한국경호경비학회 – 제39호(2014): 355–386
투고일 2014. 04. 30, 심사일 2014. 05. 26, 게재확정일 2014. 06. 18

산업보안관리에 관한 뉴패러다임의 정립: 글로벌 비즈니스를 중심으로

유 형 창

산업보안관리에 관한 뉴패러다임의 정립: 글로벌 비즈니스를 중심으로*

유 형 창*

〈요 약〉

오늘날 기업환경은 기업보안에 대한 근본적인 변화를 요구하고 있다. 이러한 변화의 핵심은 오늘날 글로벌기업의 보안관리는 중요한 경영자의 업무이며, 보안실무자는 비즈니스적 사고를 가진 매우 전문화된 교육과 훈련이 필요한 전문직이라는 것이다.

지구촌의 급격한 글로벌화의 진행은 지리적인 영역의 한계에 제한되었던 기업들의 비즈니스의 한계를 무너뜨렸다. 글로벌화와 더불어 과학기술의 발전에 따라 추동되는 급격한 기업환경의 변화는 기업연속성유지에 새로운 패러다임을 요구하고 있다. 글로벌화의 진행에 따라 국가경제에서 기업이 차지하는 비중이 점차적으로 증가하고 우리나라는 무역을 통하여 국가경제의 동력을 유지하고 있는 무역 의존적인 경제시스템으로 한국경제의 편향성이 가속화하고 있다.

글로벌 시장에서 경쟁력을 유지하기 위해서는 기존의 국내에서의 기업운영과는 다른 새로운 전략이 필요하다. 즉, 국내에서의 기업운영에서 대외적인 리스크에 대한 대응력이 어느 정도 확립되어 있으나, 해외에서의 영업활동에서는 국가마다 상이한 기업활동에 대한 관행의 차이와 지배구조의 변화 등 수많은 예상하지 못한 리스크에 직면하게 된다. 이러한 새로운 리스크에 효과적으로 대응하기 위해서는 기업리스크에 대한 새로운 패러다임이 요구한다. 특히 새로운 보안리스크에 효과적으로 대응하기 위한 뉴패러다임과 같은 사고의 유연성이 요구된다.

글로벌 시장에서 세계적인 기업과 경쟁하고 새로운 기업환경에서 발생하는 보안리스크에 효과적으로 대응하기 위해서는 기업경영진과 구성원의 보안에 대한 인식변화와 보안정책에 혁신적인 변화가 요구된다. 이러한 변화의 근간에는 기업보안업무의 확대, 보고라인의 개선, 보안실무자의 전문성과 위상의 제고, 실무자의 다양성과 보안에 대한 투자의 증가 등이 있다.

주제어 : 기업보안관리, 뉴패러다임, 지배구조, 글로벌비즈니스, 기업가치, 최고보안책임자

* 이 연구 결과물은 2014학년도 경남대학교 학술연구 장려금 지원에 의한 것임.
** 경남대학교 법정대학 경호비서학과

목 차

Ⅰ. 서 론

21세기 현대사회 환경과 구조의 변화는 변화무상하고 너무 가변적이여서 모든 분야에서 변화관리의 중요성이 핵심학습 목표로 강조하고 있으나, 미래는 항상 우리의 예상을 뛰어넘는 예측 불가능한 모습으로 표출되고 있다. 세계화의 진전에 따라 국가 간의 물리적인 국경이 사라진 개방경제환경에서 기업의 효과적인 보안관리전략은 자사의 비즈니스 기회를 예측하고 현재와 미래의 기업리스크에 적절히 대응하는 능력을 배양하고 더불어 예상하지 못한 리스크가 발생하는 경우에 기업이 치명적인 손실에 노출되지 않도록 대비함으로써 기업전반의 비즈니스 안정성을 유지하고 구성원의 생명과 기업자산을 적절하게 보호하기 위한 대응책을 의미한다.

오늘날 기업의 보안문제는 과거와 전혀 다르게 기업의 지배구조 과정으로 통합시켜야 하는 새로운 패러다임이 적용되는 개방경제시대의 다양한 산업보안에 대한 뉴패러다임의 요구와 보안전문가의 필요성은 대두한지 오래나 이에 부합하는 기업보안정책의 수립이나 기업보안전문가의 양성에 대한 프로그램의 개발은 미흡하다.

패러다임이란 원래는 과학용어였으나, 오늘날에 와서는 모델, 관념, 지각, 시각, 준거틀 등을 의미하는 것으로 보통 사용되고 있다. 보다 일반적인 의미에서 본다면 패러다임이란 우리가 세상을 '보는' 방식을 말한다. 다시 말하면 우리가 세상을 볼 때 시각적인 감각에서가 아니라, 지각하고 이해하고, 해석하는 관점에서 이 세상을

'보는' 것을 말한다(Covey, 1994: 30).

IMD(2004: 41)보고서에서 세계경제시스템을 구조화된 변동성으로 특징 지웠듯이 현대사회에서 기업의 수익성을 제고하고 지속가능한 성장을 계속하기 위해서는 이러한 변동성을 기업성장에 방해요소가 되지 않도록 안정적으로 관리하여야 할 것이다.

일찍이 세계시장에서 한국기업들과 경쟁하고 있는 외국의 다국적기업의 경우에는 오래전부터 세계시장에서의 기업보안관리의 중요성을 인식하고 기업의 주요한 업무의 하나로써 기업보안관리에 대한 투자의 증가와 실무자의 전문성 향상에 매진하여 왔다. 그러나 우리나라 기업의 경우에는 최근 농협의 전산장애와 같이 빈발하는 보안관련 사고에서 알 수 있듯이 보안에 대한 타성에서 자유롭지 못하다. 오늘날 대부분의 한국기업에서의 보안에 대한 투자는 기업의 지속가능한 성장과 안정성에 대한 미래의 투자의 개념이 아니라 소모성 비용이다. 더불어 한국기업에서는 기업보안조직에 기업보안과 국가보안업무가 혼재되어 진행됨으로써 실제적인 보안업무의 효율성과 전문성에도 한계가 명확하게 존재하고 있다. 이러한 비전문화된 기업보안업무가 한국기업의 지속가능성장을 저해하는 요인이 되고 있다.

현대조직에서의 보안은 이미 기술적인 대책만으로는 대응이 불가능한 조직의 문화나 관습에 관한 구성원의 인식문제이므로 정책적·제도적으로 관리되어야 하는 매니지먼트 업무가 되었다. 현대기업에서의 보안업무는 다양한 리스크로부터 기업을 보호하는 업무에서 비즈니스 경쟁우위를 확보하기 위한 새로운 원천으로 변화되고 있다(Briggs & Edwards, 2006: 18). 특히 오늘날 개방경제환경은 그 동안 국내에 한정되었던 보안업무가 글로벌 시장에서 기업의 비즈니스 활동과 생존을 가능하게 하려면 새롭고 다양한 글로벌리스크를 관리해야 하는 매우 중요한 업무가 되었다.

이러한 비즈니스 환경의 변화의 트렌드에 과연 우리나라 기업과 경영자의 인식은 어떠한가? 우리가 과학적이라고 신봉하는 통계학의 확률을 인용하지 않더라도 급변하는 기업환경의 대비한 리스크관리에 실패한 기업의 미래는 없으며, 설사 일정기간 동안 생존과 성장을 계속하더라도 파국은 시기의 문제일 뿐이라는 것이 역사의 진리이며, 이러한 라이프사이클은 계속 짧아지고 있다.

전통적으로 기업에서 관심을 기울인 주요한 리스크는 재무, 신용, 운영, 정보보안, 법률 리스크에 대한 효과적인 관리 능력이 경영자의 필수조건이었으나(ASIS, 2008: 8) 오늘날 글로벌 리더가 갖추어야 할 핵심적인 능력으로 보안과 리스크관리 능력을 포함하고 있다. 문제는 기업이 직면한 다양한 보안리스크를 객관적으로 수치화할 수

있는 어떤 과학적인 방법도 존재하지 않는다는 것이 보안리스크관리의 어려움이다. 혹 누군가가 과학적으로 검증된 데이터라고 제시한 체계화된 복잡한 수치계산식을 통하여 제시한 어제의 결과물도 오늘의 다양한 변수에 의해 쉽게 무력화될 수 있다. 따라서 이러한 데이터는 단지 의사결정에 참고자료로 활용될 것이다.

기업은 특성상 리스크를 감수함으로써 기업의 이윤을 획득하지만 리스크 관리에 실패하면 기업의 존재는 위태로워질 수 있다. 기업에서의 리스크는 기업목표를 달성하는 데 불리하게 작용하는 사건 혹은 사고 때문에 야기되는 손실가능성을 의미하기도 한다.

