지적 재산 침해의 숨겨진 비용

사이버 절도와 지적 재산의 유실

저자 Emily Mossburg, J. Donald Fancher, John Gelinne
일러스트레이션 Lucy Rose

기업 네트워크 침해사고가 발생해, 귀중한 지적 재산(Intellectual Property, IP)이 알 수 없는 누군가의 손에 들어간 것을 알게 되는 것은 경영자의 끔직한 악몽이다. 미 정부의 연구소라면 그 사건은 외국의 정보요원이 새로운 무기체계의 청사진을 훔치려 한 시도일 수 있고, 바이오 제약회사라면 낮은 직급의 과학자가 개발 중인 암치료제의 기밀 데이터를 가져간 사건일 수 있으며, 게임 개발사라면 해커가 미공개된 최신 1인칭 슈팅게임을 빼내간 경우일 수 있다. 그리고 무엇보다 더 큰 문제는, 정보가 캐비닛 안의 서류철이 아닌 데이터의 형태로 존재하기 때문에 침해 사건이 몇 주일 혹은 몇 개월간 발견되지 않을 수 있다는 것이다.

일반적으로 대중에 공시하도록 규정되어 있는 신용카드, 고객의 건강정보, 기타 개인식별정보의 유출 사건과 같이 보다 익숙한 사이버 범죄와 비교했을 때, 지적 재산의 사이버 절취는 대개 그늘에 가려져 있었다.

이런 종류의 시나리오가 경영자를 잠 못 들게 만드는 데는 그럴만한 이유가 있다. 지적 재산은 21세기 기업의 핵심이며, 혁신 추구의 원동력이며 경쟁력이고, 그 자체가 기업과 경제 성장의 동의어이기 때문이다. 오늘날 지적 재산은 개별 기업 가치의 80% 이상을 차지한다.[1] 그렇다면 수단, 동기, 기회로 무장한 침입자를 집요하게 추적하는 것이 놀라운 일은 아닐 것이다.

비록 지적 재산의 절취가 새로울 것도 없고 일부 지적 재산은 여전히 물리적인 수단만을 통해 획득할 수 있지만, 디지털 세계는 절취를 더 쉽게 만들었다.[2] 미국 지적 재산 집행 코디네이터(US Intellectual Property Enforcement Coordinator)인 대니 마티(Danny Marti)는 "기술의 발전, 모빌리티의 증가, 급속한 글로벌화, 인터넷이 가진 익명성은 기업 비밀의 보호를 점점 더 어렵게 하고 있다"고 말했다.[3](삽입글 "기업 비밀 보호를 위한 미 행정부의 노력"을 참고)

그러나, 일반적으로 대중에게 공시하도록 규정되어 있는 신용카드, 고객의 건강정보, 기타 개인식별정보의 유출 사건과 같이 보다 익숙한 사이버 범죄와 비교했을 때, 지적 재산의 사이버 절취는 대개 그늘에 가려져 있었다. 대부분의 사건이 광범위한 주목을 받지 못하는 이유는 아마도 대중에 대한 영향이 그다지 직접적이지 않기 때문일 것이다. 그리고 혹시나 브랜드나 평판에 손상이 가지 않을까 우려하는 기업들에게 이러한 사건을 공표하거나 보고하려는 유인이 적기 때문이기도 하다. 또한, 개인식별정보의 침해와 비교해 지적 재산의 도난은 그 결과를 파악하기가 더 어렵다. 당장 발생하는 직접적인 비용은 더 적지만 잠재적인 영향은 몇 개월 혹은 몇 년에 걸쳐 확대될 수 있다. 개인식별정보의 도난은 즉각적으로 고객, 신용등급, 브랜드 평판에 손실을 미치지만, 지적 재산의 손실은 시장 선점자로서의 이점을 뺏기고, 수익성 측면에서 손실을 입으며, 최악의 경우에는 사업의 전 부문을 경쟁자나 모방 기업에게 빼앗길 수 있음을 의미한다.

경영진들이 이러한 간접적인 가설상의 영향을 정확히 측정하는데 어려움을 겪는 것은 이해할 만 하다. 그 결과 그들은 절취 사건을 비밀로 숨기고, 지적 재산의 사이버 도난에 대해 마땅한 주의를 거의 기울이지 않는다.[4] 기업의 지적 재산과 관련된 사이버 공격의 광범위한 영향에 대한 고려 없이, 기업은 종종 지적 재산의 보호와 사고 대비에 적절한 우선 순위를 부여하지 않고 있다.

경영진에게 좋은 소식은 일반적으로 사용되는 가치평가 및 재무 모델링 원칙에 기반해서 지적 재산의 사이버 도난으로 인한 손실 정도를 측정하는 방법론이 있기 때문에, 이를 이용해 광범위한 기업 사이버리스크 관리프로그램 내에서 지적 재산의 위치를 결정할 수 있다는 점이다. 지적 재산을 둘러싼 리스크, 이의 잠재적인 손실, 그 손실이 해당 기업에 미칠 수 있는 영향에 대해 더 잘 알 수 있다면, 경영진은 지적 재산 도난의 전체적인 결과를 이해할 수 있으며, 사이버리스크 관리 프로그램을 기업의 지적 재산 관리 및 전략적 우선순위와 잘 조율할 수 있을 것이다.

기업 비밀 보호를 위한 미 행정부의 노력

미 대통령은[5] 혁신 및 창의성 부문의 글로벌 리더인 미국의 지위를 흔들 수 있는 위협, 특히 민간 기업 및 정부의 후원을 받은 기업 비밀 도용을 포함한 위협에 대해 끊임없이 경계하고 있다. 기술의 발전, 모빌리티의 증가, 급속한 글로벌화, 인터넷이 가진 익명성은 기업 비밀의 보호를 점점 더 어렵게 하고 있다. 다양한 기관이 협력하는 다면적인 전략을 통해 미 행정부는 외국 정부들과 공조해 국제적인 집행 노력을 강화하고, 기업 비밀을 보호하기 위한 산업 주도의 모범 사례를 개발하기 위해 공공 및 민간 부문의 활동을 촉진하고, 기업 비밀의 유용이 기업과 미국 경제에 미치는 해악을 이해관계자들과 일반 대중에게 알리도록 대중의 인식을 고취하고 있다.

