산업기밀 유출사고 사례분석을 통한 유형별 대응방안 연구★

장항배*

요 약

최근 기업이 보유한 산업기밀은 영업비밀보호법, 산업기술유출방지법 등 다양한 산업보안 관련 법률에 의해 보호 받고 있다. 그러나 그러한 보호에도 불구하고 산업기밀의 침해 및 유출사고는 해마다 증가하고 있다. 한국산업기술보호협회의 조사에 따르면 산업기밀 유출 예상 피해액은 연평균 “50조 원”으로 추정되며 이는 중소기업 4,700여 개의 연 매출액과 맞먹는 금액이다. 이처럼 산업기밀 유출은 국가와 기업의 경쟁력은 물론이고 경제적으로도 심각한 피해를 초래한다. 하지만 산업기밀 유출범죄에 대한 투자와 노력은 피해규모에 비해 한 없이 부족한 수준이며 일부 대기업을 제외한 대부분의 기업들이 산업기밀 유출보안을 위한 별도의 조직, 인력, 예산이 없어 산업기밀 유출에 대한 대응체계가 부족한 것이 현실이다. 본 논문은 국내외 산업기밀 유출범죄 분석을 통하여 산업기밀 유출에 따른 피해실태를 파악하고 발생원인, 유출경로 등 다양한 분류체계를 통하여 산업기밀 유출범죄에 대한 전반적인 흐름을 파악하여 관련 연구에 대한 기초자료가 될 것으로 기대한다.

A Study on The Countermeasure by The Types through Case Analysis of Industrial Secret Leakage Accident

Hangbae Chang*

ABSTRACT

Industrial secrets that companies own recently protected by various act related industrial security such as Trade Secret Act, Act on Prevention of Divulgence and Protection of Industrial Technology, etc. However, despite such protection infringement and leakage accidents of industrial secrets is increasing every year. According to a survey conducted by KAITS(Korean Association for Industrial Technology Security) annual average of estimated damage by industrial secrets leakage is estimated to be "50 trillion won." This is equivalent to the amount of annual revenue of small businesses more than 4,700 units. Following this, industrial secrets leakage causes serious damages to competitiveness of nation and companies and economic. However investment and effort to the industrial secrets leakage crime is lack of level compared to the scale of damage. Actually, most companies except some major companies are lack of response action about industrial secrets leakage because of shortage of separate organization, workforce, budget for industrial secrets leakage security. This paper aims to understand the overall flow of the industrial secrets leakage crime through various taxonomy such as cause of occurrence and leakage pathway and grasp the condition of damage from industrial secrets leakage through analyzation of internal and external industrial secrets leakage crime. This is expected to be the basis for related research.

Key words : 산업기밀, 산업보안, 산업스파이, 유출사고, 사고분석

접수일(2015년 11월 3일), 수정일(1차: 2015년 12월 9일), 게재확정일(2015년 12월 18일)

* 중앙대학교/경영경제대학 산업보안학과

★ 이 논문은 2014년도 중앙대학교 학술연구비 지원에 의한 것임.

1. 서 론

현대 사회가 고도화됨에 따라 기업이 가진 지식재산 및 기술에 대한 중요성이 대두되고 있다. 기업들은 경쟁력 확보를 위하여 기업만의 산업기술 발전에 많은 자원을 투자하고 있지만 기술에 대한 보안의식 및 대응 능력, 투자는 취약한 실정이다. 이러한 현실로 인하여 지식재산을 목표로 한 산업기밀 유출범죄는 꾸준히 증가하고 있으며, 국내 기업들과 경쟁관계에 있는 일부 국가 및 기업들은 국내 기업의 첨단 기술을 확보하기 위하여 수단과 방법을 가리지 않고 유출을 시도하고 있어 이에 따른 막대한 경제적 손실이 예상되고 있다. 산업기밀보호센터의 조사에 의하면 연도별 해외 산업스파이 적발 실적은 꾸준히 증가하고 있으며, 기술유출 피해업체의 예상 피해액은 연평균 “50조 원”으로 추정되고 있다. 이는 2014년 국내총생산의 3%에 달하는 금액으로 중소기업 4,700여 개의 연 매출액과 맞먹는 금액이다. 산업기밀 유출범죄는 국가와 기업의 경쟁력은 물론이고 경제적으로도 심각한 피해를 초래한다.