모든 기업을 운영하는 데는 리스크가 존재한다. 그러나 기업도 미시적인 시각으로 보면 개별부서의 이기주의로 부서자체의 리스크는 존재하지 않는 것처럼 보이지만 기업을 전체적인 측면에서 바라보면 수많은 리스크가 부서와 부서 사이, 업무와 업무 사이에 잠재되어 복잡하게 얽혀있다. 그러므로 전체적인 시각으로 기업을 바라보지 않으면, 설사 치명적인 리스크가 현존하더라도 누구도 인식하지 못하거나, 타부서나 타인에게 전가하려고 하는 것이 리스크관리의 특성이며, 이러한 부서간 이기주의(silos effect)를 극복하기 위해서는 통합된 전사적 리스크관리가 필요하다.

Ⅱ. 기업보안관리에 관한 뉴패러다임 논의의 배경

1. 기업보안관리의 필요성

본 연구는 글로벌 경제환경에서의 기업보안관리업무의 중요성에 대한 인식과 기업가치를 효율적으로 보호하기 위한 보안관리의 효율성을 제고시키는 방안을 강구하는 것이 목적이다.

오늘날 비즈니스 세계는 계속 복잡성이 증가하고 있으며, 비즈니스의 글로벌화는 기업의 구조와 수명에 변화를 요구하고, 전통시장의 포화상태는 기업에게 더 많은 위험성이 있는 시장개척을 수용하도록 강요하며, 지식경제로의 전환은 비즈니스 세계의 '영역'의 중요성을 잠식하고 있다. 이와 동시에 이러한 트렌드에 적응해야하는 기업의 보안리스크의 크기는 확대되고 기업통제는 점차적으로 어려워지고 있다(Briggs & Edwards, 2006: 12).

이와 같이 복잡다기하고 다양한 직능과 조직의 구조적인 문제점이 혼재되어 발생하는 보안리스크에 대한 지금까지의 단순인력에 의한 물리적 대응방식이나 몇몇 소수의 보안전문가에 의한 미시적(micro)인 방어적 대응으로는 한계가 있으므로 조직의 경쟁우위를 확보하기 위한 거시적(macro) 정책으로써 새로운 동력원의 관점으로 접근하지 않으면 변화에 따른 비즈니스 불안정성에 대한 명쾌한 해결책을 도출하기가 어렵다.

이러한 변화에 대한 기업의 대응은 과거의 직능적 조직과 지식기반의 조직에서 매트릭스 구조로 이동하고 있다. 매트릭스 구조는 '명령체계 단일화의 원칙' 즉 한 사람의 직원에게는 오직 한 사람의 상사가 있을 뿐이라는 원칙을 벗어나 두 개 이상의 직권 계열을 갖는다. 매트릭스 조직은 고도의 전문기술을 요하는 대형 프로젝트 관련 사업에서 흔히 볼 수 있으며, 조직 형태 상 자칫 혼란을 야기할 수도 있기 때문에 21세기 보안기능에는 융통성과 전문성을 갖춘 직원을 필요로 한다(Briggs & Edwards, 2006: 20).

매트릭스 구조의 기업은 구체적인 비즈니스 문제를 해결하기 위하여 다양한 기술과 전문가로 구성된 자체적인 팀을 조직하고 권한을 해당 팀에 위임하고 효과적인 관리는 공식적인 채널에 의존하기 보다는 신뢰성 있는 네트워크를 통한 기존의 조직에 구애받지 않고 업무를 진행함으로 이들의 업무수행력에 의존하게 된다.

2001년 세계의 경제심장부로 불리던 미국 뉴욕에서 발생한 9/11테러는 여러 가지로 기업에 영향을 미쳤다. 실제적으로 9/11테러는 기업보안에 대한 경영자의 사고가 획기적으로 변하게 되는 전환점이 된 사건이다. 기업보안에 대한 9/11테러의 영향에 관한 위원회보고서에 따르면 대부분의 경영자들은 처음으로 보안업무가 기업경영관리구조 전반에 광범위하게 산재되어 있으면서, 보안기능이 고도로 분산되어 보안리스크에 대한 책임추적성과 업무협력의 어려움에 대하여 놀라움을 나타냈다. 이에 대한 결과로 그룹의 보안부서를 제외한 많은 기업에서 그룹전체의 보안업무의 협력과 리더십의 구심점을 아우르는 부서를 조직하였다(Cavanagh, 2005: 17).

이 사건을 계기로 기업들은 보안조직, 기업의 연속성과 위기관리계획, 소방훈련과 대피절차로부터 훈련교본과 지침서 그리고 구성원과의 교신에 관한 모든 내용을 개정하였다. 2005년 7월 영국런던에서 발생한 폭발사건에서 배운 중요한 교훈 중에 하나가 구성원과의 교신의 중요성에 대한 것이다. 이와 동시에 모든 기업에서 정도의 차이는 있으나 기업의 보안리스크가 점차적으로 복잡해짐에 따라 기업자산을 보호

하는 특별한 전문성을 가진 인력에 의한 체계화된 조직의 필요성에 대하여 부정하는 경영자는 없다.

<표 1>과 같이 그 동안 기업경영진이 관심을 가진 기업리스크는 전략적, 정치·법률적, 재정, 기획, 보험, 안전에 대한 리스크가 대부분을 차지하였으나, 글로벌기업에서는 보안리스크가 기업경영진이 관리하여야 할 중요한 기업리스크에 포함되었다.

〈표 1〉 기업리스크 VS. 기업보안리스크

기업리스크(사례)	기업보안리스크(사례)
현금흐름의 지속가능성, 채무관리, 잘못된 사고방식, 과도한 프로젝트, 환률 변화, 기업의 지배구조, 재품생산의 실패, 경기침체, 과도한 경쟁 등	절도, 비즈니스 출장의 안전성, 납치와 유괴, 악의적인 제품손괴, 위조, 부정행위, 정보누설, 테러리즘, 이익갈등 등

자료: ARC Training(2007: 9-10)

기업의 효율성을 제일로 여기는 미국이나 선진국의 기업에서는 계속적으로 보안에 대한 전문성을 계속 요구하고 있으며, 기업환경의 차이로 수치적 비교는 어려우나 보안투자가 우리나라 기업보다도 적게는 서너 배에서 많게는 열배나 많다(Cavanagh, 2005: 22). 이에 반하여 우리나라 기업이나 정부의 보안정책이나 투자의 대상은 정보보호나 산업기밀유출에 부분적으로 치중되어 있음을 보여주고 있다.

우리 기업들이 기업의 안정성에 필수적인 이러한 보안에 투자를 줄이는 근시안이 단기적으로 비용절감으로 치부될 수는 있지만, 궁극적으로 기업의 엄청난 손실을 야기하고 언젠가는 이에 대한 대가를 치러야 하는 것이 리스크관리의 원리이며, 파국은 시기의 문제이지 리스크관리에 실패하면 기업이 파국에 이르는 지름길이 된다는 것을 알아야 한다.

보험산업의 기본이 리스크관리이다. 그러나 아쉽게도 기업경영방침이나 기업이 직면한 모든 리스크가 보험약관에 적용되지는 않는다. 급변하는 현대기업에서 다양한 리스크에 대한 대비나 투자가 없다면 기업의 현재는 있을 수 있으나 미래는 보장할 수 없다.

2. 글로벌기업의 보안트렌드

오늘날 기업의 보안조직의 구성과 규모는 조직의 다양한 특성에 의해서 결정된다.

특히 조직의 구체적인 보안업무의 필요성, 고유의 고려사항과 취약성이 보안조직의 규모를 결정짓는데 가장 주요한 요소이고 조직의 구조와 역할에 기여하는 정도에 대한 보안업무의 가치에 대한 경영진의 인식이 또 하나의 결정적인 요소가 될 것이다. 더불어 기업구조조정과 같은 경제적인 트렌드의 변화는 보안업무의 역할에 영향을 미친다.

특히 오늘날과 같은 치열한 기업 간의 경쟁 속에서의 기업조직의 효율성에 대한 경영진의 관심은 절대적이므로, 증가된 위협요소와 리스크에 대하여 좀 더 적은 비용으로 좀 더 많은 성과를 기대하는 것은 보안조직에도 예외가 아니다. 오히려 이러한 구조조정의 과정에서 보안조직의 효율성이나 전문성에 대한 인식에 의구심이 들 경우에는 보안조직은 일차적인 구조조정 대상으로 선택되기도 한다. 따라서 오늘날의 보안업무는 그 동안의 규모와 인력위주의 보안활동에서 첨단보안기기를 활용한 뛰어난 보안조직운영을 통하여 조직에 기여하는 바를 항상 객관적으로 제시하는 역량이 필요한 시기이다. 이러한 추세는 이미 오래전부터 선진국의 보안조직의 운영에 관한 MBA과정이 다양하게 제공되어 기업의 어떤 조직보다도 생산성과 업무의 효율성이 높은 활동으로 전이되고 있다.

일반적으로 GDP의 3분의 1을 담당하고, 세계무역의 3분의 2를 수행하는 다국적 기업과 같은 거대기업의 보안조직은 뛰어난 보안전문가로 구성된 독립된 조직으로 운영되는 것이 보편적인 추세이다(최선태, 2008: 23). 이것은 보안활동이 다른 조직에 예속되어 있는 경우에 조직의 부정적인 활동에 대한 객관성을 담보하기 어렵고 타 조직의 방해에 의해서 업무의 공정성에 심각한 우려가 발생하는 것을 방지하기위한 방침이다. 이러한 독립된 보안조직에서는 기업보안정책의 이행확인, 손실예방활동, 기업연속성기획, 부정행위감사, 산업안전, 소방, 기업윤리규정의 이행여부 확인 등을 포괄적으로 다루게 된다(ASIS, 2008: 10-11).

