 "Train the Trainers" 사업을 파일럿 프로젝트로 진행 중이다[15]. 또한 미국 중소기업청은 전자정부(e-Government) 시책의 일환으로 중소기업 훈련 네트워크(SBTN: Small Business Training Network)를 구축하여 미전역의 중소기업을 위한 온·오프라인 교육 및 훈련 정보를 제공하고 있다.

2.2.2 유럽 연합

유럽연합은 지난 2007년 회원국내 중소기업(SME)의 경쟁력 강화와 혁신을 위한 CIP2007-2013 프로그램을 착수 하여 2013년까지 1차 사업 완수를 목표로 하고 있다. CIP(The Competitiveness and Innovation Framework Programme)은 중소기업의 기업 혁신과 투자 유치 그리고 이를 위한 지역 거점 네트워크사업인 기업혁신프로그램

(EIP, Entrepreneurship and Innovation Programme), 단일 유럽 정보통신망 구축과 ICT(Information Communication and Technology) 기반 경제활동 활성화를 위한 정보통신기술 정책지원프로그램(ICT PSP, ICT Policy Support Programme) 그리고 재생에너지와 새로운 에너지 원천 개발을 위한 지능형 에너지 프로그램(IEP, Intelligent Energy Programme)의 3가지 세부 시행 그룹으로 구성되어 있다. 이중 ICT PSP는 유럽 발전을 이끌 핵심 대상을 중소기업(SME)으로 규정하고 이들을 위한 e-비즈니스/e-서비스관련 정보화 지원 정책을 전담하고 있다[16]. 또한 유럽 연합 내 네트워크 및 정보 보안을 담당하는 기관인 ENISA(European Network and Information Security Agency)는 유럽 연합 내 정보통신망의 안전을 위한 핵심 대상을 일반 사용자와 중소기업으로 규정하고 이들을 중심으로 한 통신망 안전 경보 시스템 구축에 대한 연구를 지원하고 있다[3][14][17].

2.3 정보 보안 교육 훈련 모델 관련 연구

개인 및 조직의 정보화와 보안에 대한 인식을 높이기 위한 방안으로는 홍보 캠페인, 교육 및 훈련, 감사, 포상 등과 같은 다양한 방법들이 연구 및 적용되고 있다[3][15][18][19][20]. 특히 교육 및 훈련은 인식 제고와 기술 습득 더 나아가 최신 기술 정보 및 동향을 파악할 수 있는 가장 직접적인 수단으로서 우리나라의 중소기업청, 국가정보원을 비롯하여 미국, 유럽 선진국에서도 중소기업의 보안 역량 강화를 위한 교육 과정 개발에 대한 연구가 활발히 이루어지고 있다.

짧은 역사에도 불구하고 정보 보호 또는 정보 보안 분야는 복합학적 특성상 이에 대한 효과적인 교육 및 훈련 모델에 대한 연구와 논의가 꾸준히 이어지고 있다. 우리나라 정보 보안 관련 교육 훈련은 주로 대학 내 정보 보안 관련 학위과정과 정보보안관련 자격증 과정을 중심으로 이루어지고 있으며 정보 보안 전문가 양성 을 목적으로 하고 있는 직업 훈련과정의 성격을 띠고 있다.

주로 대학 내 전공 교과 과정을 위한 교육 과정과 로드맵(roadmap) 개발에 대한 연구가 먼저 이루어졌으며, 초중고교 과정에서 정보 보안 의식 함양과 기술 습득을 위한 교육 및 훈련에 대한 연구가 이루어져 실제 교과 과정 개편에 반영되고 있다[21][22][23]. 또한 정보보안전문가 양성을 위한 장·단기 전문 교육 및 훈련과정 개발 및 확산의 필요성이 제기되었고[20][24] 정보보안 관련 국내외 자격 인증 제도가 도입 및 실시되고 있다.

그러나 현재 대부분의 정보 보안 교육 훈련은 대학 내 전공 교과 모델을 기반으로 컴퓨터 전기 전자 통신 공학계열의 교육 내용에 치우쳐 있으며, 중소기업을 위한 정보 보호 교육 과정 개발에 있어서 경영, 윤리 및 법률적 관점에 대한 균형이 필요하다.

또한 일반 사용자와 중소기업의 정보화 역량 수준에 맞추어 이해하기 쉬운 용어와 설명 그리고 다양한 교수법등이 적용된 보다 접근성 높은 교육 모델에 대한 연구 역시 요구되고 있다[3].