따라서 본 논문은 국내외 산업기밀 유출범죄 분석을 통하여 산업기밀 유출에 따른 피해실태를 파악하고 다양한 분류체계를 통하여 산업기밀 유출범죄의 발생원인, 유출경로 등을 알아보고자 한다.

2. 산업기밀 유출사고의 개념

2.1 산업기밀 관련 법률

2.1.1 부정경쟁방지 및 영업비밀보호에 관한 법

“부정경쟁방지 및 영업비밀보호에 관한 법”이란 국내에 널리 알려진 타인의 상표 · 상호(商號) 등을 부정하게 사용하는 등의 부정경쟁행위와 타인의 영업비밀을 침해하는 행위를 방지하여 건전한 거래질서를 유지함을 목적으로 제정되었다. 제18조에 따르면 부정한 이익을 얻거나 기업에 손해를 입힐 목적으로 그 기업에 유용한 영업비밀을 외국에서 사용하거나 외국에서 사용될 것임을 알면서 취득·사용 또는 제3자에게 누설한 자는 10년 이하의 징역 또는 그 재산상 이득액의 2배 이상 10배 이하에 상당하는 벌금에 처하도록 규정하고 있다.

2.1.2 산업기술의 유출방지 및 보호에 관한 법

“산업기술의 유출방지 및 보호에 관한 법”이란 산업기밀의 불법 해외유출이 심각한 수준에 있으나 ‘부정경쟁방지 및 영업비밀보호에 관한 법률’에 따른 처벌대상이 민간 기업비밀 누설의 경우로 한정되어 있고, 각종 법률에 산재하여 있는 관련 규정으로는 산업기밀유출 방지 및 근절에 큰 효과를 내지 못하기 때문에, 2006년 동법을 제정하여 국내 핵심기술 보호 및 산업기밀의 부정한 유출을 방지하고 산업기밀을 보호함으로써 국내산업의 경쟁력을 강화하며 국가의 안전과 국민경제의 안정을 추구하였다.

2.1.3 경제스파이(Economic espionage)

스파이 행위는 영업비밀을 절취, 또는 권한없이 전용 · 취득 · 취거 · 은닉하거나 또는 기망 · 책략 · 속임수에 의하여 취득하는 행위로 규정된다. 또한 영업비밀을 권한 없이 복사, 복제 및 스케치, 그리거나 촬영, 다운로드, 업로드, 변경, 파괴, 재생, 전송, 전달, 우동, 메일로 보내거나 통신 및 교부하는 행위도 처벌대상으로 규정하고 있다.(정연덕, 2007)

2.1.4 영업비밀 절도(Theft of trade secrets)

기본적인 영업비밀 침해행위는 권한없이 영업비밀을 절취, 전용, 취득하는 등의 행위이다. 이때 영업비밀의 소유자를 해한다는 인식을 필요로 하는데, 영업비밀의 소유자는 영업비밀에 대하여 법적 권리나 형평적 권리, 또는 사용권리가 있다고 신뢰된 사람이나 실체라고 정의된다.

2.2 산업기밀의 개념

중소기업청과 중소기업기술정보진흥원에서는 산업기밀에 대하여 공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 상당한 노력에 의하여 비밀로 유지된 유 · 무형의 기술 또는 경영정보라 정의하고 있으며[8], 법률적인 의미의 개념으로는 지적재산으로 일컬어지는 특허, 실용신안, 디자인, 상

표, 저작권, 영업비밀이 모두 산업기밀에 해당할 수 있다.

국내에서는 산업기밀의 개념을 산업보안(industrial security)과 영업비밀(trade secrets)의 개념과 혼용되어 사용되고 있어 먼저 명확한 구분이 필요하다. 산업보안은 주로 광의적 의미로 사용되어 범죄로부터 산업을 보호하는 전반적인 활동으로 정의될 수 있는 반면에 산업기밀은 산업보안에 대한 협의의 개념으로 단순히 산업기밀과 기술에 국한된 개념이라 할 수 있다[3]. 영업비밀은 앞서 본 부정경쟁방지 및 영업비밀보호에 관한 법률 제2조 제2호에 따르면 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 합리적인 노력에 의해 비밀로 유지된 생산방법/판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다.

