산업보안의 제도적 발전방안 연구:
미국 사례를 중심으로

A Study on the Institutional Improvement Directions of Industrial Security Programs:
Focused upon Policies and Practices in the U.S.

최 진 혁*

<목 차>

<요 약>

최근 산업기술·기밀의 유출로 인한 국가적·경제적 손실이 심각한 상태이고 이러한 유출은 특히 전·현직 직원과 같은 내부자에 의해서 가장 빈번하게 발생하는 것으로 나타나고 있다. 또한 산업스파이 뿐만 아니라 해킹이나 도청과 같은 기술적인 방식 등 다양한 형태로 유출이 이뤄지고 있으며, 때로는 타국의 국가기관도 개입할 개연성이 있어 이러한 문제에 대해 개별 민간기업의 노력만으로는 효과적으로 대응하기 어려운 상황이다.

이처럼 국내 산업기술·기밀의 유출이 국가경제·국익에 심각한 악영향을 미치고 기업 차원의 노력만으로는 근본적인 유출·침해의 방지가 어렵다는 사실을 감안할 때 이러한 문제를 해결하기 위한 국가 차원의 다각적이고도 체계적인 노력들이 시급히 요구되는 상황이라고 할 수 있겠다. 이에 대한 논의로 무엇보다 산업보안의 중요성에 대한 인식의 전환과 적극적인 대처가 우선적으로 필요하다고 보았다.

미국의 경우 영업비밀 유출 문제를 '국가안보'와 직결되는 개념으로 받아들여 범국가적·정부 주도의 산업보안 프로그램과 대응체계를 구축하여 운용하는 등 국가가 적극적 개입을 하고 있을 뿐만 아니라 민간 부문과도 유기적인 협조체제를 유지하고 있다. 이 연구에서는 특히 제도적·정책적 측면에서 미국의 산업보안 대응체계 사례를 중심으로 분석한 후 이를 바탕으로 국내 산업보안의 문제점을 인식하고 향후의 제도적 발전방안을 제시해 보고자 하였다.

* 경찰대학교·용인대학교 외래교수 / 한국기업보안협의회 부회장.

이 연구를 통해 도출한 시사점은 먼저 산업보안에 대한 인식의 측면에서 사회 전반적 인식이 부족하고 그 이해가 왜곡되거나 정부 차원의 투자・지원이 편향되어 있는 점을 지적하였다. 또한 산업보안과 관련한 정부의 체계적인 관리 및 조정기관・프로그램의 운용, 중소기업에 대한 보안관리 체제 구축 지원, 그리고 전문인력 양성 및 학술적 연구 확산 등에서 문제점과 개선의 필요성을 인지하였다.

따라서 산업보안에 대한 사회 전반적인 인식의 향상, 산업보안 프로그램에 대한 국가의 주도적 역할과 더불어 일관성 있는 정책적・제도적 방안의 마련, 중소기업의 산업보안 실태 개선을 위한 체계적인 지원, 보안시장의 변화 요구에 부응할 수 있도록 산업보안 관련 학과 개설 및 실무 중심의 교과과목 편성, 그리고 집중적 교육을 통한 '수요자 맞춤형 보안 전문인력'의 양성과 산업보안 전문가・강의자원(Pool)의 확보, 산업보안 문제를 조정하는 국가기관이나 전담기구의 설립 및 실효성 있는 민・관 협동체제의 구축 등을 제도적 발전방안으로 제시하였다.

주제어 : 산업보안, 산업기밀 유출, 경제스파이, 영업비밀 보호, 산업보안 프로그램, 보안 전문인력

I. 머리말

최근의 국가정보원(2009) 통계자료에 의하면 2004년부터 2008년까지 5년간 산업기밀·기술 유출 적발 건수 및 그에 따른 추산 피해(예방액) 규모가 160건(549명)에 무려 253조 4,500억 원에 달하며, 2003년 6건에 그쳤던 산업기술의 해외유출 적발 건수도 해마다 늘어나 2007년 32건, 2008년에는 42건이나 되어 2007년 대비 31%나 증가한 것으로 나타났다.[1] 한편으로는 반도체·전자·통신 등 IT(Information Technology: 정보기술) 분야에서 주로 발생했던 산업스파이(Industrial/Economic Espionage)[2] 사건이 자동차·조선·철강 등 한국이 세계적인 경쟁력을 갖고 있는 제조업으로도 빠르게 확산되고 있는 것으로 분석되었다.

2005년 이후 한국의 기술력 수준과 국제특허 출원 건수가 세계 선도적 지위로 올라섰고, 국가 R&D(Research & Development: 연구·개발) 규모 역시 그 동안 괄목할 만한 성장을 해왔다. 이렇듯 국가 경제규모가 커지고 첨단기술의 보유가 늘어나면서 국가 핵심기술, 산업기밀, 그리고 영업비밀의 보호는 국가경쟁력에 있어 매우 중요한 역할을 하고 있다. 따라서 경쟁자나 적으로부터 중요한 산업·핵심기술이나 기업의 기밀정보를 보호하는 것은 그 생성 못지않게 현대 지식정보화 사회에 있어서 중요도가 매우 높다고 할 것이다.

그러나 한편에서는 외국계 기업에 대한 기술 이전이나 국내 기업의 해외 매각, 또는 해외 현지에서의 합작투자나 생산을 통한 우회적 기술 유출 등이 오히려 한국의 국익과 국부를 위협하고 있는 실정이다. 특히 일부 기술이나 산업의 경우 경쟁국·후발국과의 기술적 격차가 날이 갈수록 좁혀지거나 없어짐으로 인해 한국의 국가 경쟁력과 미래 산업 전망에 잠재적으로 불안한 그늘을 드리우고 있는 것이 현실이다.

한국의 경우, 벤처기업으로 위장한 KSTC(Korea Semiconductor Technology

---

1) 자료: 국가정보원 산업기밀보호센터 기술유출 현황 사건 분석 통계 [http://service4.nis.go.kr/docs/nisc/drain/analysis.php].

2) 산업스파이(Industrial Espionage)의 개념 및 의의와 관련해서 다양한 의견들(Barr, et. al., 2003; 이윤호, 2004; 민수홍·이민식, 2006; 한상훈, 2000; Sepura, 1998 등)이 제시되고 있는데, 일반적으로 산업스파이는 국가안보의 목적보다는 상업적(경제적) 목적으로 수행되는 것으로서 산업기밀이나 핵심기술 등을 비밀리에 입수하기 위해 상대국 기업을 대상으로 스파이(Spy) 활동을 전개할 때 산업스파이 또는 경제스파이(Economic Espionage)라고 칭한다. 이 연구에서는 산업스파이를 경제스파이와 동의어적인 관점에서 그 개념을 정의해서 사용하려는 바, "산업스파이란 파견 주체가 누구인지와는 상관없이 경제적 목적으로 상대국의 기업이나 특정 기관이 소유하고 있는 물품의 제조방법, 판매방법, 기타 산업상·영업상 유용한 기술이나 경영정보 등 산업체의 업무에 관한 비밀--영업비밀이나 산업기밀 등--을 불법적으로 입수하거나 정탐하는 일체의 범죄행위"(한상훈, 2000: 15)로 정의할 수 있겠다.

Company)社의 간부들이 1997년 5월부터 1998년 2월초에 걸쳐 삼성·LG반도체의 전·현직 연구원 14명을 통해 첨단 반도체 기술을 빼내어 대만 기업(Nanya Technology Inc.: NTC)에 유출한 사건[3]이 산업스파이로 인한 피해의 대표적 사례다. 이로 인한 추정 피해액이 자그마치 1조 2천 5백억 원에 달할 뿐 아니라 그 범행 대상이 한국이 세계적 경쟁력을 갖고 있는 반도체 제조기술이라는 점 등으로 인해 사회적으로 큰 반향을 불러일으켰고(한상훈, 2000: 15), 이 같은 사례에 보다 효율적으로 대처하기 위해 관련 법률을 보완·개정하는 계기가 되기도 했다.

지난 몇 년간의 사례를 살펴보면 대부분의 기술 유출이 기업·기관 내부자나 퇴직자들을 통해 이뤄지고 있고, 특히 외환위기를 겪고 난 2000년 이후에는 평생직장 개념이 무너지면서 기업의 중역들까지도 핵심기술을 유출하려는 시도가 종종 적발되고 있는 실정이다. 또한 최근의 계속되는 국내외 경제 침체와 기업들의 구조조정 등 사회적·경제적 불안정으로 인해 도덕적 해이(Moral Hazard) 현상이 심화되면서 산업스파이 행위의 증가를 촉발하고 있다.

최근 국가정보원과 검·경찰, 그리고 언론 및 학계의 지속적인 홍보와 노력과 더불어 기업뿐만 아니라 대다수 국민들이 산업기밀·핵심기술 보호에 대해 보다 관심을 가지게 되었으며 그 대응방안에 대해서도 다각적으로 연구되고 있다. 그러나 대부분의 연구가 산업보안에 대한 심층적인 기술·분석이나 발전적 대안의 제시보다는 주로 기업 영업비밀 보호나 지적재산권과 관련한 단속법규나 법적 보호 등을 위주로 연구가 이루어지고 있는 실정이다. 그 결과 실제 산업보안 영역에 적용시키거나 산업기밀 유출 방지를 위해 효과적으로 접목·활용할 수 있는 실증적이고 실용적인 연구 결과의 도출로 원활하게 연결되지 못하는 한계가 있었다.

따라서 이 연구는 날로 증가하고 있는 산업기술·기밀 유출의 방지 및 산업보안 활동의 효과성 제고를 위해 특히 정책적·제도적 측면에서의 발전방안을 미국의 사례를 중심으로 검토해보고, 이러한 분석결과를 토대로 향후 산업보안의 활성화와 효율적인 산업기밀 유출방지대책과 같은 정책적 대안 마련을 위한 적시성 있는 시사점을 제시하려는데 그 주된 연구의 목적을 두고 있다.

---

3) 前 삼성반도체(現 삼성전자) 반도체총괄팀에서 퇴사하여 KSTC(Korea Semiconductor Technology Company)社 이사로 근무하던 정모씨가 1997년 7월부터 11월까지 삼성·LG반도체 前 직원들을 영입해 삼성반도체의 영업비밀인 64메가 DRAM 회로도 등의 기밀문서를 KSTC 사무실 내의 워크스테이션에 입력한 후 Data Cartridge Tape에 저장하여 대만의 NTC(Nanya Technology Inc.)사에 그 일부 출력도면을 건네줌으로써 영업비밀을 누설한 사건으로, 주범인 정모씨는 2004년 12월 미국으로부터 강제송환 되었으며 기소된 14명은 특정경제범죄 가중처벌 등에 관한 법률 위반(업무상 배임)·절도·부정경쟁방지법 위반 등의 혐의로 유죄 확정 판결 [대법원, 1999.3.12, 98도4704].

Ⅱ. 이론적 배경

1. 산업보안의 개념 및 중요성

일반적으로 산업보안(Industrial Security)[4]은 광의의 개념으로 국내에서는 특별히 구체화된 개념적 정의를 찾아보기 어려우나, 연구자는 기업・기관 등에서 행하는 보안활동(Security Programs)을 산업계 전반으로 확산하여 국가의 핵심기술이나 중요 산업기밀 또는 기업의 영업비밀 등을 보호하기 위한 제반 예방적・보호적 활동(Programs)을 포괄하는 것으로 정의하였다. 여기서 보안활동(Security Programs)[5]이란 내부 주요 자산(Asset)--인적자원, 정보・기술, 물적 자원--을 보호하기 위한 제반 체계들을 총체적으로 의미하는데, 이는 핵심기술이나 기밀정보의 유출을 차단하기 위한 활동뿐만 아니라, 인적 자원을 보호하고, 물적 자산의 손실・파괴를 막고, 위험(Risk)을 예방하거나 손실(Loss & Damage)을 최소화하기 위하여 행하는 일련의 활동들을 총칭하는 개념이다.[6]

한국산업기술진흥협회(KOITA)가 2006년 발표한 '기업연구소 산업기밀 관리실태'에 따르면 전체 조사대상 459개 기업 중 20.9%가 기밀유출 피해를 경험했다고 응답하였는데, 대기업의 경우 평균을 웃도는 24.5%가 피해를 입은 것으로 조사되었고 중소기업과 벤처기업은 각각 20.6%, 19.3%가 유출 피해를 경험한 것으로 집계되었다.[7] 한편, 한국산업기술보호협회(KAITS)가 2008년 1,176개 산업기술 보유기관(기업체・대학・연구소 등)을 대

---

4) 흔히 '산업보안'과 '기업보안' 간에 개념적 혼재가 일어나고 있으나 산업보안이란 국가 핵심기술과 산업・경영정보의 해외 유출을 막고 산업스파이를 예방하기 위한 법적・제도적 정비 과정에서 보호의 대상을 기업뿐만 아니라 모든 국가기관・정부출연기관・연구기관 등을 포괄하는 용어로 사용된다고 할 것이므로 구체적인 개념 정의와 영역의 구분은 이 연구에서 크게 실익이 없다고 보았다.