III. 우리나라 중소기업 정보 보안 역량 강화를 위한 교육 훈련 현황

우리나라의 대표적인 중소기업 보안 역량 강화를 위한 교육 훈련 과정으로는 중소기업청(SMBA, Small and Medium Business Administration)과 중소기업기술정보진흥원(TIPA, Korea Technology and Information Promotion Agency for SMEs)이 제공하는 산업보안교육과정과 국가정보원 산업기밀보호센터(NISC, National Industrial Security Center)에서 제공하는 교육 및 워크숍 과정 그리고 국가정보대학원의 산업보안 과정을 들 수 있다. 또한 한국정보보호진흥원(KISA, Korea Information Security Agency)은 '중소기업 정보보호 자가 측정 도구'와 더불어 중소기업 보안 과정을 제공하고 있다. 더불어 민간 교육기관에서의 정보 보안 교육과정을 중소기업 관점에서 살펴보고자 한다.

〔표 4〕 중소기업기술진흥원
산업보안과정(2008.3~2008.12) 교육 내용

차수	과정명
1	정보의 가치 이해하기
2	산업보안의 필요성-기술유출방지의필요성
3	관련법 이해하고 보호받기
4	기술유출시 문제점 및 피해-국가의 관점
5	기술유출시 문제점 및 피해-중소기업의 관점
6	기술유출시 문제점 및 피해-개인의 관점
7	산업보안 기술유출 방지 대책-관리적 보안
8	산업보안 기술유출 방지 대책-기술적 보안
9	산업보안 기술유출 방지 대책-물리적 보안
10	산업기밀 보호 관련기관 및 기술유출방지 사업

3.1 중소기업청 중소기업기술정보진흥원의 산업보안과정

중소기업청은 2008년 4월 현재 중소기업을 위한 정보화지원사업의 일환으로 기술 유출 방지 지원 사업을 계획·시행하고 있으며 이 중 '산업보안 교육사업'을 통해서 산업보안 과정을 제공하고 있다[표 4].

교육 내용은 전반적으로 산업 스파이 등에 의한 산업기밀 유출에 대한 인식의 향상에 초점을 맞추고 있다. 특히 '2007년 산업기밀관리실태조사' 결과를 바탕으로 핵심 산업 기술 유출 피해와 그 원인을 관리적, 기술적 그리고 물리적 보안 관점에서 설명하고 있다.

본 과정은 온라인 교육 과정으로서 산업기밀 유출의 현황과 그 피해의 심각성을 인지시키고 그 방지 대책을 제시하는 이론 교육 과정이다. 사이버테러 유형의 보안 위협에 대응한 실무 교육의 비중은 적으며 예제 및 실습 훈련은 포함되어있지 않다.

3.2 한국정보보호진흥원의 중소기업 보안과정

한국정보보호진흥원(Korea Information Security Agency)은 정보보호기술 온라인 학습장을 통하여 중소기업 보안 과정을 무료로 운영하고 있다. [표 5]와 같이 PC보안, 네트워크보안, 서버보안 그리고 데이터보안의 4분야에 해당하는 총 37개 실습자료를 초/중/고급의 3단계로 난이도를 나누어 게시하고 가상 실습 서버를 통해 직접 해볼 수 있는 실습 환경을 제공하고 있다.

그러나 중소기업을 위한 정보 보호 인식과 기초지식에 관한 이론 교육 자료, 교육과정 로드맵 또는 가이드가 없으며, 중소기업 보안교육 과정으로서 일반적인 '윈도우즈2000관리자과정'과 차별성이 없다.

별도로 한국정보보호진흥원은 '중소기업 정보보호수준 자가측정도구'를 제공하여 중소기업의 정보화 수준을 유형별로 진단함과 동시에 정보보호수준을 평가하고 그에 대한 정보보호 조치와 가이드라인을 제시하고 있다. 그러나 제시된 정보보호 대책을 이행하기 위해 중소기업이 필요로 하는 연계 교육 훈련과정에 대한 자료나 정보는 없다.

