글로벌 기업의 공급사슬보안 및 위험관리전략에 관한 연구

양정호*

<목 차>

Ⅰ. 서 론

지금까지 기업들은 공급사슬상 비용절감 및 운영효율의 개선을 위해 많은 노력을 기울인 반면 공급사슬 보안을 강화하기 위한 투자는 추가적인 비용을 발생시키고 공급사슬의 효율성을 떨어뜨릴 수 있다는 점에서 소홀히 다루어왔다. 하지만, 최근 들어 전 세계적으로 테러위협이 증가하고 국제적으로 물류보안제도를 강화함에 따라 공급사슬 보안에 대한 중요성이 높아지고 있다. 특히, 2001년 발생한 9/11 테러사태는 공급사슬 전반에 큰 혼란을 야기함으로써 기업들이 보안위험에 대한 공급사슬의 취약성을 인식하는 계기가 되었다.[1] 이와 함께 지금껏 기업들이 추진해온 공급사슬 전략들은 보안사고 발생시 신속하고 유연한 대응을 어렵게 함으로써 공급사슬의 취약성을 더욱 증가시키는 요인이 될 수 있다.[2]

* 상지대학교 무역학과 전임강사

1) 2002. 2. 18일자 포천지에 따르면, 재고증가, 국경폐쇄, 리드타임 증가, 기타 9/11사태로 인한 보안조치들이 미국 공급사슬에 미친 영향은 연간 미화 1천 5백억 달러로 추산하고 있다.

2) Routh Banomyung, “The impact of port and trade security initiatives on maritime supply

공급사슬상의 보안을 강화하기 위해서는 많은 비용이 소요되고 기존의 전략의 수정을 요한다는 점에서 기업에 많은 부담을 안겨준다. 또한 국제적으로 물류보안제도가 강화됨에 따라 공항 및 항만에서 물류적체가 심화되고 물류시스템의 효율성이 감소하게 될 것을 우려하고 있다. 하지만 물류보안시스템의 개선 및 강화는 공급사슬의 가시성을 높이고 물자, 정보, 인력 등 공급사슬 구성요소에 대한 감시와 통제를 강화함으로써 물류비용을 줄이는 한편 보안사건이나 시장수요변화에 신속하고 유연하게 대응하는 등 많은 혜택을 가져다줄 수 있을 것으로 기대된다. 가령, 화물의 도난, 마약밀수 및 불법이민 등의 발생건수를 줄이고 물류보안규정의 준수에 따른 신속하고 안정적인 통관의 보장 및 화물보험료의 인하 등의 혜택을 누릴 수 있으며, 선박 및 항만에 대한 테러분자들의 공격에 대비한 물류보안시스템의 개선은 자연재해나 운송사고와 같은 기타의 비상상황에 대한 대응력을 높임으로써 공급사슬 구조를 안정시킬 수 있다.

관건은 보안상의 목적과 공급사슬의 효율성이라는 상반된 목적이 상호 균형을 이룰 수 있도록 하는 것이다. 본 논문은 먼저 글로벌 공급사슬의 취약성을 증가시키는 요인들을 분석하고 공급사슬 보안시스템의 개선을 통해 기업이 얻을 수 있는 편익의 관점에서 공급사슬보안에 대한 투자의 필요성을 제기하고자 한다. 다음으로 보안사고의 효율적인 예방과 효과적인 대응을 통해 피해를 최소화하기 기업이 선택할 수 있는 전략적 요소들을 검토함으로써 공급사슬상 보안위험을 관리하기 위한 합리적인 방법들을 모색하고자 한다.

Ⅱ. 보안위험과 공급사슬의 취약성

1. 공급사슬의 취약성

영국의 Cranfield 대학의 연구보고서[3]에서는 공급사슬 취약성(vulnerability)을 “공급사슬의 외부적인 위험뿐만 아니라 내부적인 위험으로부터 발생하는 심각한 혼란에 대한 노출”로 정의하고 있다. 기업경영의 글로벌화, 급격한 수요변화, 제품 및 기술수명주기 단축 등으로 공급사슬상의 불확실성 및 혼란이 증가함에 따라 기업들은 글로벌 공급사슬의 운영 및 통제에 있어서 많은 어려움에 직면

chain management”, *Marit. Pol. Mgmt.*, Vol. 32. No. 1., January/March 2005, p. 3.

3) Cranfield School of Management (2002), *Supply Chain Vulnerability*, report on behalf of DTLR, DTI and Home Office.