5) 현재 국내에서 보안활동(Security Programs)에 대한 명확한 정의나 체계화된 분류를 찾기 어려운 관계로 연구자가 그간의 국내외 학술적 연구, 미국산업보안협회(American Society for Industrial Security) 전문과정과 영국 유학과정에서 획득한 자료, 국제형사경찰기구(INTERPOL)와 대통령 경호실(現 대통령실 경호처) 및 경찰청에서의 직무 경험, 그리고 글로벌 IT 기업과 국내 대기업 보안관리자로서의 실무 경험을 바탕으로 다음과 같이 분류해 보았는데, 일반적으로 보안활동에는 인적・환경적 보안요소 및 전자기적 보안시스템을 포함하는 물리적 보안(Physical Security), 위험[영향]평가(Risk Assessment), 정보보호(Information Protection), IT보안(IT Security), 비상기획(Emergency Planning & Response), 위기・재난관리(Crisis/Disaster Management), 사업 연속성 계획(Business Continuity Planning), 테러 예방 및 사업장 내 폭력 방지(Counterterrorism & Workplace Violence Measures), 사건・사고 관리 및 조사(Incident Management & Investigations), 보안교육・컨설팅(Security Education & Consulting) 및 보안감사(Security Reviews & Audits) 등 다양한 프로그램들이 포함된다.

6) 이 연구에서는 '부정경쟁방지 및 영업비밀 보호에 관한 법률' 상의 '영업비밀(Trade Secrets)'과 '산업기술유출 방지 및 보호에 관한 법률' 상의 국가 핵심기술 등이 포함되는 '산업기술'을 산업보안의 주요한 개념적 범주이자 산업보안 활동의 주요 대상으로 하였다.

7) 자료: "산업기밀 유출 방지 위한 융합보안 모델" [보안뉴스, 2009, http://www.boannews.com/media/view.asp?idx=19043&kind=1# / 2009. 12. 28].

상으로 설문조사한 결과, 종업원 1,000명 이상 기업의 보호수준이 가장 높게 나타났고 기업의 규모가 작을수록 보호수준이 낮게 나타났다(이창무, 2009: 66). 그리고 중소 벤처기업의 기술유출이 전체의 64%를 차지하고 있었는데, 이는 중소 벤처기업의 기술력은 향상되는 반면 보안관리시스템이 대기업에 비해 상대적으로 허술하기 때문으로 분석된다(국가정보원, 2009: 14).

한편 세계 보안시장의 추이(Trend)가 일상생활 속의 '지식정보보안(Knowledge-Information Security)' 영역으로 급속하게 진화・확대되고 있어 미국과 EU(유럽연합) 등 선진외국들은 이러한 새로운 패러다임(Paradigm)에 맞는 보안산업의 육성과 관련 분야의 경쟁력 강화에 재빠르게 주력해오고 있다. 한국 지식경제부도 2008년 12월 "지식정보보안산업 [5개년] 육성계획"을 발표하여 지식정보보안산업을 미래 경제를 이끌어갈 신성장 동력으로 지목하면서 정보보안, 물리보안, 융합보안을 포함하는 지식정보보안 시장 규모를 확대하고 한국을 보안산업 강국으로 육성하겠다는 의지를 표명하였다.[8)]

이와 같이 보안산업이 날로 성장하고 그 분야와 시장 규모도 확대되고 있지만 무엇보다 선행되어야 할 중요한 점은 바로 산업기술・기밀의 유출로 인한 막대한 경제적 손실과 국가경쟁력 약화 및 국제 자본 유치에 미칠 악영향을 미연에 방지하는 것이다. 최근 경제전쟁이 날로 치열해지면서 산업기술・기밀의 유출 사고도 급증하고 있는 상황인바, 이제는 기업의 범주를 넘어 국가적 차원에서 국가 경쟁력 확보를 위해 핵심기술 및 영업비밀・기밀정보 등에 대한 보안의 중요성이 나날이 커지고 있다.

2. 국내 산업보안 현황

기업은 영업비밀과 보유하고 있는 영업비밀이나 기술 및 중요 정보를 보호하기 위해 보안체계를 정비하고 내부규정을 보완하여 보안 또는 정보보호 책임자를 지정하는 등 자구적인 노력을 강구하여야 함에도 불구하고 보안관리 규정이나 보안관리자를 지정・운용하는 기업・연구소・기관의 비율이 높지 않아 기술・기밀 유출로 곤란을 겪는 경우가 많은 것이 현실이다. <표 1>에서 볼 수 있는 바와 같이, 국가정보원(2009) 자료에 의하면 2004년부터 2008년까지 적발된 160건의 기술유출 사건 중 유출 주체가 퇴직(전직)사원인 경우가 가장 많은 89건으로 55.6%였고, 현직 사원이 43건으로 26.9%, 그리고 협력업체가 16건으로 10%의 순으로 나타났는데, 주목할 부분은 전・현직 사원이 모두 132건으로 전체의 82.5%에 달해 유출의 주된 경로인 것으로 드러났다.

---

8) 자료: "2013년, 지식정보보안산업 3조 → 18조 시장으로!" [보안뉴스, 2008, http://www.boannews.com/media/view.asp?page=1&idx=13173&search=key_word&find=kisia / 2008. 12. 15].

<표 1> 기술유출 주체별 분석 및 유출의 유형 (2004~2008)

구 분	건수	%	구 분	건수	%
퇴직직원	89	55.6	매 수	89	55.6
현직직원	43	26.9	무단보관	30	18.75
협력업체	16	10	내부공모	17	10.6
유치 과학자	6	3.8	공동연구	9	5.62
투자업체	3	1.85	위장합작	6	3.8
기 타	3	1.85	기 타	9	5.62
계	160	100%	계	160	100%

국가정보원 산업기밀보호센터(2009) 자료를 중심으로 재구성

1) 법적 규제(처벌) 측면

KSTC/NTC 사례의 경우 그 추정 피해액이 1조 2천 5백억 원에 달했고 산업기술 유출에 대한 전 국민적 경각심을 불러일으킨 중요한 사건이었지만, 동 사건의 피의자들 중 2명에게만 실형이 내려졌고, 1명은 무죄, 나머지 16명에게는 집행유예가 선고될 정도로 그 법적 처벌이 피해의 심각성에 비해 너무나 미약한 수준이었기 때문에 첨단기술 유출과 관련한 국내 실정법의 실효성에 대하여 의문이 제기되기 시작하였으며, 미국이나 영국 등 선진국들의 주요 기술의 해외유출에 대한 대처방식을 비교・검토하여 보다 효과적인 대응 수단을 강구해야 한다는 인식이 제고되는 계기가 되었던 것이다(표창원, 2003: 28).

현재 영업비밀 보호 및 산업기술 유출 방지 등 산업보안과 관련한 국내의 형사적 규율은 '부정경쟁방지 및 영업비밀보호에 관한 법률'과 '산업기술 유출 방지 및 보호에 관한 법률' 외에도 형법 등 여러 법률에 존재한다. 그러나 영업비밀을 보호하는 형법상의 여타 규정은 상기 법령에서 다루지 못한 영업비밀 침해의 수단이나 방법 등을 처벌할 수 있고 그 형량의 적용에 있어 가중처벌도 가능하다는 점에서는 의미가 있지만, 보다 직접적인 보호와 실효성 제고를 위해서는 현행 산업보안 관계법의 개선 및 처벌의 강화가 중요하다는데 많은 학자들이 의견을 같이 하고 있다(김재봉, 2002: 34; 한상훈, 2000; 곽경직, 1998).

2) 제도적・정책적 측면

현재 지식경제부, 국가정보원, 방송통신위원회, 중소기업청, 검・경찰 등에서 국가 핵심기술 및 산업기밀 보호를 위한 정책과 활동이 시행되고 있기는 하지만 유기적 협력을 통한 시너지 효과(Synergy Effect)의 창출 보다는 각 기관의 독자적 활동으로 인한 비협력과 때로는 경쟁으로 인해 오히려 국가적 자원을 낭비하는 결과를 초래하고 있다. 이는 효과적인

산업보안 정책의 집행에 제동을 걸 것이며, 더구나 이러한 현상이 계속될 경우 각 정부 부처에 의해 양산되는 독립적인 정책들로 인해 기업의 피로도는 점점 가중될 수밖에 없는 바, 아직은 산업보안 체계의 정착 및 활성화에 있어 국가 제도적・정책적 측면에서의 가시적인 효과는 보이지 않는 실정이다.

요약컨대, 국가경제 및 국가안보의 차원에서 산업보안 활동이 수행되어져야 함에도 불구하고 전반적인 산업보안 의식이 부족과 함께 범국가적 차원에서의 적극적인 대처가 미흡했다고 볼 수 있다. 그리고 정부 주도의 산업보안 프로그램 운영이 허술하다는 점, 산업보안 기능의 조정기관이 부재하여 산업기밀 유출에 대한 대응 정책들이 효율적으로 연계되지 못하고 있다는 점도 문제점이라고 하겠다. 따라서 전체적으로 산업보안의 중요성에 대한 국가 차원에서의 재조명이 필요한 시점이라고 여겨지며 기존의 체계적이지 못하고 단편적인 보안 프로그램 운영의 한계점을 극복해야 할 필요가 대두되고 있는 것이다.

3) 경영관리적 측면

(1) 인적 보안 문제

산업보안에 있어서 특히 기술 유출과 관련하여 인적 자원 관리를 언급할 때 고려해야 할 사항은 (기술)인력의 이동에 부수되는 잠재적 기술 유출과 전・현직 직원 등에 의한 기업 내 특정 기밀의 유출을 구분해야 한다는 것이다. 왜냐하면 기술유출 방지를 위한 기업의 노력은 잠재적으로 우수 인재의 이동 제한까지 포함하려 할 수도 있지만, 그러한 수준에서의 논의는 자칫 자유로운 개인의 이윤 추구 활동과 직업 선택 및 전직(轉職)의 자유를 침해하는 결과를 낳을 수 있기 때문이다. 따라서 경영관리적 측면에서 인적 보안 문제에 대한 검토는 전・현직 직원에 의한 산업기밀・기술 유출 방지 측면에 국한해서 살펴보는 것이 타당할 것이다.

국가정보원(2009) 통계를 살펴보면 산업기술・기밀은 주로 기업 내부인에 의해 누설[9]되는데 이는 전・현직 직원 및 거래 관계자 등에 의한 누설이나 유출 등을 방지하기 위한 체계적인 보안관리가 부족하기 때문이다.[10] 특히 그나마 보안 관련 인력의 확보나 재원 조달 측면에서 비교적 양호한 환경을 보유한 대기업을 제외한 대다수 중소기업이나 연구소 등의

9) 국가정보원(2009) 자료에 의하면 2004년부터 2008년까지 적발된 160건의 기술유출 적발 사례 중 유출의 주체가 전・현직 사원이었던 경우가 모두 132건으로서 전체의 82.5%에 달해 전・현직 사원이 유출의 주된 경로인 것으로 드러났다.

10) 과거 정보통신부와 한국정보통신수출진흥센터에서 공동으로 주관하였던 “IT기술 해외유출 방지협의회 1차 회의(2003)”에서 발표된 바에 따르면, 국내 149개 기업을 대상으로 한 조사 결과, 보안관리 규정을 보유하고, 보안관리자(담당자)를 배치하여, 보안 관련 점검을 실시하는 기업은 각각 전체의 67.2%, 62.6%, 45% 정도인 것으로 드러났다. 또한 임직원 보안서약을 받는 기업은 77.2%, 퇴직자 [기밀준수] 서약을 받는 기업은 61.2%, 거래처로부터 [기밀준수] 서약을 받는 기업은 71%, 보안 관련 교육경험을 받은 기업은 35.5%로 나타났다(표창원, 전게서: 54).

경우 실질적인 보안관리 실태는 상당히 열악하다고 할 것이다. 이처럼 사실상 기업의 비밀을 지키는 주체도 사람이고 침해·위해를 가하는 주체도 사람이므로 인적 자원의 적정한 관리는 보안의 주요한 목표 중 하나이자 기본적인 내용이라고 하겠다.