3.3 국가정보원 산업기밀보호센터의 산업보안 교육/컨설팅

국가정보원 산업기밀보호센터는 '산업기술보호법'상 '국가핵심기술'로 지정된 기술을 보유 및 관리하는 기관을 대상으로 보안 교육 및 보안대책을 제공하고 있다. '국가핵심기술'이란 국내외시장에서 기술적, 경제적 가치가 높거나 관련 산업의 성장 잠재력이 높아 해외로

〔표 5〕 한국정보보호진흥원 정보보호기술온라인 학습장 중소기업보안 교육 과정

구분	초급	중급	고급
PC보안	• 사용자 계정 정책 보안 • 익명 보안 옵션 Windows XP • 관리자 계정 보안 • Windows XP 폴더 보안 • 레지스트리 보안 • 인터넷 익스플로러 보안 • 인터넷 연결 방화벽ICF • 윈도우 NetBIOS 서비스 보안	• 패치 및 업데이트 관리 • 전자메일보안 • 파일 및 폴더 암호화 • DoS공격 방어 • 이벤트 로그 분석 • 인터넷 익스플로러 악성 프로그램 대응 • 악성 프로그램 대응. bat 레지스트리 실행 • 터미널 서비스 보안	없음
네트워크 보안	없음	• router의 snmp접속 제한	• snort및 원격 Syslog Logging 설정 • snort를 이용한 침입탐지
서버 보안	• 사용자 권한 할당 • TCP/IP 필터링 • 익명 보안 옵션	• IPSec 보안 • 악성 프로그램 대응서비스 • 웹 응용프로그램 보안 (SQL Injection 공격 방어) • IIS 웹 서버 보안 • DNS 서버 보안 • 웹 응용프로그램 보안 (XSS 공격 방어) • MS-SQL Database 기본 보안 설정 • PHP에서 SQL Injection 취약성 해결	• 악성 프로그램 대응 dll • rpm 패키지 관리 명령을 이용한 변조된 파일 확인 • nmap을 이용한 백도어 찾기 • chkrootkit을 이용한 rootkit 탐지 • nikto를 이용한 웹 취약성 분석
데이터 보안	없음	• SSH tunnel을 이용한 MySQL 접속 • MySQL file read제거 문제	없음

유출될 경우 국가의 안전 보장 및 국민 경제의 발전에 중대한 악영향을 줄 우려가 있는 산업 기술로서 '산업기술의 유출방지 및 보호에 관한 법률 9조'에 따라 지정된 산업기술을 말한다. 2007년 8월 기준으로 전기. 전자, 자동차, 철강 등 분야에서 총 40개의 국가핵심기술이 선정 되었다.

국가정보원 산업기밀보호센터는 방문 교육 신청을 신청한 기업체에 한하여 국가정보원 산업보안 담당관이 직접 방문하여 최근 산업스파이 사건을 중심으로 산업보안 의식 교육을 제공한다.

국가정보원 산업기밀관리센터는 기업체/연구소를 위한 보안대책을 제시하고 있다[표 6]. 산업스파이에 의한 산업기술 유출은 대부분이 주로 내부자(전/현직 직원)에 의한 인적보안 사항이 대부분인 관계로 인적보안에 대한 중요성과 그에 상응하는 출입 통제 등의 물리적 보안 정책 등이 주된 내용이다.

3.4 국가정보대학원 산업보안 과정

국가정보대학원에서 제공하고 있는 산업보안 과정의 교육내용은 다음과 같다[표 7]. 경제단체, 정부투자 및 출연기관 및 기업체 임직원을 대상으로 산업보안 교육을 제공한다.

〔표 6〕 국가정보원 산업기밀보안센터에서 제시하는 보안대책

보안분야	보안대책	보안분야	보안대책
관리적보안	• 내부인원에 대한 보안관리 • 외부인원에 대한 보안관리 • 중요자료에 대한 보안관리	기술적보안	• PC보안관리 • e-mail 보안관리 • 해킹방지를 위한 보안대책
물리적보안	• 중요시설의 보호관리 • 출입자 통제	보안사례	• 국내전자업체A 사: 출입절차, 물품 반 • 출입 절차 규정, 시설 보안, 통신보안,IT 보안, PC보안 • 국내전자업체B사: 보안규정, 홍보및 보안 교육, 보안점검, 출입통제, 차량출입통제, 시설보안, IT 보안 • 국내 연구원: 협력업체 보안점검, 보안서약서 징구

