한국경호경비학회 – 제28호(2011): 103-130

투고일 2011. 7. 31, 심사일 2011. 8. 9, 게재확정일 2011. 9. 23

기업보안과 비즈니스의 전략적 협력에 관한 연구

유 형 창

기업보안과 비즈니스의 전략적 협력에 관한 연구*

유 형 창**

〈요 약〉

본 연구는 글로벌 비즈니스 환경에서의 한국기업의 수익성과 기업안정성 제고를 위한 기업보안과 비즈니스의 전략적 협력에 관한 연구이다.

현대기업환경은 하루가 다르게 과학기술이 복잡해지고 국경에 상관없이 새로운 경쟁자들이 등장하면서 아무리 거대한 기업이라도 혁신적인 사고로 무장한 새로운 기업에게 하루아침에 시장을 내주어야 하는 상황이 빈발하고 있다. 이러한 새로운 환경에서 살아남기 위해서는 새로운 관점의 기업경영관리기법에 대한 패러다임의 변화이다. 한국기업이 과거를 답습하는 낮은 수준의 보안리스크관리방법으로는 기업수익에 도움이 되는 보안관리가 되지 못한다.

21세기 70억에 육박하는 인구가 살고 있는 지구촌은 급격한 생태계변화에 직면해있다. 급격한 기후환경의 변화는 순식간에 수십만 명의 이재민을 발생시키고, 신종전염병으로 수백만 마리의 가축을 생매장시키는 광경을 우리는 매순간 목격하고 있다. 이러한 변화는 지구촌에 살고 있는 인간의 삶의 근본적인 방식의 변화를 추동하고 있다. 우리의 경제적인 삶의 근간인 기업생태계도 여기에 예외가 될 수는 없다. 21세기 기업환경에서 생존하기 위해서는 경영진 수준의 보안리스크관리가 필요하며, 보안리스크관리를 통한 기업경쟁력을 제고를 위해서는 기업의 보고라인을 새롭게 정립하여야 할 것이다.

기업도 변화하는 환경에 민감하지 않으면, 하루아침에 시간의 뒤안길로 사라질 수 있음을 명심하여야 한다. 현대기업의 새로운 리스크 중에 특히 한국기업들이 안이하게 대처하는 분야가 보안리스크이다. 과거와 다르게 훨씬 대규모이고 전파 속도가 빠른 보안리스크는 경영진이 다루어야 하는 주요한 기업리스크 중에 하나이다. 현대기업에 핵심적인 영향력을 미치는 보안리스크에는 기업 브랜드와 평판의 보호, 생산과 운영의 연속성, 고객신뢰의

* 이 연구결과물은 2011 학년도 경남대학교 학술연구 장려금 지원에 의하여 작성되었음.
(This Work was supported by Kyungnam University Foundation Grant, 2011)
** 경남대학교 법정대학 경호비서학과 교수

유지가 우선한다. 본 연구에서는 이러한 보안리스크를 효과적으로 다루기 위한 기업보안과 비즈니스의 전략적 협력에 관하여 제시하였다.

주제어 : 보안리스크, 비즈니스 안정성, 기업가치, 전략적 협력, 보안 프로그램, 운영비용

목 차

Ⅰ. 서 론

기업의 존재목적은 수익창출이다. 기업은 이러한 수익창출을 위하여 활용가능한 모든 전략과 기법을 동원한다. 기업의 전략이란 기업이 가능한 최대의 이익을 올리면서 지속가능한 성장을 위해 기업의 총체적인 모든 역량을 개발하고 활용하는 과학과 기술의 총량이다(유필화 & 지몬, 2010: 14).

21세기 비즈니스 세계에서의 보안활동은 리스크로부터 기업을 보호하는 역할에서 기업경쟁력의 새로운 원천으로 변화되고 있다고 주장하였다(Briggs & Edwards, 2006: cover story)

현대기업의 보안전문가는 보안에 대한 자신의 정체성에 대하여 명확한 인식을 가져야 하는데, 기업에서 보안업무와 비즈니스가 상충될 경우에 비즈니스가 우선이라는 것이며, 기업보안전문가는 보안에 관한 전문지식을 가진 비즈니스맨이어야 한다. 이것이 이윤을 추구하는 기업에서의 보안활동의 한계이자 가장 중요하게 고려하여야 할 업무지침이다(Kovacich, 2003: 67).

본 연구에서 비즈니스는 사업, 상업적 조직이나 상업적 활동을 포괄하는 의미로 사용하였으며, 전략적 협력에서의 전략의 어원의 살펴보면 이 개념 자체가 어떻게 발전하였는지 알 수 있다. strategus라는 단어는 고대 아테네에서 군사 사령관이나 전쟁 위원회의 구성원을 뜻했다(보스턴컨설팅그룹 전략연구소, 2001: 53). 근본적으

로 전략이란 용어는 전쟁에서 적을 속이는 술책이라는 뜻을 가지고 있으나, 오늘날에는 기업전략 등 비군사적 분야에서 빈번하게 사용된다. 기업보안프로그램은 어떤 기업에서 조직자산을 보호하기 위한 모든 보안활동과 관련된 조직, 인력, 장비와 같이 보안목적 달성에 기여하는 일체를 의미한다.

기업은 인간가치의 실현을 위해서 존재하기 보다는 이윤의 획득을 목적으로 운용하는 자본의 조직단위로써 기업을 통하여 이윤추구라는 목표를 실현하기 위해서 인간이 만든 조직이다.

기업에서 비즈니스에 대한 고려 없이 보안 프로그램을 구축하는 것은 매우 쉬운 일이다. 그러나 보안실무자들은 비즈니스에 대한 이해를 바탕으로 보안 프로그램을 기업에 적용하여야 기업주에게 인정을 받을 수 있다. 오늘날 기업은 중요한 결정을 하는 경우에 기업보안에 대한 고려 없이 정책결정을 하는 경우는 거의 없기 때문에 기업에서의 보안프로그램은 기업정책과 전략적인 보조를 같이하여야 한다. 기업 비즈니스와 조화가 맞는 이러한 보안전략이 기업보안부서의 운영자금의 획득이나 새로운 재원이 필요할 경우에 타부서의 협력을 얻는데 효과적이다.

그러나 기업정책에 보안에 관한 선언적인 문구를 적용한 경우에도 실제적으로 이러한 기업의 보안전략이 비즈니스 현장에서는 원활하게 적용되지 않는다. 어떤 기업이든 실제적으로 주주의 가치와 이익실현, 사업 확장과 기업평판과 같은 비즈니스에 관한 절실한 문제를 제쳐 두고 보안을 기업의 우선고려대상을 여기는 기업은 드물다. 이것은 전략적인 관점에서 보안과 비즈니스 사이의 전략적인 협력을 강화하기 위한 실제적인 증거가 많지 않다는 의미이다.

오늘날 다국적기업의 소수의 보안관리자 만이 보안 프로그램의 목적과 목표를 기업의 이익실현의 관점과 부합하여 전략적인 계획을 만들어 기업의 다른 전체적인 부서의 목표인 수익극대화에 반하는 의사를 표시한다. 그러나 이러한 보안전략도 보안활동으로부터 발생하는 가치에 대응하여 영업부서와 같이 보안을 개별적인 비용으로 분류하기 위해서 보안활동에 관한 비용편익분석도구를 개발하여야 가능하다.

일반적으로 경영자는 보안에 투자되는 비용은 말 그대로 비용으로 생각한다. 따라서 이러한 비용을 최소화하여 기업활동에 장애가 없다면 최고의 보안관리정책이라고 인식할 것이다. 대부분의 기업에서 기업회계기준에 보안에 대한 항목을 명확하게 구분하여 예산을 책정하는 기업은 많지 않다. 그러므로 체계적으로 보안프로그램을 적용하기 보다는 예상치 않은 사고가 발생하는 경우 기업손실을 최소화하기 위한

대응차원에서 보안활동을 실시하는 것이 보편적이다.