⑵ 산업보안 프로그램에 대한 이해 미흡

현대의 다양한 산업보안 활동 중 물리적 보안의 경우를 예를 들면, 기업이나 기관의 전반적 시설과 구조물에 대한 보호는 물론, 내부에 잠재되어 있는 유·무형의 정보 가치와 정상적인 관리·운영까지도 보호함을 목적으로 한다. 이는 보안방벽을 이용하거나 제한·통제구역 같은 특별히 보호되는 구역을 설치하고 시설물에 대한 차폐, 시정장치를 하는 등의 단순한 물리적 격리·보호에서 한 단계 더 나아가 도·감청의 방지, 출입자의 통제, 중요한 인적 자원에 대한 보호, 시설물의 위장, 통신·네트워크 시설에 대한 보안, 서류함·우편물 및 복사물 보안, 데이터 입·출력 관리, Critical Facilities--전력 공급원이나 소방시설 등--관리 등과 같이 보다 다각화되고 적극적인 보안상의 관리를 포함하는 개념이다.[11]

국내 일부 대기업의 경우 기밀문서에 대한 보안 수준은 최첨단을 달리거나 매우 엄격한 보안상의 규정을 적용하고 있기도 하지만[12] 전반적인 보안 프로그램에 대한 이해나 체계적인 관리 및 실효성 있는 운영 부분에 있어서는 아직도 미흡한 실정이다. 산업보안 프로그램이 기업의 영업비밀 유출과 직접적으로 관련되는 매우 중요한 사항이라는데 대한 기업들의 인식·이해 부족, 그리고 단순한 보안기술의 구현이나 외형적인 보안시스템의 설치에만 주로 의존하고 있는 보안체계의 구성 및 적용상의 미비는 한국사회에 있어서 보안의식의 결핍과 기술유출 위험에의 노출 상황을 잘 보여주는 단면이라고 하겠다.

⑶ 보안의식의 부족

앞에서 설명한 인적 자원의 관리나 체계적인 산업보안 프로그램의 운영도 중요하겠지만 산업기술·기밀의 유출과 관련한 문제점으로 가장 근본적인 것은 바로 전반적인 보안의식(Security Awareness)의 부족이라고 하겠다. 보안의식의 부족과 관련한 근거로는 다음의

---

11) 예컨대, 정보자료에 대한 보안관리의 경우 문서, 도면, 사진, 마이크로필름, 녹음·녹화테이프, 자기테이프, 천공테이프, 휴대용 USB 메모리 저장장치를 등의 각종 저장매체(Media)에 이르기까지 다양한 형태의 보안상 고려가 필요하며, 보호 대상 정보의 무단복제나 훼손·변조의 방지, 그리고 사후 원천적 폐기 절차 등을 위한 프로세스까지도 포괄하는 특별한 주의가 필요하다. 최근에는 IT 기술 기반과의 접목을 통한 정보보호 활동까지도 포함하면서 그 영역을 넓혀가고 있다.

12) S전자의 경우 신기술 프로젝트 진행 시 '3불(3不)' 원칙이 있는데, 첫째, 특수 종이로 제작되어 복사가 불가능하고, 둘째, 프린터 출력이 안 되며, 셋째, 연구원 컴퓨터는 개인별 스마트 카드(Smart Card)가 없으면 작동되지 않는다는 것이다(자료: 한국경제, 2003, "철통보안 24시," http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=101&oid=015&aid=0000670121/ 2003. 12. 22).

두 가지 부정적 인식에 기인한다. 그 첫째는 보안관리를 할 만한 가치가 있는 기술이나 정보가 없다고 보기 때문이라는 것이고, 둘째는 보안을 부수적이고 2차적이며 생산성이 없는 비용 지출성 업무로 인식하기 때문이다. 실제로 지난 5년간의 산업보안 관련 통계자료를 분석해보면 대부분의 기업 형태에서 퇴직(전직) 사원이 기업의 기밀이나 영업비밀 유출의 주된 경로로 나타나고 있으며, 현직 사원과 협력업체 직원이 그 뒤를 잇고 있어 산업기밀 유출 사건·사고의 대부분이 경쟁업체 종사자 보다는 기업 내부인 또는 관련자에 의해 이루어지고 있음을 알 수 있었다(국가정보원, 2009; 한국산업기술진흥협회, 2009).

Ⅲ. 미국의 산업보안 대응 체계

한국의 경우 불과 십여 년 전까지만 해도 다른 개발도상국과 마찬가지로 선진국으로부터 첨단기술을 도입하고 모방해야 할 필요성 때문에 기술유출 방지 대책 마련에 그리 큰 관심을 가지지 않았던 것이 사실이다. 하지만 이미 여러 분야에서 기술우위국의 위치에 올라 선 한국의 현재 위상에서 효과적인 기술유출 방지대책 마련의 필요성과 적절한 산업보안 프로그램 구축의 절실함은 이제 모두가 공감하고 있는 바이다. 그러나 산업기술과 영업비밀 유출 방지를 위한 잘 정비되고 체계적인 법과 제도를 구비한다는 것이 결코 쉬운 일만은 아닐 것이다. 여기서는 산업기술이나 영업비밀의 유출 방지를 위해 국가 안보적 차원에서 접근하면서 가장 적극적으로 국가(정부)가 개입하고 있는 미국의 산업보안과 관련한 제도적·정책적 측면에서의 대응 체제를 살펴보고 주목할 만한 시사점을 도출해 보고자 한다.

1. 산업보안에 대한 정책적 고려

미국에서는 산업보안의 핵심을 '영업비밀(Trade Secrets)'에 대한 보호에 두고 이를 국가안전보장과 연계된 차원에서 이해하고 있다. 즉, 영업비밀의 유출은 국부의 손실을 의미하고 이는 궁극적으로 '미국의 국가안보에 대한 위협(Threat to U.S. National Security)'[13]으로 이어진다는 인식이 영업비밀 보호활동의 출발점이 되고 있는 것이다. 미국 연방정부의 주도로 영업비밀을 보호하기 위한 각종 시책을 시행하거나, 국가 정보기관의 방첩(Counter-intelligence) 역량의 우선순위를 산업스파이 행위의 예방과 단속에 두고 있는 실정은 이러한 미국의 안보적 관점에서의 산업보안에 대한 인식을 반영하는 것이라고 하겠다.[14]

---

13) NCIX(National Counterintelligence Executive): Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, January 2002.

14) 미국 FBI(연방수사국)는 [2003년] 국내 방첩활동의 방향을 기술정보 보호에 맞춰 전면 수정하고, 전국

미국의 안보관에 대한 이 같은 인식은 냉전 종식 이후 소위 '총체적 또는 포괄적 안보(Comprehensive National Security)'라는 개념이 보편화된 데 따른 것으로 볼 수 있다. 즉, 냉전시대에는 군사적 안보가 국가안보의 중요한 부분을 차지하고 있었던데 비해 냉전 종식 이후 경제안보(Economic Security) 분야의 중요성이 더욱 부각되었던 것이다. 이러한 경제안보의 중요성에 대한 미국의 시각은 정부의 각종 발표에서 잘 나타나고 있다. 1995년과 1996년 백악관에서 발표한 '국가안보전략(National Security Strategy)'에서는 경제안보를 "국가 이익은 물론 국가 안보의 필수적 일부"라고 강조하였으며, 1993년 11월 Warren Christopher 당시 국무장관은 상원 외교위원회에서 행한 연설에서 "탈냉전 시대의 국가안보는 경제안보와 절대 분리될 수 없으며 경제정책은 미국 대외정책의 새로운 중심이 되고 있다"라고 하였다.[15]

그러므로 산업보안에 대한 국가 안보적 관점이 우선시되는 미국에서 영업비밀을 보호하기 위하여 국가가 주도적 역할을 수행하고자 하는 것은 필연적인 결과라고 할 것이다. 이처럼 국가가 영업비밀 보호를 위해 정부 각 부처나 기관의 인력과 예산을 동원하고 관련되는 정책들을 집행하는 것이 미국 내 영업비밀 보호의 제도적·정책적 측면이라고 할 수 있겠다. 이러한 필요에 따라 미국이 연방정부 차원에서 영업비밀을 보호하기 위해 적용하는 정책들에는 크게 세 가지 고려가 작용하고 있는 것으로 보인다.

첫째는 국가 정보활동의 소극적 측면인 방첩활동(Counterintelligence)을 담당하는 정부기관을 중심으로 범국가 차원의 방첩활동을 효율적으로 전개하면서 '산업보안'을 그 주된 활동 분야로 상정하고 있다는 것이다. 이와 관련, 외국의 정부나 기업 등으로부터 자국 정부, 기업 기타 주체가 보유한 영업비밀을 보호하는 활동인 산업보안은 방첩의 한 분야로서 날로 그 중요성을 더해가고 있다.[16]

56개 지부에 산업정보의 보호를 위한 방첩본부를 신설하고 정보원 167명을 보강한 것으로 알려졌다. FBI의 이러한 변신은 소프트웨어와 같은 과학적 연구의 성과에서 국방기술에 이르는 미국의 첨단 산업정보가 외국 스파이활동의 대상이 됐다는 분석에 따른 것으로서, 이와 관련하여 Robert S. Mueller FBI 국장은 의회 청문회에서 "산업정보 보호가 대테러 정보활동에 버금가는 중요성을 갖는다"고 강조한 바 있다(한국일보, 2003, "FBI '산업스파이 꼼짝마'", http://news.naver.com/main/read.nhn? mode=LSD&mid=sec&sid1=104&oid=038&aid=0000194046 / 2003. 8. 4).

15) 미국에서 산업스파이로 인한 영업비밀의 절취를 예방하기 위해 연방 입법의 필요성을 논의한 2개의 주요한 청문회가 있는데, 그 첫 번째는 1996년 2월 28일에 있었던 'The Senate Select Committee on Intelligence and the Senate Judiciary Subcommittee on Terrorism, Technology and Government Information」에서의 합동 청문회(Joint Hearing)였고, 두 번째가 1996년 5월 9일에 개최된 'The Sub-committee on Crime of the House Judiciary Committee」에서 행해진 것이었다. 당시 FBI 국장이었던 Louis J. Freech는 동 청문회에서 "산업스파이 활동 예방·규제를 위한 연방 입법은 주로 실리콘 밸리(Silicon Valley)와 우주항공 분야를 대표하는 산업계의 많은 인사들로부터 요청되어 졌다"라고 밝혔다(Mossinghoff, et al., 1997: 191-193).

16) 미국 FBI가 산업보안 차원에서 행하는 경제스파이법 위반사범에 대한 수사활동과 검찰의 기소 등은 영업

둘째는 연방정부 부처・기관이 보유하고 있는 정보 중 영업비밀로서의 성격을 가지는 정보를 포함한 일체의 정보를 보호하기 위한 정책이다. 이는 특히 잠재적으로 군사 분야에서 활용 가능한 과학 분야, 즉 원자력 기타 군수산업 분야의 기술 개발을 정부가 주도하는 과정에서 발생할 수 있는 영업비밀의 유출을 어떻게 예방할 것인가에 대한 고려를 그 출발점으로 하고 있는 것으로 보인다.

셋째는 연방정부가 민간기업의 영업비밀 보호에 대한 경각심을 고취하고 적절한 정보적 지원을 통해 이를 지원하고자 추진하는 정책의 측면이다. 연방정부가 주도적으로 새로운 산업스파이 수법이나 경향 등에 대한 정보를 공공 및 민간 분야에 신속하게 제공하기 위한 체계를 구축하려는 정책이 이에 해당한다.

2. 산업보안 관련 정부조직 및 프로그램

1) NCIX(Office of the National Counterintelligence)

미국 연방정부 내에서 산업보안을 그 주된 임무로 하는 정부조직으로는 우선 NCIX/ONICX(Office of the National Counterintelligence)를 들 수 있다. NCIX는 산업보안을 포함하는 국가 차원의 방첩활동을 총괄적으로 기획하고 조정하면서 이에 대해 의회에 보고하는 책임을 지고 있는 정부조직이다. NCIX가 이처럼 산업보안에 관한 국가적 차원의 기획 임무를 수행하는데 반해 이에 따르는 구체적인 법 집행의 임무를 담당하고 있는 주된 정부조직은 FBI(Federal Bureau of Investigation: 연방수사국)라고 할 수 있다.

NCIX는 1994년 Aldrich Ames 사건[17] 직후 Clinton 행정부가 국가 방첩역량 강화를 위해 창설했던 NACIC(National Counterintelligence Center)의 후신으로서 2001년 1월 Presidential Decision Directive/NSC-75호를 근거로 출범하였다. 이는 산업보안을 포함한 방첩활동에 있어서 국내는 FBI가, 해외는 CIA(Central Intelligence Agency)가 담당하던 종래의 체계가 각 정부 부처・기관들의 방첩 목표를 국가적 차원에서 통일적으로 조정해 줄 필요를 제대로 충족하지 못했다는 반성에서 출발하여 FBI, CIA, NSA(National Security Agency) 등을 중심으로 하여 합동으로 설립된 조직이다.

NCIX의 주요 임무(Key Responsibilities)는 크게 네 가지로 나눠진다. 첫째, 주요 국가자산(Critical National Assets: CNA)을 파악하는 것이다. 방첩활동을 통하여 국가자산으로서 보호해야 할 대상들이 무엇인지 정기적으로 규명해 나가는 작업은 방첩활동의 출발점

비밀 보호의 법적 측면 중 형사적 제재 방안의 일환에 해당되므로 방첩활동의 영역에서는 논외로 한다.