〔표 7〕 국가정보대학원 산업보안 과정 교육 내용

교육 주제	교육 내용
외국의 산업 정보 탐지 동향	• 주요국 정보기관의 경제 · 산업정보 탐지 활동 양상과 사례 • 대처방안 제시
산업보안관리 실무	• 인원 · 문서 · 시설 · 사이버보안 등 보안업무 개관과 각 분야별 첨단기술 • 산업정보 관리요령 및 보안대책 등 실무내용 연구 · 토의
산업기밀 유출 사례 및 대책	• 국내외에서 발생한 주요 산업기밀 유출사례 및 피해실태를 정밀분석하고 재발 방지 대책 등을 구체적으로 연구 · 검토
사이버 보안관리	• 사이버공간을 이용한 기 업 내부의 첨단산업기밀 외부 유출사례 • 해킹(크래킹)등 외부에 의한 불법적 컴퓨터 침투 방지를 위한 방화벽 설치요령과 실질적 보안 관리 대책 모색
보안관리 우수업체 사례	• 대기업 · 중소기업 · 정부출연 연구소 등의 우수 보안관리 사례 발표 및 토의

3.5 기타 민간교육기관의 정보보호 교육 현황

일부 교육기관을 제외하고는 대부분의 민간 교육기관에서 정보보안 관련 교육 과정은 정보보안 전문가양성을 위한 전문과정과 취업대비 정보보안관련 자격증과정이 대부분을 차지하고 있다. 중소기업을 위한 특화된 정보보안 교육 과정을 찾는 것은 어렵지만 일반적인 정보보안 담당자들을 위한 단기 실무 교육과정의 현황을 중심으로 살펴보면 다음과 같다.

3.5.1 한국정보보호교육센터

정보 보안관련 대표적인 민간 교육 시설인 한국정보보호교육센터(http://www.kisec.co.kr)에서는 정보 보안 관련 지식이 필요한 실무자들을 위하여 정보 보안 단기 교육과정과 더불어 보안 컨설팅 서비스를 운영하고 있다[표 8].

〔표 8〕 한국정보보호교육센터의 정보보안 교육과정 (2008. 8)

과정명	교육기간	비용(만원)
웹해킹/대응실무	5일	80
모의해킹및취약점분석실무	5일	80
해킹사고분석및컴퓨터포렌식	5일	80
침해 대응체계 구축 및 운용실무	5일	80
서버 보안시스템구축실무	5일	80
웹서버보안분석및설계	5일	80
PC보안 기술실무	5일	80
시스템해킹/대응실무	5일	80
암호기술 및 PKI	5일	80
악성코드제작및 분석기술	5일	80
Windows Internals	5일	89
리버스엔지니어링	5일	89
정보보안컨설팅	5회	120
윈도우 후킹	35시간	110
윈도우 내부구조	30시간	70
침해대응체계구축 및 컴퓨터포렌식	30시간	70
역공학분석	30시간	70
시스템해킹 대응실무	30시간	70
웹해킹 대응실무	30시간	70
자격증과정(SIS, CISSP)	5일	89

3.5.2 삼성 멀티캠퍼스

정보 기술 관련 민간 교육 기관인 삼성 멀티캠퍼스(http://www.multicampus.co.kr)가 제공하는 전체 교육 훈련과정은 난이도에 따라 입문/핵심/고급 과정으로 분류되어 있다.

[표 9]는 이중 정보 보안과 관련된 교육 과정으로서 대부분이 핵심 및 고급 과정에 해당한다. 즉, 교육 과정을 수강하기 위해서는 컴퓨터 및 정보 통신에 대한 초급 이상의 지식과 기술을 요구하고 있음을 알 수 있다.

〔표 9〕 삼성멀티캠퍼스 정보보안 관련 교육과정 (2008. 8)

과정명	수준	교육기간	비용(만원)
정보보호 기본	입문	4일	65
Windows서버 보안실무	핵심	5일	70
Network 보안실무	핵심	5일	75
Unix/Linux보안	핵심	5일	70
실무자를 위한 정보시스템보안	핵심	4일	65
보안 진단 및 침해사고 대응	고급	5일	75

3.5.3 한국 HP교육센터

정보 기술관련 민간 교육 기관인 한국 HP교육센터(http://education.hp.co.kr)의 정보 보안 관련 교육과정은 다음과 같다[표 10].