비즈니스 환경의 변화에 따라 기업보안관리의 주요한 관심도 전략적으로 변화를 계속하고 있다. 2004년 MORI 결과에 따르면 97%의 응답자가 보안이 그들의 관심사항이라고 응답하였고, 응답자의 50%는 매우 큰 관심사항이라고 응답하였다(Business Security Survey 2004). 더불어 응답자의 82%는 보안에 5년 전보다 더 많은 투자를 하며, 57%는 앞으로 5년간 더 많은 투자를 보안에 할 것이라고 응답하였다. 이러한 결과로 볼 때 현대기업들은 보안업무가 전반적인 비즈니스의 관심사항에 대하여 기여하고 있음을 인정하고 있는 것처럼 보인다. 아래의 <표 2>와 같이 구체적인 항목

에 대한 조사결과는 효과적인 보안관리가 다양한 기업의 핵심적인 목표에 기여하고 있는 것에 대한 응답이다.

〈표 2〉 기업보안관리의 중요 영향력에 대한 관심도

항목과 영향력	최고의 영향	약간의 영향	영향력 없음	평가 불가
기업 브랜드와 평판의 보호	74	18	7	1
구성원의 안전성 보장	69	26	5	0
구성원의 채용/유지 보장	26	52	22	0
지적재산의 보호	44	41	14	1
고객신뢰의 유지	79	14	6	1
주주신뢰의 유지	70	23	5	2
생산과 운영의 연속성	80	15	4	1

자료: Briggs & Edwards(2006: 27)

이 조사에서는 투자자의 중요한 고려사항으로 기업보안역량에 대한 관심이 획기적으로 증가하고 있음을 보여주고 있다. 투자자의 87%는 만약 어떤 기업이 보안사고를 신속하고 효과적으로 다루지 못한다면 기업에 대한 투자자의 인식이 변하게 될 것이라고 응답하였다. 또한 61%는 보안사고가 발생하는 경우에 기업브랜드와 평판에 영향을 미치게 될 것이며, 50%는 주가에 유사한 영향을 미치는 반면에, 단지 과반에 미치지 못하는 45%는 고객충성도(Customer Loyalty)에 영향을 미치게 될 것이라고 생각했다.

위와 같은 기업의 다양한 가치를 보호하기 위해서는 기업의 경쟁력에 부합하는 최상의 보안전문가를 채용하고 전문성을 유지하며 다른 어떤 부서의 업무와 마찬가지로 글로벌 비즈니스 트렌드에 부합하는 역량을 가진 인재를 선발하고 이에 상응하는 보상을 하여야 한다.

3. 기업가치의 보호

보안프로그램을 일반적인 상품이나 서비스의 경우처럼 투자대비효과(ROI)에 분석을 가지고 기업주나 조직을 설득하거나 판매하지 않는 것이 오랫동안 보안업무가 가지고 있는 문제점으로 지적되었다. 이러한 관행은 아마 보안업무가 상업적인 관점

으로 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? 그러나 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.

보안의 가치를 측정하기 위한 흥미로운 접근법은 Bruce Larson에 의해서 시도되었는데, 그는 American Water의 보안책임자이다. CSO Online에 2006년 발표한 기고문에서 Larson은 "가치보호"에 대하여 제안하였는데, 여기에서 Larson은 보안업무가 단지 비즈니스의 낭비적인 요소를 방지하는데 불과하다는 고전적인 사고방식의 문제점을 극복하기 위하여 그는 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 다른 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 활용하는지에 대하여 설명하고 있다. 이러한 Larson의 가치보호(value protection) 매트릭스는 다음과 같다(http://www.csoonline.com/article/print/220829, Value made visible, Scott Berinato, 2006).

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

Larson의 가치보호 매트릭스에 대해서 American Water의 운영담당부사장인 Steve Schmitt는 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 불과하다. 그러나 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 연결될 수도 있다. 따라서 결과적으로 이벤트 영향력 E를 추가적인 비용의 증가 없이 축소하는 방법을 찾는 것이 기업주가 가장 바라는 가장 효율적인 방법이 될 것이다.

Ⅲ. 한국 기업보안관리의 문제점

1. 매스컴의 문제점

세계화시대의 기업자산의 보호는 기업의 안정성에 필수적인 요소이며, 기업자산 보호의 일차적인 책임은 기업에게 있다. 세계 각국에 진출한 다국적(혹은 무국적)기업자산을 특정 국가가 나서서 보호하는 데에는 한계가 있으며, 지분구조와 경영권의 다각화에 따라 다국적기업의 소속국가의 개념도 점차 모호해지고 있다.

일찍이 세계를 상대로 기업경영을 한 서구의 다국적기업들은 이러한 기업자산보호의 중요성을 직시하고 오래전부터 기업자산보호업무를 수행하는 기업 보안조직의 전문화를 이루었으며, 이미 대부분의 다국적기업은 보편화된 보안조직과 시스템화된 운영을 기업경영의 필수업무로써 적용하고 있다. 이에 반하여 우리나라의 보안업무를 다루는 매스컴의 태도나 우리의 산업보안에 대한 인식은 상당히 안이하다. 여기에 매스컴은 산업보안의 문제를 기술유출방지가 전부인 것처럼 다루었다. 최근에는 175만 명의 고객 정보가 유출된 현대캐피탈 전산망 해킹, 19일 동안 계속된 농협의 전산망 장애 등 그 동안 과학기술의 편리성에 비해 너무나 안전성에 대한 투자를 등한시 하였던 IT보안에 누적된 문제점에 대한 경보등이 켜졌다.

보안사고가 발생할 때마다 매스컴에 반복되는 피상적이고 일반론적인 대책으로는 빈발하는 보안사고를 막을 수 없다. 더불어 피해액 위주의 보안사고에 대한 보도나 하드웨어에 대한 투자만으로 보안손실의 방지와 기업경영자나 구성원의 인식을 바꿀 수 없다. 경영자는 왜 보안에 대한 투자를 해야 하는가? 얼마나 투자해야하는가? 누가 집행하고, 어디에 투자해야하는가에 대한 개별기업의 고유의 특성에 대한 합리적인 데이터가 없으면 결코 보안에 대한 투자는 일시적인 소모성 비용이라는 인식을 바꿀 수가 없다. 문제는 이러한 보안투자의 필요성에 대하여 합리적인 분석이 가능한 산업보안전문가가 우리나라에 극히 적다는 것이다. 이것이 빈발하는 기술유출사건과 전산망 장애가 기업의 실제적인 대책으로 연결되지 않고 매스컴의 일시적인 이슈로서 머물게 되는 한계이다.

우리나라에 산업전반에 대한 보안체계를 수립하고 집행의 효율성을 판단할 수 있는 전문가는 부족한 원인은 성장위주의 기업경영과 교육과정의 부재를 들 수 있다. 더불어 현재의 형사사법기관이나 유사기관에서의 경력을 바탕으로 대기업이나 다국적기업에서의 보안관리자로서의 업무를 수행하는 실무자의 전문성도 한계가 있다. 그러나 아직까지 산업보안전문가를 양성하는 교육프로그램의 수요적합성에 대한 어떠한 연구도 없었다.

지금의 우리나라 대학의 정보보호, 경찰행정, 경영정보, 경호 관련학과의 편향적이며 국부적인 교육과정으로는 결코 산업전반의 안정성을 제고하거나 기업의 보안리스크를 관리하는 학제적 지식을 가진 전문가를 양성할 수 없다.

21세기 보안의 글로벌 트렌드는 정보보호와 물리적 보안의 통합과 비즈니스와의 체계적인 연계성이다. 현재의 우리나라의 미시적 교육으론 첨단과학을 활용한 조직화되는 보안리스크를 방지하기에는 역부족이다. 현대사회의 보안손실을 최소화하기 위해서는 다양한 학문적 전문지식을 활용해야 하는 대표적인 융합학문분야가 보안분야이다. 따라서 첨단화되는 보안리스크를 효과적으로 방지하기 위한 전략적 사고를 갖은 산업보안전문가 양성을 위해서는 대학교육과정의 미시적사고와 할거주의가 극복되어야 할 것이다. 보안의 본래의 의미인 불안전성의 극복은 하나의 제품이 아니라 계속적인 프로세스를 관리할 전문가의 능력에 좌우된다.

경영자가 기술유출과 같은 보안활동에 대한 투자를 하기 위해서는 기업에 얼마만큼의 위협요소가 존재하는지에 대한 구체화된 데이터를 제시하여야 경영자의 투자를 이끌어낼 수 있다. 이러한 구체적인 데이터는 전문적인 보안진단을 바탕으로 한

기업체의 위험관리수준에 대한 평가를 바탕으로 하여야 한다.