17) CIA 요원이었던 Aldrich Ames가 9년간 舊소련에 미국의 기밀사항을 넘겨오다 FBI에 적발된 사건으로서, 과거 FBI와 CIA가 상호 배타적으로 국내와 해외정보를 나누어 담당하던 미국의 방첩체계에 대한 반성의 계기가 되었던 사건이다.

이 된다고 할 것이다. 둘째, 보호 대상들을 위협하는 요인들과 그 보호 우선순위를 평가하여 국가적 위협요인 발견 및 우선순위 평가(National Threat Identification and Prioritization Assessment)를 작성하는 것이다. 셋째, 주요 국가자산들을 보호하는데 어떠한 취약점이 있는지를 평가하는 것이다. 마지막으로, 이러한 국가자산들을 보호하기 위한 국가 방첩전략(National Counterintelligence Strategy)을 수립하는 것이다.

NCIX가 주요 국가자산(CNA)을 규정하는데 기준이 되는 두 가지 가이드라인(Guideline)이 있는데, 첫째는 보호대상인 정보(Information), 정책(Policies), 기술(Technologies), 산업(Industries) 등을 경쟁 대상국이 획득, 변형, 입수하는 경우 미국의 국가적·경제적 안보(Economic Security)를 심각하게 저해하는 경우이어야 한다는 것이다. 둘째는 이러한 자산들이 정부 소유인지 민간 소유인지를 불문하고 국가적으로 손실되어서는 안 되는 성질을 가지고 있어야 한다는 것이다. 이러한 가이드라인은 미국의 방첩체계가 민간부문의 기술 등의 산업정보에 대해서 경제안보적 관점에서 국가 방첩역량의 우선순위를 두고 있음을 분명하게 보여주는 것이라고 하겠다.

NCIX는 이러한 주요 임무들을 수행하는 가운데 연구·개발과 기술의 보호 및 경제 방위를 주된 방첩활동 목표 중 하나로 설정하고 있다(<표 2> 참조). NCIX는 또한 '(1995년도) 정보수권법(Intelligence Authorization Act for Fiscal Year 1995)' 제809(b)조(Section 89(b))에 의거하여 외국의 경제첩보 수집 및 산업스파이 행위가 미국 기업에 초래하는 위협에 대한 최신 정보를 의회(The Permanent Select Committee on Intelligence of the House of Representatives and The Select Committee on Intelligence of the Senate)에 매년 보고할 의무를 지고 있다. 이 때 이러한 연례보고서(Annual Report) 작성에는 연방정부의 다양한 조직들이 참여하게 된다.[18]

<표 2> NCIX의 방첩목표(Counterintelligence Mission)와 내용

분야별 임무	보호대상	보유주체	위협(Threat)
물리적 공격 방어	인적·물적 자산, 정보 자산	정부 부처 및 기관	테러리스트, 국가가 배후인 비밀 공격
연구·개발 기술보호	기술	정부 부처·기관, 미국 기업, 민간연구소	외국에 의한 절취

18) 미국 국방부의 Defense Security Service, Air Force Office of Special Investigations, Army Counter-intelligence Center, Naval Criminal Investigative Service, Defense Intelligence Agency, Defense Threat Reduction Agency 등 군 관련 정보·보안기관들과 법무부의 FBI, CIA, NSA, 국무부(Department of State)의 Bureau of Intelligence and Research 및 Bureau of Diplomatic Security, 상무부(Department of Commerce), National Reconnaissance Office, 에너지부(Department of Energy) 등의 연방정부 부처 및 기관들이 참여하고 있다(NCIX, 2002).

기반시설 보호	정보 네트워크, 주요 국가 기반시설	공공・민간기구	외국의 정보 공격, 내부자에 의한 위협
경제 방위	영업비밀, 지적 재산, 금융시스템	미국 기업 정부 기관	외국에 의한 절취, 정보 공격, 내부자에 의한 공격
정부 재산 보호	미국 정부기관의 완전성	정부 공공분야	외국에 의한 부패 관행
對간첩	위 전부	위 전부	이적 내부자

자료: http://www.pnsr.org/data/images/michelle.pdf에서 인용 작성

2) FBI & CIA

NCIX와 달리 FBI(Federal Bureau of Investigation: 연방수사국)는 수사권과 결부되어 보다 직접적인 산업보안 활동을 담당하고 있는 미국의 법 집행 주무기관이라고 할 수 있다. 특히 1996년의 경제스파이법(Eonomic Espionage Act of 1996) 제정과 함께 FBI의 이런 역할은 더욱 강화되어 왔다고 할 수 있다. 사실상 NCIX가 출범하기 이전부터 FBI는 방첩기관으로서 외국의 경제스파이 행위에 대처하기 위한 활동을 전개해오고 있었으며 1994년 「경제방첩프로그램(Economic Counterintelligence Program)」은 그 대표적 사례이다. 이 계획에 따라 FBI는 영업비밀 보호를 위한 외사, 방첩 및 범죄수사 관할권을 확대하고 전문인력 및 수사역량을 보완한 바 있으며, '현안 위협요소(Issue Threat List)'에 외국의 산업정보 활동을 포함시켜 FBI의 주요 활동목표로 설정하기도 하였다.[19]

한편, FBI가 주도하는 산업보안 활동에 있어서 국가 정보기관인 CIA(Central Intelligence Agency)의 역할은 경제스파이 행위에 대한 수사가 외국과 관련되어 있는 경우에 한정되고 있다. 즉, FBI의 수사가 외국의 정권(Foreign Power/Sovereignty) 또는 그 관리(Agent of Foreign Power)를 대상으로 하거나 미국의 대외정보 및 해외 방첩활동에 영향을 줄 가능성이 있는 경우에는 FBI가 CIA의 장(長)이 겸하는 중앙정보국장(Director of Central Intelligence: DCI)의 조정을 받도록 두 기관 간에 협정을 맺고 있는 것으로 알려져 있다.

---

19) '현안 위협요소(Issue Threat List)'는 FBI가 중점 수사대상으로 삼고 있는 7가지 범죄행위 목록이다. 그 상세한 내용을 살펴보면, ① 국가 중요기술 목록(National Critical Technologies List)과 국방부의 중요 군사기술 목록(Department of Defense: Military Critical Technologies List)에 포함된 기술을 목표로 하는 외국의 정보활동, ② 국가의 산업역량과 지위를 침식당할 우려가 있는 미국 기업의 각종 정보 및 기술의 수집행위, ③ 외국 또는 외국의 단체가 미국 정부에 사전통고 없이 요원을 파견, 비밀리에 수행하는 활동, ④ 미국 국방시설 및 국가 전시 대비 활동계획과 관련된 사항에 대한 수집활동, ⑤ 대량파괴무기 취득 및 확산과 동 무기의 인수・인도 체제와 관련되는 정보활동, ⑥ 미국에 관한 정보, 대외정책 관련 사항 및 공무원을 대상으로 하는 정보활동, ⑦ 비밀수단을 동원하여 미국 정부 혹은 국민에 대한 여론조작을 목표로 하는 정보활동 등이 이에 해당한다(Watson, 1995: 146-153 & 문정인, 2002: 232).

3) National Industrial Security Program(NISP)

「National Industrial Security Program(국가산업보안프로그램: NISP)」은 연방정부 행정부처 및 기관(U.S. Government Executive Branch Departments and Agencies)이 체결하는 계약 상대방에게 허가 없이 '비밀로 분류된 정보(Classified Information)'를 공개하는 것을 방지하고, 허가 받은 공개의 경우에도 이를 적절히 통제(Control)하기 위하여 마련한 필요요건(Requirements), 제한(Restrictions), 기타 보호장치(Safeguards)를 총칭하는 개념이다.[20] 연방정부가 정부 부처·기관들이 보유하고 있는 영업비밀을 보호하기 위해 1990년대에 도입한 이후 시행해오고 있는 제도로서 산업보안과 관련된 국가정책의 대표적인 사례로 볼 수 있다.

NISP는 연방정부와 민간산업 부문 간에 기밀정보를 보호하기 위한 파트너십(Partnership)을 보여주고 있다는 측면에서 그 의미와 시사하는 바가 크다고 하겠다. NISP는 비밀로 분류된 정부 관련 계약에 대한 보안요건(Security Requirements)에 보다 통일성을 획득하기 위한 목적으로 다음 4가지의 주요한 원리를 가진다. 첫째, 보안절차에 있어서 통일성 확보, 둘째, 보안절차, 특히 시설 및 인원 통제(Clearances)와 관련한 상호주의(Reciprocity) 원칙의 이행, 셋째, [특히 기관 감사의 경우] 중복되거나 불필요한 요구사항(Requirements)의 제거, 그리고 마지막으로 보안비용의 절약 등이 바로 그것이다.

NISP와 관련된 전반적인 정책결정의 책임은 National Security Council(국가안전보장회의)에 있으며 그 집행의 책임은 대통령이 국방장관에게 위임하고 있다. 한편, National Archives and Records Administration(정부문서기록관리처) 소속 Director of the Information Security Oversight Office(정보보안감시국장)은 NISP를 시행하는데 필요한 구체적 지침(Directives)을 작성하여 각 정부기관에 하달하고 그 시행 여부를 감독하는 임무를 수행한다. 이에 따라 NISP의 집행 책임을 맡고 있는 국방부(Department of Defense)에서는 지난 1995년 1월 NISP 매뉴얼(National Industrial Security Program Operating Manual: NISPOM)[21]을 제정하여 구체적인 업무기준을 설정, 시행해오고 있다.

---

20) The NISP recognizes four different 'Cognizant Security Agencies': (1) CIA, (2) Department of Defense, (3) Department of Energy, (4) Nuclear Regulatory Commission. / 'DoD 5220.22-M」(National Industrial Security Program Operating Manual: NISPOM) 참조 (January 1995).

21) 미국 CIA, 국방부, 에너지부, 원자력규제위원회(Nuclear Regulatory Commission) 등이 공동으로 1995년 1월부로 제정·공포하였으며, 2006년 2월 28일 재발행 되었다.

4) NISP 매뉴얼(National Industrial Security Program Operating Manual)

NISP 매뉴얼(National Industrial Security Program Operating Manual: NISPOM)은 NISP(국가산업보안프로그램)를 실제적으로 집행하는데 기준이 되는 원칙과 절차들을 정해놓은 것이다. 모두 11개 장(Chapter)과 부록(Appendices)으로 구성된 NISPOM은 보안점검 및 인가(Security Clearances), 보안교육·훈련 및 브리핑(Security Training and Briefing), 비밀(기밀)의 등급 분류 및 표시(Classification and Marking), 기밀정보 보호(Safeguarding Classified Information), 방문 및 회의(Visits and Meetings), 하도급 계약(Subcontracting), 자동화된 정보시스템 보안(Automated Information System Security), 특수한 [보안]요건(Special Requirements), 국제적 보안요건(International Security Requirements), 기타 정보(Miscellaneous Information) 등의 주제 하에 각 연방정부 부처 및 기관들이 보안조치를 하는데 있어서 준수해야 할 원칙들을 제시하고 있다.[22] 특히 CIA 국장이 정부 부처와 계약을 체결하는 계약 당사자나 용역 프로그램 수행자 등의 인물 및 관련되는 정보가 보관된 시설에 대해 검사(Inspect)하고 모니터링(Monitoring) 할 수 있도록 하고 있다.[23] 이는 대외 방첩활동의 주무기관인 CIA가 공공부문의 산업보안에 관한 임무를 수행하고 있는 일면을 보여주는 것이라고도 하겠다.

<표 3> NISP 매뉴얼(National Industrial Security Program Operating Manual: NISPOM)

Chapter	제 목	내 용
1	General Provisions and Requirements (총칙 및 의무/요건)	서문, 일반적 요건, 보고 의무 [기타 정보 공개 통제와 관련한 보호대책들]
2	Security Clearances (보안 점검 및 인가)	시설 및 인원에 대한 인가, 외국(인)의 소유/통제/영향 하에 있는 경우(FOCI)의 보안 인가
3	Security Training and Briefings (보안 교육·훈련 및 브리핑)	보안 교육·훈련 및 브리핑 규정
4	Classification and Marking (등급 분류 및 표시)	비밀(기밀)의 등급 분류 및 표시 의무
5	Safeguarding Classified Information (기밀정보의 보호 조치)	기밀정보의 보호 조치에 관한 9개조 규정

22) NISPOM의 내용상 변동이나 추가적 설명은 국방부 산하 'Defense Security Service (Industrial Security Program Office)'에서 발간하는 「Industrial Security Letter」를 통해 이뤄진다.

23) "The Director of Central Intelligence Agency may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information."