〔표 10〕 한국HP교육센터의 정보보안 관련 교육과정 (2008. 8)

과정명	교육기간	비용(만원)
최신해킹기술 및 방어기술	5일	80
네트워크정보기술	5일	80
정보보호컨설팅	4일	80
web hacking & security	3일	54
HP-UX Security I	5일	90
LINUX Network Security	5일	80
PC보안 기술 실무	2일	32
무선네트워크보안	2일	32
웹보안프로그래밍실무	5일	80
정보보호 솔루션 운영실무	5일	80
기업보안관리자실무	5일	80
Windows Server 2003 Security	2일	32

IV. 우리나라 중소기업의 정보보안 역량 강화를 위한 교육 훈련의 문제점

4.1 중소기업의 정보 보안 역량 강화에 대한 인식 저조

2008년 현재 한국산업인력관리공단은 '중소기업 핵심직무능력향상 지원사업'을 통하여 중소기업의 경쟁력 강화와 인적자원개발을 위한 핵심 과정을 선정하여 중소기업 사업주와 근로자의 교육 훈련을 유도하고 있다. 2008년 선정된 중소기업 핵심직무 분야는 [표 11]과 같

은 총 8개 훈련영역이며 각 영역별로 총 73개 훈련과정이 지원되고 있다.

그러나 중소기업의 경쟁력 강화를 위한 핵심직무 분야에서 기업의 정보 보안 (Information Security)과 관련된 직무가 고려되지 않은 결과 73개의 핵심직무훈련과정에서 중소기업의 정보보안관련 과정은 찾을 수 없다.

이미 미국, 유럽 선진국들이 자국 내 중소기업의 정보보안 역량이 국가 및 지역 전체의 사회적, 경제적 안전에 핵심적 요소임을 인식하고 발 빠르게 대응책을 마련하고 있는 것과 비교하여 우리나라는 아직까지 적극적 노력이 이루어지지 않고 있다고 볼 수 있다.

〔표 11〕 한국산업인력관리공단 '중소기업 핵심직무능력향상 지원사업'의 핵심직무 훈련 영역

훈련영역	훈련과정수	훈련영역	훈련과정수
전략경영	11	HRD리더쉽	13
인사조직관리	9	품질관리	7
영업마케팅유통	14	생산관리생산기술	6
재무회계	9	기술경영연구개발	4

4.2 중소기업의 정보 보안 역량 강화에 있어서 소기업 (small business)에 대한 인식 저조

앞서 언급한 바와 같이 우리나라 전체 산업체수 기준으로 약 96%가 소기업 및 소상공인 규모의 기업이다. 그러나 현재 중소기업청이나 국가정보원등의 중소기업의 정보 보안 역량 강화를 위한 각종 교육 훈련 및 지원사업에서 소기업 및 소상공인에 대한 인식과 배려가 미흡하다.

단적인 예로 중소기업청 중소기업기술정보진흥원이 2008년부터 제공하고 있는 중소기업을 위한 '무료 온라인 산업보안교육과정'은 '2007년 산업기밀관리실태조사' 결과를 바탕으로 산업기술 유출 방지의 필요성을 인식시키기 위한 교육내용으로 구성되어있다. 그러나 '산업기밀관리실태조사'의 조사대상을 살펴보면 부설연구소를 보유한 일반, 벤처, 이노비즈(Inno-BIZ), 벤처·이노비즈 인증 중소기업으로서 기계 소재, 정보통신, 서비스업, 건설업 등의 7개 업종, 서울, 경기, 충청, 영남, 기타의 5개 지역의 1200개 기업을 대상으로 하였다. 즉, 부설연구소를 거느리고 핵심 산업기술을 보유한 기업을 대상으로 한 것으로 이는 우리나라 전체 산업체수 기준 96%에 달하는 소기업 및 종사자 5인 미만 영세 소상공인과는 거리감이 있다.

또한 한국정보보호진흥원의 '정보보호실태조사' 역시 우리나라 5인 이상 종사자 규모의 기업체를 대상으로 정보보호에 대한 대책을 관리적, 기술적, 물리적 측면에서 조사하고 더불어 침해사건 사례와 피해 현황을 조사하였다.

국가정보원의 산업기밀보호센터의 경우 관리 대상은 국가로부터 인증 받은 '핵심 기술'을 보유한 기업이다. 즉 기업 부설 연구소를 가지고 있으며, 국가로부터 '핵심 기술'로 인증 받은 기술을 보유하고 있는 기업을 대상으로 보안 교육과 컨설팅을 제공하고 있다. 그러나 이러한 자격 조건은 소기업 또는 영세 소상공인에게는 벽이 높다고 할 수 있다.