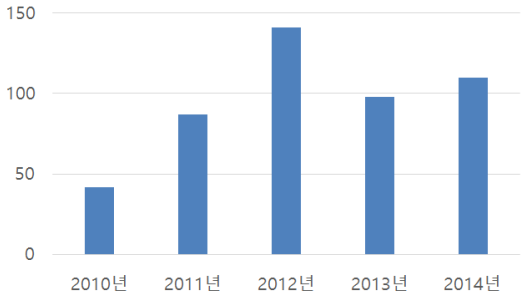
따라서 영업비밀이란 일상적으로 사용하고 있는 기업비밀과는 달리 주로 법률적인 개념으로 볼 수 있으며, 산업기밀 보다는 광의의 개념으로 정의할 수 있다.

3. 산업기밀 유출범죄 사고분석

산업기밀 유출범죄 사고분석의 통계 데이터를 가장 많이 공개하고 있는 곳은 산업기밀보호센터의 기술유출 통계이다. 본 논문에서는 산업기밀보호센터의 자료뿐 아니라 경찰청, 중소기업청 등의 다양한 산업기밀 유출범죄 사고사례자료를 수집하여 분석하였다.

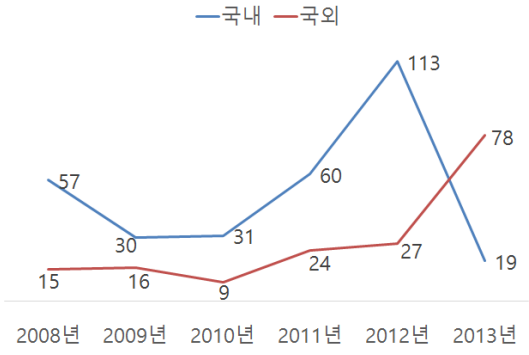
3.1 산업기밀 유출범죄 적발건수 및 유출국가

(그림 1)을 보면 해마다 산업기밀 유출사고는 증가하고 있으며 지난 5년간 경찰이 적발한 산업스파이 범죄는 472건에 이른다. 산업스파이 범죄에 따른 피해규모도 “50조 원”에 육박할 정도로 막대한 손실을 입히고 있어 큰 문제가 되고 있다. 이러한 유출 규모에 따르면 산업기밀의 유출은 기업의 경쟁력과 경제력, 생존권을 위협하며, 더 나아가 국가경제와 국가안보에 결정적인 영향을 미칠 수 있다[5].



(그림 1) 산업기밀유출방지법 및 영업비밀보호법 위반 사건 수
(경찰청, 2010년~2014년/최근 5년)

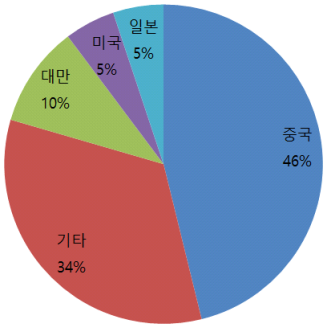
아래의 (그림 2) 경찰통계연보 자료에 따르면 산업기밀유출사범 검거건수는 매년 증가하는 추세를 보이고 있으며, 2013년에는 국외로 유출하려는 건수가 급격하게 증가하였다.



(그림 2) 산업기밀유출사범 검거현황
(2013 경찰통계연보, 경찰청, 2014.11. 재구성)

세계시장에서 우리나라의 기술력이 경쟁력 있다는 것을 의미하며, 앞으로도 각국의 산업기밀 범죄의 대상이 될 가능성이 높은 것으로 분석된다. 산업기밀보호센터의 기술유출 분야별 현황을 보면 우리나라가 높은 경쟁력을 가지고 있는 정밀기계(34%), 전기 · 전자(26%), 정보통신(14%) 분야에서 많은 산업기밀 유출사건이 일어나고 있으며 산업스파이의 표적 기술은 점점 대기업의 IT 분야 기술에서 중소기업의 정밀기계 분야로 이동 및 확대 되고 있다. 또한 2003년부터 최근까지 해외로 유출된 산업기밀 유출사고를 분석해 본