6	Visits and Meetings (방문 및 회의)	방문 및 회의 관련 규정
7	Subcontracting (하도급 계약)	원계약자의 책임(Prime Contractor Responsibilities) 규정
8	자동화된 정보시스템 보안 (Information System Security)	책임, 승인 및 보안모드, 통제 및 관리, 네트워크에 관해 각각 규정
9	Special Requirements (특수 보안의무/요건)	통제대상 및 예전 통제대상 자료, 국방부 중요 핵무기 설계정보, 정보 자료
10	International Security Requirements (국제적 보안요건)	일반·배경 정보 및 외국 이익을 위한 미국 보유 정보의 공개 관련 규정
11	Miscellaneous Information (부칙)	부칙 및 추가 정보

자료: http://www.fas.org/sgp/library/nispom/nispom2006.pdf 내용 참조하여 작성

5) ANSIR(Awareness of Nation Security Issues and Response) 프로그램

「Awareness of Nation Security Issues and Response: ANSIR(국가보안 현안 인식 및 대응)」 프로그램은 주로 국내 분야의 방첩업무에 관한 책임을 맡고 있는 FBI에서 시행하고 있는 정책이다.[24] 특히 산업보안의 측면에서는 이 프로그램을 통해 영업비밀에 대한 침해 수법의 변화, 침해 위험의 증가 가능성 등과 같은 정보를 민간기업에 적시에 적절하게 알림으로써 피해를 미연에 방지할 수 있도록 국가보안 현안과 관련된 정보 지원·제공(확산)을 그 목적으로 한다. FBI는 1970년대 초 「Development of Espionage, Counterin telligence and Counter- terrorism Awareness(DECA: 스파이, 방첩 및 대테러 인식 경보」 프로그램을 운영해 왔었는데, DECA 프로그램은 냉전적 국제질서 하에서 미국 국민과 자국 기업들을 간첩행위와 테러행위로부터 보호하기 위해서 도입되었던 것으로서 냉전시대의 종식과 함께 그 변화를 모색하게 되었고 이것이 ANSIR 프로그램으로 거듭나게 된 것이다.

FBI는 이러한 ANSIR의 도입 배경을 세 가지로 설명하고 있다. 첫째, 외국 정보기관들이 민간부문의 경제정보에 대한 수집활동을 강화하기 시작했다는 측면이다. 둘째, 국내외적으로 테러 공격의 위협이 증가했다는 점이다. 셋째, 컴퓨터 시스템에 대한 침투행위(Computer Intrusion)와 컴퓨터 바이러스가 확산되면서 국가 차원의 경제적 손실이 급증했다는 것이다.[25] 이 중 특히 첫 번째와 세 번째 배경은 ANSIR가 산업보안의 측면에서

24) FBI는 2003년 4월 17일 이 프로그램을 무기한 중지한다고 공고하면서 ①민간 부문에 제공하는 정보와 서비스의 질을 높이기 위한 유사 프로그램과의 통합, ② 국토안보부(Department of Homeland Security) 출범에 따른 업무 재조정 등을 그 이유로 밝혔다.

25) 출처: FBI Deputy Assistant Director of National Security Division의 미 의회 증언

담당하고 있는 역할과 책임을 암시하는 것이라고 볼 수 있다.

이와 같이 미국 기업과 보안책임자 등에게 국가보안 상의 위협 및 경고 정보를 제공하고 새로운 안보환경에 적응하기 위하여 도입된 ANSIR는 그 목적에 가장 적합한 형태로 프로그램을 운영하기 위한 변화를 모색해왔다. 이에 따라 ANSIR 프로그램의 현재의 특징들이 나타나게 되었는데, 민간 기업을 주된 프로그램의 수혜 대상으로 한다는 점과 전자우편(E-mail)을 이용하여 신속한 경보 발령을 가능하게 한 점 등이 그것이다.

첫째, ANSIR는 자발적으로 프로그램에 가입하여 정보를 수령하기를 희망하는 가입자들을 대상으로 하는 자발적 프로그램이며 민간 기업이 주 가입자라는 특징을 갖는다. 자발적인 참여가 원칙이므로 가입 조건에 별도의 제한을 두고 있지 않아 개인, 기업, 정부기관 등 가입을 희망하는 누구라도 프로그램에 가입하여 관련 정보를 공유할 수 있다. 가입자들 가운데는 정부 부처, 법 집행기관 등이 포함되어 있으나 대부분의 가입자는 민간 기업들인 바, 이는 산업보안 측면에서 이 프로그램이 담당하고 있는 역할의 중요성에 기인하는 것으로 보인다.

ANSIR 프로그램은 '스파이 기술·기법'에 초점을 맞추어 25,000여개 민간 기업들에게 보안 관련 최신 정보를 E-mail 또는 팩스를 통해 알려주는 한편, 56개 FBI 지부에 정기적으로 민간기업 관련자들과 보안문제를 협의하도록 하고 있다(과학기술부, 2002: 43). 또한, 동 프로그램을 통해서 외국 정보기관들이 경제정보를 획득하기 위해 사용하는 수법들, 컴퓨터 시스템에 대한 침투 기법들, 컴퓨터 바이러스와 관련된 최신 정보 등을 적시에 제공함에 따라 민간 기업들은 이러한 정보를 자체적으로 수집하는데 따른 비용을 절감할 수 있음은 물론이고, 영업비밀이 유출되었을 경우 입게 될 경제적 손실을 미연에 방지할 수 있을 것이므로 이러한 기대가 ANSIR 프로그램 가입자의 급격한 증가로 이어졌다고 하겠다.

둘째, ANSIR는 신속한 정보의 전달을 위하여 E-mail을 수단으로 사용하고 있다는 특징을 갖는다. 1996년 도입된 'ANSIR E-mail'은 정보 전달의 편의성과 속도 측면에서 획기적 발전을 가져온 계기가 되었다고 평가된다. ANSIR E-mail은 17개 하위부문(Infrastructures)으로 분류되어 있어서 가입자가 희망하는 부문만을 선택하여 가입할 수 있도록 하고 있는데, 대부분 가입자는 17개 전 부문에 동시 가입하고 있는 추세이다. 한편, 인터넷 매체의 편의성에도 불구하고 그 보안상 취약성이 문제점으로 지적될 수 있겠으나 FBI에서는 FBI Law Enforcement On-line(LEO)을 인터넷 서비스 공급자로 이용하여 보안문제를 해결하는 것으로 밝히고 있다.

[http://www. fbi.gov/congress/congress01/ansir040301.htm / 2001. 4. 3].

3. 민간부문의 산업보안 활동

미국의 정부조직은 아니지만 민간기구들이 연방정부의 산업보안 관련 활동에서 어떤 의미를 가지는지 알아보는 것도 미국의 산업보안 체계를 이해하는데 중요한 도움을 줄 것으로 생각한다. 美 연방정부는 민간기구・단체와의 협력체계를 구축, 민간기구들이 보유한 전문성을 산업보안 정책의 수립에 활용하고 있다. 이러한 활동을 담당하는 대표적인 민간기구로는 American Society for Industrial Security(ASIS: 미국산업보안협회)와 Computer Security Institute(CSI: 컴퓨터보안연구소/협회)를 들 수 있다.

1) American Society for Industrial Security(ASIS)

American Society for Industrial Security(ASIS: 미국산업보안협회)는 전 세계적으로 약 33,000명의 회원과 208개 지부를 가진 세계 최대의 민간보안 단체(기구)이다. 보안 관련한 전문가・관리자들을 협회원으로 하는 ASIS는 이사회, 상설위원회, 지역 부회장, 지부 회장 등 4개 기본 조직으로 구성되며, 각 책임자는 자발적 봉사자로서 협회로부터 어떠한 보상도 받지 않는다. ASIS는 민간 보안산업의 활성화와 전문성 제고를 위해 1955년에 설립된 이래 기업, 언론, 정부조직, 기타 일반인들을 대상으로 보안관리 업무의 가치와 역할을 홍보하고 그 활동을 지원하는 것을 목표로 하여 현재까지 활발하게 활동해오고 있다.

ASIS는 특히 NCIX(Office of the National Counterintelligence)가 매년 의회에 보고하는 '외국의 경제정보 수집 및 산업스파이 활동에 대한 연례보고서(Annual Report to Congress on Foreign Economic Collection and Industrial Espionage)'의 작성 과정에서 그 연구・조사 결과를 외국으로부터의 경제적 위협(Foreign Economic Threat)을 평가하는데 반영하는 역할을 담당[26]함으로써 연방정부와의 협력 체계를 다져오고 있다. 또한 FBI・법무부 등과 공조하여 산업보안 관련 교육과 인력 양성, 정보 제공, 정책 건의 등 기능을 수행하고 있으며, 기업 정보자산 관리과정, 시설보안 관리과정 등의 교육 프로그램을 운영하면서 각종 보안 관련 문제에 대한 대안을 제시하기도 한다. 그리고 Security Management 등 산업보안 관련 잡지(3종)를 발간하여 각 회원(사)에 배포하는 한편, 전시회・세미나 등 국제교류 활동도 수행하며, 보안 전문자격증(CPP, PSP, PCI 등)[27]을 발급하고 인터넷 정보자료센터도 운영하고 있다(국가정보원, 2005: 3-4). ASIS의 주요 활동을 상세하게 살펴보면 다음과 같다.

---

26) 2002년 동 보고서에서 ASIS는 2001년 지적재산의 절취행위에 따른 미국 내 피해액을 3천억 달러로 추산・보고한 바 있다.

27) CPP(Certified Protection Professional: 공인보안전문가), PSP(Physical Security Professional: 물리적 보안전문가), PCI(Professional Certified Investigator: 공인조사전문가).

첫째, 교육 프로그램의 운영이다. ASIS의 교육 프로그램은 워크샵(Workshop)과 연수 프로그램이 있다. 워크샵의 주요 내용은 물리적 보안 개관, 출입통제, 자산보호, 사건・사고 조사, 테러 및 직장 내 폭력 방지 등 보안활동(Security Programs)에 대한 개론적이거나 전문적인 관심 사항을 주제로 한다. 통신・금융 등 보다 특화된 분야의 보안 전문지식을 필요로 하는 신청자들에 대하여도 보안상의 문제나 위험 또는 기법의 변천 등을 주제로 워크샵을 개최하여 교육을 하고 있다. 또한 연수 프로그램으로 경제환경의 변화에 따른 경영상 문제점들에 대한 대처능력 향상을 위한 강좌를 개설하는 한편, CPP 등의 자격증 수험생들을 위한 전문 단기 연수(Review) 프로그램도 개설・운영하고 있다.

둘째, 연례 세미나 및 전시회이다. ASIS의 행사로 보안 분야의 일반적인 사항과 특수 분야에 대한 지식 공유와 정보 교환, 그리고 관심 제고를 위해 “연례 보안세미나 및 전시회(International Annual Seminars & Exhibits)” 등을 개최하고 있는 바, 매년 세계 각국의 보안전문가 및 보안산업 종사자, 그리고 정부기관과 학술 분야의 관계자들이 참석하여 최신 산업보안 동향과 보안기술・장비・용역 관련 정보를 교환하거나 공유하고 있다.

셋째, 정보의 제공이다. ASIS는 소속 협회원들에게 보안 또는 관련 분야의 정보 및 자료를 제공하기 위하여 「정보자료센터」를 운영하며, 전문가 접촉, 온라인 전산망 정보 탐색, 도서관 논문 열람 등을 위한 「인터넷 데이터베이스」도 운영하고 있다. 또한, ASIS는 FBI, 법무부 등 미국 사법・수사기관의 보안업무 관련 활동을 지원하고 있기도 하다.

넷째, 보안전문가 시험 주관 및 자격증(Certificates) 발급이다. ASIS는 복잡한 보안문제에 대한 효과적인 대처를 위해 보안전문가의 양성에 노력하고 있다. 1977년 연례 세미나에서 CPP(공인보안전문가) 자격증[28]의 발급을 결정하여 2008년까지 8,000여명에게 CPP 자격증을 발급하였다. CPP 자격증은 각종 보안업체 뿐만 아니라 일반 기업에서도 보안 분야 종사자에게 필수적인 조건으로 제시하는 등 보안 전문자격증의 활용이 계속 증가하고 있는 추세에 있다(국가정보원, 2004: 17-21). 최근에는 CPP 외에도 PCI(공인조사전문가)와 PSP(물리적 보안전문가) 등의 자격증 관련 과정과 발급도 주관하고 있다.