이 전략의 일부로서 기업들은 또한 기업 비밀 보호에 있어 증가하는 도전과제들을 해결하는 데 중요한 역할을 수행한다. 기업 비밀 절취에 대한 일차 방어선은, 강건하고 제대로 구현된 사이버 보안 및 데이터 관리/보호 전략의 존재와 중요 사건 발생에 대비한 위기상황 계획이다. 미 행정부는 기업들로 하여금 기술발전 속도에 보조를 맞춘 기업 비밀 보호 접근법을 포함해 기업 비밀 절취의 리스크를 경감시킬 수 있는 실무 방안의 상호 공유를 고려토록 장려하고 있다.[6]

— 대니 마티, 미 지적 재산 집행 코디네이터, 미 대통령실

현대 지적 재산 절취의 양태

과거의 지적 재산 절취는 주로 회사에 불만을 가졌거나 절취의 기회를 가졌던 직원이 서류, 컴퓨터 디스크, 시제품을 들고 사라져 버리는 형태였다. 범인은 기업 비밀에 대해 직접적인 지식을 갖고 있거나 어떤 행태로든 범행을 저지르고 기밀을 빼낼 수 있도록 물리적인 접근이 가능했다. 그래서 물리적 접근이 가능한 소수의 사람들만이 용의선 상에 올랐으며, 때문에 절취는 위험한 일이었다.

이와는 대조적으로 디지털 시대의 지적 재산 절도범들은 상대적인 익명성을 띠고, 언제 어디서나 범행을 저지를 수 있어 용의자의 범위도 넓고 깊어졌다. 전·현직 직원들, 경쟁업체, 범죄자와 재미 삼아 범죄를 저지르는 해커, 외국 정부의 요원들도 범인이 될 수 있다. 지적 재산 자체가 원래의 목적일 수도 있고, 기회가 생겨 이를 악용한 것일 수도 있다. 대규모로 기업의 데이터를 훔치는 것이 더 쉬워지면, 훔친 대규모 데이터 안에서 지적 재산에 해당하는 것들을 발견할 가능성은 더 높아진다.[7]

시장에 먼저 진출해야 시장의 승자가 될 수 있을 때, 지적 재산을 훔치는 것—또는 도난 당한 지적 재산을 사는 것—은 맨땅에서 혁신에 투자하는 것보다 훨씬 빠르고 비용도 적게 든다. 일부 분야에서는 연구개발(R&D) 비용은 증가하고 있는 반면 시장의 기회는 축소되고 있다. 예를 들자면, 성공할 수 있는 유전(油田)의 수가 제한적이고, 특허를 받을 수 있는 특정 질병 치료용 신약 개발의 진입장벽이 높기 때문에 경쟁자의 기업 비밀을 훔치는 것이 빠른 이익을 향한 보다 확실한 길을 보장할 수도 있다.

가장 도난의 위험이 높은 자산은 무엇일까? 당연히 절도범들은 특허와 상표권과 같은 이미 공공 영역에 위치한 지적 재산보다는 회사의 기밀을 주로 노리게 된다. 범죄자

들에게 가장 가치 있는 것은 쉽게 현금화 할 수 있는 기업 비밀과 독점적 기업정보이다. 기업 비밀에는 신약 실험 데이터, 페인트 제조 공식, 생산 공정, 독특한 디자인 등이 해당되며, 독점적 기업정보에는 셰일 오일의 매장지에 대한 지질학적 조사결과, 합병 계획, 기업 협상 및 전략에 대한 정보가 해당된다. 데이터 애널리틱스를 위한 소프트웨어 코드와 같이 저작권이 있는 데이터 또한 요즘에 인기 있는 목표물이 되었다. 다양한 불법 시장에서 가치 있는 정보의 폭이 넓어 졌기 때문에 지적 재산 절취는 거의 모든 산업과 부문에 걸쳐 문제가 되고 있다.

지적 재산 사이버 절취의 손실 범위 측정

컴플라이언스와 공시 규제 요건으로 인해 기업들은 사이버 공격의 영향에 주의를 기울이게 되었다. 굴지의 유통 기업, 의료 서비스 업체, 은행, 정부 기관에서 발생한 잘 알려진 사고들을 살펴보면, 이들 규제 요건은 대개 개인식별정보, 결제 데이터, 개인건강정보의 도난에 초점을 맞추고 있다. 대부분의 주(州)정부는 정보가 도난 당했을 수 있는 고객과 직원들에게 이러한 공격에 대해 공개하도록 규제하고 있으며[8], 연방 보안 규제는 중요한 영향이 예상되는 주요 개인식별정

그림 1. 사이버 공격의 14가지 영향 요인

그래픽: Deloitte University Press | DUPress.com

보 관련 사이버 사건을 공시하도록 조직들에게 요구하고 있다.[9] 그 결과, 기업은 사이버 공격의 영향을 논할 때 고객에 대한 고지, 신용도 모니터링, 법률적 판결, 규제적 징벌을 포함한 이들 사이버 공격에서 공통적으로 발생하는 비용에 집중하는 경향을 보인다. 이에 대한 전례가 많기 때문에, 경영진들은 잘 알려진 데이터 침해 사건의 정보에 근거해 개인식별정보 유출 시 발생할 수 있는 회사의 손실을 계산할 수 있다.