실제적으로 보안활동의 가치를 수치화하는 것은 상당히 어렵다. 왜야하면 보안활동이란 개연성 있는 손실상황에 대한 예방활동을 주로 하여 운영되므로 이러한 예방활동의 효과를 수치화하는 것은 어떤 회계기법을 사용하더라도 정확할 수는 없다. 또한 어떤 사건도 그 이전의 사건이나 장차 일어날 사건과 동일하지는 않다(Bernstein, 1996: 339).

세계화를 지향하는 한국기업에서 보안업무의 중요성은 대두한지 오래나 경영진과 보안실무자 모두가 실제적으로 어떻게 기업의 보안프로그램을 설계하고 운영하는 것이 기업목표달성에 가장 부합하는지에 대해서는 체계화되지 못하고 있다. 그러므로 유행적으로 기술보호나 정보보안과 같이 특정한 분야에 편중하여 관심과 예산을 집중하는 미숙함을 드러낸다. 그러나 이러한 즉흥적인 보안대책으로는 기업보안의 효과를 기대하기 어렵다. 현장의 보안실무자 모두가 명심하여야 할 격언은 '보안효과는 가장 약한 연결고리의 강도에 비례한다(Schneier, 2003: 103).'라는 것이다.

그 동안 한국기업들은 인력에 의한 출입통제, 전자적인 보안관리와 같은 제한된 분야에 편향된 보안관리에 주력하여왔으며, 지금도 이러한 기업에서의 보안업무의 관행은 크게 변화지 않고 있다. 21세기 들어 대부분의 글로벌 기업에서 추구하는 경영진 차원의 보안관리가 정착된 한국기업은 없다. 이것은 아직도 한국기업은 보안리스크에 대한 위험성과 기업에 미치는 영향에 대하여 과소평가하고 있다는 단면이다. 그러나 지금과 같은 한국기업에서의 보안관리 방법으로는 좀도둑과 같은 작은 손실은 감소시킬 수 는 있으나, 핵심 구성원에 의한 부정행위와 같은 기업에 치명적인 손실을 미치는 보안리스크에는 크게 도움이 되지 않는다.

일반적으로 기업보안부서의 핵심적인 업무는 기업구성원과 기업자산을 보호하고 기업활동에 의해서 발생한 법적책임으로부터 기업을 보호하는 업무를 수행한다(Kidd, 2001: 6).

보안업무가 다른 업무와 명확하게 구분되거나 전문화되지 않는 상태에서의 기업경영자는 보안에 대한 투자를 소모성비용으로 간주하거나, 보안업무의 전문화의 필요성을 인식하지 못 하나, 글로벌기업의 보안관리는 과거의 경비원의 업무였던 출입자관리나 미미한 기업손실에 중점을 두기보다는 기업경영에 치명적이거나 큰 영향을 미치는 보안리스크관리에 대응하는 방향으로 기업의 보안리스크를 바라보는 패러다임이 변하고 있다.

보안리스크(security risk)란 조직 자산을 위험에 빠뜨리는 원인이 되는 모든 이벤트를 말한다. 여기에는 허가되지 않는 사용, 손실, 피해, 노출, 개인이익, 개인이나 집단의 정치적 이익을 위하여 수익을 목적으로 한 조직자산의 변경, 자산을 위험에 빠뜨리는 모든 실체, 사람을 위태롭게 하는 리스크를 포함한다(Talbot & Miles, 2009: 7).

세계화의 물결속에서 대부분의 기업들은 자국의 치안력이 미치지 못하는 나라에서의 영업활동을 확대하고 있으나, 여기에서 발생하는 많은 보안리스크에 효과적으로 대응하지 못하고 있다. 본 연구에서는 기업의 보안활동의 가치와 비즈니스와 상충관계를 완화하기 위한 기업 내·외부 보안프로그램과 비즈니스의 전략적인 협력을 통한 기업의 이윤극대화와 기업경쟁력의 요소로서의 보안프로그램의 중요성에 대하여 연구하였다.

그러나 아쉽게도 지금까지의 우리나라의 기업보안관리에 대한 선행연구는 대부분이 온라인에 관한 정보기술(IT)에 대한 연구이고, 단편적으로 기업보안활동 강화에 대한 연구가 몇 편 있었으나, 이에 대한 연구도 기업전반의 보안직무에 대한 연구가 아니라 산업기술보호와 산업스파이방지에 대한 연구이다(오일석, 2007; 정병수, 2007; 신성균/박상진, 2009; 김순석/신제철, 2010; 최진혁/박준석, 2010; 노민선/이삼열, 2010).

본 연구에서는 기업보안에 관한 선행연구와 같은 미시적이며, 특정한 주제에 국한하지 않고 세계화시대에 기업보안과 비즈니스의 포괄적이고 전략적인 협력을 통한 한국기업의 경쟁력 향상에 기여하는 것을 연구목표로 하고, 이를 위한 연구방법으로 국내외 문헌, 인터넷자료, 글로벌 기업의 보안직능에 대한 연구자료 등의 문헌적 연구를 기초로 하였다.

본 연구는 보안업무의 특성상 미래가치에 대한 투자로서의 보안업무이므로, 실제적으로 보안활동의 결과를 수치로 검증하기는 본질적인 한계와 기업전반의 내·외부 조직의 포괄적인 협력을 언급하고 있으므로 개별 요소들의 구체적인 논증과 수치화의 한계를 가지고 있으므로, 이러한 한계점을 보완하기 위하여 조건화된(conditioned) 환경에서의 보안활동의 투자에 대한 성과에 대한 정량적 후속 연구가 지속되었으면 한다.

Ⅱ. 기업보안의 가치

1. 기업가치의 보호

보안프로그램을 일반적인 상품이나 서비스의 경우처럼 투자대비효과(ROI)에 분석을 가지고 기업주나 조직에 판촉이나 판매하지 않는 것이 오랫동안 보안업무가 가지고 있는 문제점으로 지적되었다. 이러한 관행은 아마 보안업무가 상업적인 관점으로 효율성의 대상으로 인식하게 된 것은 기업에서의 보안활동이 전문화되면서 부터이고, 오래전부터 보안업무는 국가가 국민에게 제공하는 공공재의 기능을 하였기 때문에 비용편익분석의 대상이 아니었다.

그러면 보안서비스도 기업의 여러 가지 상품이나 서비스처럼 판매나 효율성을 증가시키는 것이 가능한가? 보안업무에 오래된 경험법칙과 같은 공식에 의해 매출을 올리거나 지출을 감소시킬 수 있는 방법이 존재하는가? 만약 기업의 구매책임자의 오래된 경험법칙을 엄격하게 적용한다면 보안은 편익이 아니라 비용으로 여기게 될 것이다. 이에 대하여 기술의 진보에 따라 정보기술보안에 대한 가치를 보여주려는 시도가 보안전문가에 의해 제안되었다.

효과적인 보안과 리스크 관리란 시장 기회를 예측하고 적절히 대응하는 능력인 동시에 기업이 갑작스럽게 붕괴하지 않도록 준비하는 것이라 할 수 있다(Parrett, 2007: 25).

보안의 가치를 측정하기 위한 흥미로운 접근법은 American Water의 보안책임자인 Bruce Larson에 의해서 시도되었다. CSO Online에 2006년 발표한 기고문에서 Larson은 “가치보호(value protection)”에 대하여 제안하였는데, 여기에서 Larson은 보안업무가 단지 비즈니스의 낭비적인 요소를 방지하는데 불과하다는 고전적인 사고방식의 문제점을 극복하기 위하여 새로운 방법론을 제시하였다.