---

28) ASIS가 주관하는 CPP(공인보안전문가) 제도는 민간자격증으로서 한국의 국가자격시험인 경비지도사와는 상당한 차이가 있다. ASIS 자체 통계(1997년)에 의하면 CPP 자격증 소지자의 60% 이상이 20년 이상의 보안업체 경력 또는 이에 상응한 근무경력을 갖고 있는 것으로 밝혀졌다. 또한 전체의 95% 이상이 15년 이상 보안 관련 경력을 갖고 있는 것으로 나타났으며, 학력 수준 또한 전체의 50%이상이 대학원 수료 이상의 학력을 갖고 있는 것으로 드러나 전문가로서의 충분한 자격요건을 갖추고 있다고 평가된다. 또한 ASIS는 CPP 자격시험이 보안전문가로서의 전문성과 자격을 충분히 검증할 수 있도록 Professional Certification Board(PCB: 전문심사위원회)를 통해 정기적으로 시험 내용을 점검하고 있다. 미국 내 CPP 자격증의 소지는 단순히 보안・경비요원들을 지도・감독하는 관리자가 아니라 포괄적이고 종합적인 보안프로그램을 설계・운용・관리할 수 있는 보안전문가로서 인정받는 것이며, 이는 급여에 반영될 뿐만 아니라 고위 관리직으로 성장할 수 있는 중요한 요건이 되기도 한다(이창무, 전게논문: 71-72).

2) Computer Security Institute(CSI)

ASIS와 달리 Computer Security Institute(CSI: 컴퓨터보안연구소/협회)는 주로 정보보안(Information Security) 영역의 전문가들을 주요 회원으로 하여 조직된 국제적 민간기구인데, 특히 정보보안과 관련된 교육 프로그램을 개발하여 그 수요자들에게 제공하는 데 주안점을 두고 있다. 연방정부와의 Partnership과 관련해서는 FBI와 합동으로 매년 작성하는 "Annual CSI/FBI Computer Crime and Security Survey(CSI/FBI 컴퓨터범죄 및 보안 관련 연례조사)"가 대표적이다. CSI가 주관하여 FBI와 함께 실시하는 동 연례조사의 주요 목적은 미국 내 컴퓨터 범죄의 규모와 추이를 파악하여 보안인식을 높이고 보다 효과적인 대응을 도와주려는 것이다. 2009년 실시된 제14차 조사에서는 특히 컴퓨터 공격의 종류/빈도/피해액, 공격의 대상, 사건·사고 발생 시 대응, 내부자에 의한 공격, 보안 관련 예산/정책/도구/만족도, 보안 관련한 아웃소싱(Outsourcing)의 정도, 보안 준수 이행 절차 등에 관한 문항들이 포함되어 있다. 한편, FBI가 그 본부(Headquarters)와 일부 지부에 설치한 Regional Computer Intrusion Squads(지역 컴퓨터 침해사건 수사대) 산하에 설치한 National Infrastructure Protection Center(국가 기간자본 보호센터)가 CSI와의 협력 창구로 알려져 있다.[29]

3) 산업보안의 경영관리적 측면

민간 기업이 보유하고 있는 영업비밀 보호를 위해 예방적 차원에서 도입하고 있는 각종의 대책들이 산업보안의 경영관리적 측면에 해당한다. 기업이 영업비밀을 보호하기 위해 경영관리적 측면에서 시행하는 각종 대책들은 해당 기업의 정보가 민·형사상 영업비밀로서 보호받기 위한 법적 요건들을 충족하고 있는가에 대한 고려로부터 출발하게 되는 것이다.

대다수의 미국 기업들에서 공통적으로 찾아볼 수 있는 영업비밀 보호의 경영관리적 측면은 체계화된 보안활동(Security Programs)을 포함하는 구체적 영업비밀 보호조치(Protective Measures)와 이러한 조치들의 효율성에 대한 평가, 그리고 기업 내 영업비밀의 내용과 관리에 대한 검사·평가를 임무로 하는 영업비밀 감사(Trade Secret Auditor) 제도 등으로 구분할 수 있겠다. 따라서 미국의 영업비밀 보호를 위한 경영관리적 측면에 있어서 주목할 점은 일반적으로 '합리적 조치'의 일환으로 행해지는 정보 분류(Classification)

---

29) FBI의 National Infrastructure Protection Center는 민간기업과 연방 정부기관과의 협력체계 구축을 통하여 통신, 에너지, 물류, 은행·금융 거래, 구급활동 및 정부활동 등을 공격 대상으로 하는 사이버 상의 위협을 예방하고 이에 대응하기 위해 산업스파이 행위를 포함한 지능범죄, 네트워크 침입 행위, 개인정보 침해 행위, 소프트웨어 불법복제 행위 등의 범죄에 대한 단속을 主임무로 하고 있다. 국토안보부의 출범으로 산하 '정보분석 및 기간자본 보호국장(Information Analysis and Infrastructure Protection Directorate)'에게 관련 정보를 제공하는 역할을 함께 수행하고 있기도 하다.

조치, 비밀준수 계약이나 보안교육 등의 인사적 보안 조치, 물리적 보안, IT 보안 및 정보보호 등이 경영관리 상의 원칙과 절차라는 형태로 일종의 '규범화' 과정을 거쳐야 한다는 점이다.

이는 기업이 영업비밀을 보호하기 위해서 준수해야 할 원칙과 절차들을 명료하게 정함으로써 영업비밀의 유출 위험을 줄이거나 피하고자 하는 경영 전략의 일환으로 볼 수 있다. 그리고 이러한 원칙과 절차들을 규정하는데 전제가 되는 영업비밀의 결정 및 적정한 관리와 관련한 문제를 전문가에게 위임하는 영업비밀 감사를 도입함으로써 위험도를 줄이고 효율성을 높이고자 하는 것이다.

<표 4> 산업보안의 제도·정책적 측면 비교

구분	한국	미국	일본
조정기관	없음	NCIX (Office of National Counterintelligence)	산업경제성 산하의 산업구조심의회
조정기관의 업무	없음	산업보안을 포함한 국가 차원의 방첩활동 총괄 기획, 조정 및 의회 보고 책임	국가 산업발전의 기본적 전략 수립 및 자국 산업의 대내외적 경쟁력 확보
수사기관	경찰 및 검찰 (전담부서 없음)	FBI	경찰 (경제사범 및 지능 범죄 수사 전담반)
민간기업 主 접촉기관	지식경제부, 국가정보원, 방송통신위원회, 중소기업청, 특허청 등 산재	FBI	산업경제성
민간기업과 접촉 방식	제한된 정보 및 교육	무료 교육 및 정보 제공	가이드라인 및 지침 제공
주요 정책 프로그램	없음	-국가산업보안프로그램 (NISP) -FBI의 ANSIR	-지적재산전략대강 -영업비밀관리지침 -기술유출방지지침 -지적재산 취득·관리지침

Ⅳ. 한국 산업보안의 제도적 발전방안

최근 세계 각 국이 자국 산업의 비교 우위를 유지하고 국익을 지켜나가기 위해 산업 경쟁력의 원천인 핵심기술의 적정한 보호와 관리를 법적·제도적·정책적으로 다루고 있다. 한국도 국가 핵심기술·산업기밀의 보호와 유출 방지는 이미 현안으로 등장한 시급한 과제로서 국민경제에도 큰 영향을 미치기 때문에 국제적인 경쟁력이 있는 중요·핵심기술과 산업기밀, 그리고 기업의 영업비밀에 대한 적절한 보호조치와 통제·관리를 강화해야 할 필요성을 인지

해왔다. 그러나 실제 국내 산업보안 영역에서 활동하고 있는 전문가들의 경험을 토대로 확인해보면 산업보안에 대한 전반적인 인식, 체계적·종합적 관리, 정부의 투자 및 균형 있는 지원, 그리고 전문인력 양성 및 학술적 연구 확산 등의 여러 분야에서 문제점을 인식하면서 개선의 필요성을 제안하였다. 여기서는 앞에서 살펴본 미국의 사례 연구에서 인지한 시사점들을 중심으로 국내 산업보안 활동의 효과성 향상과 제도적 발전을 위한 방안을 논의하고자 한다.

1. 전반적인 산업보안 인식의 제고

산업보안 활동에 있어서 가장 주요한 것은 사회 전반적으로 보안에 대한 필요성과 중요성을 인식하여 보안의식을 고취시키고 체계적인 보안관리 체제를 확립하는 것이지만, 국내의 현실은 행정·입법·사법부 중 직접적 관련이 있는 기관·부서와 일부 관심 있는 학계, 그리고 대기업만을 중심으로 보안에 대한 인식 향상 및 체계적 보안관리를 위한 노력이 이루어지고 있는 것이 문제이다. 산업보안에 대한 충분한 인식과 보안의 필요성을 자각하지 않은 상태에서는 어떠한 보안적 조치나 관리·통제 프로세스도 그 효과를 제대로 발휘하기는 어렵다.

지금까지의 실태를 살펴보면 한국에서는 산업스파이에 의한 기술 유출 등 산업보안 상의 문제를 개별 기업 차원의 문제로 보았기 때문에 국가 차원에서는 이러한 문제에 대해 적극 대처하지 않았던 것으로 보인다. 다시 말해, 해외로 유출되는 산업기밀이나 영업비밀이 국가경제 내지는 국가안보에 심각한 영향을 미친다고 충분히 인식하지 못했다는 의문이 제기되는 상황이었다. 비록 산업보안과 관련된 몇몇 정책들이 시행되었지만 구체적이거나 체계적이지 못해 실효성이 적은, 단기과제나 특정 사건(Issue)에 의해 급하게 만들어진 것이 대부분이라고 할 수 있다.[30] 더욱이 이런 노력들은 기업들에 잘 알려져 있지 않으며, 실제로 활용할 수 있고 믿을 수 있는, 법적·제도적·정책적으로 공인된 지침에까지 이르지는 못하고 있다.

따라서 현재 산업보안 분야에서 정부와 유관기관, 그리고 기업 및 최고경영자(CEO)들의 보안에 대한 인식이나 보안의식의 부족은 가장 시급히 다루어지고 선결되어야 할 문제라고 하겠다. 더불어 기업들이 영업비밀 침해나 기술유출 시도에 대응하기 위해서 나아가야 할 방향과 대안을 국가적 차원에서 정의하고 이를 적극적으로 추진, 홍보하려는 노력이 필요할 것이다. 이제부터라도 산업기밀·영업비밀의 보호 및 기술유출 방지를 위한 국가적 책임과

30) 예를 들면, 경찰청의 경우 "첨단산업 기술유출 방지 활동(2003)"이라는 책자를 통하여 첨단기술과 보안이라는 맥락 속에서 산업보호 활동의 대상, 침해자, 유형 등을 개괄하고 산업기밀 유출사례를 보여주면서 기업 차원에서의 산업비밀 보안관리 요령과 산업스파이에 대한 형사법적 대응방안 등을 제시하였으며, 특허청의 경우에도 "영업비밀 보호 어떻게 하나?(2001)"라는 책자에서 영업비밀 보호제도의 개요와 내용을 살펴보면서 영업비밀 침해행위의 유형과 영업비밀 침해에 대한 구제수단을 정리하고 영업비밀 보호 및 관리 전략을 제시하였다.

중요성을 인식하고 보다 장기적 전망과 관점에서 산업보안 대책을 강구해야 한다고 본다.

2. 산업보안에 대한 왜곡된 이해 및 투자의 편향성 교정

산업보안에는 여러 분야의 다양한 보안활동(Security Programs)이 있음에도 불구하고 현재의 국내 실정을 보면 산업스파이 예방과 같은 산업기밀 유출 방지활동 및 포괄적인 의미가 아닌 협의의 정보보호(정보보안) 영역을 담당하는 IT보안이 주로 강조되고 있다.[31] 이것은 미국이나 영국 같은 선진국들의 경우와는 사뭇 다른 양상으로, 실제로 산업보안의 핵심적인 부분을 차지하는 다른 중요한 영역들(Programs)[32]이 간과되거나 또는 IT보안의 우산 속에 오히려 역으로 귀속되는 기현상을 보이고 있다. 특히 미국의 경우 위험평가, 비상기획, 위기·재난관리, 사업의 연속성, 사건·사고 관리 및 조사, 테러 예방 및 사업장 내 폭력 방지 등의 보안활동이 매우 중요하게 간주되고 있음은 시사하는 바가 크다고 할 것이다.

지난 2008년 12월 지식경제부가 발표한 '지식정보보안산업 육성계획'의 경우 "2013년까지 정보보안, 물리보안, (IT)융합보안 등 3대 원천 분야에 총 1,500억원의 R&D(연구·개발) 예산을 집중 투자해서 핵심 원천기술을 확보하고 열악한 국내 지식정보보안업체의 기술개발역량을 강화할 계획"[33]이라고 밝혔으나, 그 실체를 살펴보면 전반적인 보안산업의 육성·강화라기보다는 융합보안을 기치로 내세웠지만 실제로는 그 집중 투자 대상과 전문인력 양성 및 자격증 활성화 등의 제반 내용들이 IT보안 분야 및 연관 학계 위주로 초점을 맞추고 있음을 발견할 수 있다.[34] 사실상 미국·영국 등 주요 선진국에서는 범죄와 테러 및 재난

---

31) 한국의 경우 1990년대 말부터 시작된 벤처(Venture) 열풍과 함께 많은 IT·인터넷 벤처기업들이 생기며 급성장하였고 더불어 수많은 IT 인력들이 배출되면서 IT보안에 대한 관심도 고조되었으며, IT보안 관련 전문인력 양성을 위한 폭넓은 투자가 이루어졌다. 그로 인해 기존의 산업보안에 대한 개념적 정의와 영역 범위가 고학력·기술인력으로 포집된 IT보안을 위주로 재정립되는 기이한 현상을 낳게 되었다.