인터넷과 같은 정보통신 네트워크의 특성상 개별 노드(node)의 보안 취약성은 언제든지 전체 네트워크의 피해로 확산될 수 있다. 또한 의료, 금융, 개인 정보와 같은 민감한 정보는 정보침해가 발생한다면 규모의 크고 작음을 떠나 사회 안전에 큰 타격을 가져올 수 있다.

그러므로 우리나라 산업 구조의 기저를 이루고 있는 소상공인과 소기업을 국가 정보 보안의 핵심 대상으로 새롭게 인식해야 할 때이다.

4.3 중소기업의 특성을 고려한 세분화된 정보 보안 교육 훈련 모델 연구 필요

중소기업의 경영, 조직 및 경영 환경적 특성 등을 고려한 세분화된 정보 보안 교육 훈련 모델에 대한 연구가 필요하다.

지금까지 대학 및 초중고 교육과정과 달리 실제 기업 경영 관점에서 요구되는 정보보안 교육 훈련에 대한 연구는 상대적으로 많지 않다. 그 결과 현재 중소기업청, 국가정보원 그리고 한국정보보호진흥원을 비롯하여 많은 민간 정보보안관련 교육 훈련기관에서 제공하는 중소기업을 위한 정보 보안 교육 및 훈련들을 살펴보면 내용 및 형식면에서 일관성과 체계가 부족하다고 할 수 있다.

중소기업을 위한 정보 보안 교육 훈련 프로그램 개발 시 내용 및 형식면에서 일반 사용자 보안과 기업 보안 특성이 모두 반영되어야하며, 또한 산업 스파이 등에 의한 기업기밀 유출 그리고 사이버 테러와 같은 다양한 보안 위협에 대한 균형적 고려와 요구된다.

더불어, 정보 보안 침해 사고 이후의 복구와 사후 대

책 등에 대한 기업 경영상 실제적인 가이드라인을 중소기업의 눈높이에 맞춰 제공할 수 있어야 할 것이다.

예를 들어, 중소기업 특히 소기업 및 소상공인 규모의 경우 내부 인력을 정보 보안 전문가로 훈련시켜 네트워크부터 시설 보안에 이르는 보안 실무를 기존의 업무와 병행하도록 하는 것은 쉽지 않은 일이다. 따라서 기업의 정보보안 업무를 전문 보안업체에 맡기는 아웃소싱이 늘어날 전망 아래 아웃소싱 과정 전반에 대해 감사(audit)와 평가(evaluate)할 수 있는 중소기업을 위한 가이드라인이 필요하다.

V. 결 론

보안은 유·무형의 인적·물적 자산에 대한 인가되지 않은 유출, 변조, 훼손, 삭제를 방지하는 기술적 · 관리적 수단이다. 현재의 기업 경영 환경에서 내 · 외부의 불법적인 보안 침해 시도로 부터 보호해야 하는 대상은 생산 설비부터 사내 컴퓨터 시스템 내 파일 그리고 소속 인력에 이르기까지 매우 다양하다.

중소기업의 정보 보안 역량 강화를 위해서는 먼저 정보 보안 교육 훈련 관점에서의 중소기업의 특성에 대한 연구가 요구되며, 기업의 규모, 업종, 성격 등에 따라 차별화된 교육 훈련 모델이 개발되어야한다. 또한 정보 보안 환경의 동적인 특성상 지속적인 보안 경보 및 대응 기술에 대한 정보가 신속히 전달되고 조치되어야한다. 특히, 소기업과 소상공인의 비중에 대한 인식을 제고하고 이들의 보안 역량 강화와 경보 및 대응 체계에 대한 연구가 필요하다.

참고문헌

[1] United Sates Government Accountability Office (U.S. GAO), "INTERNET SALES: Undercover Purchases on eBay and Craiglist Reveal a Market for Sensitive and Stolen U.S. Military Items", United Sates Government Accountability Office (U.S. GAO) GAO report number GAO-08-644T, April 10 2008.

[2] 통계청, 2006 사업체기초통계조사, 통계청 국가통계포털 (KOSIS), 2007.

[3] Marco Thorbruegge, Slawomir Górniak, "EISAS-European Information Sharing and Alert System A Feasibility Study 2006/2007", European Network and Information Security Agency (ENISA), 2008.