대부분의 기업 활동이 추구하듯이 기업의 주요한 목적이 기업의 수입을 증가시키고 효율성을 증가시키는데 목적을 둔다면 보안업무 자체는 이러한 두 가지 목적을 달성하는데 직접적인 목표가 아니므로, 보안활동의 가치를 강조하기 위하여 반드시 새로운 방법을 찾아야 한다. 가치보호에 대하여 Larson은 보안활동에 기업에서 시간과 자금을 투입하는 것은 지속적인 기업성장을 유지하고 새로운 성장의 뿌리를 내리게 하기 위함이다. 여기에서 Larson은 가치보호 매트릭스를 어떻게 활용하는지

에 대하여 설명하고 있다. 이러한 Larson의 가치보호 매트릭스는 다음과 같다 (http://www.csoonline.com/article/print/220829, Berinato, April 01, 2006. 2011, 3, 20 일 접속).

VP=(N–E)/N
(VP: 가치보호), (N: 통상적인 운영비용), (E: 이벤트 영향력)

Larson의 가치보호 매트릭스에 대해서 American Water의 운영담당부사장인 Steve Schmit는 Larson의 방정식은 단지 대부분의 보안부서에서 추구하는 '적절한 보안업무의 창출'을 의미하기 보다는 최고경영진이 원하는 '보안업무의 가치를 증명하는 것'이라고 지적하였다. 이러한 방법은 리스크에 대하여 기업가와 파트너에게 더 명확하게 이해하게 하였으며 리스크를 축소시키는 더 향상된 방법을 제시하였다.

Larson의 매트릭스에서 이상적으로는 예기치 않게 발생하는 이벤트 영향력(event impact)의 값이 0이면 최상이나, 실제적으로 예상치 않는 사건이 발생하지 않는 것은 단순히 이상적인 가정에 불과하므로 보안부서는 가치보호가 1에 접근할 수 있도록 노력하여야 한다. 이러한 접근방법에는 이벤트 영향력을 감소시키는 방법과 통상적인 운영비용을 증가시키는 방법이 있다.

그러나 여기에서 통상적인 운영비용 N에 대한 선택권은 항상 보안부서에 있는 것이 아니며, 실제적으로 선택권이 주어진다 하더라도 보안부서 스스로가 곤란한 상황을 자초하는 결과를 가져올 수도 있다. 극단적으로 통상적인 운영비용의 축소는 보안팀의 운영자인 보안요원의 해고로 이어질 수도 있다. 따라서 결과적으로 이벤트 영향력 E를 추가적인 비용의 증가 없이 축소하는 방법을 찾는 것이 기업주가 가장 바라는 가장 효율적인 방법이다.

2. 통상적인 운영비용

통상적인 보안활동과 관련된 운영비용(normal operation cost)에 대한 정의를 어떻게 할 것인가에 대한 합리적인 평가기준의 제시가 가치보호 방정식을 경영진 혹은 다른 부서의 관리자에게 보안업무를 이해시키는 관건이 될 것이다. 대부분의 기업에서 보안비용을 개별적인 운영비용으로 분리하여 정규 예산항목에 반영하는 경우는 많지 않다. 단순하게 정보보호분야에 국한하여 시스템의 다운타임을 가치로 계산하

여 환산하는 방법을 활용할 수는 있으나, 온라인이 아닌 오프라인에 대한 손실에 대한 가치평가는 너무나 광범위하여 구체적인 항목을 나열하기에도 한계가 있다. 어떤 조직에서든 적정한 보안예산에 대한 명확한 평가가 이루어지기는 어려울 것이다. 이러한 한계점이 보안업무의 정당화 혹은 수치화의 한계이자 흥미로운 보안영역의 과제이다.

상대적인 차이는 존재하지만 세상의 모든 분야에서 일반적 혹은 통상적이라는 기준은 유동적이다. 일반적이라는 용어는 디지털 영역이나, 기계의 지침에서는 적용이 가능하나 인간의 활동영역에서는 적용되지 않는다(Clairmont, 1999). 그만큼 기준은 유동적이고 예측불가능하고, 보안의 상충관계는 주관적이다(Schneier, 2003: 17).

컴퓨터와 네트워크의 보안에 관해 많은 것을 알더라도 그것은 사람의 문제를 해결하는 데에는 도움이 되지 않는다. 사람이 개입하기 시작하면 문제는 정말 어려워진다. 컴퓨터보안은 디지털 영역에서만 작동하나, 정보를 디지털 세상에 묶어두는 것은 거의 불가능하다(Schneier, 2000/2001: 370). 우리나라의 보안활동이 초급단계에서 머무는 이유 중에 하나가 모든 보안에 관한 문제를 정보보호 혹은 온라인보안의 문제로써 접근하려는 근시안이다. 따라서 Larson의 가치보호 방정식은 나름대로 창의적이나 통상적인 운영비용을 네트워크의 다운타임에서 구하려 하듯이 가치보호의 대상을 전자적인 영역에 한정하는 것이 Larson 매트릭스의 한계이다.

기업활동을 포함한 우리의 생활에서의 보안은 결코 전자적인 영역에서의 문제가 아니라 인간이 느끼는 현실의 문제이다. 즉 일반적인 보안비용이라는 기준은 수학적인 기준이 아니라 조직의 구성원, 경영진이나 기업주의 인식이 기준이 될 것이다.

가치보호 방정식에서의 통상적인 보안비용은 기업의 보안활동과 관련되어 발생한 손실을 기준으로 하는 것이 근사치에 가깝다. 즉 기업이 보안활동에 대한 예산을 배정하는 경우에 연간 발생하였던 손실을 기준으로 과거의 평균적인 손실액보다 많은 예산을 책정하여 운영하고, 이러한 결과를 연말에 다시 평가하여 다음 연도의 예산에 반영하는 방식으로 탄력적으로 운영하는 것이 탄력적 보안활동의 근간이 된다.

여기에서 중요한 것은 평균적인 연간손실의 평가에서 눈에 보이지 않는 가치를 누락해서는 안 된다. 즉 우연히 발생한 안전사고 같이 치부되는 정전사고나 원인이 불명확한 사보타지에 의해서 발생한 손실도 기업에서 발생한 손실을 구성하는 것이다.

3. 간접손실의 영향력

Larson은 가치보호 매트릭스에서 주장하는 예상하지 않는 손실사건 즉, 이벤트에 따른 영향력을 비용으로 크게 대응비용, 복구비용, 벌금, 손실예산과 관련된 비용, 인식이나 평판손상과 관련된 비용으로 모두 다섯 가지 유형으로 분류하였다.

여기에서 제시하는 분류는 IT분야에 한정된 매우 간단한 분류이고 실제적으로 적극적인 보안대책의 수립에 실패할 경우에 보안과 관련된 손실의 종류는 매우 다양하다. 이러한 비용에 관하여 Larson은 측정할 수 있는 것은 우선 측정하고, 측정할 수 없는 것은 측정하지 않거나 나중에 측정하는 것이 중요하다고 하였다. 실제적으로 모든 이벤트의 경우에 이전에 언급한 모든 비용 항목이 발생하는 것은 아니다. 또한 모든 비용은 측정할 수 있는 것이 아니라, 어떤 비용은 잠재된 상태로 있고, 즉시 측정하기 곤란하거나 나중에 피해가 발생하는 항목도 있다. 더불어 물리적으로 도식화된 비용이라도 실제적으로 주의 깊게 평가할 경우에 수치가 변동될 수 있으므로, 전문적인 평가가 실제적인 업무의 성패를 좌우한다.

그러므로 어떤 경우라도 예기치 않게 발생한 손실비용은 관련된 모든 비즈니스 공정관리자나 해당분야의 전문가와 함께 계속적으로 실제적인 가치와 비교하는 것이 중요하다.