하게 된다. 더욱이 물품의 조달·생산·판매 및 인도에 이르는 공급사슬상 모든 활동은 상호 연계되어 이루어지기 때문에 글로벌 공급사슬의 운영과정에서 발생하는 변동은 그 정도의 심각성에 관계없이 공급사슬 전반에 미치는 효과가 크고 공급사슬 구조를 불안정하게 만든다. 높은 불확실성과 불안정한 공급사슬 구조는 리드타임, 재고 및 비용의 증가와 함께 기업의 현금흐름을 악화시키는 한편, 고객의 요구에 신속하고 유연한 대응을 어렵게 함으로써 기업의 경쟁력을 약화시킨다.

공급사슬의 취약성을 높이는 공급사슬위험요인[4]으로는 테러 및 보안위협 외에도 허리케인이나 홍수, 지진과 같은 자연재해에서부터 공장가동 중단, 자재부족과 같은 운영상의 혹은 일상적 위험, SARS와 같은 전염병, 사보타주와 같이 인간에 의해 행해지는 재난, 그리고 세관검사로 인한 통관지연, 운송지연 등에 이르기까지 다양하다.[5] 자연재해나 동맹파업 혹은 테러리스트들의 공격과 같은 외부적인 요인들뿐만 아니라 기업의 경영전략의 또한 공급사슬구조에 영향을 미칠 수 있다.[6] 최근 기업들은 JIT 생산방식 및 린(lean) 관행을 채택하고 생산 및 물류시설을 집중하는 한편, 아웃소싱은 늘리되 공급선을 단순화하는 등 공급사슬상 재고 및 낭비요소을 제거하거나 줄임으로써 공급사슬의 효율성을 높이는데 주력해 왔다. 이러한 전략은 시장상황이 안정적인 경우 공급사슬의 효율성을 증가시키지만 시장상황이 불안정한 경우에는 공급사슬의 취약성을 높이는 원인이 되고 있다.

공급사슬상 파트너의 수와 규모, 경험, 그리고 능력은 모두 공급사슬 보안에 영향을 미친다. 공급자의 수가 적을수록 보안사고 발생시 대안적인 공급선을 확보하기 어렵기 때문에 공급중단으로 인한 공급사슬 혼란이 발생할 가능성이 커지게 되며 마찬가지로, 공급사슬 파트너의 규모가 작을수록 공급사슬보안에 대한 투자가 제한을 받을 수밖에 없기 때문에 공급사슬 전반에 걸쳐 동일한 수준의 보안을 확보하기 어렵다.[7]

Hendrick and Singhi[8]는 단일 조달시스템, 낮은 재고수준, 낮은 유연성 등 지

4) 공급사슬 위험은 최초 공급자로부터 최종 소비자에 이르기까지 계획된 물자의 흐름을 방해하거나 중단시키는 우연한 사건으로 정의할 수 있다(Donald Waters, *Supply Chain Risk Management*, KOGAN PAGE, 2007, p.7).

5) Ravi Sarathy, "Security and the Global Supply Chain", *Transportation Journal*, Fall 45, 4, 2006, p.30.

6) John F. Frittel, "Port and Maritime Security: Background and Issues", *Military Technology*, Nov. 2006, pp.88~94.

7) Ravi Sarathy *op. cit.*, pp.41~42.

8) Kevin B. Hendrick and R. Vinod Singhal, "An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm",

나치게 효율성을 강조한 공급사슬 구조는 공급사슬 혼란에 대한 취약성을 높일 수 있다고 한다. 마찬가지로 외부조달에 대한 의존도가 높은 공급사슬의 경우 위험에 취약할 수밖에 없고 이러한 구조를 가진 공급사슬하에서 보안관련 위험의 발생가능성 역시 높아지게 된다.

2. 국제물류보안제도의 강화

공급사슬상의 보안이 확보되지 않으면 개별기업 및 경제전반에 영향을 미칠 수 있다는 점에서 미국을 비롯하여 세계 각국 및 다국적 정부기구에서는 국제물류보안제도를 강화하기 위한 법규 및 정책들을 개발해왔다. 물류보안제도는 ISPS Code와 같이 IMO나 WCO와 같은 국제기구를 중심으로 도입된 강행적 규제와 CSI나 C-TPAT와 같이 참여당사자에게 경쟁적인 이점을 제공함으로써 물류보안을 강화하는 한편, 물자의 이동을 촉진하기 위한 자율규제 프로그램들이 있다. 이들 보안프로그램들의 주된 목적은 국제물류시스템상의 테러위협을 줄이고 물류보안을 강화하기 위한 것으로 공급사슬 네트워크상의 효율성과 물류보안 간의 균형을 고려한 것은 아니다. 따라서 기업 입장에서 이들 프로그램을 준수하고 이행하기 위해서는 많은 시간과 비용이 소요[9]될 뿐만 아니라, 이러한 제도 자체가 공급사슬의 효율성 및 효과성에 심각한 부작용을 초래할 수 음을 우려하고 있다.