32) 보안활동(Security Programs)에는 인적·환경적 보안요소 및 전자기적 보안시스템을 포함하는 물리적 보안(Physical Security), 정보보호(Information Protection), 위험평가(Risk Assessment), 비상기획(Emergency Planning & Response), 위기·재난관리(Crisis/Disaster Management), 사업연속성 계획(Business Continuity Planning), IT보안(IT Security), 테러 예방 및 사업장 내 폭력 방지(Counterterrorism & Workplace Violence Measures), 사건·사고 관리 및 조사(Incident Management & Investigations), 보안교육 및 컨설팅(Security Education/Awareness and Consulting), 그리고 보안감사(Security Reviews & Audits) 등 다양한 프로그램들이 포함된다.

33) 자료: 아이뉴스24(www.inews24.com), 2008, "2013년까지 지식정보보안산업 18조원 규모 육성," http://itnews.inews24.com/php/news_view.php?g_serial=379394&g_menu=020200/ 2008. 12. 15.

34) 예를 들면, 2013년까지 300억 원을 투자해 3,000여명의 지식정보보안 전문인력을 양성하겠다고 밝혔으나 그 분야를 보면 디지털 포렌식(Digital Forensics), 윤리적 해커 등이었고, 3대 원천 분야에 대한 투자도 R&D에만 집중되어 있으며, 또한 자격증 활성화 역시 정보보안전문가(SIS)의 활용 범위 확대 방안으로만 언급되어 있다.

방지를 위한 보안활동에 물리적 보안, 비상기획, 위기·재난관리, 테러 예방 및 사업장 내 폭력 방지, 그리고 사건·사고 관리 및 조사 등 복합적인 산업보안 프로그램 위주로 운영되고 있음을 감안할 때 IT보안 위주로 융합하려는 한국의 현재 상황에 시사해주는 바가 많다고 하겠다.

3. 국가 주도 산업보안 프로그램의 운영

한국의 경우 정부 주도의 산업보안 프로그램 운영이 허술하다. 경찰과 검찰의 예를 들면, 최근 몇 년 간 산업보안과 관련하여 적극적인 개입의 노력을 시도하고 있으나, 산업기밀의 해외 유출 예방활동이나 산업스파이 범죄에 대한 직접 인지·수사보다는 제보나 고발에 의존하는 경우가 대부분이고, 특히 지적재산권 관련 불법복제 단속이나 저작권 관련 고소·고발 사건 수사에 치중하고 있는 실정이다. 그리고 '산업기밀보호센터'와 같이 산업보안 분야를 전담하는 부서를 개설·운영해오고 있는 국가정보원의 경우에도 수사기관이 아니기 때문에 독자적으로 산업기밀 유출 관련 업무를 수행하는 데는 태생적인 한계를 가지고 있다.

이에 반해, 앞에서 살펴본 미국의 경우에는 범정부적인 '국가산업보안프로그램(NISP)'을 운영하면서 IT와 원자력 등 핵심기술의 유출 방지를 위한 총체적인 대책을 수립·시행하고 있다. 이러한 점에서 한국도 정부 주도의 산업보안 프로그램 운영이 산업기술·기밀 유출의 방지를 위한 보다 실질적인 차원에서 검토될 필요가 있다고 하겠다. 향후 산업보안 분야의 발전을 위해서는 국가 차원의 주도적 지원과 법적·제도적 뒷받침이 중요한 바, 우선 국가적 차원에서 산업보안에 대한 인식을 개선하고 구체적·체계적이며 실효성 있는 산업보안 관련 정책의 시행이 필요하다. 이는 기업들이 산업기술·영업비밀의 침해에 대응하기 위해 나아가야 할 방향과 대안을 국가적 차원에서 정의하고 이를 적극적으로 추진, 홍보하려는 노력이 전제되어야 하며, 정부도 산업기밀·영업비밀 보호 및 기술유출 방지를 위한 국가적 책임과 중요성을 인식하고 보다 장기적인 전망과 관점에서 산업보안 대책을 강구해야 할 것이다.

4. 산업보안 기능의 중심 조정기관 운영

한국의 경우 미국의 NCIX(Office of the National Counterintelligence)와 같이 산업보안과 관련한 정부 각 부처의 업무와 권한 등을 조율하는 별도의 중추기관도 없고 특정한 기관에 그와 같은 권한을 부여하고 있지도 않다. 따라서 지식경제부, 방송통신위원회, 특허청, 국가정보원, 중소기업청, 경찰, 검찰 등 관련된 기관의 산업기밀 유출에 대한 대응 정책과 활동들이 효율적으로 연계·조율되지 못하고 때로는 비생산적인 업무의 중복과 심지어는 불필요한 경쟁이 빚어지기도 한다.[35] 예를 들어, 각 기관별로 수집·관리하는 IT 산업 및

기업 관련 정보의 공유나 종합이 이루어지는 시스템이 구비되어 있지 않아 각 기관들이 중복적으로, 그리고 원점부터 자체적·독자적으로 정보 수집을 해야 하는 형국이다.

기관 간의 이 같은 비협력과 경쟁이 계속될 경우 산업기술의 해외 유출을 막을 수 있는 소중한 시간과 자원을 낭비하는 것은 물론이며, 이로 인해 초래될 국가자원과 국익의 낭비는 효과적인 산업보안 정책 집행에 제동을 걸 것이고, 더구나 이러한 현상이 계속될 경우 각 정부 부처에 의해 양산되는 수많은 정책들로 인한 기업의 부정적 인식은 점점 증가될 수밖에 없을 것이다. 결국 산업기술의 해외유출 방지에 대한 보다 효과적인 대책을 마련하기 위해서는 위와 같은 문제점을 극복하기 위한 산업보안 관련한 국가 중추적 조정기관의 설립이나 지정이 시급히 필요하다고 본다.

5. 중소기업 보안체계에 대한 지원

중소기업중앙회가 2008년 125개 중소기업을 대상으로 실시한 "산업기술 보호에 대한 의식" 조사 결과, 응답한 업체의 88.8%가 산업기술 보호에 취약한 것으로 나타났고, 90.4%는 '기술보호 시스템이 필요'하다는 뜻을 표명했다. 또한 산업기술을 부당하게 빼앗긴 중소기업의 43.7%가 별다른 대응조치를 취하지 않았다고 보고하기도 하였다.[36] 이 조사 결과에서 보듯이 한국 중소기업의 약 90% 정도가 산업기술의 유출에 적절히 대비하지 못함으로써 산업기술 유출에 취약한 것으로 밝혀진바, 관련 대책 마련이 시급하다는 지적이 지속적으로 제기되고 있는 실정이다. 또한 한국산업기술진흥협회(KOITA)가 2009년에 중소기업청과 합동으로 기술연구소를 보유한 중소기업(표본기업) 504개사[37]를 대상으로 한 "산업보안 역량수준" 조사 결과, 중소기업의 평균 산업보안 역량은 100점 만점에 51.8점으로 '취약수준'인 것으로 나타났다. 특히 6개 영역 지표 중 '유출사고 시 대응'은 33.9점으로서 '위험수준'으로 평가되었다(한국산업기술진흥협회, 2009: 1-4).

이처럼 대기업과 달리 중소기업의 경우 재정적·환경적 요건의 제약도 있겠지만 산업보안에 대한 인식이 특히 부족한 것으로 지적되었다. 따라서 중소기업의 경우 보안 관련 규정

35) 특허청의 경우 부정경쟁 방지 및 영업비밀 보호에 관한 법률 개정안에 필요한 범죄통계 자료를 얻으려 했지만, IT기술 유출과 관련된 사건들이 별도로 통계상에 분류되어 있지 않아 실태 조사에 많은 어려움을 겪었다고 한다. 또한 과거 정보통신부에서 구성한 'IT기술유출방지협의회'에 민간과 정부 각계의 참여가 이루어졌음에도 불구하고, 법률 소관부처인 특허청이 빠져 있었다는 점 또한 이러한 협의체의 실효성에 의심을 갖게 하였던 부분이다.

36) 자료: 보안뉴스(www.boannews.com), 2008, "중소기업 88.8% '산업기술 보호에 취약,' http://www.boannews.com/media/view.asp?idx=11015# / 2008. 8. 26.

37) 동 조사에서 모집단은 2008년 12월말 기준 기업연구소를 보유한 16,076개사였고, 역량평가 체계는 기업의 보안경영 활동에 있어서 필요한 업무를 정책·적응·대응의 3개 분야 6개 영역으로 구분하여 평가하였다(한국산업기술진흥협회, 2009: 1).

마련, 보안서약서 징구, 주기적인 보안교육, 정기적인 보안점검・감사 등 기본적인 보안관리 활동부터 잘 정립해 나가는 것이 필요할 것이다. 한편으로 중소기업의 보안에 대한 인식 부족과 미흡한 투자도 개선해 나가야겠지만 입법적 고려를 포함하는 정부 차원에서의 장려 및 체계적 지원의 필요성도 시급히 요청된다. 그리고 중소기업에 대한 산업보안 관련 지원에 있어서 정부 주무부처가 지식경제부, 중소기업청, 국가정보원 등 여러 곳으로 혼재되어 있음으로 인한 비효율성과 단발성 정책・제도 시행으로 야기되는 문제점도 지적되고 있으므로 가급적 통일되고 일관성 있는 정책적・제도적 방안 마련과 효율적인 지원이 중요할 것이다.

6. 산업보안 전문인력의 양성

국내 전문적인 산업보안 인력의 양성이 절실함에도 불구하고 기업들은 아직까지 보안인력의 양성을 '투자'가 아닌 '지출(소비)'의 개념으로 인식하고 있는 경향이 다분한 실정이다.[38] 종합적이며 체계적인 교육을 받고 산업보안 현장 경험이 풍부한 CSO(Chief Security Officer: 최고보안책임자)와 같은 보안 전문인력의 양성이 시급하지만 그를 위한 산업보안 전문가 Pool(자원)이 없고 전문 교육과정 및 산업보안 관련 교수진이 절대 부족한 것이 현실이다.

이창무(2009)에 의하면 미국 대학의 산업보안 관련 학과 교과과정에서 볼 수 있듯이 보안분야 산업이나 기업체의 보안 담당부서에 배치되어 바로 활용할 수 있는 체계적이고 실무적인 과목 위주로 편성하여 철저하게 보안시장의 변화 요구에 부응할 수 있도록 집중적인 교육이 필요하다고 주장한다. 또한 국내 보안산업의 새로운 변화와 확대에 발맞추어 산업보안 관련 학과를 개설하고 전문과정을 증설하는 한편, 교육과정(Curriculum)을 실무 중심의 산업보안 전문과목으로 재편하고 산업보안 분야에 대한 전문적 강의가 가능한 실무전문가 및 교수자원(Pool)의 확보가 무엇보다도 시급한 상황이라고 보았다(이창무, 전게논문: 67-73).

따라서 국내 보안산업의 성장과 산업보안 전문인력에 대한 수요의 증가에 유의하여 앞으로는 보다 장기적이고 거시적인 안목에서 산업보안 시장의 변화 요구와 고객의 필요・요구에 부응할 수 있는 '고객(Client) 또는 수요(Needs) 맞춤형 보안 전문인력'의 양성이 시급하다고 하겠다. 이와 더불어 보다 효과적인 산업보안 활동 및 보호 역량의 강화를 위하여 범죄학・심리학・법학(형사법 및 지적재산권・영업비밀 보호 등과 관련된 법률)・사회학・경찰

38) 자료: 보안뉴스(www.boannews.com), 2009, "인사담당자 83%, '사내 산업보안전문가 양성 필요'," http://www.boannews.com/media/view.asp?page=1&idx=17132&search=key_word&find=%BC%AD% BF%EF%B0%FA%C7%D0%C1%BE%C7%D5%B4%EB%C7%D0%BF%F8 / 2009. 7. 16.

학 등 인접 학문 분야와의 연계적 연구도 필요할 것으로 보인다.

7. 민·관 협조체제의 구축

산업보안 활동의 효과성·효율성 제고를 위해서 앞서 살펴본 미국의 경우와 같은 적극적인 민·관 협동체제의 구축도 신중히 고려해봄직 하다. 미국 FBI의 '국가보안 현안 인식 및 대응(ANSIR)' 프로그램이 민간 기업과의 적극적인 교류와 정보 공유를 바탕으로 하는 것처럼, 정부의 주무부처나 조정기관과 기업의 보안관계자들이 함께 참여하는 민·관 협의체의 설치와 활용을 활성화하여 산업보안에 관련된 정보를 신속히 공유하고 정부와 기업 간의 협조·조정사항에 대해 상호 협의하고 미래의 대안이나 발전방향 등을 연구 개발할 수 있다면 이를 정부의 산업보안 정책에 적극 반영할 수 있기 때문이다.