반면, 잠재적인 지적 재산 절취의 비용에 대해 추측하려고 하면, 이들 비용의 대부분이 "숨겨져" 있거나 간접적이어서 파악하고 계량화하기가 어렵다 (그림 1). 비용에는 규제 준수, 홍보, 변호사 비용, 사이버 보안 개선 등과 같이 잘 알려진 비용들도 있지만, 브랜드 가치 훼손, 계약 취소, 미래 기회 상실과 같이 몇 개월이나 혹은 심지어 몇 년간에 걸쳐 발생하는 눈에 잘 띄지 않고 구체적이지 않은 비용들도 존재한다. 경영진이 이러한 장기적이고 간접적인 비용을 평가하기가 어렵기 때문에, 잠재적인 지적 재산 절취의 전체적인 범위를 파악하고 계량화하는 것이 사이버 방어 전략의 우선순위를 정하고자 하는 기업의 역량에 있어 필수적이다.[10]

사이버리스크에 대한 재무 리스크 모델의 적용가능성을 고려할 때, 딜로이트 리뷰 이번 호 기사인 "사이버리스크 계량화"에서는 표준 모델이 유용할 수 있지만 해당 기업의 속성에 부합하는 잘 정의된 사이버리스크 모델의 개발이 중요하다고 역설한다.[11] 여기서 설명한 접근법은 특정 시점에서 조직마다 다른 특수한 환경을 고려한다.

사이버리스크를 정확히 추정하려면 충분한 정보에 기반한 의사결정이 필요하고, 경영진은 시간이 지남에 따라 전반적인 영향 범위가 어떻게 펼쳐질 수 있는지를 정확히 이해해야만 한다. 그러기 위해서 기업은 침해 후 영향이 지속될 수 있는 충분한 기간을 고려해야 하는데, 이는 크게 다음 세 국면으로 나눌 수 있다.

사고 분류. 공격을 발견하고 나서 며칠간 또는 몇 주간 동안, 기업은 대응팀을 급히 구성해 무엇이 발생했는지 분석하고, 명백한 간극을 메우고, 비상 사업연속성 대책을 작동하고, 법률 및 홍보 차원에서 대응한다.

영향 관리. 그 다음 몇 주 혹은 몇 개월간, 기업은 관계 및 IT 인프라 복구 또는 증가하는 법률적 문제의 처리 등을 포함한 사고의 직접적인 결과를 처리하고 축소하기 위해 대응 절차를 실행한다.

사업 복구. 그 다음 몇 개월 혹은 몇 년 동안, 기업은 적극적으로 사업 손해를 복구하고, 정보 절취를 통해 수익을 기대하는 경쟁업체에 역공을 노리며, 장기적 대책에 초점을 맞춰 사이버 방어를 강화한다.

각 단계에서 발생하는 비용을 모델화하기 위해, 조직은 자신의 여러 전문 분야를 종합한 접근법을 적용할 수 있는데, 알고 있는 사업 지식을 이용해 발생 가능성 있는 사이버 공격의 시나리오를 구상하여 어떤 행동이 필요한지 파악할 수 있다. 그 후 지적 재산 절취의 진정한 비용을 계산하기 위해 일반적으로 활용되는 가치평가 방법을 적용할 수 있다. 위의 세가지 국면 전반에 비용을 대응시킴으로써 경영진은 더욱 정확하게 전체 대응주기에 걸친 기업의 사이버리스크의 구체적인 모습을 파악할 수 있다.

시나리오: 피해의 범위

위에서 묘사된 평가 과정을 설명하기 위해 400억 달러의 기업가치를 가진 가상의 IT 기업을 대상으로 한 다음의 시나리오를 살펴 보자. 씽투씽(Thing to Thing)이라는 이름의 이 기업은 사물인터넷 기술의 관리를 지원하는 네트워크 제품을 개발한다.

시나리오 기반의 방법론—다양한 범위와 강도의 구체적인 보안 침해를 상정하고 그 영향을 모델링하는 것—을 적용하면 실제적이고 자세하게 지적 재산의 라이프 사이클을 탐색할 수 있다. 그 결과 민감한 기업 정보의 이동과 저장에서 발생하는 리스크를, 이것이 내부적, 외부적, 악의적 또는 우연적이든 그 성격에 관계없이 더 깊이 인식할 수 있다.

실리콘밸리에 위치한 이 기업은 직원 수가 6만명, 영업이익률이 12.2%이며, 핵심 사물인터넷 네트워크 제품의 개발 및 출시를 지원하기 위해 R&D, 생산, 마케팅에 상당한 투자를 해왔다. 제품 출시 6개월 전, 연방 기관이 씽투씽에게 신제품 개발 정보를 호스팅하는 기업의 설비 중 하나에서 사이버 침해가 발생했음을 알려줬다. 초기 조사에서 외국 정부를 위해 일하는 사이버 침입자가 30개의 네트워크 장비 제품라인 중 15개와 관련된 지적 재산을 절취했음이 밝혀졌는데, 이들 제품라인은 향후 5년 간 기업 총 매출의 1/4에 공헌할 것으로 예상됐었다. 해커의 동기는 분명치 않았으나, 분석 결과 해커는 그 정보를 이용해 이전에 밝혀지지 않은 설계 상 결함을 밝히거나 악용할 수 있고, 더 심각한 경우 씽투씽의 새로운 제품에 악성 코드를 심을 수도 있다는 것이 밝혀졌다. 상황은 더욱 악화되어, 침해 경보 30일 후 실리콘밸리의 한 유명 블로거가 그 외국 정부가 그 네트워크 제품을 역설계(Reverse engineering, 제품을 분해하여 설계를 알아낸 후 복제하는 것)했다는 증거를 발표했는데, 이는 씽투씽이 시장 경쟁에서 패배해 기업 가치가 크게 하락할 수 있음을 시사했다.