3. 물류보안비용

9/11 사태는 1천 9백억 달러에 달하는 피보험 재산과 약 900억 달러에 달하는 경제적 손실을 초래하였다.[10] 테러리즘의 직접적인 결과로 발생하는 비용은 인명의 손실, 재산의 파괴, 단기적 경기침체 등을 들 수 있다. 이들 비용은 지속적인 테러위협으로 인한 불확실성이 증가함에 따라 보안사고의 예방을 위해 생산에 투입될 기업의 자원을 전용함으로써 더욱 증가하게 된다. 한편, 국경, 공항 및 항만의 폐쇄, 선박의 억류, 통관화물의 검색강화 등 테러행위에 대한 정부의 과잉대응은 물류시스템의 혼란을 더욱 악화시키고,[11] 불확실성의 증가에 따른

Production and Operations Management, 14 (1), Spring 2005, pp.695~711.

9) Russel and Saldanha (2003) 은 보안관련 공급사슬 비용을 6천 5백억 달러로 추산하고 있다.

10) *Ibid.*, p. 525.

11) 9/11 테러사건 이후 미국 정부는 미국 국경을 통과하는 항공기 및 물자의 이동을 제한하였다. 이러한 조치로 안정적인 국제수송에 의존하는 JIT 생산시스템에 혼란을 초래하여 크라이슬러는

보험비용의 증가 및 전체 공급사슬의 효율성 및 효과성 감소 등 간접적으로 수반되는 비용도 만만치 않다.[12]

공급사슬보안체계를 구축하기 위해 불가피하게 발생하는 비용들이 있다. 정부에서 일정수준의 화물보안을 강행적으로 요구할 수 있고, 미국 국토보안국(DHS: Department of Homeland Security)과 같이 보안책임을 담당하는 정부기관에서 보안비용 명목으로 새로운 요금을 징수할 수도 있다. CBP(Bureau of Customs and Border Protection)와 같은 정부기관의 규제는 컨테이너 봉인의 채택을 증대시킬 수 있고 CSI나 C-TPAT와 같은 보안프로그램 참여의 유인을 제공할 수 있다.[13] 컨테이너가 현물심사대상으로 선정되거나 홍콩항에서 제안하는 바와 같이 전수검사(universal screening)가 실시되는 경우 컨테이너의 양륙 및 검사에 소요되는 비용을 수반하게 된다. 각국 정부의 물류보안 강화에 따른 검사비율이 증가함에 따라 항만혼잡이나 통관지연이 발생하고 그로인해 공항이나 항만으로부터 내륙으로의 연계운송이 원활히 작동하지 않는 경우 기업의 생산계획이나 배송계획에 차질을 발생하게 되고, 이는 결국 재고수준 및 처리비용의 증가로 이어져 기업의 운전자금 및 현금흐름에도 영향을 미치게 된다.[14] 뿐만 아니라 검사과정에서 컨테이너 화물의 손상이 발생하는 경우 그 비용은 고스란히 운송인과 수입업자가 떠안게 된다. 게다가, 보안상의 문제를 노출하고 있는 컨테이너에 대해서는 벌금을 비롯하여 일정한 규제조치를 받게 되는 바, 그러한 비용이나 책임에 대한 분쟁이 발생할 소지가 있다. 공급사슬보안과 관련하여 발생하는 이들 비용들은 운임이나 제품가격에 포함되어 결국 서비스 사용자 및 소비자들에게 전가될 가능성이 높다.

Lee and Whang[15]은 공급사슬 혼란으로 인한 결과로 비용의 증가, 인도지연, 제품과 서비스의 원활한 흐름 방해, 리드타임 증가, 수량, 품질, 정시배송에 대한 불확실성 증대 등을 지적했다. 여기에 고객서비스 수준 하락으로 인한 매출하락, 보안 및 기타위험의 증대로 인한 보험료 상승 등은 간접적으로 영향을 미

수 주 동안 생산차질을 빚게 되었고, 포드의 경우 생산량이 13%나 감소하였다. 이와 같은 결과는 테러공격의 직접적인 결과로 발생한 것이 아니다.

12) IMF에서 조사한 자료에 따르면 무역보안강화조치에 따른 비용증가는 연간 1억 6천만 달러로 추산하고 있으며, 재고보유량의 증가에 따른 추가적인 자금부담은 연간 7억 5천만 달러에 이른다고 한다. 또한 위험증가에 따른 보험료 부담은 연간 약 30억불로 20% 정도 증가할 것으로 예상하고 있다.(Neil Shister, "The Business Case to Justify Security Investments", *World Trade*, Vol. 19, No 12, Dec 2006, pp.44~50.)

13) Ravi Sarathy *op. cit.*, p.42.

14) John F. Frittel *op. cit.*, pp.88~94.