영국의 글로벌 기업보안전문가 교육기관인 ARC training에서는 어떤 사업장에서 간단한 전기누전에 의하여 IT서비스를 제공하는 사업장이 대형화재로 소실되었을 경우에 나타날 수 있는 손실의 종류는 다음과 같이 다양하다. 운영상의 손실(생산차질의 발생), 이윤손실, 사고조사비용, 업무중단으로 가용인력의 급여손실, 고객이탈, 고객손실, 소송손실, 신용손실, 보험료의 할증, 보험청구액의 조정, 직원의 재고용, 직원의 재훈련, 임시 숙박시설과 장비사용료, 화재장비의 교체, 전산시스템의 재구축과 프로그램의 재설치, 자료가용성의 손상, 사업장 인근의 피해, 운송업체의 비용, 예방정비, 재청소와 재단장, 통신장비의 복구, 기업이미지 하락, 원재료의 손괴, 완성품의 손괴, 고객신뢰도의 하락, 시장점유율의 하락, 정상운영에 따른 광고비, 현금흐름의 문제, 업무재개 전의 보건안전시설의 점검, 협력업체의 손실, 이전의 시장점유율을 회복하기 위한 더 향상된 서비스의 제공 비용 등 재난이 발생할 경우 파급손실액은 직접손실액의 평균 10배에 달한다(ARC training, 2008: 6-7).

Ⅲ. 보안 프로그램과 내부관계

1. 세계화와 보안기능

세계화란 새로운 통신 기술의 발전으로 전 지구적 상호작용이 증가한 새로운 현실에서 국경선은 상품과 금융자본의 자유로운 이동을 방해하는 장벽이라기보다는 지리적인 경계선으로 존재할 뿐이다. 본래 세계화라는 용어는 기술 혁명의 전 세계적 파급효과로 일어나는 과정을 중립적으로 묘사한 것이었다. Charles Doran (Brzezinski, 2004/2004: 208 재인용) 교수가 내린 유용한 정의에 따르면 '세계화'란 정보기술과 세계 경제의 상호작용으로 비롯된 현상이다. 그것은 정보와 재정, 무역, 상업, 행정 영역의 국제적 업무 강도와 범위, 양, 가치로 나타난다. 지난 10년간 이러한 상호작용에서 나타난 급속한 증가는 세계화의 과정을 가장 잘 측정하게 해 준다.

서로 상이한 문화적인 배경과 특성을 가진 기업 간의 인수합병(M&A)이 급격히 진행되는 세계화의 현실은 기업에서 첨단기술을 개발하는 것도 어려운 일이지만 개발된 기술을 기업의 상품이나 서비스로 연결하여 기업의 성과로 연결되기까지의 기업자산을 지키기 위한 새로운 프로세스의 정립이 더욱 중요한 시대가 온 것이다. 영리를 목적으로 하는 기업은 새로운 경쟁의 룰에 따라서 기업의 경쟁력유지와 기업자산을 효율적으로 보호하기 위한 새로운 자산보호(Protection of Assets) 프로그램을 운영하여야 한다.

세계화가 이제까지 스스로를 '다국적'이라는 이름 붙여 온 세계 주요 기업과 금융기관들에 의해 가장 열광적으로 받아들여졌다는 것은 의미심장하다. 이러한 다국적 기업의 비즈니스 전략에 대응하기 위해서는 한국기업도 효과적인 자산보호시스템과 제도를 도입하여 글로벌 트렌드에 맞는 보안리스크관리 프로그램을 정착하는 것이 기업의 생산성과 안정성유지의 중요한 요소가 되었다.

미국부정조사가협회(ACFE)에 의하면 기업매출의 약 6%가 종업원의 부정행위(fraud)로 인하여 사라지고, 총손실액은 미국에서만 4천억 달러에 달한다고 발표하였다(성태경, 2003: 2). 따라서 이러한 부정행위를 방지하기위한 대응책은 많은 전문가의 노력과 조직의 유연성이 요구되나, 서양의 기업문화와 상이한 기업문화를 가진 한국기업의 대응책은 이러한 커다란 보안리스크의 실체에 대하여 명확하게 파악하지 못하고 있다. 예로서 산업기술유출에 대하여 기술적인 대응책으로 일관하거나 고

용관계의 불안전성에 따라 최근 급증하는 금융기관 구성원의 자금횡령과 부정행위에 대한 국내금융기관의 내부통제시스템은 상당히 허술하여 이러한 구성원의 부정행위를 촉발하는 원인이 되기도 한다.

사회의 안녕과 질서를 유지하기 위해서는 시대상황에 부합하는 법과 질서가 구성원에게 공정하게 적용되어야 하듯이 먼저 체계적인 기업자산보호를 위해서는 경영진과 구성원이 동의하는 명확하고 엄격한 기업보안 정책과 절차의 수립이 우선되어야 한다. 변화된 기업환경에서의 정책과 절차를 엄수하도록 경영진에서부터 관련 협력업체까지 지속적인 교육과 훈련이 뒤따라야 하나, 보안은 구성원의 인식과 문화의 반영이므로 경영진과 구성원의 보안에 대한 의식변화가 선행되어야 할것이다.

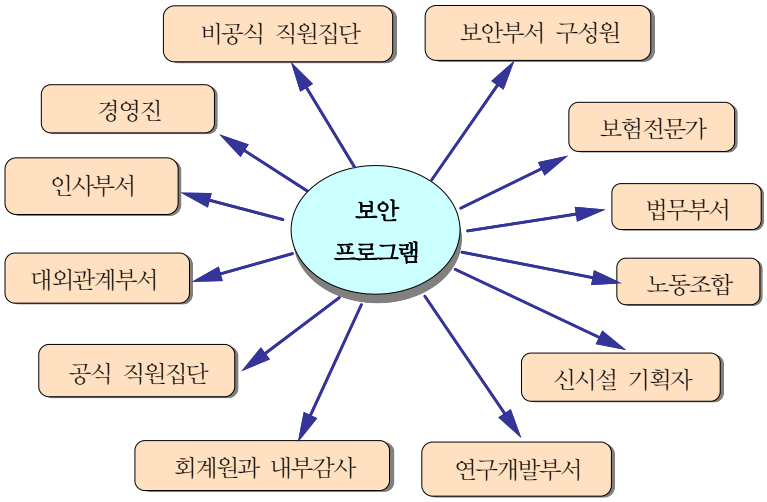
2. 보안과 기업내부관계

기업 자산보호 프로그램의 주요한 목적은 모든 구성원들이 보안 조직의 일부분이 되도록 동기를 부여하는 것이다. 그러므로 개개인의 구성원들을 기업자산보호를 위한 책임을 그들 자신의 업무의 필수적인 요소로서 당연시 하도록 고양시켜야 한다.

그러나 여러 가지 보안과 손실예방의 교재에서나 실무의 관점에서 외부와의 관계는 강조되는데 비하여 내부의 관계는 종종 상대적으로 경시되었다. 반면에 대다수의 보안 전문가들의 분석에 의하면 조직이나 기업에서의 최고의 위협요인은 보안 활동을 통하여 채용이 된 직원이나 내부인 으로부터 기인한다고 하므로 보안 프로그램은 오히려 내부관계에 초점을 맞추는 것이 현명하다.

예를 들어 보안 프로그램과 내부관계에 관한 구성요소를 <그림 1>에서 보여준다. <그림 1>에서와 같이 어느 기업에서 기업경영진이 해당 기업의 보안관리의 목표를 규정한다. 그러면 실무자나 보안부서는 지원자의 선발과 징계적인 활동과 관련된 사항을 동일한 업무로서 수행하여야 한다. 그리고 노동 문제(예, 소요나 파업)의 발생이 예상될 시에는 손실이 최소화되어야 함과 더불어 노동조합 계약에서 보안 활동의 한계를 규정한다. 또한 보안 실무자는 정규적, 비정규적 집단으로부터의 비난과 피드백을 현명하게 조정하여야 할 것이다. 이러한 구성원의 여러 의견의 경청과 기본적인 욕구가 충족된 직원들에 의하여 기업의 손실은 줄어들 것이다.