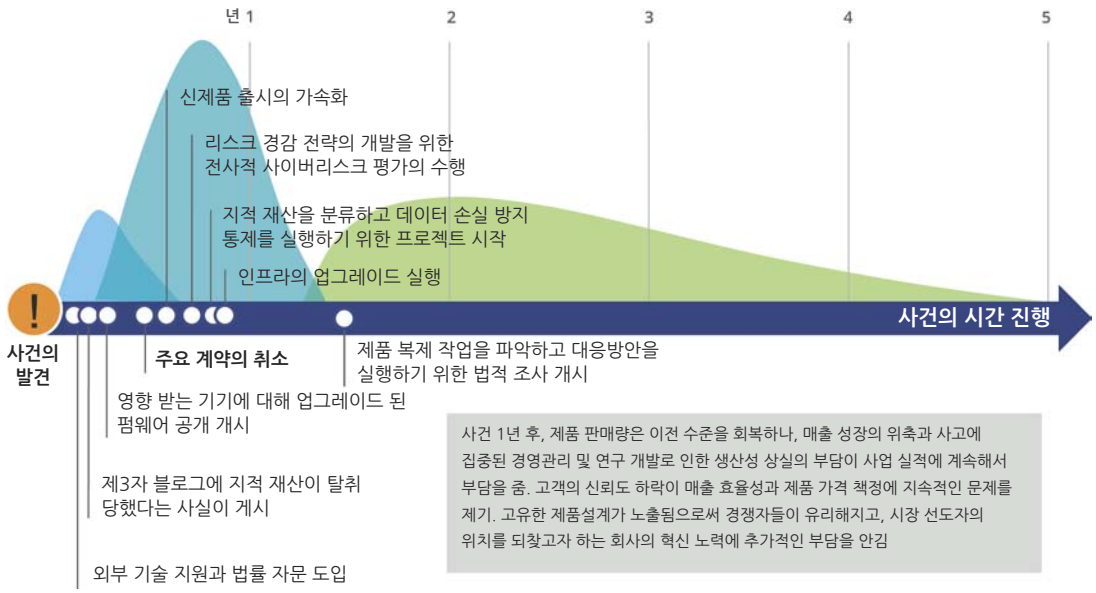
초기의 사고 분류 국면에서, 씽투씽은 이해관계자들에게 다가가고 대중 이미지 캠페인으로 체면을 세우기 위해 최고의 홍보회사에서 거물급 인사들을 채용한다. 또한, 회사는 사건 조사를 위한 변호사들 및 디지털 포렌직 업체, 사건 분류를 돕고 침해를 해결하기 위해 사이버 보안 회사를 고용한다.

영향 관리 국면에서는, 계획되어 있던 신제품 판매 및 출하를 연기할 수 밖에 없었으며, 그 사이에 공격 대상이었던 기기들의 취약점을 수정해주는 펌웨어(Firmware)를 개발해 공개한다. 연구개발 인력은 이미 과부하가 걸린 상태였지만, 씽투씽은 사이버 절취범에게 추월 당하지 않도록 새로운 기기의 출시를 2달 앞당기기로 결정하고, 이로 인해 회사는 추가적인 R&D 인력을 채용해야 한다. 하지만 자사의 네트워크 환경 및 제품을 보호하는 씽투씽의 능력에 대한 고객의 신뢰 상실은 더 심화된다. 정부는 주요 계약을 취소했는데, 이는 매출의 5%에 해당할 것으로 추정되었으며 또한 기존 고객들이 떠나가면서 5%의 추가 손실을 입게 된다.

장기적인 사업 복구 국면에서는, 회사는 더 강력한 사이버리스크 관리 전략 및 실행 계획을 입안하기 위해 전사적인 평가를 수행한다. 여기서 다양한 추진계획들이 도출되어, 지적 재산 재고조사, 분류, 보호 프로그램, 전사적 보안 인프라의 업그레이드 프로젝트 등이 계획된다. 이들 모두가 추가적인 비용을 발생시킨다. 게다가, 사건 관련 조사 및 소송 비용이 수년 동안 증가하고, 고객과 이해관계자들의 신뢰를 재구축하기 위한 홍보비도 증가한다. 제품 판매는 1년 후 결국 정상적인 수준을 회복하나, 사고를 처리하기 위해 인력을 재배치한 결과로 발생한 여러 부서의 운영 차질로 인해 운영 효율성은 떨어진다.

그림 2의 사이버 사건 대응 시각표는 침해 시나리오의 사

그림 2. 씽투씽의 사이버 사건 대응 시각표



주: 영향 곡선은 대응 과정의 세 국면에 걸쳐 발생하는 비용의 상대적인 규모를 나타냄 **그래픽: Deloitte University Press | DUPress.com**

건 및 영향이 시간의 흐름에 따라 어떻게 전개되는지를 보여준다. 사이버 공격의 전체적인 결과를 일반적으로 구성하는 14개의 영향 요소[12] 중 일부—침해사고 고지 비용 또는 사후 모니터링의 제공 등—는 개인식별정보 데이터의 침해에 해당되기 때문에 씽투씽의 사례에는 적용되지 않는다. 회사는 법률 자문, 홍보, 조사, 사이버 보안의 개선 등 기타 직접 비용을 감당해야 하지만, 이들은 상대적으로 파악하기 쉽고 어느 정도까지는 계량화하기도 쉽다.

지적 재산 절취의 비용 중, 보다 간접적이고 나중에 발생하는 비용은 파악하거나 계산하기 힘든데, 도난 당한 지적 재산 그 자체의 가치 손실, 운영 차질, 계약 취소, 브랜드 가치 훼손, 보험료 상승 등이 이에 해당한다(표 1). 씽투씽의 분석가는 이 지적 재산 사이버 절취 사고의 비용이 전 기간에 걸쳐 총 32억 달러가 넘는다고 산출한다.

이제부터 우리는 지적 재산 절취로 인해 씽투씽에 발생한 두 가지 주요 손실—네트워크 제품의 무결성 훼손과 5년짜리 정부 계약 취소—을 골라 비구체적인 비용에 대한 평가 방법론을 설명하고자 한다. 도난 당한 지적 재산의 영향과 계약 취소를 평가하기 위해 다음과 같이 일반적으로 사용되는 원칙들을 적용할 것이다.

- **존재/부존재 가정법.** 이 접근법은 절취가 발생하지 않았을 경우의 가치와 비교해 절취 이후 자산의 가치를 추정한다. 그 차이가 사고로 인한 영향의 가치이다.

- **미래 이익(비용)의 현재가치.** 돈의 시간 가치를 고려해 자산의 예상 이익을 계산하기 위해, 비용을 공격이 발견된 특정 시점과 결부시킨다.