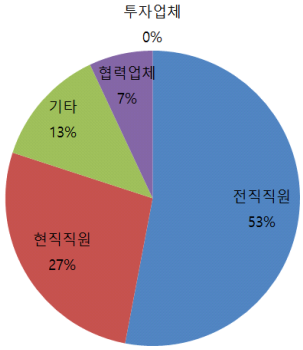
결과 기술의 주요 수요 국가는 중국(46%)로 가장 많으며, 대만 · 미국 · 일본 등 국내 기술의 발달로 인하여 선진국으로 다양화 되고 있는 추세이다.



(그림 3) 해외로 유출되는 산업기밀의 수요 국가

3.2 산업기밀 유출범죄의 주체와 동기에 따른 분석

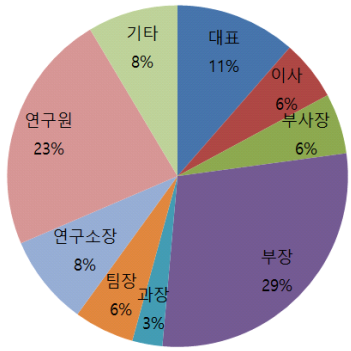
최근 몇 년간 발생한 산업기밀 유출사고를 통해 살펴보면 일반적인 범죄와 다른 특징이 있다. 산업스파이의 주체가 대부분 전 · 현직 직원이라는 점이다. (그림 4) 산업기밀보호센터의 산업스파이 주체를 살펴보면 산업기밀 유출범죄 같은 경우는 피해자가 전혀 모르는 사람이 아닌 함께 일하거나 일했던 전 · 현직 직원에 의해 일어나는 내부유출이 80%를 차지할 정도로 높게 나타나고 있으며, 그 외에 협력업체나 공동연구에 참여하는 피고용인에 의하여 이루어지고 있다.



(그림 4) 산업스파이 주체
(산업기밀보호센터, 2010년~2014년/최근 5년)

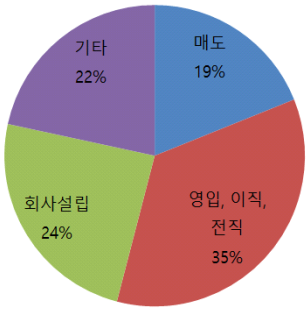
이들은 해당 기술의 가치를 잘 알고 기술 접근권한이 있는 사람들로써 금전적 유혹, 개인 영리, 인사·처우 불만 등의 이유로 언제든지 산업기밀 유출범죄에 가담하거나 주체가 될 수 있다. 산업기밀 유출범죄의 동기는 계획적인 것과 우발적인 것으로 나눌 수 있다. 대부분 금전적인 유혹과 회사설립 등 계획적으로 기업기술에 접근하며, 공금횡령 · 기밀자료를 무단 저장 등 내부감사에 의한 적발, 승진 · 인사에 대한 불만, 불화로 인한 해임, 경영상태의 악화 등 사람이 심리적 변화를 느껴 발생하는 우발적 범죄 또한 주요 요인이다.

이렇게 발생한 산업기밀 유출범죄의 주도자 직책을 살펴보면 (그림 5)와 같다. 회사의 대표, 이사, 부사장 등 고위급 직책을 가진 임원들이 33%, 부장 29%로 해당 기업의 기술에 대하여 가치를 잘 알고 기업에서 기밀자료에 대한 접근권한이 높은 사람들이 대부분을 차지하고 있다. 또한 연구소장과 연구원 등 기술개발에 직접적으로 참여하여 기술에 대하여 가장 잘 파악하고 있는 연구관련 종사자들도 31%를 차지하고 있다.