[4] 유진호, 지상호, 송혜인, 정경호, 임종인, "인터넷 침해사고에 의한 피해손실 측정", *정보화정책*, 한국정보사회진흥원, 제15권 제1호, pp. 3-18, 2008.

[5] 한국정보보호진흥원, "2007 정보보호 실태조사-기업편", 정보통신부, 한국정보보호진흥원, 2007.

[6] "2008 국가정보화 백서", 한국전산원, 2008.

[7] 김경규, 류성렬, 신호경, 김문선,"정보화 발전모형 기반의 중소기업 정보화 수준평가: 중소제조업을 중심으로", 중소기업연구, *한국중소기업학회*, 제29권 제2호, pp.41-71, 2008.

[8] 김재윤, 이훈희, 이정우, "중소기업의 정보화 성공요인에 관한 근거이론적 연구", *중소기업연구*, 한국중소기업학회, 제26권 제4호, pp.1-22, 2004.

[9] 이재관, 김선희, "정보 리터러시가 소상공인의 온라인 활동 수준에 미치는 영향", *중소기업연구*, 한국중소기업학회, 제 29권 제1호, pp. 49-64, 2007.

[10] 김종우, 이지우, 백유성, "소기업의 응집력, 과업의 존성, 협력 및 성과간의 관계", *중소기업연구*, 한국중소기업학회, 제17권 제3호, pp.99-122, 2005.

[11] 이계우, "중소기업 훈련 컨소시엄사업을 위한 정부 정책의 효율성", *중소기업연구*, 한국중소기업학회, 제27권 제2호, pp. 175-203, 2005.

[12] "사이버범죄유형", 경찰청 사이버테러대응센터, 2008.

[13] "기밀유출 현황", 국가정보원 산업기밀보호센터, http://www.nisc.go.kr/docs/nisc/drain/analysis.php, 2008.

[14] "A Users' Guide: How to Raise Information Security Awareness", European Network and Information Security Agency (ENISA), 2008.

[15] "SBC Computer Security Workshop", Small Business Corner(SBC), National Institute of Science and Technology(NIST), http://csrc.nist.gov/groups/SMA/sbc/workshops. html, 2008.

[16] The European Parliament and the Council of the European Union, "Decision No 1639/2006/Ec of the European Parliament and of the Council of 24 October 2006 establishing a Competitiveness and Innovation Framework Programme (2007 to

2013)", *Official Journal of the European Union*, L310/15-L310/40, 2006.

[17] "IT-Sicherheit Für kleine und mittlere Unternehmen", *Eine Schriftenreihe der SAP AG*, SAP AG, 2005.

[18] 오창규, 김종기, "효과적인 정보보호 교육 및 훈련을 위한 프레임워크 개발", *정보보호학회지*, 제13권 제2호, pp. 59-69, 2003.

[19] 김기윤, 나현미, "정보보호관리자에 대한 직무분석", *통신정보보호학회지*, 제10권 제3호, pp. 63-74, 2000.

[20] 송철복, "정보보호 단기 교육과정", *정보보호학회지*, 제13권 제2호, pp. 26-31, 2003.

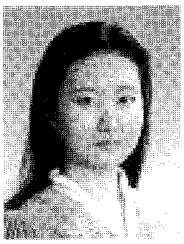
[21] 양정모, 이옥연, 이형우, 하재철, 유승재, 이민섭, "대학의 정보보호 관련학과 교육과정분석과 모델 개발에 관한 연구", *정보보호학회논문지*(2003.6), pp.18-26, 2003.

[22] 류희수, "초등 정보보호 교육과정 분석", *정보보호학회지*, 제14권 제6호, pp.62-69, 2004.

[23] 이민섭, "정규학교에서의 정보보호교육 강화 방안", *정보보호학회지*, 제13권 제6호, pp.67-78, 2003.

[24] 이형우, 이민섭, "정보보호 인력양성 방안에 관한 연구", *정보보호학회지*, 제13권 제2호, pp. 70-80, 2003.

〈著者紹介〉



문현정 (Moon, Hyun Jeong)
정회원

1995년 2월: 숙명여자대학교 전산학과 졸업
1997년 2월: 숙명여자대학교 전산학과 석사
2002년 2월: 숙명여자대학교 컴퓨터과학과 박사
*국제공인정보시스템보안전문가 (CISSP)
<관심분야> Business Contingency Planning, Security Resilience, Artificial Intelligence