새로운 보안시설들이 잘 계획되고, 건축가, 기술자, 그리고 보안실무자가 합동으로 시설물 계획 시에 예방전략을 설계하고 이것을 토대로 건축물이 완공된 다음에 불필요한 장비(예, 경보기)를 설치하지 않음으로써 추가적인 경비를 절약하게 될 것이다. 더불어 영업비밀이나 다양한 기업정보는 절대로 철저한 보호 아래에 관리 ·



* 출처: Purpura, 1998: 78.

〈그림 1〉 보안프로그램과 내부관계

유지되며, 특히 연구개발에 관한 정보의 보안은 중요하다. 기업의 회계부서와 감사요원은 기업손실방지에 대하여 협동적인 전략을 수행하는데 도움이 된다.

보험 전문가는 일반적으로 손실예방 전략의 수립이나 보험료를 절감하는데 도움이 되고 또한 법무부서의 여러 분야의 법률적인 조언이 보안부서에 필수적이다. 그러나 무엇보다도 보안실무자들이 보안 프로그램의 중심이므로, 보안관리자는 실무자들의 요구사항을 만족시키기 위해서 모든 것을 가능하게 하여야 한다. 보안부서의 적절한 보안정보를 보장하는 관련 외부부서와의 좋은 신뢰감은 외부기관에서 원만한 관계유지에서 비롯되며, 이러한 정보는 기업이 최고로 관심을 가지는 것이다. 그러므로 일반적으로 경영진과의 원활한 의사소통은 다양한 이유에서 지극히 중요하다. 예를 들어, 보안 프로그램의 목적이 관리자 모임을 통하여 모든 직원들에게 신속하게 전달되고 생산성이나 이익에 관하여 관리자로부터의 피드백 또한 보안 전략을 세우는데 도움이 된다.

3. 경영진의 지원

기업이나 조직에서 경영진의 지원은 효과적인 보안 프로그램을 위하여 필수 불가

결한 조건이므로 새로운 자산보호대책을 수립할 경우 경영진의 지원은 구성원과의 좋은 인간관계를 고양시키고 업무수행을 원활하게 하므로 보안 실무자와 경영진의 빈번한 대화는 매우 중요하다. 따라서 기업구조에서 보안조직이 어디에 위치하든 간에 기업보안관리자는 반드시 경영진에 직접적으로 보고와 만남이 가능하여야 한다(Briggs & Edwards, 2006: 14).

Harvard Business Review에서는 이상적으로, 최고보안관리자는 독립성을 보장받기 위하여 최고경영자나 최고운영책임자에게 보고할 수 있어야 한다고 하였다(Cecere & Mark, 2001: 24).

보안조직이 경영진의 흥미를 이끄는 방법 중에 하나는 기업의 이익을 증가시키는 투자분야로써 보안업무를 강조하는 것이다. 경영진을 설득하기 위해서는 비즈니스의 원칙과 실무에 관한 해박한 지식은 효율적인 교류를 위하여 "기업관리 언어(회계자료)"로써 제시됨으로써 실무자에게 도움을 주어야 한다. 따라서 글로벌 기업의 보안관리자는 기초적인 회계지식을 이해하거나 회계지식을 가진 전문가가 보안부서에 배속되어야한다.

다국적기업에서는 경영진의 지원을 원활하게 얻기 위한 보안부서의 전략으로 외부 보안서비스보다 더 효율적인 서비스를 제공한다는 것을 증명하고 보안부서의 가치를 정량화(수치화)하는 것이다. 이것이 현대기업에서 일반화된 아웃소싱과 기업다운사이징의 흐름에서 살아남기 위한 보안부서의 현실이다. 급격한 변동성에 직면한 기업의 보안부서는 손실발생에 대한 조사가 실시되었던 사례부터 보안요원의 이직률에 대한 것까지 모든 것을 추적하여 자료화한다. 이러한 다양한 보안직무를 통한 데이터는 기업내부 직원들에게 보안부서의 기능이 긍정적으로 평가되고 보안 서비스를 향상시키는데 도움이 된다.

이러한 내부 고객의 만족상황은 서면과 전화조사를 통해서 더 잘 측정되기도 한다. 더불어 보안 활동에 기인한 효과적인 보안 대책으로 내부손실을 최소화하는 활동을 수치화한다.

예를 들어, 보안부서에서 근로자가 보상을 청구한 사건에 대하여 손실발생의 원인에 대한 현장실사를 통하여 수년 동안 해당기업의 근로자가 기업을 속여서 보상을 요구하여 지급하였던 금액을 되돌려 받음으로써 보상금을 절약하게 된 경우나, 또 다른 기업경영진의 지원을 받는 방법은 연봉 5천만 원의 조사요원이 검수원과 창고관리자의 공모에 의하여 무단으로 반출된 평균 5억 원의 재고손실을 회복시키는 성

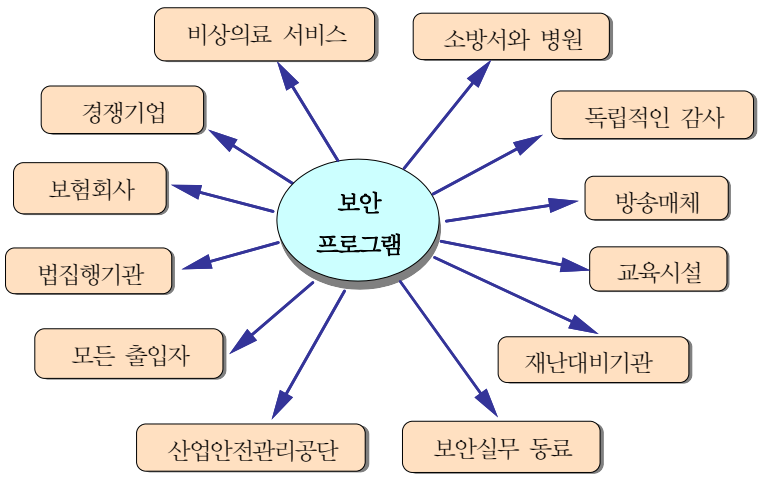
과를 구체적으로 경영진에게 보여준다(Hollstein, 1995: 61-63).

Ⅳ. 보안 프로그램과 외부관계

보안 프로그램과 외부 조직이나 집단에 관한 논의에서 기업보안의 목적에 도움이 되는 사항과 법집행 기관과 여러 공공 서비스 기관을 중요시하며, 공동체와 미디어 그리고 외부 보안 동료들이 외부관계에 포함된다. 외부와의 관계에 관한 <그림 2>에서 본 바와 같이 법 집행 기관에서 시작하여 공공 서비스 기관들은 민간 부문의 보안 프로그램에 필수적인 요소이다.

보안 프로그램과 관련된 기업 외부기관과의 좋은 교류와 협력관계의 유지는 범죄나 재난이 발생할 경우에 신속한 대응에 매우 중요하다. 관련 교육시설 또한 보안연구에 도움이 될 뿐만 아니라 잠재적인 보안 지원자들의 공급처 역할을 한다.

보안 관리자는 관련 자문위원회에 도움을 주거나 보안운영에 관한 새로운 기법을 전달하기 위해서 교육시설에서 가르치기를 원한다. 또한 가능하다면 보안에 관하여 일반대중에게 도움을 주기 위해서 방송매체를 이용하기도 한다. 그리고 비슷한 문제점



* 출처: Purpura, 1998: 78.

〈그림 2〉 보안 프로그램과 외부관계

을 가진 다른 기업이나 보안 동료들은 좋은 아이디어의 교류에 중요한 원천이 된다.

국제 보험전문가와 같은 보험 회사들은 보험료를 줄이는 방법으로 보안 전략을 향상시키는 정보를 제공하고 독립적인 감사나 공인회계사는 보안 프로그램의 취약점을 발견하거나 지적할 수 있다. 고객들과 같은 외부인이 조직을 방문했을 경우에, 보안 장치(예, 출입관리 시스템)에 의해 심각하게 불편함을 느껴서는 안 되나 동시에 기업 손실 또한 방지되어야 한다. 따라서 친절한 안내와 협력적인 활동은 보안 프로그램에 여러 외부기관들이 관련될 경우에 강조되어야 한다.

