산업보안의 중요성과 기술유출의 예방법

벤처기업에겐 앞서나가는 독창적인 지식정보가 존재기반이자 생존의 열쇠이다. 애써 개발한 첨단기술을 철저히 보호함으로써 벤처기업 스스로를 보호하고 국가경쟁력을 제고시킬 수 있다. 기술을 보호하고 지키기 위한 벤처기업인들의 적극적인 관심과 노력은 백번 강조하여도 지나침이 없다. 국가경쟁력을 흔들고 있는 핵심기술 유출의 심각성과 대처의 중요성을 알아본데 지난호에서 이어 이번호에는 구체적 유출사례와 유출경로 그리고 예방법에 대해 살펴본다.

우리나라는 최근 5년간 기술유출로 인해 22조원의 시장가치의 피해를 입은 것으로 추정되고 있으며 기술보호 수준의 미흡함과 유출사건의 은폐 속성을 고래할 때 피해액은 그 보다 훨씬 클 것으로 추정된다. 또 손실액 및 장래 기대이익을 고려하면 기술유출로 인한 손실은 엄청나다.

벤처기업의 핵심기술 유출 사례

사례 1. 바이오 테크놀로지의 기반을 이루는 미생물발효장비 생산업체인 코바이오텍 직원인 이모씨 등은 2001년 9월경 세포배양기, 자동공정시스템 등 미생물발효장비의 설계도면을 CD등에 담아 가지고 나와 바이오씨엔에스라는 동종회사를 설립해 이를 활용하는 한편, 2002년 12월경 중국 동방생물공정유한회사와 합작을 시도하고자 위의 자료를 누설하였다가 적발되었다.

사례 2. 경찰청 특수수사과는 2004년 5월 12일 국내 벤처기업 S사가 개발한 반도체 성능측정 장비인 '번인챔버' 설계도면이 유출된 사실을 적발했다. 이 사건은 C사의 강모 부사장이 경쟁업체인 S사의 전 생산부장 이씨를 매수해 번인챔프 설계도를 유출한 것이다. C사는 자체생산을 추진했다가 실패하자 3월 29일 일본의 협력업체로 유출했다. 설계도를 유출해 국내 첨단기술의 해외유출에 따른 피해 우려가 제기되고 있다.

사례 3. 원격화상교육 솔루션 개발업체인 텔리젠의 프로그래머 조모씨 등은 2003년 7월경 경쟁사인 포부를 설립한 후 그해 10월경까지 텔리젠의 개발환경을 이용해 동사에서 개발한 '웹튜더'와 동일한 기능을 가지는 '포부캠'을 만들어 메신저 등을 이용해 포부로 송부해 판매하다가 적발되었다.

핵심기밀의 요건과 유출경로

우리나라는 '기업비밀 침해행위의 형사상 주체'를 임직원 등 내부종사자뿐 아니라 제3자의 부정한 이익을 얻거나 기업에 손해를 가할 목적으로 그 기업에 유용한 영업비밀을 취득, 국내외에서 사용하거나 제 3자에게 누설한 침해자를 말하며 이들은 5년 이하의 징역 또는 재산상 이득액의 2배 이상 10배 이하의 벌금형을 물어야 한다.

'기업비밀'은 공연히 알려져 있지 않고 독립된 경제적 가치를 가지는 것으로서, 상당한 노력에 의해 비밀로 유지된 생산방법 · 판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말하며, 기업이 핵심기밀을 독점으로 사용하고 침해 시 법적인 사후보호를 받기 위해서는 위와 같은 요건을 구비해야 한다.

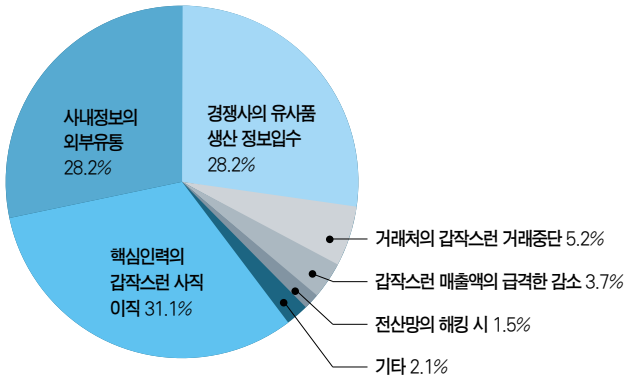
우리나라 기업비밀 유출사건은 약 44%가 해외로 유출되고 그중 80%가 IT기술로 밝혀졌다. 또 참신하고 획기적인 기술을 보유하고 있는 벤처기업의 피해도 점점 확산되고 있는 실정이다.

국가정보원이 500개 업체 임직원 1000명을 대상으로 조사한 자료에 의하면 인력스카우트, 관계자 매수에 의한 기업비밀 정보유출이 절대적으로 높은 수치를 차지하고 근래에 와서는 합작 및 기술협력에 의한 유출, 정보통신을 이용한 해킹, FAX, E-mail 및 도청에 의한 침해와 복사 유출도 높게 나타났다.