표 1. 씽투씽의 사고 비용

비용 요소	비용 (백만 달러)	총 비용 중 비율
기술적 조사	1	0.03%
대고객 침해사고 고지	해당 사항 없음	0.00%
사후 고객 보호	해당 사항 없음	0.00%
규제 준수	해당 사항 없음	0.00%
홍보	1	0.03%
변호사 비용과 소송	11	0.35%
사이버 보안의 개선	13	0.40%
보험료 상승	1	0.03%
부채 조달 비용 증가	해당 사항 없음	0.00%
운영 차질	1,200	36.83%
고객 관계의 가치 상실	해당 사항 없음	0.00%
취소된 계약의 가치	1,600	49.11%
브랜드 가치 훼손	280	8.59%
지적 재산의 유실	151	4.63%
합계	3,258	100.00%

- **산업 벤치마크 가정.** 다양한 자산과 관련된 가치 혹은 재무적 영향을 산출하기 위해 전형적인 산업 벤치마크들이 사용된다. 기술이나 브랜드 사용에 대한 저작권료 등이 이에 해당한다.

지적 재산 절취의 가치 계산에 이러한 원칙을 사용하는 데 덧붙여, 기업은 그 지적 재산의 내용연수가 5년이라고 가정한다. 씽투씽의 시나리오에서는 지적 재산 절취의 영향으로 제품 라인 총 매출액의 25%가 영향을 받는다고 가정한다. 또한 추가적인 재무적 영향을 계산하기 위해 실현 가능했던 지적 재산 로열티 수익률을 2.5%로 가정하는데, 이는 비교 가능한 관련 기술들의 사용권 계약 및 상장된 하드웨어 테크기업들의 이익 마진율을 기초로 한 것이다. 이 로열티 수익률은 궁극적인 재무적 가치를 평가하는 데 사용된다. 최종적으로, 이러한 유형의 지적 재산과 관련된 리스크에 의거해 12%의 할인율을 적용, 위에서 설명한대로 필요한 계산을 수행해 현재가치를 구한다. 이러한 재무적 모델링 기법과 그 기초가 되는 가정들을 사용해 산출한 지적 재산 유실의 비용이 대략 1억 5천만 달러에 해당한다는 결론이 도출된다.

정부 계약의 가치를 계산하기 위해 또 다시 씽투씽의 시나리오에서 5년간의 정부 계약이 회사의 총 연간 매출액의 5%에 달한다고 가정함을 상기하자. 그 계약이 유효한 경우 5년 간 발생할 회사의 순 현금흐름을 12%의 할인율로 할인하면 150억 달러의 가치가 산출된다. 그 계약의 상실로 연 매출액은 5%, 이익률은 2%가 감소하게 되며 (매출액이 감소하면 회사의 영업이익률은 낮아지는데 고정비가 줄어든 매출액에 배부되기 때문이다) 그 결과 16억 달러 이상의 손실을 입게 된다.

이 두 사례는 표 1에서 볼 수 있는 것처럼 지적 재산 사이버 도난의 총비용 중 일부일 뿐이다. 경영진이 지적 재산 도난으로 인한 손실의 전체적인 규모를 파악하지 못하고 있는 상황에서, 사업에 미치는 실제 영향은 훨씬 더 클 수 있다. 실제로 시나리오에 따른 두 가지 손실의 규모는 1억 5천만 달러인데, 이는 32억 달러에 달하는 총손실 중 아주 작은 부분만을 보여줄 뿐이다.

포괄적인 지적 재산 방어와 대응 준비도

이런 시나리오를 도출하는 이유는 놀랄 만큼 큰 숫자로 충격을 주려는 것이 아니다. 그보다는 사이버 침해의 여파에서 가장 중요한 영향을 조명함으로써 경영진이 지적 재산 도난의 전체 결과를 이해할 수 있게 하려는 것이다. 일단 경영진이 디지털 지적 재산의 보호가 중요하다는 점을 인식하게 되면 이런 시나리오는 조직의 준비 수준을 점검하는 가이드가 될 수 있다. 가능한 공격의 시나리오를 철저히 검토하고 어떻게 사업이 영향을 받을 수 있는지에 대한 실질적인 모습을 구체화해, 조직의 리더는 어떻게 지적 재산의 보호와 관련된 사이버리스크를 관리할지를 정보에 기반해 전략을 수립할 수 있다.

시나리오 기반의 방법론—다양한 범위와 강도의 구체적인 보안 침해를 상정하고 그 영향을 모델링하는 것—을 적용하면 실제적이고 자세하게 지적 재산의 라이프사이클을 탐색할 수 있다. 그 결과, 민감한 기업 정보의 이동과 저장에서 발생하는 리스크들을, 이것이 내부적, 외부적, 악의적 또는 우연적이든 그 성격에 관계없이 더 깊이 인식할 수 있다. 시나리오를 통한 작업은 지적 재산 유실의 숨겨진 비용과 폭넓은 영향도를 측정할 수 있다. 잠재적인 피해의 가치를 계산하고 보이지 않는 비용을 드러나게 함으로써 고위경영진과 이사회 수준에서 생산적인 대화를 시작할 수 있다. 경영진은 구체적인 데이터를 가지고 가장 큰 비용이 발생하는 영향을 최소화하기 위해, 어디에 투자하는 것이 최선인지를 정보에 기반해 결정할 수 있다. 막연하고 공포스러운 위협은 보다 명확히 정의되고, 적들은 적극적인 전략과 방어로써 물리칠 수 있는 대상으로 보이기 시작한다. 개발주기의 전 과정에 걸쳐 지적 재산 리스크를 평가함으로써 파괴적인 사이버 공격의 가능성에 대한 두려움을 확신으로 바꿀 수 있다. 사이버 절취범의 공격을 당한다 해도 조직은 대응하고 회복할 수 있다.