보안사건을 다루는 매스컴의 보도태도도 상당한 문제점을 갖고 있다. 예를 들어, 대부분의 산업스파이 사건의 피해액은 적게는 수십억에서 많게는 수조원에 이를 정도로 천문학적 금액에 이르나, 보도기관들은 실제적인 피해액에 대한 구체적인 분석 없이 피해업체의 주장을 그대로 발표되고 있으나, 이러한 피해액의 산정은 대부분이 유출된 해당기술이 기업이 의도한대로 최대로 시장에서 수익을 올릴 경우를 가정한 경우이므로 실제적인 피해액은 훨씬 적을 수밖에 없다. 그러나 오직 피해당사자의 발표나 주장을 그대로 인정하는 것이 현재 보도기관의 선정적 보도태도에 기인한다. 기술유출에 대한 대책도 대부분이 지나치게 기술적인 대책에 의존하는 태도와 경영자의 의식의 문제점 그리고 법과 제도의 미흡을 지적하는 기사가 거의 모든 기술유출사건에 따라오는 만능의 해결책이다. 그러나 이러한 일반론적인 대응책은 결코 경영자의 투자를 이끌어내는데 한계가 있으며, 구성원의 보안에 대한 의식과 문화가 변하지 않으며 결코 급증하는 보안손실을 통제하기는 어렵다.

2. 보안업무의 편향성

오늘날 미디어에 회자되듯이 기업보안업무를 산업기술유출방지에만 중점을 둘 경우에는 온라인(IT)보호가 기업보안업무에서 상당히 중요한 역할을 차지하는 것처럼 보이며, 온라인보호가 보안리스크 관리대책의 전부인 것처럼 여겨진다. 그러나 오늘날 보안의 글로벌 트렌드는 물리적 보안과 기술적 보안의 통합(convergence)을 어떻게 이루어내는가이다. 사업장에 수없이 설치된 CCTV와 엄격한 출입통제시스템 그리고 보안서약서가 가시적인 보안수준을 제고하는 것처럼 보이지만 허가된 출입자(종업원)에게는 크게 효과가 없다.

오히려 임직원 모두에게 기업의 보안정책에 대한 홍보를 주기적으로 실시하고 효과적인 교육시스템을 통하여 개인의 사소한 보안활동이 구성원 모두에게 직접적인 도움이 된다는 인식을 심어주어서 조직원 전체가 보안 의식을 가질 수 있도록 노력하여야 한다. 산업스파이 방지를 위한 보안시스템의 구축에서 중요한 것은 시스템의 번잡함을 최대한 배제하여야하고, 상황에 따라서 시스템의 탄력성 있는 적용이 효율성을 극대화하게 될 것이다.

미국정부 및 기업의 보안 전문가들도 기술유출의 약 75%가 스파이 활동 등과 같

은 인적 정보원에 의한 것이고, IT를 활용한 유출은 6%에 불과한 사실을 잘 알고 있으면서도 여전히 전통적인 IT 보안 정책을 고수하고 있다고 비판하였다. 2004년에 미국 기업은 IT 보안에 4,440억 달러를 소비했으며, 79%의 기업이 2005년에도 동일 혹은 증가한 금액을 투자할 것으로 조사되었다(Cavanagh, 2004: 28).

그러나 현재 일어나고 있는 기술유출의 대부분은 내부자와 연관되어 발생한 것이므로 "첨단 네트워크 보안장비를 갖춘다고 해서 기술유출문제가 해결된다는 생각은 난센스다. 오히려 이러한 첨단시스템은 인간관계를 가장한 사회 공학적 기법에 의해 손쉽게 무력화된다.

2004년 ASIS에서 조사한 결과를 보면 미국기업의 CSO 가운데 보안분야의 자격증 소지자는 49%, 이중에서 70%는 보안관리분야인 CPP(Certified Protection Professional)자격이고 단지 4%만이 IT분야(CISSP, CISA)의 자격증을 갖고 있는 것으로 나타났다(Harowitz, 2005). 반면 우리나라는 기업보안전문가는 IT보안전문가로 치부하기도 한다. 이것은 기술유출방지를 IT보안으로 생각하는 것과 같다. 그러나 기술유출은 기술 자료가 스스로 유출되는 것이 아니라 사람에 의해서 유출되는 것이므로 기술유출방지는 디지털자료관리가 아니라 인간이 가진 탐욕에 대한 통제와 취약성에 대한 통찰력과 비즈니스 프로세스관리이다.

우리는 보안대책을 주로 첨단 기술 도입에 치우쳐서 생각하는 경향이 높다. 물론 이것이 가장 쉬운 접근법인 것은 사실이나 이러한 제한적인 접근은 더 큰 위협요소를 간과하는 잘못을 저지르기도 한다. 첨단기술보호에서도 무엇보다 중요한 것은 기술적인 보안대책보다는 다양한 보안 프로세스가 제대로 운영될 수 있도록 하는 개별 조직의 보안환경의 조성이다. 최신 보안 기술이나 솔루션 도입만으로 기업이 당면한 보안 문제를 해결할 수는 없다. 아무리 좋은 제품이나 서비스를 갖고 있더라도 정책이나 이를 뒷받침할 전문인력이 없다면 결국 투자비용만 낭비하게 되는 결과를 가져올 것이다.

좋은 보안정책이란 보안 관련 전담 인력이 얼마나 있는지, 정책이 제대로 세워져 있는지, 일상적인 업무에서 어떻게 적용되고 있는지, 보안이 취약한 부분에 대해서 집중적으로 관리하고 있는지, 보안사고 발생에 대비한 계획은 세워져 있는지 등에 대한 기업의 계속적인 확인이다. 여기에 사고가 발생하기 전에 미리 예방하는 시스템의 확립도 포함된다.

이 보안 정책 프로그램에서 중요한 것은, 기업 구성원들이 바로 강력한 보안 시스

템 구현의 핵심 요소라는 점이다. 최상의 기술과 절차를 적용한다 하더라도 구성원들이 조직자산의 보안에 관련한 자신의 역할을 숙지하고 실천하지 못한다면 그 효과가 제한적일 수밖에 없다.

강력한 보안 기술과 정책을 무력화시키는 것은 숙련된 해커가 아니라, 대부분 보안에 대한 지식 또는 인식이 부족한 기업의 내부 구성원들이다. 보안 취약점에 노출된 기업자산을 효과적으로 보호하려면 기업의 전 구성원들이 보안 정책과 정보 자산 보호에 있어서 자신의 역할과 그 중요성을 기본적으로 이해하고 있어야 하고 일상의 과정에서 보안관리의 중요성에 대하여 구성원 스스로가 인식하여야 한다. 이러한 이해가 선행되지 않는다면, 기업의 자산과 수익을 보호하는데 있어서 구성원들의 참여와 기여는 기대하기 어려울 것이다.

이와 같이 기업들은 첨단 기술만으로는 보안을 보장할 수 없다는 점을 반드시 인식해야 한다. 아무리 공고한 첨단 보안 기술을 보유하고 있다고 하더라도 이를 적용하는 제대로 된 보안문화가 확립되어 있지 않다면 보안 환경 자체가 크게 위협받을 수 있다. 따라서 성공적인 조직자산 보호를 위해서는 최신 기술, 포괄적인 정책 및 절차, 그리고 충분한 교육과 동기부여 등 체계적인 프로세스를 반드시 확립해야 한다. 이를 통해서만이 기업의 귀중한 자산을 능동적으로 보호할 수 있는 환경을 구현할 수 있게 된다는 것을 경영자들은 인식해야 할 것이다(「디지털타임스」, 2006).