1. 법 집행기관

만약 경찰이나 검찰과 같은 법집행기관의 도움이 없으면 기업과 같이 민간부문에 의해 발의된 범죄혐의자의 처벌은 불가능할 것이다. 그러므로 경찰과 검찰은 공공법집행의 주요한 구성되고 상호협력은 필수적이다. 법체계상 경찰은 "법 집행 공무원의 지휘관"으로 불리는 검사에 의해 지휘 · 감독되고 해당 검사는 형사사건을 발의하는데 넓은 재량권(범죄수사, 공소제기 등)을 가지고 있다. 기업들은 법 집행기관과의 원만한 협력관계를 유지함으로써 조직내부의 범죄발생에 대한 처리와 사고발생 시 손실을 최소화하는데 많은 조력을 받을 수 있다(Purpura, 1998: 86).

그러나 민간 보안요원이 관할 사법관할지역에서 기본적인 요구 조건을 따르지 않는다면, 사건은 성공적으로 처리되지 못할 것이다. 좀도둑 사건을 예를 들면, 관련법과 사법당국의 요구에 따라서 절도혐의자를 매장 안에서 체포하기 보다는 물건을 가지고 매장을 나온 다음에 좀도둑의 체포를 요구하는데 이것이 사건의 구성을 확실하게 한다.

이와 같이 법 집행기관과의 외부 관계는 보안 프로그램에서 중요하며 상호의존과 협력은 향상된 범죄대응 능력을 기를 것이다. 그리고 다양한 정보의 공유는 이러한 업무 관계를 향상시키는데 주요한 요소이고, 법 집행 기관들은 가끔 민간부문에 도움이 되는 정보를 제공하는데 전문적인 범행다발지역의 존재, 불량 수표 위반자, 위조자, 사기꾼에 대한 중요한 정보는 민간부문의 손실을 방지하는데 도움을 줄 것이다.

법 집행기관과 더불어 여러 공공서비스 기관인 소방서, 응급 의료단, 119구조대는 보안 프로그램에 매우 유용하다. 이러한 공공서비스기관의 대응능력에 대한 분석은 새로운 시설을 계획할 때 특히 중요하며, 비상시 대응시간과 효율에 관련된 요소는

보안 프로그램의 비용을 절감하고 관련 정보는 계획수립에 도움을 준다.

2. 지역 공동체

기업들은 기업이 영업하는 장소에 대한 포괄적인 이해를 필요로 하고, 지역공동체의 관습에 대하여 이해하여야 한다. 기업이 지역 공동체에 대하여 어떤 좋은 의도를 가지고 있다 하더라도 지역 공동체의 이해가 없으면 오히려 지역 공동체와 마찰을 일으키게 된다(Briggs & Edwards, 2006: 42). 따라서 특정 사업장이 위치한 지역의 주민들이 해당 기업을 공동체의 일부로 생각한다면 기업운영에 많은 도움을 얻을 수 있으며 기업이 공동체로부터 공격을 받을 가능성도 많이 줄어들 것이다.

이와 같이 새로운 기업이 어떤 지역에 사업장의 설립을 계획할 경우에 지역공동체와의 원만한 관계는 특히 중요하게 된다. 특히 기업이 외부환경을 바꾸려고 하거나 환경오염 문제의 원인일 경우에는 NGO와 같은 시민단체를 비롯한 지역공동체와의 좋은 관계의 유지는 필수적이다. 그러므로 거주자들에게는 기업의 공동체를 위한 투자계획이나 산업안전 계획과 노력에 관한 정보를 명확하게 제공해주어야 한다(Purpura, 1998: 88).

공동체에서의 기업의 위치는 지역공동체와의 관계와 운영원칙이나 이해관계자는 사업장의 보안에 직간접적으로 영향을 미치고 사업장에 대한 공동체의 역량은 지속적으로 유지된다. 따라서 기업은 지역의 이해관계자와 효과적인 대화채널을 열고 운영하면서 지역에 대한 포괄적인 이해를 바탕으로 평화로운 공존을 추구한다.

올바른 경영 프로세스와 구조는 공동체 대표와의 적절한 행동에 대하여 격려하고 보상의 실시와 사업장의 노동력을 지역 공동체에서 채용하거나 교육에 대한 투자를 실시한다. 이러한 기업의 사회적인 활동은 긴밀하게 기업의 보안전략과 연계되며, 보안과 기업의 사회적 책임 사이에 협력관계를 잘 형성하는 기업은 비즈니스와 더불어 보안업무를 제휴하기가 훨씬 용이하게 된다(Briggs & Edwards, 2006: 38).

산업재해를 방지하기 위한 기업체의 산업안전활동은 도덕적인 의무일 뿐만 아니라, 기업의 생존과 손실방지를 보장하기 위해서 필요하다. 만약 대중 매체에 계속해서 해당 기업에 관한 기사가 실리게 되면, 지역 거주자들은 해당 기업들이 지역공동체에 강력한 영향력을 행사하고 있다고 생각할 것이다.

공동체를 안심시키는 것을 포함하는 또 하나의 배려는 추가적인 문제를 발생하지

않기 위해서 공공서비스 기관과 좋은 관계를 유지하는 것이고 이러한 유기적인 치밀한 계획이 지역 경찰의 비용증가의 원인이 되는 범죄 문제를 억제시킬 것이다. 이와 같은 배려가 화재, 의료, 그리고 여러 비상서비스기관에도 적용된다. 만약 기업이 직접적으로 지역 공동체를 돕기 위해서 특별한 프로그램에 참여한다면 외부와의 관계는 더욱 향상될 것이다.

3. 대중매체관리

현대인들은 실시간으로 중계되는 지구촌 소식을 누구나 손쉽게 접할 수 있다. 따라서 어떤 조직에서 발생하는 뉴스거리는 언제나 대중매체의 좋은 기사가 된다. 따라서 어떤 사건이 내부적으로 통제되지 않고 곧바로 대중에게 알려지는 경우에는 조직에 심각한 문제를 발생시킨다.

대중매체는 경우에 따라 보안프로그램에 도움이 되기도 하지만 방해가 되기도 한다. 그러므로 대중매체를 자신의 지지자로 만드는 노력을 기울여야 한다. 그러나 가끔은 기자회견에서 제공된 정보를 넘어선 정보에 관심을 갖는 대중매체의 구성원들 때문에 어려움이 발생하므로 긍정적인 관계를 유지하는 것은 상당히 가치 있는 일로써 대중매체와의 부적절한 관계는 서로를 상호 비방하는 악순환을 발생시키며 기업의 이미지에 상당한 부담이 되기도 한다.

따라서 거의 대부분의 대기업들에서는 잘 교육되고 경험이 많은 대외 홍보담당이 대중매체를 관리한다. 보안실무자도 이러한 대중매체의 생리를 잘 이용하는 것이 효과적으로 대중매체로부터 보안부서를 보호하게 한다. 사전에 기업정책에서 대외 홍보부서의 지정된 사람만이 대중매체에 정보를 제공할 수 있다고 지정해 두고 모든 보안 실무자들이 이러한 대중매체에 대한 정책을 이해하고 있을 때, 실수나 당황하는 일이 최소화 될 것이다(Purpura, 1998: 88-89).

"대중매체로부터의 스트레스에 어떻게 대처할 것인가"라는 Security Management의 기사에서 많은 대중 매체와 관련된 유용한 생각들에 관하여 지적하고 있다(Security Management 24, 1980: 8-11). 이 기사에서는 인터뷰 준비의 중요성, 자신이 어떻게 말할 것인가를 이해하는 것, 대략적인 질문에 대비하는 것, 조심스럽게 대답하는 것에 대하여 강조하고 있다.