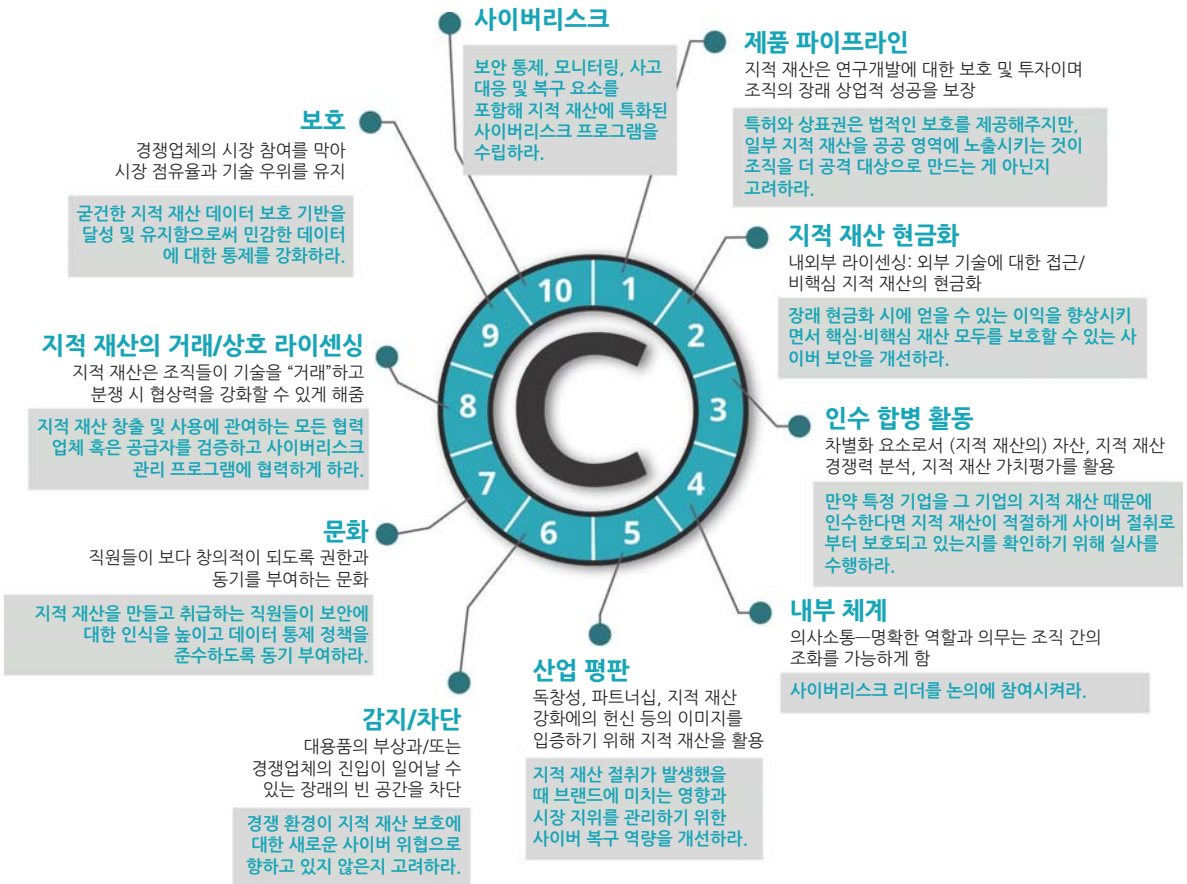
이렇게 강화된 인식으로 인해 회사의 전반적인 지적 재산 관리 전략에 사이버리스크 전략을 통합할 수 있다. 과거 딜로이트 리뷰에 게재된 "마법사와 트롤: 발전하는 기술, 특허 개혁, 지적 재산의 새시대(Wizards and trolls: Accelerating technologies, patent reform, and the new era of IP)"에서는 지적 재산 전략이 포괄해야 하는 9가지의 차원을 간략히 서술했었다.[13]

그러나 사이버 절도의 수단이나 동기가 증가함에 따라, 경영진은 사이버리스크의 차원 또한 기업의 지적 재산 관리 전략 프레임워크 안에 포함시켜야 한다 (그림 3). 전반적인 지적 재산 관리프로그램에 대한 고위경영진 수준에서의 거버넌스에 사이버리스크 관리 요소에 관한 명시적인 감독이 포함되야 한다. 그리고 기타 많은 지적 재산 관리 프로그램의 요소가 사이버리스크 이슈와 연관되어 있음을 인식해야 한다.

보다 포괄적인 사이버리스크 접근법은 조직의 지적 재산 전략을 효과적인 사이버리스크 프로그램과 동기화하고 조화시켜, 지적 재산의 라이프사이클 전반에 걸쳐 적절한 보안 통제, 모니터링, 대응 절차가 잘 수행되도록 개발자, IT, 법무, 리스크관리, 영업 및 기타 분야의 리더들을 참여시키기도 한다. 특히 개발 초기 단계에서 지적 재산의 가치를 이해하고 보호하는 것이 중요하다. 기업의 가장 중요한 비밀을 보호하기 위해 "선출원주의(최초의 출원자에게 권리를 부여하는 것)"나 "감지/차단"과 같은 지적 재산 보호전술에 의존하는 것이 중요하긴 하지만, 이로 인해 지적 재산은 "성숙 단계"에 이르기 전부터 가치를 가진다는 점을 간과할 수 있다. 개발 초기 단계에 있는 지적 재산은 특허 출원을 결정하기 훨씬 전부터 경쟁자나 적에게도 동일한 가치가 있을 수 있다. 따라서, 디지털 형태를 가진 지적 재산은 개발과정이 진행될수록 보호를 시작해야 할 필요성이 기하급수적으로 증가한다. 적어도 적대적인 기업이 회사의 가장 소중한 기밀에 접근하고 이를 훔쳐갈 수

그림 3. 효과적인 IP 전략의 차원

기업 IP 관리 프로그램은 잘 정의된 사이버리스크 관리 차원을 포함할 수 있도록 확장되어야 하며 사이버리스크 관련 이슈들은 필요에 따라 다른 9가지 요소 내에 통합되어야 한다.



그래픽: Deloitte University Press | DUPress.com

있는 속도에 상응하도록 빠르게 대응해야 한다.