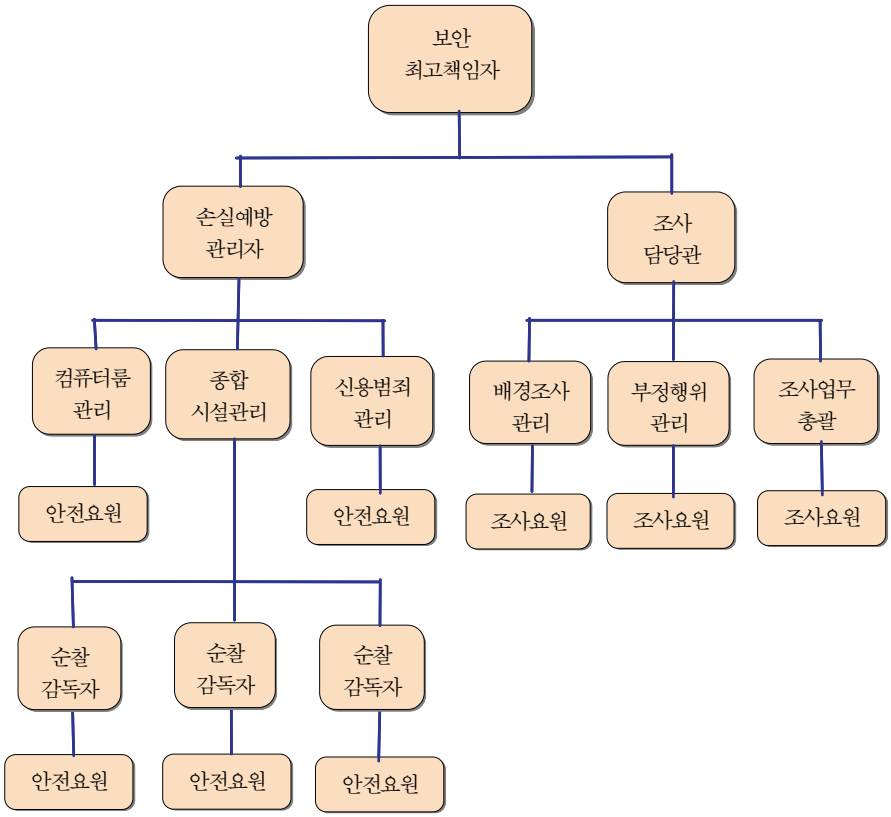
3. 부정행위조사기능의 부재

기업의 경쟁력은 건실한 기업문화에서 출발한다. 위기에 강한 기업은 기업구성원이 기업정책을 신뢰하고 정책의 적용에 공정하고 엄격하여야 한다. 다양한 구성원들이 모여 있는 다국적기업이 이러한 보편적인 기업정책의 적용에서 취약점을 노출하게 되면 기업의 안정성은 크게 흔들리게 될 것이다.

현대기업경영의 화두 중의 하나가 윤리경영이다. 2001년 파산신청을 한 미국의 에너지회사 엔론(Enron)과 같은 세계적인 규모의 기업이 기업내부의 부패행위로 붕괴되어가는 모습을 우리는 빈번하게 접하게 된다. 다국적기업에서는 이러한 부정행위를 방지하는 업무가 기업보안업무의 핵심이다. 한국기업에서 보안리스크를 효과적으로 대응하기 위해서는 필요에 따라 보안이슈에 적절하게 대응하는 것도 필요하지만 포화된 경쟁사회에서 자신의 욕망을 채우기 위해 질주하는 인간의 탐욕을 통제

하고 감시하는 부정행위 조사부서의 운영이 핵심이다.

<그림 1>은 모든 기업들이 공통적으로 적용해야 한다는 강제성은 없지만 오늘날 경쟁력 있는 외국의 다국적기업의 가장 기본적인 보안부서의 조직도이다(Sennewald, 2011: 17). 여기에서도 조사업무가 보안조직의 매우 주요한 업무임을 알 수 있고 추가적으로 업종에 따라서 정보보호나 브랜드보호와 같은 새로운 전문보안업무가 더해지기도 하며, 이러한 조정은 기업의 특성에 따라 좌우될 것이다.



자료: Sennewald(2011: 17)

〈그림 1〉 다국적기업의 보안부서조직도

<그림 1>과 같이 다국적기업의 보안관리의 핵심적인 직무에는 구성원의 부정행위를 조사하고 감시하는 조사부서가 존재하나 한국기업의 보안부서의 업무영역에는

구성원의 부정행위(fraud)에 대한 조사 및 기업정책과 절차의 이행여부확인에 관한 권한이 없거나 감사업무로 착각하는 기업이 대부분이다. 이것은 외국계 다국적기업들의 보안부서의 핵심적인 업무 중에 하나가 구성원의 부정행위방지업무와 구체적인 기업규정의 준수여부의 확인과 비즈니스 절차의 이행여부의 확인에 속하는 것과 비교하면 한국기업에서의 보안부서의 위상이나 업무활동은 아직도 단순한 물리적 시설보안이나 정보보호에 머물러 있음을 알 수 있다.

오늘날 빈발하는 기술유출과 같은 보안사고의 대부분이 내부인과 관련되어 있듯이 모든 구성원에게 공통적으로 적용되는 기업보안에 대한 구체적인 프로세스의 준수여부를 확인하는 권한을 보안부서에 부여하고 이에 대하여 경영진 차원에서 엄격하게 관리하는 것이 기술유출을 방지하는 첫걸음이 될 것이다. 아래의 <표 3>은 부정행위조사업무와 회계감사와의 차이를 보여준다.

〈표 3〉 감사와 조사의 비교

	회계감사	부정행위조사
시 기	반복적 그리고 정기적으로 실시	부정행위조사는 의심되는 상황 발생시
범 위	회계감사의 범위는 재무자료 전반	의심되는 특정한 부분에 대한 자료실사
목 적	회계감사결과를 의견으로 제시	부정행위여부를 조사하고 원인을 규명
결 과	감사결과로 과거의 오류가 회복되지 않음	부정행위조사로 부정행위자의 책임여부를 규명하고 손실을 복구함
방 법	회계감사기법	부정행위조사기법
가 정	회계감사는 전문적인 의구심을 가지고 실시	부정행위조사는 책임자에게 책임을 묻게 되므로 증거확보가 중요

자료: 성태경 외(2003: 27)

부정행위조사업무의 중요성은 대부분의 기술유출은 전·현직 종업원에 대한 경쟁사의 스카우트나 매수에 의한 것이므로 내부자의 기술(정보)보안 의식을 높이고 유출 시도를 막을 수 있는 내부 프로그램을 구축하는 게 외부로부터의 침입을 막는 것보다 우선시돼야 한다.

투명성기구(TI)가 세계 30개국을 상대로 뇌물을 주는 기업인을 대상으로 조사한 '2008 뇌물공여지수(BPI)'을 살펴보면(「한국일보」, 2008), 한국은 10점 만점에 7.5로 나타나 22개국 가운데 남아프리카, 대만과 함께 공동 14위를 차지한 것에서 보이듯 우리나라의 청렴성지수는 OECD국가들 중에서도 하위권에 맴돌고 있는 것을 고려

하면 우리나라 국민들이나 기업의 구성원들이 경제활동에서 부패에 대한 용인정도가 크나 보안업무부서에서 부정행위방지 업무를 수행하지 않는 것은 상당한 아이러니가 아닐 수 없다.

이것은 동서양의 의식구조가 기업에도 영향을 미치기 때문으로 생각된다. 국화와 칼의 Benedict(1989)는 사막의 종교를 배경으로 한 죄와 벌의 서양문화는 부정행위자에 대한 고발과 엄벌에 처하는 것을 당연시 하는 반면에 명예와 부끄러움의 동양문화(정성본, 2005: 21 재인용)는 구성원의 부정행위에 대하여 상대적으로 관대하며, 내부고발자에 대한 보호제도도 허술하다. 그러나 기업에서 명확한 비즈니스 프로세스가 모든 구성원에게 공정하게 적용되지 않는다면, 상당수의 구성원은 언제든지 부정행위를 행할 가능성이 있다. 이것이 우리나라 기업에서 보안부서의 핵심 업무로써 구성원의 부정행위조사권한의 부여와 적절한 관리통제를 하여야하는 이유이다.

Ⅳ. 기업보안관리의 뉴패러다임

1. 기업보안관리 직무의 확대

세계화와 과학기술의 발전에 따라 기업의 영업환경이 급변하였으나 한국기업에서의 보안업무는 과거와 비교하여 크게 변화하지 않고 있으며, 한국기업과 세계시장에서 경쟁하고 있는 글로벌 다국적기업과 비교하여 상당히 제한적인 영역에 머물고 있다. 이러한 보안직무의 한계는 기업에서의 보안부서의 중요성에 대한 인식과 비례한다. 우리나라의 경우 관련 법령에 의거하여 주요 공기업과 대기업에서의 보안업무는 비상대비자원관리법에 의한 비상계획관과 향토예비군설치법에 의한 예비군부대지휘관이 직·간접적으로 기업보안업무에 참여하고 있다. 그러나 이들이 법령에 의거한 업무 외에 글로벌보안환경의 변화에 따른 <표 4>와 같은 다양한 업무를 수행하지는 않는다.

그러나 관련법령에 의하여 채용이 의무화되거나 권장되는 경우이므로 사실상 기업보안의 최고책임자의 역할을 하는 경우가 많다. 이에 반하여 기업보안업무의 복잡성은 가속화되어 관계법령에서 규정된 직무를 벗어난 다양한 보안업무를 군대에서 습득한 국가방위개념의 보안지식으로 기업보안활동을 수행하기에는 어려움이 가중

되고 있는 것이 현실이다. 따라서 정형화된 체계 없이 기업마다의 다양한 형식과 구성으로 필요에 따라 주로 총무조직이나 업무지원부서의 하나로 보안조직을 구성하여 운영하고 있는 것이 우리나라 기업의 현실이다.

개별적으로 기업의 고유한 특성이 존재하므로 현재 우리나라 기업보안업무의 직무범위에 대한 구체적인 합의는 없다. 이러한 직무범위의 불명확성은 아직은 기업보안에 대한 중요성에 대한 인식의 한계와 보안활동이 기업에 기여하는 역할에 대한 제한으로 귀결된다. 여기에 기초한 직무범위의 한계의 근간에는 보안실무자의 전문성의 한계에서도 기인하게 된다. 실제적으로 다국적기업의 아시아지사나 한국지사에서 글로벌보안기준에 부합하는 업무를 부여하는 경우에도 한국의 보안실무자의 업무수행력의 한계를 드러내는 경우가 많았다.