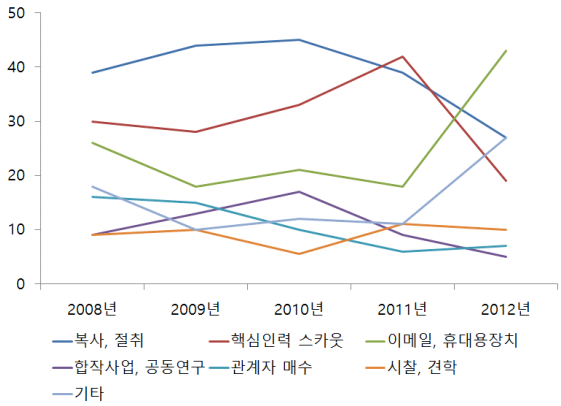
(그림 5) 산업기밀 유출범죄의 주도자 직책

유출된 산업기밀을 이용하여 산업기밀 유출범죄자들이 행하는 일은 다음 (그림 6) 같다. 개인의 계획적인 이직이나 다른 기업의 제안으로 인한 영입, 이직, 전직(35%)의 비율이 가장 높게 나타나고 있고, 유출한 기술을 직접 활용하여 경쟁 회사를 설립(24%)하는 경우도 많이 발생하고 있다. 또한 금전적인 이득을 취하기 위해 경쟁 기업이나 국가에 매도(19%)하는 경우도 적지 않게 나타나고 있다.



(그림 6) 유출된 산업기밀의 활용

산업기밀 유출범죄는 개인의 단독 범행도 많이 이뤄지고 있으나 2인 이상이 공모하여 범행을 저지르는 경우가 상당수를 차지하고 있다. 산업기밀 유출범죄의 피해기술이나 유출수단을 보면 (그림 7)과 같이 나타난다. 2011년 전에는 핵심인력 스카웃, 복사, 절취 등 직접적인 문서의 이동이나 지식을 가진 핵심인력의 이직으로 인한 기술유출이 발생하였는데, 2011년을 기점으로 위의 사례가 줄어들고 이메일, USB, 외장하드 등의 휴대용저장장치를 이용한 범죄기술이 많이 활용되기 시작하였다.



(그림 7) 산업기밀 유출범죄의 피해기술 및 유출수단
(새누리당 김한표 의원, 2013.10. 재구성)

최근 산업기밀 유출사건을 살펴보면 법에는 저촉되지 않으면서 합법을 가장한 산업기밀 유출사건이 발생하고 있다. 기업에 대한 인수합병, 매수(M&A), 컨설팅, 기술자문 등 합법적인 절차를 통하여 산업기밀을 유출해 가기 때문에 피해가 발생한 이후에야 범죄사실을 인지하고, 인지한다고 하여도 별다른 대응책을 마련하기 어렵다. 실제 국내에서 발생한 하이디스 사건(2002)을 보면 비오이그룹이 기술을 공유한다는 명분으로 양사의 전산망을 통합하였지만 인수한지 7개월만에 중국공장에서 하이디스의 기술을 활용해 LCD를 생산 하였고, 쌍용자동차 사건(2004)을 보면 쌍용자동차를 인수한 중국 상하이자동차가 '최대 주주'라는 지위를 활용하여 국내 기업의 첨단 기술을 해외로 유출하였다. 이 사건들은 합법을 가장한 산업기밀 유출사건이기 때문에 대응하기가 어려울 뿐만 아니라 국가의 경쟁력과 경제력까지 심각한 피해를 초래한다.

4. 산업기밀 유출범죄 분석 시사점 및 결론

본 논문에서는 산업기술 발전을 저해하는 산업기밀 유출범죄에 대한 조사와 분석을 통하여 산업기밀 유출에 따른 피해실태를 파악하고 발생원인, 유출경로 등 다양한 분류체계를 통하여 산업기밀 유출범죄에 대한 전반적인 흐름을 파악해 보았으며, 이에 대한 시사점과 해결방안은 다음과 같다.

첫째, 산업기밀 유출범죄는 매해 증가하고 있다. 지난 5년간 경찰이 적발한 산업스파이 범죄는 472건에 이르며 범죄에 따른 피해규모도 "50조 원"에 육박하며, 중소기업 4,700여 개의 연 매출과 맞먹는 금액으로 막대한 손실을 입히고 있다. 이러한 손실을 최소화하기 위한 범 국가적인 대응체계 마련과 중소기업의 보안체계 구축을 위한 CEO의 관심과 의식향상이 필요하다.