성장, 시장 점유율, 혁신에 있어서 지적 재산과 사이버리스크의 중요성을 고려한다면, 지적 재산과 사이버리스크는 최고경영진 수준에서 관리되는 여타의 전략적 추진계획들과 함께 다뤄져야 한다. 최고경영진이 중요하게 고려해야 할 또 한가지는 반드시 조직의 지적 재산 전략 중 사이버리스크 요소가 더 폭넓은 전사적 리스크 접근법과 IT/사이버리스크 프레임워크 내에 잘 조화되도록 해야 한다는 점이다.[14] 예컨대, 지적 재산의 사이버리스크 노출 정도를 측정하기 위한 리스크 평가 방법론이나 지표들이 기업의 다른 분야에서 리스크를 측정하는 방법과 일관성이 있어야 한다. 지적 재산 요소를 포함한 전체 사이버리스크 프로그램은 조직의 전사적 리스크 관리 프로그램 하에서 실행되어, 경영진이 전체 리스크의 맥락에서 지적 재산 관련 사이버리스크를 들여다 볼 수 있게 지원해야 한다.

이런 맥락 내에서 리스크를 인식한다면, 경영진들은 사이버리스크 프로그램이 업무 프로세스에 얼마나 잘 통합되어 있는지 뿐만 아니라, 회사가 얼마나 효과적으로 지적

성장, 시장 점유율, 혁신에 있어서 지적 재산과 사이버리스크의 중요성을 고려한다면, 지적 재산과 사이버리스크는 최고경영진 수준에서 관리되는 여타의 전략적 추진계획들과 함께 다뤄져야 한다.

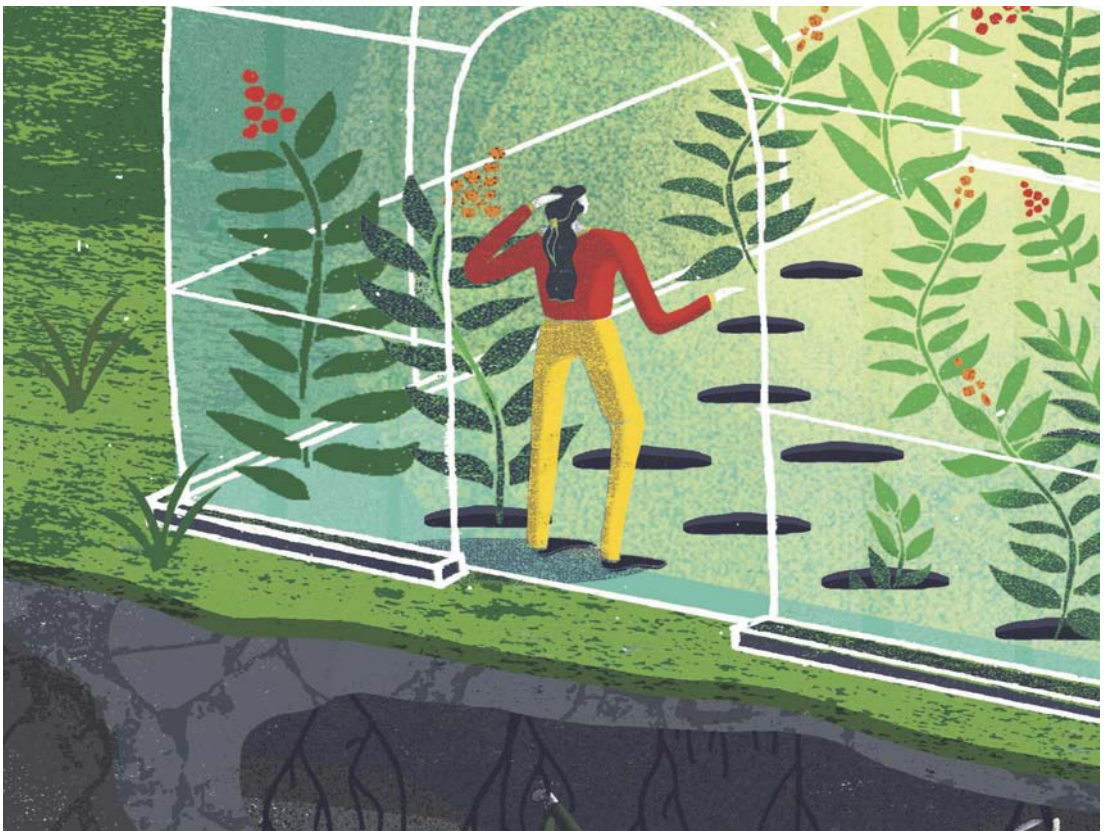
재산을 관리하는지 입증하기 위해 어려운 질문을 제기할 수 있다. 실무적으로 아래의 질문들이 이에 해당한다.

- 지적 재산에 접근하는 사람 수를 어디까지 줄일 수 있는가?
- 지적 재산을 취급하고 보호하는 일상 업무 중 취약한 연결 고리는 어디인가?
- 회사의 데이터 관리와 보호 전략이 충분하며 잘 이해되고 있는가?
- 회사의 가장 전략적인 (지적 재산) 자산에 대한 위협을 감지하기 위해, 민간 분야 및 정부의 사이버 위협 공유 역량을 충분히 활용하는 것을 포함해, 사이버 모니터링 역량이 잘 정비되고 우선시 되고 있는가?
- 만약 회사의 혁신 생태계가 협력업체, 공급자, 제3자에게까지 확장된다면, 통제와 정책이 기업의 경계를 넘어 적절히 확장될 수 있는가?
- 선의의 연구자나 개발자가 회사의 데이터 저장 및 관리, 유지 정책에 대해 잘 알고 있음으로 인해 부주의한 정보 노출이 일어나지 않고 있는가? 이 마지막 항목은 "보호"는 단지 기술적인 기능이 아닌 인간 인식의 작용이라는 점을 시사한다. 지적 재산의 전 라이프사이클에 걸쳐 조직원은 소중한 회사의 기밀을 보호해야 하는 자신들의 중요한 역할을 잘 인지하고 있어야 한다.