중요한 것은 가급적 'One-Stop Service'를 받을 수 있도록 하는 방안이 우선적으로 고려되어야 한다는 점이다. 즉, 기업의 입장에서는'하나의 기관'에게서 통합적 서비스를 받을 수 있도록 시스템이 구축되어야 한다는 것이다. 또한 국가적 차원에서의 지원과 개입이 필요한 문제(유출·침해 등)의 특성과 기업의 자율성에 대한 국가기관의 침해를 두려워하는 기업의 정서가 충분히 고려된 가운데 실질적이고 실효성 있는 민·관 협력체제의 구축이 필요하다. 즉, 이러한 상호 간의 차이를 인지하고 국가 경쟁력 제고와 국익의 보호라는 공동의 이해에 기반한 협조체제의 구축이 요구된다 하겠다(표창원, 전게서: 233).

V. 맺음말

이 연구의 과정에서 검토된 실증자료 및 국내의 사건·사례들에 대한 분석에 의하면 이미 산업기술·기밀 유출로 인한 국가적·경제적 손실이 심각한 상태이고, 이러한 유출은 주로 전·현직 직원과 같은 내부자에 의해서 가장 빈번하게 발생하는 것으로 나타나고 있다.[39] 또한 산업스파이 뿐만 아니라 해킹이나 도청과 같은 기술적인 방식 등의 다양한 형태로 유출이 이뤄지고 있으며, 때로는 타국의 국가기관도 개입할 개연성이 있는 등 이러한 문제에 대해 개별 민간기업의 노력만으로는 효과적으로 대응하기 어려운 상황으로 판단된다.

이 연구에서 살펴본 바와 같이 미국에서는 영업비밀 유출 문제를 '국가안보'와 직결되는 개념으로 받아들여 범국가적·정부 주도의 대응체계를 구축하여 운용 중에 있으며, 일본의

39) 2004년부터 2008년까지 5년간 적발된 160건의 기술·기밀 유출 사건들 중의 대부분이 경쟁업체 종사자보다는 기업 내부인(전·현직 직원) 또는 관계자에 의해 행해졌다(국가정보원, 2009; 한국산업기술진흥협회, 2000).

경우에도 국가 경쟁력의 핵심으로서 '지적재산권 전략'의 일환[40]으로 국가가 적극적인 개입을 하고 있는 실정이다. 이와 같이 국내 산업기술·기밀의 유출이 국가경제(국익)에 심각한 악영향을 미친다는 점, 또한 민간기업 차원의 노력만으로는 근본적인 유출·침해의 방지가 어렵다는 사실을 감안할 때 이러한 문제를 해결하기 위한 국가적 차원의 다각적이고도 체계적인 노력들이 시급히 요구되는 상황이라고 할 수 있겠다.

연구자가 미국 사례를 중심으로 분석·검토한 국내 산업보안의 제도적 발전방안에 있어서 우선 무엇보다도 산업보안의 중요성에 대한 국가(정부)와 사회 및 기업 차원에서 인식 향상과 공감대 형성이 필요할 것이다. 그것이 미국의 경우와 같이 '국가안보'와 직결되는 개념이 되든지 또는 일본에서와 같이 국가 경쟁력 차원이든 간에 국가의 정책 결정과 제도의 형성 과정에 있어서 기준이 될 수 있도록 공통되고 공유할 수 있는 기본적인 개념의 형성이 중요하다. 이렇듯 산업보안에 대한 국가적 인식과 정책적 방향의 결정이 선결과제라고 하겠다. 이를 바탕으로 이 연구를 통해 도출한 시사점은 다음과 같다. 먼저 산업보안에 대한 인식의 측면에서 사회 전반적인 인식이 부족하고 그 이해가 왜곡되거나 정부 차원의 투자·지원이 편향되어 있는 점을 지적하였다. 또한 산업보안 관련 국가 주도의 체계적인 관리나 조정 기관·프로그램의 운용, 중소기업에 대한 보안관리 체제 구축 지원, 그리고 전문인력 양성 및 학술적 연구 확산 등에서 문제점과 개선의 필요성을 인지하였다.

이에 대한 논의로 산업보안과 관련되는 문제는 개별 기업 차원에 국한되는 것이 아니라 국가경제 내지 국가안보에 심각한 영향을 미칠 수 있으므로 국가(정부) 차원에서 산업보안의 중요성과 필요성에 대한 인식의 전환과 적극적인 대처가 우선적으로 필요하다고 보았다. 그리고 산업보안 프로그램에 대한 국가의 주도적 역할과 더불어 일관성 있는 정책적·제도적 방안의 마련, 중소기업의 산업보안 실태 개선을 위한 체계적인 지원, 보안시장의 변화 요구에 부응할 수 있도록 산업보안 관련 학과 개설 및 실무 중심의 교과과목 편성, 그리고 집중적인 교육을 통한 '수요자 맞춤형 보안 전문인력'의 양성과 산업보안 전문가·강의 자원(Pool)의 확보, 산업보안 문제를 조정하는 국가기관이나 전담기구의 설립 및 실효성 있는 민·관 협동체제의 구축 등을 제도적 발전방안으로 제시하였다.

---

40) 일본에서는 지적재산 보호와 관련한 국가 전략으로서 '지적재산전략대강(知的財産戰略大綱)' 등의 정책 프로그램을 채택, 운영하고 있다.

참 고 문 헌

1. 국내문헌

과학기술부(2002),「과학기술정보 보호체제 강화방안」, 서울: 과학기술부.

곽경직(1997), “영업비밀 침해와 구제 및 소송상 諸문제,” 인권과 정의, 97(6): 42.

국가정보원(2005~2009),「첨단산업기술보호동향」3호~10호, 서울: 국가정보원.

_____(2004),「산업보안 Focus」, 서울: 국가정보원.

김재봉(2002), “영업비밀의 형사법적 보호방안,” 형사정책, 제14권 제1호: 169-196.

문정인(2002),「국가정보론」, 서울: 박영사.

민수홍・이민식(2006), “외국의 신종범죄 발생 현황과 대책,” 치안논집 제22집, 치안정책연구소.

박준석(2006), “한국 민간보안・시큐리티(Security) 산업의 발전방안,” 龍仁大學校 논문집, 제24집.

이윤호(2004),「현대사회와 범죄의 이해」, 서울: 삼경문화사.

이창무(2009), “시큐리티(Security) 전문인력 양성에 관한 고찰: 대학교육을 중심으로,” 산업보안연구학회 논문지, 제1권 제1호: 62-74.

장향배・송지훈(2009), “산업기술 유출 방지를 위한 보안시스템 평가 탐색적 연구,” 산업보안연구학회 논문지. 제1권 제1호: 50-61.

정보통신부(2004),「IT기술 해외유출 방지 방안에 관한 연구」, 서울: 정보통신부.

정보통신부・한국정보통신수출진흥센터(2003),「IT기술 해외유출 방지 협의회 1차 회의 자료집」(2003. 6. 13).

특허청(2004),「영업비밀 보호 가이드북」, 대전: 특허청 산업재산보호과.

표창원(2003).「IT기술 해외유출 방지방안에 관한 연구」, 서울/용인: 경찰대학.

한국산업기술진흥협회(2009),「중소기업 산업보안역량 수준 평가결과 요약」, 한국산업기술진흥협회(KOITA).

한상훈(2000).「산업스파이에 대한 형사법적 대응 방안: 연구보고서」, 서울: 한국형사정책연구원.

2. 국외문헌

ASIS International(2007),「Trends in Proprietary Information Loss: Survey Report」, ASIS International(www.asisonline.org).

Barr, K., Beiting, M., and Grzesinski, A(2003), “Intellectual Property Crimes,” American Criminal Law Review. Vol. 40: 777.

Fink, Steven(2002),「Sticky Fingers: Managing the Global Risk of Economic Espionage」, Lincoln, NE: iUniverse, Inc.

Godfrey, E.R(2004), “Inevitable Disclosure of Trade Secrets: Employee Mobility v. Employe's Rights,” Journal of High Technology Law, Vol. 3(1): 161-179.

Mendell, R.L(2003), 「The Quiet Threat: Fighting Industrial Espionage in America」, Springfield, IL: Charles C Thomas Pub Ltd.

Morris, D.J., Ettkin, L.P., and Helms, M.M.(2000). "Issues in the Illegal Transference of US Information Technologies," Information Management & Computer Security, Vol. 88(4): 164.

Mossinghoff, G.J., Mason, J.D., and Oblon, D.A.(1997), "The Economic Espionage Act: A New Federal Regime Of Trade Secret Protection," Journal of the Patent and Trademark Office Society, Vol. 79: 191-210.

Naef, W.E.(2003 & 2007), "Economic and Industrial Espionage: A Threat to Corporate America?," Infocon Magazine, Issue 1.

Nasheri, Hedieh.(2005), 「Economic Espionage and Industrial Spying」, Cambridge, U.K.: Cambridge University Press.

NCIX.(2002), 「Annual Report to Congress on Foreign Economic Collection and Industrial Espionage-2002」, The Office of the National Counterintelligence Executive.

ONCIX.(2004 & 2003), 「Annual Report to Congress on Foreign Economic Collection and Industrial Espionage-2004 & 2003」, The Office of the National Counterintelligence Executive.

Sepura, Karen.(1998), "Economic Espionage: The Front Line of a New World Economic War," Syracuse Journal of International Law and Commerce. Vol. 26: 133-134.

Snyder, H., and Crescenzi, A.(2009), "Intellectual capital and economic espionage: New crimes and new protections", Journal of Financial Crime, Vol. 16(3). 245-254.

Watson, Patrick.(1995), "The FBI's Changing Mission," in Godson, R., and Schmitt, G. et al. (eds.). U.S. Intelligence at the Crossroads: Agendas for Reform, New York: Brassey's, 146-153.

長内健(2003). 企業秘密保護法入門 [改訂增補版]. 民事法研究會.

千野直邦(2003). 營業秘密の法的保護. (株)中央経濟社.

3. 인터넷 사이트

경찰청: www.police.go.kr

국가정보원(NIS): www.nis.go.kr

국가정보원 산업기밀보호센터(NISC): http://service4.nis.go.kr/

국회도서관: www.nanet.go.kr

보안뉴스: www.boannews.com

ASIS(미국산업보안협회): www.asisonline.org
(ISC)²: www.isc2.org
National Counter-intelligence Center(NACIC): http://www.nacic.gov/
National Institute of Crime Prevention(NICP): www.nicp.net
NISPOM: http://www.fas.org/sgp/library/nispom/nispom2006.pdf

Abstract

A Study on the Institutional Improvement Directions of Industrial Security Programs:

Focused upon Policies and Practices in the U.S.

Choi, Justin Jin-Hyuk

This study examined the institutional improvement directions of industrial security programs, particularly focusing upon policies and practices in the U.S., to enhance the effectiveness of industrial security programs in Korea. This study also aimed to investigate the significance of institutional and/or policy implementations in preventing economic espionage attempt.

Data leakage and/or loss of trade secrets in corporations has been a scary proposition and a serious headache to both the CEOs and the CSOs(Chief Security Officers). Security professionals or practitioners have always had to deal with data leakage issues that arise from e-mail, instant messaging(IM), and other Internet communication channels. In addition, with the proliferation of wireless and mobile technology, it's now much easier than ever for loss by data breaches to occur, whether accidentally or maliciously or even by an economic espionage attempt.

The researcher in this study used both a case study and a comparative research to analyze the different strategies and approaches between the U.S. and Korea in regard of implementing policies to mitigate damages by economic espionage attempts and prevent them from occurring. The researcher first examined the current policies and practices in the U.S. in terms of federal government's and agencies' approach and strategies on industrial security programs and their partnerships with private--commercial--sectors.

The purpose of this paper is to explain and suggest selected findings, and a discussion of actions to be taken on implementing a proactive and tactical approach to enhance the effectiveness of industrial security programs to fight against information loss or data leaks. This study used case reviews, literatures, newspapers, articles, and Internet resources relating to the subject of this study for triangulation of data. The findings during this research are as follows.

This research suggests that both the private and the governmental sector should

closely cooperate in the filed of industrial security to strengthen its traditional prevention strategies and reduce opportunities of economic espionage as well. This study finally recognizes both the very importance of institutional development led by the Government in preventing economic espionage attempts and its effectiveness when properly united with effective industrial security programs.

Key Word : Industrial Security, Information Leaks, Economic Espionage,
Trade Secrets, Industrial Security Programs, Security Professionals

논문투고일 2010.1.31, 심사일 2010.2.15, 게재확정일 2010.3.17