그밖에도 공동연구, 시찰견학 산업연수, 절취, 폐휴지수집 등의 방법으로 정보가 세나가고 있었다. 기업기밀은 공개되면 그 가치를 상실하므로 신속히 조사하고 공개되지 않도록 대응하여야 한다.

그러나 무엇보다 사전에 예방하여 기업비밀이 유출되지 않도록 보호하는 것이 가장 중요하다.

표1. 산업기밀의 유출 및 침해의 인지경로(2001년)



자료 : 국가정보원

기술유출 사고 관련기관 연락처

정보통신부	주간 : 750-1262, 야간 : 750-2160 http://www.mic.go.kr
한국정보보호진흥원	주 · 야간 : 118(지방은 02-118) http://www.cyber118.or.kr
국가정보원 정보보안 119	주 · 야간 : 3432-0462 http://www.nis.go.kr
경찰청 사이버테러대응센터	주 · 야간 : 02-3939-112 http://ctrc.go.kr

기업비밀 유출 방지 요령

기업비밀을 효과적으로 보호 · 관리하기 위해서는 기술을 보호하려는 의지와 노력이 필요하다. 기업비밀보호팀이나 감사반을 통해 문서정리 잠금장치, 파지방치유무, 출입문 잠금장치, 보관함, PC암호조치 여부, E-mail통신현황 등을 정기적으로 점검하는 한편, 기업비밀이 포함된 문서, 재직·퇴직 사원, 방문객 관리에도 신경을 써야 한다. 또 타사로부터 침해소송을 당하지 않기 위한 노력도 필요하다.

1) 기업비밀이 포함된 모든 서류에 비밀을 포함하고 있다는 표시와 함께 유출금지를 알리는 경고표시를 함은 물론, 중요한 기업비밀일수록 격리된 장소 및 용기에 보관하여 비밀누설의 가능성을 최소화하는 노력이 필요하다. 기업비밀문서는 최소의 인원으로 취급자의 범위를 제한하는 한편 비밀관리기록부를 비치하여 출납을 기록함으로써 관리상태를 정기 또는 수시로 점검한다.

2) 사원의 채용시 재직 또는 퇴직후 일정기간 동안 비밀유지를 의무화하는 계약을 체결하거나, 그 근거규정이 될 수 있는 기업비밀의 누설금지, 경쟁기업으로의 전직제한, 경쟁적 창업행위의 금지 등을 내용으로 하는 근거규정을 사규로서 마련한다.

3) 신입사원은 물론 재직자에게도 기업비밀 보호에 관한 지속적인 직무교육을 실시하여 기업비밀에 관한 관리방법을 철저히 주지시킴은 물론 퇴직 후에도 기업비밀보호를 위한 책임과 의무를 준수하여야 한다는 기본인식을 가지도록 한다.

4) 외래 방문객의 경우는 사전에 방문목적을 파악하여 방문증을 패용하도록 하고, 가급적 기업비밀이 공개될 우려가 있는 장소의 출입을 제한하도록 하며, 특정상황에서는 방문객에게 비밀준수 각서에 서명토록 할 필요가 있다.

5) 기업은 자신의 기업비밀을 보호하기 위한 적극적인 노력은 물론, 타사로부터 침해소송을 당하지 않기 위한 노력도 필요하다. 예컨대, 신입사원이 다른 기업으로부터 전직해 왔을때 전직장에서 맺은 기업비밀 관리에 관한 계약 등을 검토하고, 이 과정을 통해 타회사의 종업원을 채용함으로써 부당한 스카웃이나 또는 기업비밀 침해로 인한 제소를 당하는 일이 없도록 대비해야 한다.

이외에도 기업비밀 유출을 막기 위해 관리제도 및 보존방법의 연구 등 기업비밀 전반에 관한 기획, 조정, 감독 업무를 수행할 수 있는 전담부서를 설치하는 것도 생각해 볼 수 있다.

또한 회사건물, 생산시설, 물류창고, 통신, OA장비 등 기업의 독자적인 보유 생산시설을 보안 유지하는 것이 좋다.

기업비밀 유출방지에 관심과 노력 필요

산업기밀의 유출을 막기 위해서는 주요부처에 전담조직을 만들고, 홍보와 지도교육을 할 수 있는 전문인력을 양성하여야 한다. 또 경영자의 의식과 실천의지는 기업의 윤리경영을 확립한다. 핵심기술 개발자는 영업비밀보호를 기본 소양으로 알고, 그외 책임과 의무를 다하는 마음가짐이 중요하다.

기업비밀이 유출되었을 때는 사고내용을 정확히 파악한 후 관련기관에 신고한 후 법적대응을 강구하는 것이 좋다.

우리 벤처기업이 개발한 첨단기술을 철저히 보호함으로써 업체 스스로도 보호하고 국가경쟁력도 제고시킬 수 있다. 이에 무엇보다 벤처기업인들의 적극적인 관심과 노력이 요구된다.