마지막으로, 정책과 기술 통제라는 전통적인 의미에서의 보안 개선으로 절취를 방지할 확률은 높일 수 있지만 완벽한 방지는 불가능하다. 침해에 잘 대응하는 조직은 그로 인한 손실을 경감할 수 있다. 절취로 인한 피해규모가 50억 달러에 달해야 할 필요가 없는 것이다. 사고에 대한 대응은 경험을 통해 배울 수 있지만 그렇다고 해서 진짜 사고가 터지기를 기다려야 된다는 의미는 아니다. 사이버 공격 시뮬레이션은 기술 조직과 영업 조직이 핵심 임무의 프로세스를 분석하고 복구하는 능력을 시험해 볼 연습장을 제공한다. 더 중요한 것은 전 조직이 결단력 있게 행동하는 능력을 시험해 볼 수 있다는 점이다. 연습을 통해 경영진은 "그들이 모르는 것이 무엇인지" 알 수 있고 그 결과 피할 수 없는 "진짜 사고"에 대해 더 잘 연마된 사고 대응 계획을 수립할 수 있다.

지적 재산 노출 간극의 축소

지적 재산은 회사의 핵심 사업에 필수적이고, 지적 재산에 대한 사이버 공격 위험이 상존하기 때문에, 지적 재산 절취 리스크의 관리는 지적 재산 전략의 핵심이 되어야 하고 CEO, CFO, 법률 자문 그리고 동등하게 중요한 CIO와 CISO의 소관으로 다뤄져야 한다. 기업의 지적 재산 전략은 연구개발, 특허와 저작권, 현금화 및 기타 지적 재산 계획과 함께 사이버리스크 요소를 포함해야 한다. 리스크가 증가하는 것을 알고 있는 상황에서, 최고경영진이 최선을 다해 지적 재산을 보호하는 것은 투자자, 직원, 고객과 협력 업체에 대한 의무다. 기업의 경영자와 이해관계자들의 목표는 동일하다. 가치 있는 혁신을 보호하고 가능하게 함으로써 기업의 미



래 경쟁력과 성장을 지원하는 것이다.

이를 수행하면서 진정한 복구 능력을 구축하기 위해 최고 경영진은 지적 재산의 사이버 절취가 유발하는 전반적인 사업 리스크에 전사적인 전략적 초점을 맞춰야 한다. 기업이 소유한 지적 재산이 무엇인지, 어디서 어떻게 지적 재산을 보호해야 하는지를 정확히 아는 것과 지적 재산의 사이버 보호를 전반적인 지적 재산 관리 프로그램에 통합시키는 것이 전략의 핵심이 되어야 한다. 많은 기업에서 지적 재산이 성장과 경쟁력의 동인이 될 때, 그 잠재적인 손실과 오용의 전체적인 영향을 이해하는 것이 단순히 리스크의 인식에 그치지 않고 행동을 시작하는 좋은 출발점이 될 것이다. **DR**

에밀리 모스버그(Emily Mossburg)*는 딜로이트 투쉬 LLP의 프린시펄이며 사이버리스크 서비스의 복구능력 관련 포트폴리오를 이끌고 있다.*

J.도날드 프랜처(J.Donald Francher)*는 딜로이트 금융 자문 서비스 LLP의 포렌직 서비스의 프린시펄이자 글로벌 리더다.*

존 겔린(John Gelinne)*은 딜로이트 투쉬 LLP의 사이버리스크 서비스 디렉터다.*

*본고에 대한 딜로이트 투쉬 LLP의 **사라 로빈슨(Sarah Robinsons)**의 공헌에 감사의 말을 전한다.*

Endnotes

1. Ocean Tomo, "2015 annual study of intangible asset market value," March 5, 2015, www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/.
2. National Research Council, *The digital dilemma: Intellectual property in the information age*, 2000, www.nap.edu/read/9601/.
3. Danny Marti (Intellectual Property Enforcement Coordinator, Executive Office of the President), statement in email communication with the authors, April 2016.
4. Fred H. Cate et al., "Dos and don'ts of data breach and information security policy," Centre for Information Policy Leadership at Hunton & Williams, March 2009, www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1234&context=facpub.
5. Referring to President Barack Obama.
6. Marti statement, April 2016.
7. In 1971, RAND Corp. analyst Daniel Ellsberg leaked the Pentagon Papers, at the time the largest whistle-blower leak in history; over a course of months, Ellsberg had painstakingly photocopied 7,000 pages of secret documents. In contrast, recent leaks based on digital information—Edward Snowden's revelations, the so-called Panama Papers, multiple WikiLeaks data dumps—have involved *terabytes* of private and classified data. Thefts of this scale were impossible before flash drives and the Internet. A target, whenever a leak comes to light, can no longer assume that the leak's scale—and its eventual impact—is limited. See Andy Greenberg, "How reporters pulled off the Panama Papers, the biggest leak in whistleblower history," *Wired*, April 4, 2016, www.wired.com/2016/04/reporters-pulled-off-panama-papers-biggest-leak-whistleblower-history/.
8. A full list of state data breach disclosure laws can be found at the National Conference of State Legislatures site, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, accessed April 18, 2016.
9. No single federal rule or statute governs the loss of all forms of PII. Rules include an OMB rule directing all federal agencies to have a notification policy for PII; relevant legislation may include the HITECH Act, the Federal Trade Commission Act, and the VA Information Security Act.
10. Jess Benhabib et al., "Present-bias, quasi-hyperbolic discounting, and fixed costs," *Games and Economic Behavior* 62, no. 2 (2010): pp. 205–23.
11. JR Reagan, Ash Raghavan, and Adam Thomas, "Quantifying risk: What can cyber risk management learn from the financial services industry?," *Deloitte Review* 19, July 2016, http://dupress.com/articles/quantifying-risk-lessons-from-financial-services-industry.
12. Deloitte Development LLC, *Beneath the surface of a cyberattack*, 2016, http://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.
13. John Levis et al., "Wizards and trolls: Accelerating technologies, patent reform, and the new era of IP," *Deloitte Review* 15, July 28, 2014, http://dupress.com/articles/intellectual-property-management-patent-reform/.
14. One such framework is described by the phrase "secure, vigilant, and resilient." See Deloitte, *Changing the game on cyber risk: The imperative to be secure, vigilant, and resilient*, 2014, www2.deloitte.com/us/en/pages/risk/articles/cyber-risk-services-change-game.html.