둘째, 2013년을 기점으로 국외로 유출하려는 건수가 급격하게 증가하였다. 이것은 세계시장에서 우리나라의 경쟁력이 있다는 것을 의미하며, 앞으로 산업기밀 범죄의 대상이 될 가능성이 매우 높다는 것으로 생각할 수 있다. 산업기밀보호센터의 기술유출 분야별 현황을 보면 우리나라가 높은 경쟁력을 가지고 있는 정밀기계(34%), 전기 · 전자(26%), 정보통신(14%) 분야에서 많은 산업기밀 유출사건이 일어나고 있으며

산업스파이의 표적 기술은 점점 대기업의 IT 분야 기술에서 중소기업의 정밀기계 분야로 이동 및 확대 되고 있다는 것을 알 수 있다. 또한 기술유출의 주요 국가는 중국이 절반을 차지할 정도로 많으며, 미국 · 일본 등 국내 기술의 발달로 인하여 선진국으로의 유출도 발생하고 있다. 이와 같은 문제를 해결하기 위하여 해외 진출 기업에 대한 보안관리를 전담할 수 있는 별도의 기구설립과 현지에서 근무한 직원들에 대한 보안의식 함양교육 등이 필요하다.

셋째, 산업스파이의 주체는 피해자가 전혀 모르는 사람이 아닌 함께 일하거나 일했던 전 · 현직 직원에 의해 일어나는 내부유출이 80%를 차지할 정도로 높게 나타나고 있다. 이들은 금전적인 유혹과 회사설립 등의 계획적 범죄가 83%로 대부분 계획적으로 기업 기술에 접근한다는 것을 알 수 있으며, 공금횡령 · 기밀자료를 무단 저장 등 내부감사에 의한 적발, 승진 · 인사에 대한 불만, 불화로 인한 해임, 경영상태의 악화 등 사람이 심리적 변화를 느껴 발생하는 우발적 범죄가 17%로 나타나고 있다. 기업의 보안시스템 구축 · 보안교육 등 내부 보안관리는 물론이고 직원들의 근무환경과 처우개선 노력의 병행이 필요하다.

넷째, 산업기밀 유출범죄의 주도자 직책을 살펴보면 회사의 대표, 이사, 부사장 등 고위급 직책을 가진 임원들이 33%, 부장 29%로 해당 기업의 기술에 대하여 가치를 잘 알고 기업에서 기밀자료에 대한 접근권한이 높은 사람들이 대부분을 차지하고 있다. 또한 연구소장과 연구원 등 기술개발에 직접적으로 참여하여 기술에 대하여 가장 잘 파악하고 있는 연구관련 종사자들도 31%를 차지하고 있다. 또한 개인의 계획적인 이직이나 다른 기업의 제안으로 인한 영입, 이직, 전직(35%)의 비율이 가장 높게 나타나고 있고, 유출한 기술을 직접 활용하여 경쟁 회사를 설립(24%)하는 경우도 많이 발생하고 있다. 또한 금전적인 이득을 취하기 위해 경쟁 기업이나 국가에 매도(19%)하는 경우도 적지 않게 나타나고 있다. 이것으로 보아 상대적으로 기술을 잘 파악하고 있고 기술을 유출할 수 있는 권한을 가진 직책에게 산업스파이 제안이 많이 오며, 산업기밀 유출범죄에 가담할 기회가 많다는 것을 알 수 있다. 이에 따라 핵심인력에 대한 분류 및 별도 관리가 필요하다.

다섯째, 산업기밀 유출범죄는 개인의 단독 범행도 많이 이뤄지고 있으나 2인 이상이 공모하여 범행을 저지르는 경우가 69%를 차지하고 있다. 산업기밀 유출의 경우에는 같이 기술을 개발하던 연구원들이 함께 공모를 하거나 고위직 임원이 직원을 포섭하여 같이 범죄를 저지르는 경우가 많다. 이와 같은 문제를 해결하기 위하여 산업기밀에 직접적으로 접근 가능한 연구인력에 대한 관리가 필요하다.