<표 4>는 글로벌 시장을 장악하고 있는 다국적기업의 보안직능을 나타낸다. <표 4>에서와 같이 모든 한국기업이 제한된 보안직능을 수행하는 것은 아니지만 대체적인 한국기업의 보안직능에는 산업기술과 정보유출의 방지, 출입통제와 절도방지, 시설보안시스템의 운용과 유지, 정보기술(IT)보안관리에 중점을 두어 다국적기업과 비교하여 명백한 편향성과 한계가 존재한다. 한국기업에서의 이러한 보안관리직능의 한계가 보안실무자의 전문성의 한계로 이어지고 기업에서의 위상이나 대우가 외국계 다국적기업과는 비교하기가 힘들 정도로 열악한 상황으로 이어지고 있다. 현대기업에서의 보안직능이 현실적으로 확대되어야 함에도 불구하고 경영자의 의식, 한국기업의 지배구조, 경영기법과 연관성이 있으므로 한국기업에서의 보안직능의 확대를 가로막고 있다.

〈표 4〉 다국적기업의 보안직능

보안조직의 직능
① 보안리스크관리를 위한 보안전략기획(기업경영전략과 일치)
② 보안시스템관리(침입감지시스템, 대응시스템, 출입통제시스템, CCTV)
③ 요인보호와 비즈니스 출장보안기획
④ 내부자 절도의 조사업무
⑤ 채용 전 적격심사와 구성원의 규정이행
⑥ 사기행위와 같은 지식인 범죄
⑦ IT보안과 컴퓨터범죄(IT부서와의 협력유지)
⑧ 침해, 절도, 사업장 침입과 점거, 집단항의와 행동
⑨ 약물과 알코올남용

⑩ 범죄손실을 포함한 자산범죄
⑪ 사보타지와 방화
⑫ 납치와 테러리즘(악의적 폭파위협전화)
⑬ 금품강요와 이익갈등과 같은 비윤리적 행위
⑭ 산업스파이와 정보유출 방지
⑮ M&A 대상 기업에 대한 실사
⑯ 공급라인을 통한 절도와 제품의 전용 방지
⑰ 악의적 제품손상과 제품위조
⑱ 정치적 불안정성에 대한 분석
⑲ 조직범죄와 부패(특히 고위직)

자료: ARC Training(2005: 11) 편집

2. CSO 체제의 구축

보안리스크의 발생에 따른 기업연속성과 수익에 대한 손실이 확대됨에 따라 이에 대한 대응도 기업경영차원의 주요 기능으로 보안리스크에 대한 관심이 증대되었다.

2001년 9/11테러 이후에 기업의 보안을 책임지는 경영진에 속하는 최고보안책임자(CSO, Chief Security Officer)가 주목받고 있는데, 글로벌 기업에서의 CSO는 경영진, 관리자, 구성원의 보호, 시설자산과 정보자산의 보호를 보장하기 위한 활동, 보안조직의 운용, 사업장 보안의 적용과 조정을 하부 관리자를 통하여 수행하고 대부분의 CSO는 재무, 시설, 네트워크/정보기술, 구성원에 대한 위험에 대한 모든 안전성을 보장하며, 정보수집과 리스크의 평가, 사고에 대한 대응에 대하여 국내외 모든 보안기능들을 관리한다(ASIS, 2008: 8). 따라서 오늘날 CSO는 기업의 비즈니스 과정에서 발생하는 재무범죄의 손실, 문서위조, 사람에 대한 범죄, 사보타지, 위협, 비상사태, 불법적인 행위, 기업자산과 환경에 대한 범죄에 대응하기 위한 최상의 서비스를 개발하고 제공한다. CSO란 기업보안을 위한 정책수립은 물론 기술적 대책과 법률적 대응까지 총괄하는 최고보안책임자로서 CSO는 기업전반의 보안정책의 수립·실행·관리·교육과 법률적 대응에 이르기까지 기업보안에 대한 전반적인 책임을 맡는다.

<표 1>에서와 같이 기업리스크에서 보안리스크가 차지하는 중요성이 강조됨으로 글로벌기업에서 리스크관리 문화를 새로 만들고 지속적으로 발전시키는 일을 수행하는 직책이 CSO이다. 2001년 9/11테러 이후에 그 동안의 개별적인 보안업무의 한계를 인식하고 통합적인 보안업무의 중요성을 느낀 미국기업들은 CSO 채용을 늘리고 있

으며, CSO가 빠른 속도로 미국 기업들의 최고경영진의 구성원으로 주요 의사 결정권자가 되고 있으며, CEO에게 없어서는 안 될 동반자가 되고 있다(Parrett, 2008: 25).

기업구조에서 보안조직이 어디에 위치하든 간에 CSO는 반드시 경영진에 직접적인 보고라인과 만남이 가능하여야 한다. 2001년 Harvard Business Review에서는 이상적으로 CSO가 독립성을 보장받기 위하여 최고경영자나 최고운영책임자에게 보고할 수 있어야 한다고 하였다(Cecere & Mark, 2001: 24).

오늘날 다국적기업의 CSO는 대부분이 부사장급이며, 33%는 CEO에게 직접 보고하는 직속된 독립조직이다. 미국에서 2007년에 조사된 자료에 따르면 기업이나 조직체의 보안 정책의 입안과 이사회에 참석할 수 있는 권한을 가진 최고보안책임자(Security Executive)의 연봉 평균은 322,181 달러였다(Matlacha, 2007: 23-24). 미국기업의 최고보안책임자는 평균적으로 20년 이상의 경력과 석·박사학위(M.S. or Ph. D)를 가졌거나 학사학위 소지자는 25년 이상의 경력자 있었으며, 미산업보안협회(ASIS) 공인 보안자격증인 CPP 자격을 갖는 것을 개인들이나 기업에 의해 선호되었다(최선태, 2008: 410).

2007년 Foushée Group의 조사에서 CSO가 기업의 모든 네트워크와 정보보호시스템에 대한 안전성을 보장하는 책임을 갖고 있느냐에 대한 질문에 대하여 그렇다는 응답은 26%에 불과하고, 74%는 네트워크와 정보보호시스템의 안전성에 대한 책임은 IT부서의 업무로써 분류하고 있는 것으로 조사되었는데(Matlacha, 2007: 28), 이것은 보안기능의 효율적인 운영을 위하여 온오프라인의 융합과정이 꾸준히 진행되고 있으나, 모든 네트워크와 정보보호시스템에 대한 안전성의 보장은 CSO의 핵심적인 업무에 속하지는 않는다는 의미이다.

다국적기업의 CSO는 급변하는 국제경제와 산업에 대한 거시적 안목과 감각, 비즈니스 트렌드에 대한 분석력이 필수적이다. 지금까지의 보안실무자는 정보기술(IT)에 대한 한정된 전문지식으로 마치 조직 전반에 대한 보안업무를 수행하려 하였는데 반하여 오늘날 산업분야에서 필요로 하는 CSO는 정보기술에 대한 기본 지식과 더불어 거시경제와 산업분야에 대한 안목과 감각, 정보수집과 위험분석, 의사전달력까지 겸비해야 하고 기업의 최고 보안책임자로서 기업 비즈니스 안정성을 제고하는 업무를 수행하여야 한다.

지금까지 기업들은 보안을 기술적인 문제로 인식했으나, 현재 보안은 경영활동의 주요한 업무의 일부로 다뤄지고 있으며, 현대기업에서의 보안은 기술적인 문제로 한

정되지 않는다. 즉 "보안은 조직의 위험의 정도를 어떻게 관리하느냐의 관점에서 불확실성이 상존하는 현대기업경영에서 중요성이 배가 되고 있으나, 아직까지 우리나라에선 대부분의 기업들이 최고정보관리자(CIO)가 CSO를 겸하거나, 보안관련 전문전담부서조차 설치돼 있지 않은 경우도 허다하다. 그리고 보안담당자가 있더라도 대부분 정보보호부서에 속한 팀장이나 과장의 직책을 갖고 있기 때문에 기업의 거시적 보안정책을 제안하고 결정에 참여할 수 있는 권한은 거의 없다. 그러나 현대기업경영은 변화에 어떻게 대응하고, 신속하게 변화에 대한 정보를 수집하고 분석함으로써 기업의 진로를 결정하는 정보수집력과 분석력이 뛰어난 기업만이 생존할 수 있다.

급변하는 글로벌 환경에서 살아남으려면, 재난관리, 보안관리, 정보관리 등으로 산재된 기업의 조직과 운영이 CSO체제를 중심으로 보안조직과 활동을 통합하여, 비즈니스에 관한 정보가 통합되어 조직내부에 원활하게 흐르게 될 때, 기업의 생존과 안정성은 향상될 것이다.