오늘날 수많은 기업들이 경영진에게 효과적인 대화의 기술에 대하여 훈련하고 있

고 이러한 과정은 매우 다양하나, 대부분의 참가자들은 적대적인 의도를 가진 질문에 대하여 어떻게 대응할 것인가를 시청각자료의 도움으로 지도 받고, 문제점을 교정 받는다. 현대조직에서의 보안실무자도 대중매체와의 인터뷰에서 지켜야 할 핵심적인 권고사항에 대한 교육을 통하여 대중매체와의 대응법에 익숙하여야 한다.

Ⅵ. 결론 및 제언

1. 결론

본 연구는 글로벌 비즈니스 환경에서의 한국기업의 수익성과 기업안정성 제고를 위한 기업보안과 비즈니스의 전략적 협력에 관한 연구이다. 그 동안 한국기업은 성장성 위주로 규모를 키우는데 매진해왔다. 이런 결과로 2010 포춘 글로벌 500기업에서 삼성전자가 32위에 오른 것을 비롯하여 10개의 기업이 매출기준으로 글로벌 500대 기업에 들어갈 정도로 한국기업들은 글로벌 시장에서 당당히 경쟁할 수 있는 규모로 성장하였다. 반면에 기업환경은 변하여 기업의 안정성과 수명은 과거와는 전혀 다르게 급변하였다.

기업의 평균수명은 30년이라는 것이 통설이었으나 현재의 급변하는 기업환경 속에서 기업의 평균수명은 갈수록 짧아지고 있다. 리처드 포스터는 그의 저서 '창조적 파괴'에서 "1957년 S&P500 기업 중 74개 기업만이 40년 후에도 S&P500 지수에 남았고 그 중 불과 12개 기업만이 S&P500 기업 평균보다 우월한 성과를 거뒀다"고 밝혔다. 스트라틱컨설팅은 유럽과 일본의 세계적 기업 평균수명이 단 13년에 불과하다는 조사 결과를 발표했고 신용평가사 S&P에 따르면 기업의 평균수명은 15년 정도밖에 안 되며, 액센추어 보고서에서는 20년 전 S&P 500대 기업 수명은 50여 년이었지만 지금은 15년에 불과하다며 2020년에는 10년으로 단축될 것으로 내다봤다.

급변하는 시장환경변화에 유연하게 대응하지 못하는 기업의 미래는 없으며, 현대기업에서 리스크관리에 실패한 기업의 지속성장은 없다. Carlos Ghosn 르노-닛산회장은 현대기업의 경영자의 주요한 자질로 리스크관리력을 들었다.

현대기업은 기업의 내부생산성을 통한 혁신의 한계와 더불어 기존 시장의 포화에 따른 새로운 리스크가 있는 시장에로의 진입을 강요하고 있다. 한국기업들은 계속적

인 경영혁신을 통하여 경영 시스템이 상당 수준 선진화되어 경영의 효율성을 통해 경쟁 우위를 확보하게 되었으나 새로운 환경에 대한 리스크에 대응하는 것이 예전만큼 쉽지는 않다.

시장경쟁이 격화되고 글로벌화 가속화됨에 따라 공정 개선을 통한 경쟁 우위를 유지하는 기간도 갈수록 짧아지고 있다. 주요 선진 기업들의 비용 절감 및 생산성 향상 수준은 이미 정점에 달한 것으로 보인다. 이러한 의미에서 최근 각광을 받는 것이 블루오션이다. 새로운 업종의 개척과 타 업종과의 융합(convergence)을 통한 시너지의 창출도 증가 추세에 있다.

이와 더불어 예상치 못한 리스크에 어떻게 대응하느냐가 기업의 연속성에 핵심이 되었다. 과거의 보안관리는 기업경영차원에서 다루기에는 경비한 정도의 영역에 속하였으나, 예상치 못한 새로운 리스크가 빈발하고 있는 오늘날에는 새로운 리스크에 탄력적으로 대응하지 못하는 경우 기업의 수명을 다하게 될 수 도 있다. 현대기업이 대응해야하는 새로운 리스크에는 지구온난화와 같은 기상이변, 새로운 전염병의 창골, 민주화를 주장하는 국가의 불안전성의 고조, 빈부격차의 확대에 따라 빈곤층의 반사회화, 식수오염과 같은 다양한 환경오염 등 전통적인 사고와 대응방법으로는 관리가 어려운 새로운 상황으로 전개되고 있다.

기업보안과 비즈니스의 전략적인 협력의 궁극적인 목적은 기업의 핵심경쟁력의 제고와 유지하는 것이다. 기업은 고객이 원하는 제품과 서비스를 적시에 제공하여 새로운 시장을 창출하면서 기업의 수익을 극대화한다.

그러나 전통적인 방법인 생산성과 품질 향상, 원가 절감에만 치우치면 내부 지향적 혁신으로 그치게 되어 레드오션에서 쉽게 나올 수가 없다. 시장의 변화 속도가 빠르고 불확실성이 증대되는 상황에서 내부 역량만으로 혁신을 수행하는 것은 한계가 있다.

현대기업환경은 하루가 다르게 과학기술이 복잡해지고 국경에 상관없이 새로운 경쟁자들이 등장하면서 아무리 거대한 기업이라도 혁신적인 사고로 무장한 새로운 기업에게 하루아침에 시장을 내주어야 하는 상황이 빈발하고 있다.

이러한 새로운 환경에서 살아남기 위해서는 새로운 관점의 기업경영관리기법의 패러다임이다. 한국기업이 과거를 답습하는 낮은 수준의 보안리스크관리방법으로는 기업수익에 도움이 되는 보안관리가 되지 못한다. 21세기 기업환경에서 생존하기 위해서는 경영진 수준의 보안리스크관리가 필요하며, 보안리스크관리를 통한 기업경

쟁력을 제고를 위해서는 기업의 보고라인을 새롭게 정립하여야 할 것이다.

2. 연구의 함의 및 제언

본 연구의 목적을 달성하기 위하여 기업 내·외부의 관련조직과의 전략적인 업무협조를 통한 보안리스크 관리효과에 대하여 구체적으로 분석하였다. 현대기업에서의 보안문제는 기업의 수익성의 문제뿐만이 아니라 기업경영의 안정성에 직접적으로 영향을 미치게 된다.

따라서 기업보안업무는 기업경영전략이나 리스크관리 전략과 일치하지 않으면 결코 경영진 차원에서 기업의 보안업무를 논의하거나 전략적인 의제로 다루어지지 않을 것이다. 이젠 한국기업의 낮은 수준의 규모에 의한 보안관리 방법론에 대한 패러다임을 바꾸어야 한다.

그러나 아쉽게도 글로벌 비즈니스를 지향하는 한국기업에서의 보안관리는 생산이나 영업, 관리 분야의 경영관리의 선진화에 비하여 전문화되지 않는 총무업무의 하나이거나 독립적인 직무가 아닌 부수적인 관리업무 정도로 취급하고 있다. 이러한 보안관리에 대한 한국기업의 관행은 성장과 매출위주의 기업경영에서 기인한다. 반면에 글로벌 비즈니스 환경은 결코 한국기업만의 예외적인 특례를 허용하지 않는다. 글로벌 다국적기업과 비교하여 평균적으로 한두 단계 낮은 보안실무자의 조직에서의 직급과 권한의 한계, 보안문제에 대하여 경영진에 직접적으로 보고라인이 확보되지 않는 상황은 한국기업의 보안관리 현황을 단적으로 보여주는 것이다.

기업전반에 대한 보안리스크에 대한 구체적인 분석 없이 유행처럼 특정한 보안이슈가 발생하는 경우 보안관리에 대한 대응이 달라져서는 결코 해당 기업에 적합한 효과를 얻기 힘들다. 그러나 한국기업은 기업전반의 보안리스크에 대한 대응보다는 기밀보호나 IT시스템에 대한 보호에 보안재원의 대부분을 투자하고 있는 한계를 보이고 있다.