여섯째, 산업기밀 유출범죄의 피해기술이나 유출수단은 2011년 전에는 핵심인력 스카웃, 복사, 절취 등 직접적인 문서의 이동이나 지식을 가진 핵심인력의 이직으로 인한 기술유출이 주를 이루다가 2011년을 기점으로 위의 사례가 줄어들고 이메일, USB, 외장하드 등의 휴대용저장장치를 이용한 범죄기술이 많이 활용되기 시작하였다. Boris Parad(1997)의 저서를 보면 산업스파이의 유형을 72가지로 구분하여 정리하였으며 주요 방법으로는 스카우트(hiring away), 평가(evaluation), 전시회를 통한 상품의 유치(trade show exhibit), 유령회사(dummy/shell company), 컴퓨터 접속(computer hook-up), 입찰 경쟁(bidding war), 방문(visiting), 자료전송 중 가로채기(interception of data transmission), 정보 브로커 활용(information broker), 도청 및 감청(public airways), 위장취업(infiltration), 중고품 시장(used equipment market), 미인계(women intelligence agents), 인터넷(internet) 등 다양한 방법으로 분류하였다. 이와 같은 유출 수단에 대한 개별 보안관리 지침을 마련하고, 유출빈도가 높은 수단에 대한 보안관리를 위한 easy check 시스템을 도입할 필요가 있다.

최근 산업기밀 유출사건을 살펴보면 법에는 저촉되지 않으면서 합법을 가장한 산업기밀 유출사건이 발생하고 있다. 기업에 대한 인수합병, 매수(M&A), 컨설팅, 기술자문 등 합법적인 절차를 통하여 산업기밀을 유출해 가기 때문에 피해가 발생한 이후에야 범죄사실을 인지하고, 인지한다고 하여도 별다른 대응책을 마련하기 어렵다. 실제 국내에서 발생한 하이디스 사건(2002), 쌍용자동차 사건(2004)등 합법을 가장한 산업기밀 유출사건이기 때문에 대응하기가 어려울 뿐만 아니라 국가의 경쟁력과 경제력까지 심각한 피해를 초래한다.

본 논문은 국내에서 일어난 산업기밀 유출사고에 대한 분석을 통하여 산업기밀 유출에 따른 피해실태를 파악하고 다양한 분류체계를 통하여 산업기밀 유출범죄의 발생원인, 유출경로 등을 알아보았다. 산업기밀 유출사고는 점점 첨단화 · 지능화 · 고도화 되어 가고 있으며, 이에 따른 대응방안을 마련하는 것이 시급하다. 따라서 본 논문을 통해 산업기밀 유출범죄에 대한 전반적인 흐름을 파악하고 관련 연구에 대한 기초자료가 될 수 있기를 기대한다.

참고문헌

[1] 정연덕, “직무발명 관련 과학기술연구자의 권리보호,” 서울대학교 노동법연구, 제23권, pp. 281-307, 2007.
[2] 박성필, ‘기술유출 방지를 위한 핵심인력 보상체계′, 국가정보원 산업기밀보호센터, 2009.
[3] 이창무, “산업보안의 개념적 정의에 관한 고찰,” 한국산업보안연구, 제2권, 제1호, pp. 73-90, 2011.
[4] 노시영, ‘기술유출 방지를 위한 정보시스템 보안방향’, 국가정보원 산업기밀보호센터, 2007.
[5] 이창환, “보안정책에 미치는 영향요인에 관한 연구: 기업보안관리 담당자 인식조사 중심으로,” 가천대학교 대학원, 2011.
[6] 김원준, 이재훈, ‘경찰청 브리핑’, 경찰청, 2012.
[7] 백영준, “영업비밀보호법의 適用上 限界,” 한국산업재산권법학회 논집, 제23권, pp. 37-61, 2007.
[8] 한국산업기술진흥협회, ‘중소기업 산업기밀관리 실태조사 보고서′, 중소기업청, 2008.
[9] 산업기밀보호센터. ‘산업보안정보′, 산업기밀보호센터.
[10] B. Parad, ′Commercial Espionage: 79 Ways Competitors Can Get Any Business Secrets′, Global Connection, 1997.

[저 자 소 개]

장 항 배 (Hangbae Chang)

2006년 연세대학교 정보시스템관리 박사
2007년 대진대학교 경영학과 조교수
2012년 상명대학교 경영학과 조교수
2014년 중앙대학교 산업보안학과 부교수

email : hbchang@cau.ac.kr