3. 보안실무자의 다양화

지난 수십 년 동안 기업보안은 보호와 손실예방에 중점을 둔 '방어적인' 접근법에 의해서 지배되어 왔다. 따라서 보안책임자는 비즈니스 기능을 더 효과적으로 수행하는데 도움을 주는 활동보다는 언제나 비즈니스 활동을 제지하는 '출입구에서의 보안요원'의 모습으로 비쳐졌다. 지금까지의 한국기업에서의 보안업무에 대한 전문성은 보안선진국과 유사하게 대부분 군이나 경찰과 같은 보안업무와 유사한 조직의 경력을 바탕으로 기업에서 보안직능을 수행하는 것이 일반적인 보안실무자의 전문성의 바탕이 되었다.

The Conference Board의 조사에 의하면 아직까지도 미국에서의 기업보안분야는 과거 경찰이었거나 보안 관련 경력자들에 의하여 거의 대부분의 실무자들로 구성되었다(The Conference Board, 2003). 이 조사에 의하면 보안실무자의 거의 3/4은 전통적인 보안분야 경력자였는데, 이중 31%는 경찰, 19%는 정보기관, 21%는 군대 경력자였으나, 오늘날 기업보안기능에서 다양성이 필수적으로 요구되는 아래와 같은 상당한 이유가 존재한다.

첫째로, 보안에 대한 전략적 중요성에 대한 인식이 증가함으로써, 이러한 결과로 보안부서는 과거보다 더 상위직급에서 운영되어야 할 필요성이 제기된다. 이러한 필

요성을 충족시키기 위해서는 전체적으로 새로운 기법인, 리더십의 부여, 의사소통, 과거의 경력이나 전술적 지식 이상의 활동과 네트워킹 지식이 필요하게 된다. 전략적 사고자와 전술적 사고자 사이의 구분은 보안과 비즈니스를 효과적으로 제휴하려는 기업의 가장 구분된 중요한 요소 중의 하나이다.

둘째로, 매트릭스 조직에서는 경찰이나 군 경력자의 배경을 가진 사람들과는 대조되는 경영과 리더십에 대한 특별한 접근법이 요구된다. 과거 유형의 조직은 명령과 통제관리 형태로서 상대적으로 확실성의 정도가 높은 수준의 지시를 조직의 상층부에서 내려지고 즉시 아래로 전달되는 형태인 반면에, 오늘날 기업환경에서 보안부서의 영향력은 보안부서의 능력을 기업전반의 모든 개개인이나 팀들과 협력하거나 협조하도록 설득하는데 균형을 유지하여야 한다. 이러한 공정은 보안전문가와 비전문가 사이의 대화로 기업업무수행에 필수적이다. 또한 이러한 이해증진은 기업보안직능이 '고객중심'을 대표하는 것으로 더욱 중요한 의미를 가진다.

셋째, 전통적인 보안기능은 비즈니스 공정을 '어렵게 만드는 업무'로써 인식되는 분야의 접근방법과 결합되어 있었다. 공식적인 보안훈련은 리스크를 꺼리는 경향이 있는 반면에, 비즈니스는 경쟁업체에 앞서거나, 새로운 시장을 개척하거나 이윤을 극대화하기 위하여 계산된 리스크를 수용할 필요성이 있다.

넷째, 기업보안직능은 위법적 행위를 자행하는 사람, 혁신적이고 고정된 틀을 벗어나 생각하는 사람들의 관리를 필요로 한다(Boeodzicz, 1996). 경찰, 응급의료서비스와 지방 비상기획부서와 같은 보안관련 직업에 대한 연구에서 전통적인 보안분야에서의 '장기간' 경험은 기업에서 요구하는 보안사고에 대한 혁신적인 대응을 저해하는 요소가 된다고 지적하였다. 오늘날의 보안책임자는 계속적으로 독립적인 사고력, 가정과 행동양식 그리고 혁신에 도전하는 의지와 같은 것들의 품성을 평가하여 팀의 가치를 극대화하려한다. 따라서 '어느 부서와 마찬가지로 보안직능에서도 한계를 넘어서려고 노력하거나 계속적으로 주어진 업무에 도전하는 사람들을 필요로 한다.'

다섯째, 보안업무에서도 '인적요인'의 가치에 대한 인식이 증대되고 있다. 실무에서 많은 보안전문가들은 일반적으로 감정의 영향력, 인간행동에 대한 인식과 공포를 포함한 인간 역동성 요소의 실패에 대응하여 보안사고와 응급상황을 다루는 방법을 훈련한다. 감정지수는 효과적인 협력관계의 형성에서 핵심적인 요소이지만, 보안과 위험관리에서 인적요소는 기술적인 보안기술에 비하여 일반적으로 중요성이 간과되어 왔다.

보안과 리스크 전문가는 비이성적인 방법으로 어떻게 리스크가 사회적으로 형성되었는가에 대하여 정확한 인식을 필요로 하며, 구성원의 이성에 상관없이 구성원의 공포와 관심사항에 대하여 민감하여 대응하여야 한다. 다시 말하면 기업은 효과 없는 대책에 비용을 낭비하지 않아야 하듯이, 구성원의 감정적 불안정성에 중점을 두어, 물리적 안정감의 중요성만큼이나 반드시 구성원의 감정적 안정감을 평가하여야 한다.

Ⅴ. 결론 및 제언

오늘날 기업환경은 비즈니스 보안에 대한 근본적인 변화를 요구하고 있다. 이러한 변화의 핵심은 오늘날 기업보안관리는 중요한 경영자의 업무의 하나라는 것이다. 과거의 기업보안에 대한 주요한 패러다임은 대부분이 군대나 준군사조직에서 인용하였으나, 지금도 이러한 과거의 타성에서 자유로운 기업은 많지 않다. 왜냐하면 비즈니스 보안에 대한 새로운 패러다임을 요구하는 경영자가 없고 대부분의 보안실무자는 과거의 자신의 경력을 바탕으로 기업보안업무를 수행하기 때문이다. 더불어 이제까지의 보안업무는 기업자산에 대한 물리적인 보호조치가 주요한 업무였다. 이 경우에 보안부서는 권위주의적인 형태로 운영되었으므로 종종 근로자의 반감을 사거나 적대적인 업무로 인식되기도 하였다. 또한 보안활동에 대한 정보는 과도하게 통제되었으므로 이러한 통제가 보안활동의 불신을 가중시키는 역할을 하였다.

이와 같이 과거의 대부분의 보안프로그램은 보안부서와 다른 부서와의 건설적인 협력관계가 거의 없었으며 보안활동의 비용절감이나 적절한 기술을 도입하여 생산성을 향상시킨다는 생각에는 관심이 없었다.

그러나 오늘날 비즈니스에는 현대적인 경영기법들이 활용되고 있다. 보안리스크 관리나 손실관리와 같은 개념에는 더욱 더 이러한 기법의 활용이 요구되며, 효과적인 자산보호 프로그램을 개발하고 운영하기 위해서는 이러한 방법들을 적극적으로 활용하여야 한다. 새로운 비즈니스 환경에서 기업의 경쟁력을 향상시키기 위해서는 반드시 변화된 환경에 대한 통찰력을 바탕으로 최신기법을 활용하고 보안활동이 기업의 기본적인 목표와 직접적으로 일치하도록 비즈니스 활동과 전략적으로 협력하여야 한다.

지난 10여 년 동안에 보안관리는 기업의 주요한 현안으로 부상하였고 몇몇의 기업에서는 상대적으로 다른 현안보다 우선권과 영향력이 크다. 앞서가는 기업의 '성공의 비밀'과 다른 기업들의 단점을 통한 배움이 21세기 기업보안에 대한 비전을 제시하고 21세기 기업의 어려움을 타개하는데 도움을 줄 것이다. 보안직능은 구체적인 위협요소에 대한 대응보다는 비즈니스 운영자에 의해서 진행되고 이러한 방법이 잘 작용하기 위하여 복잡하고 빠르게 변화하는 세계에서 비즈니스의 현실을 어떻게, 무엇을 반영할 것인가를 경영자의 시각에서 전략으로 결정하여야 한다(Briggs & Edwards, 2006: 21).

연구결과로 글로벌기업의 효과적인 보안리스크관리를 통한 비즈니스안정성과 수익성제고를 위해서 보안과 비즈니스의 긴밀한 협력에 필요한 몇 가지 주요한 특성을 제시하였다.

첫째, 보안부서의 기본적인 역할은 보안을 직접적으로 적용하거나 기업을 위한 보안이 아니라, 기업의 모든 비즈니스 분야에서 구성원의 매일의 행동과 의사결정에 보안직능이 반영되도록 구성원을 납득시킨다.

둘째, 보안부서는 규정의 적용보다는 변화관리의 비즈니스이며 신뢰된 사회적 네트워크를 통하여 영향력을 미치게 한다.

셋째, 보안은 리스크를 예방하기 보다는 기업이 리스크를 수용하는데 도움을 주므로 새로운 비즈니스 전개에서 기업의 전면에 위치한다.