한국기업의 안정성과 수익을 향상시키기 위해서는 유행적인 특정한 보안이슈에 편향적인 보안관리의 관행이 가시적으로 기업경영에 도움이 되는 것처럼 보이지만 장기적으로 더 큰 보안리스크에 대한 대응력을 약화시킴으로써 기업에 상당한 손실을 야기하게 될것이다.

21세기 들어서 다국적기업에서 일반화된 독립적으로 경영진에게의 보고라인을

가진 최고보안관리자(CSO)를 중심으로 한 기업전반에 대한 보안리스크 관리는 한국기업에 시사하는 바가 크다. 변동성과 불확실성이 확대되고 있는 현대기업의 보안리스크는 경영진에 의하여 직접적으로 판단하지 않으면 기업경영에 상당한 어려움을 발생하므로 보안리스크에 대한 경영진에 의한 전략적인 접근과 사고의 전환이 요구된다.

본 연구는 포괄적으로 기업수익성제고와 안정성 향상을 위한 기업보안관리와 비즈니스의 전략적 협력에 대하여 검토하고 있기 때문에 세부적인 직능별 협력에 대한 설명에 있어서 한계점을 안고 있다. 따라서 각 분야별 심층적인 협력에 대한 세부적 분석에 대한 연구가 필요하다. 아울러 통계 패키지를 이용한 양적분석방법을 통해 기업보안활동에 따른 기업수익성 제고와 안정성에 미치는 영향에 대한 구체적인 내역에 대한 검증 필요성이 있으나, 실제적으로 보안활동의 따른 미래효과를 수치화하는 것은 추정치에 그칠 가능성이 크다. 본 연구의 이와 같은 한계점과 구체적인 검증은 추가적인 연구가 필요하다.

참고문헌

1. 국내문헌

김순석, 신제철 (2010). 산업기술유출 방지를 위한 핵심인력 관리방안에 관한 연구. **한국경호경비학회지, 25,** 109-130.

노민선, 이삼열 (2010). 중소기업의 산업보안 역량에 대한 영향요인 평가. **한국행정학보, 4-3,** 139-159.

보스턴컨설팅전략연구소 (2001). **전쟁과 경영**. 서울: 21세기 북스.

성태경 (2003). **부정 · 사기에 대한 현황과 대책**. 서울: 대성사.

신성균, 박상진 (2009). 민간조사원(탐정)을 활용한 기업보안활동의 강화방안 : 산업 스파이에 대한 대응방안을 중심으로. **한국경호경비학회지, 20,** 199-228.

오일석 (2007). **산업기술유출 방지를 위한 국가 및 기업의 대응 방안 연구**. 고려대 정보경영공학전문대학원 석사학위논문.

유필화, 헤르만 지몬 (2010). **유필화와 헤르몬 지몬의 경영담론**. 서울: 오래.

정병수 (2007). **산업스파이의 실태분석 및 대응방안에 관한 연구.** 동국대 대학원 석사논문.

최선태 (2011). **기업보안관리론.** 서울: 진영사.

최진혁, 박준석 (2010). CPTED 전략이 산업보안의 효과성 향상에 미치는 유용성에 관한 실증연구. **한국경찰학회보, 24,** 283-322.

Bruce Schneier/채윤기 옮김 (2001). *Secrets & Lies.* 서울: 나노미디어.

Peter L. Berstein/안진환, 김성우 옮김 (2008). **리스크.** 서울: 한국경제신문사.

Richard Foster/정성묵 옮김 (2010). **창조적 파괴**. 서울: 21세기 북스.

Willarm G. Paprett/양승우 옮김 (2008). **위기의 CEO**. 서울: 중앙북스.

Zbigniew K. Brzezinski/김명섭 옮김 (2004). **제국의 선택**. 서울: 황금가지.

2. 국외문헌

ARC training (2008). *Security Management Stage 3*: 6-7.

Brian R. Hollstein (1995). "*Internal Security and the Corporate Customer*," Security Management: 61-63.

Bruce Schneier (2003), *Beyond Fear-Thinking Sensibly About Security in an Uncertain World-*,

Copernicus Books.

Bruce Schneier (2000). *Secrets & Lies*, John Wiley & Sons.

Carl A. Roper (1999). *Risk management for security professionals*, BH.

Cecere, Mark (2001). "*Drawing the Lines*," Harvard Business Review.

Charles A. Sennewald (2003). *Effective Security Management*, BH.

Dan M. Chilcut (1995). "*Making Sense of Environmental Complice*", Risk Management.

Dennis DeConcini (1994). "*The Role of U. S. Intelligence in Promoting Economic Interests*," Journal of International Affairs. vol. 48, no. 1.

Gerald L. Kovacich, Edward P. Halibozek (2003). *The manager's handbook for corporate security*, BH.

James F. Broder (2006). *Risk Analysis and The Security Survey*, 3rd ed. BH.

John J. Fay (1993). *Encyclopedia of Security Management -Techniques & Technology*, BH.

Julian Talbot & Miles Jakeman (2009). *Security risk management*, John Wiley & Sons: 7.

Patsy Clairmont (1999). *Normal Is Just a Setting on Your Dryer*, Tyndale House Publishers.

Peter Pitorri (1998). *Counterespionage for American business*, BH.

Philip P. Purpura (1998). *Security and Loss Prevention*, BH

RachelBriggs, Charlie Edwards (2006). *The Business of Resilience*, London: Demos.

Richard A. Calalli (2004). *Managing for Enterprise Security*, Carnegie Mellon University.

Robert J. Fisher, Gion Green (1998). *Introduction to Security*, 6th ed, BH.

Security Management 24. (1980). *Stress from the press-and How to meet it*." No. 2: 8-11.

Steward Kidd (2001). *Global corporate security-Experience & Lessons*: 6.

Thomas E. Cavanagh, Meredith Whiting (2003). *Corporate Security Management*, Organization and Spending Since 9 · 11.

3. 인터넷 자료

http://www.csoonline.com/article/print/220829, Value made visible, Scott Berinato, April 01, 2006. 검색일 2011. 3. 20.

【Abstract】

A Study for strategic cooperaton of enterprise security and business

Ryu, Hyung-Chang

This study is the research of enterprise security for raising the profitability and stability of Korean companies in global business environment and strategic cooperation of business.

As the scientific technology gets complicated as day goes by and new competitors appear regardless the border in the modern business environment, the situation happens frequently which the huge company hands over their market to the new one armed with the innovative thinking overnight. To survive such new environment, the answer is the change of paradigm regarding business management method at the new point of view. With the low level of security risk management of Korean companies which stick to old habit, the security management which helps the companies secure profits is not affordable.

The global village where the population of 7 billions live in 21st century is facing up to the rapid ecological adaptation. The rapid change of climatic environment creates the hundreds of thousands of sufferers in a moment, and we have been watching the millions of livestock are buried alive due to new contagious disease everyday. Such change encourages the humans in global village to change the basic way of living. The business ecosystem which is the basic root for economic life cannot be an exception. To survive the business environment of 21st century, the security risk management at management level is required and the reporting line of companies should be established newly for raising business competing power through security risk management.

The companies should bear in mind that they can be disappeared into our old memories overnight if they are not sensitive to the changing environment.

Out of new risks for the modern companies, the field especially Korean companies are dealing easily is the security risk. Not like past, the security risk which's size is much more massive and its propagation velocity is very fast is the one of important business risks which the management should take care. Out of security risks which influence on the modern companies significantly, the brand of companies, protection of their reputation, continuity of production and operation and keeping customer's trust are prior to the others. This study offered the suggestion regarding enterprise security and the strategic cooperation of business to deal with such security risk effectively.

Key Words : Security Risk, Business Stability, Enterprise Value,
Strategic Cooperaton, Security Program, Normal Operation Cost