넷째, 보안은 책임의 분산과 시간의 흐름에 따른 상대적인 중요성의 변화와 같은 항상 새로운 비즈니스에 대한 고려사항에 대응하여야 하므로 보안부서는 결코 정체되어 있거나 고정된 실재물이 되어서는 안 된다. 오늘날 혁신적인 많은 기업에서 보안의 역할은 전통적인 보안의 역할보다는 전반적인 기업의 탄력성에 관심을 기울인다.

다섯째, 보안직능은 전략과 운영활동 모두를 포함하므로, 보안부서는 반드시 이러한 두 가지 서로 다른 업무를 구분하여야 한다.

여섯째, 보안부서의 힘과 정당성은 보안에 국한된 전문지식으로부터 나오는 것이 아니라, 비즈니스에 대한 통찰력, 구성원의 기능, 관리능력과 의사사전달의 전문성에 좌우된다.

글로벌기업의 보안부서는 반드시 다음과 같은 방향을 지향하여야 한다.

첫째, 보안활동을 통하여 기업제반의 '활동을 자유롭게 한다.' 보안실무자는 그들의

권한과 정당성이 기밀성에서 기인하기 보다는 개방성과 투명성에서 기인한다는 것을 이해해야 하며, 기존의 '보안에 대한 사회적 통념'을 변화시키는데 매진해야 한다.

둘째, 과거의 '은밀하게 행해진 보안업무 수행기법'의 관행을 벗어나야 한다. 보안실무자는 '보안사건'에 대하여 과장되게 반응하지 않으며 더 많은 자원과 권한을 획득하기 위한 기회로서 이러한 상황을 냉소적으로 활용하거나 자기 자신의 이익을 위해서 타인의 무지를 활용하려고 해서도 안 된다.

셋째, 비즈니스를 우선으로 하여 업무를 수행한다. 이러한 사고는 기업 지배구조와 같은 새로운 조직구성의 원리에서부터 해외 사업장의 운영과 같은 새로운 비즈니스 업무처리에 모두 적용된다.

넷째, 최상의 해결책만을 추구하지는 않는다. 절대적 보안이란 불가능한 것이므로, 절박한 경제적인 필요성이 발생한 곳에서도, 최상의 해결책만을 고집하는 기업의 결정은 바람직하지 않다.

다섯째, 좋은 인간관계를 장려한다. 기업 내부에서와 더불어 기업과 주주 사이에서 강력한 보안부서만의 방벽의 설치는 기업의 친구를 잃을 뿐만 아니라 결국에는 모든 조직에 손상을 미친다.

여섯째, 의사전달의 중요성을 이해한다. 기업전반에 걸쳐 선명성을 얻고, 보안직능이 필요한 곳에서 핵심적인 의사결정에 영향력을 발휘하고 인식의 오류를 바로잡음으로서, 보안서비스가 기업전반에 구현되도록 노력한다.

마지막으로 글로벌기업의 보안부서는 반드시 다음의 역할을 수행하여야 한다.

첫째, 전통적인 보안업무의 한계를 넘어서 비즈니스 연속성, 기업평판의 관리, 리스크관리와 기업의 책임을 포함한 전반적으로 보안업무 영역을 확장한다. 이러한 업무의 확장은 네트워크의 중요성과 변화관리 기법이 강조되어야 하고 기업전반을 관리하기 위한 부가적인 압력이 발생한다.

둘째, 가능한 경영진과의 최단거리의 보고체제를 구축하고, 기업전반의 기업보안의 핵심 조정자로서 행동한다.

셋째, 기업 내·외부 비즈니스 환경변화에 민감하게 탄력적으로 대응한다.

넷째, 전략적 계획, 비즈니스의 전략적 우선순위에 반한 부서활동의 평가지표, 다른 비즈니스 부서와 더욱 공식적인 연계를 위한 활동과 같이 보안과 비즈니스의 긴밀한 협력관계를 구축하기 위하여 계속적으로 더 많은 노력과 활동이 필요하다는 것을 이해한다.

위와 같은 역할을 원활하게 수행하기 위해서 앞서가는 글로벌기업의 보안관리자는 변화가 상존하는 글로벌 경제전쟁에서 기업경쟁력을 제고하기 위하여 효율적인 리더로서 기업의 최고경영진에게는 신뢰할 수 있는 동료로, 보안부서에서는 민주적·개방적 유형의 리더십을 가지고 부서를 이끌어야 한다.

참고문헌

1. 국내문헌

성태경 외. (2003).「부정사기에 대한 현황과 대책」. 서울: 대성사.

정성본. (2005).「선불교 개설」. 서울: 한국선문화연구원.

최선태. (2008).「기업보안핸드북」. 서울: 진영사.

_____. (2011).「기업보안관리론」. 서울: 진영사.

2. 외국문헌

ARC Training. (2005). *Security Management Stage 1(Core Skills)*: 9-13.

ASIS. (2008). Chief Security Officer Guideline.

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

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

Cecere, Mark. (2001). "*Drawing the Lines*," Harvard Business Review: 24.

Charles A. Sennewald. (2011). *Effective Security Management*. BH: Boston.

Charles A. Sennewald and John K. Tsukayama. (2001). *The Process of Investigation: Concepts and Strategies for Investigation in the Private Sector*. 2nd edition. BH: Boston.

E Boeodzicz. (1996). '*Security and risk: a new approach to managing loss prevention*' International Journal of Risk, Security and Crime Prevention 1, no 2.

Foushée Group, Inc. Matlacha, FL. (2007). *Top global security executive (chief security officer)*. 2007 Security and Compliance Compensation Survey: 23-24

James F. Broder. (2000). *Risk Analysis and The Security Survey*. 2nd edition. BH: Boston.

IMD World Competitiveness Yearbook 2004: 41.

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

Rachel Briggs/Charlie Edwards. (June 2006). *The Business of Resilience. Corporate security for the 21st century*. Demos.

Robert J. Fisher/Gion Green. (1998). *Introduction to Security*. 6th edition. BH: Boston.

Russell L. Bintliff. (1992). *The Complete Manual of Corporate and Industrial Security*. Prentice-Hall, Inc.

Ruth Benedict. (1989). *The Chrysanthemum and The Sword: Patterns of Japanese Culture*. Mariner Books.

Sherry L. Harowitz. (2005). *The Very Model of a Modern CSO*. Security Management.

Stephen R. Covey. (1994).「성공하는 사람들의 7가지 습관」. 김경섭, 김원섭(역). 서울: 김영사: *The 7 habits of highly effective people*.

Steven Fink. (2002). *Managing The Global Risk of Economic Espionage*. Dearborn.

Thomas E. Cavanagh. (2005). *Corporate Security Measures and Practices: An overview of security management since 9/11:Organization and Spending since 9/11* (New York: The Conference Board).

UN, *Global Challenge·Global Opportunity*. (Sep. 2002). Johannesburg Summit 2002.

William C. Cunningham and Todd H. Taylor. (1985). *Private Security and Police in American*. The Hallcrest Report. Chancellor Press.

William C. Cunningham et al., (1990). *Private Security Trends: 1970~2000*. The Hallcrest Report Ⅱ. BH: Boston.

William G. Parrett. (2008).「위기의 CEO」. 양승우(역). 서울: 중앙 books: *The Sentinel CEO*.

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

Global Trends 2015. (2000). *A Dialogue About the Future With Nongovernment Experts*. National Intelligence Council.

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

3. 기타자료

「디지털타임스」. (2006). 기업 보안 프로세스 정립이 절실. 11. 6: 27.

「한국일보」. (2008). 한국 기업, 해외 비즈니스 뇌물 관행 '여전'. 12, 10.

http://www.csoonline.com/article/print/220829, Value made visible, Scott Berinato, April 01, 2006). 검색일 2011. 6. 20.

【Abstract】

A Study for New Paradigm Settlement on Business Security Management: Focus on Global Business

Yu, Hyung-Chang

Current business environment asks the fundamental changes about business security. The essences of these changes are that the security management of today's global business is important task of managers and the security practitioner is professional who needs very specialized education and training with business thinking.

Rapid process of globalization of global village tore down the business limit that was restricted on the geological areas' limitation. Rapid business environments' change that is driving depends on development of science and technology with globalization needs new paradigm to keep business continuity. With the process of globalization, Korea, which importance is gradually increasing in the national economy, has trade dependent economic system, which keeps power of national economy through trade, so Korean economic tendency is accelerating.

To keep competitiveness in global market, new strategy that is different with existing domestic business management is necessary. That is, capacity of coping with outside risk in domestic business management is established in some degree, but business activities in foreign countries faces at numerous unexpected risks that differ from country to country such as difference with the custom, changes of corporate governance etc. To cope with these new risks effectively, new paradigm for business risk is necessary. Especially, flexibility of thinking like new paradigm is necessary to cope with new security risk effectively.

To cope with security risk that occurs in the new business environment effectively and competes against international company in global market, company management and members' changes of cognition about security and innovative changes in security policy is necessary. In the basement of these changes, there is expansion of business security tasks,

improvement of report line, enhancement of professionalism and status of security officers, variation of hands-on workers and increasing of investment to the security etc.

Key words : Corporate security management, New paradigm, Governance, Global Business, Business value, Chief Security Officer