15) Hau L. Lee and S. Whang, "Higher Supply Chain Security with lower cost: Lessons from total quality management", *International Journal of Production Management*, Vol. 96, 2005, pp.289~300.

칠 수 있는 부분들이다.

4. 물류보안과 공급사슬의 효율성

공급사슬보안의 근본적인 목적은 보안사고로 인해 공급사슬이 붕괴되는 것을 방지하거나 혹은 그로 인한 혼란을 최소화하기 위한 것이다. 보안사고로 인한 공급사슬 혼란에 대비하여 재고수준을 늘리거나 공급중단사태에 대비하여 생산시설을 확충하고 공급선을 다변화하기 위해서는 비용이 증가하게 된다. 하지만, 이러한 투자는 고객관계의 개선과 제품출시기간의 단축 등 장기적인 관점에서 기업에 이익을 가져다주고, 공급사슬 혼란으로 인한 성과부진을 회피하는데 도움을 줄 수 있다. 다시 말해 공급사슬상의 보안을 강화하기 위해 단기적으로 지출되는 비용이 공급사슬보안체계의 개선과 공급사슬의 안정적인 운영을 통해 얻을 수 있는 장기적인 이익과 균형을 유지할 수 있다면 보안시스템의 개선을 위한 비용투자나 공급사슬비용의 증가가 정당화될 수 있다. 문제는 장기적인 관점에서 더 큰 위험 및 비용을 회피하기 위해서는 단기적인 비용지출이 필요하다는 점을 인식하고 있음에도 그로인한 장기적인 이익을 측정하기 어렵기 때문에 기업들은 공급사슬구조를 견고히 하고 보안을 강화하기 위한 대규모 투자를 꺼리는 경향이 있다는 점이다.[16] 이와 관련하여 Sodhi[17]는 글로벌 공급사슬 내에서 공급사슬보안 향상을 통한 장기적인 이익과 단기적인 비용을 지속적으로 평가할 것을 권고한다. 기업들은 보안문제발생시 공급사슬 혼란으로 야기되는 비용과 공급사슬상 보안위험을 관리하기 위해 추가적으로 발생되는 조달 및 재고비용 그리고 효율적인 공급사슬관리를 통해 절감할 수 있는 생산 및 재고비용 등을 지속적으로 비교·평가하는 한편, 공급사슬상 위험의 진원지(source), 위험발생의 가능성, 그리고 그러한 위험이 기업과 고객 등 공급사슬 전반에 미칠 영향에 대한 철저한 평가를 실시할 필요가 있다. 이러한 정보는 공급사슬상 변동을 야기하는 근본원인을 분석하여 공급사슬 프로세스를 개선하고 기업들이 공급사슬의 재설계에 대한 의사결정을 하는데 도움을 준다.

한편, Stanford 경영대학원과 Manufacturing Institute가 공동으로 수행한 연구보고[18]에 따르면 조사대상 기업들은 공급사슬보안에 대한 투자를 통해 공급

16) James B Rice and Caniato Frederico, “Building a Secure and Resilient Supply Network”, *SCMR*, Sep./Oct. 2003, p.28.

17) M.S. Sodhi, “How to do Strategic Supply Chain Planning”, *Sloan Management Review*, Fall 2003, pp.41～48.

18) Barchi Peleg illai, Gauri Bhat and Lesley Sept, *Innovators in Supply Chain Security*, The

사슬 가시성 개선, 공급사슬효율 향상, 고객서비스 개선, 효율적인 재고관리, 리드타임 단축, 비용절감 등 많은 혜택을 보고 있다고 한다. 따라서 공급사슬보안을 위한 투자는 비용요소라기보다는 공급사슬의 효율성 및 효과성을 위한 필수적인 요소로 인식되어야 한다.

Ⅲ. 공급사슬 보안 및 위험관리전략

9/11 테러사태를 계기로 테러위협이 증가하면서 지금까지 화물도난, 마약과 같은 불법화물의 밀거래, 불법이민을 줄이는데 치중하였던 물류보안에 대한 인식이 변화하고 있다. 정부 및 기업들은 공급사슬 전반에 걸친 보안확보의 필요성을 인식하고 공급사슬의 효율성과 효과성을 지속적으로 유지하기 위한 다양한 방법들을 모색하고 있다.

테러위협으로 인한 불확실성의 증가는 산업의 글로벌화, 제품의 다양화, 제품수명주기의 단축 등 비즈니스 환경의 변화로 인해 기업들이 이미 경험했던 문제들과 크게 다를 바가 없기 때문에 공급사슬의 성과를 높이기 위해 기업들이 이미 추진했던 공급사슬관리전략이나 위험관리시스템을 더욱 확고히 함으로써 보안효과를 높일 수 있다. 기업들은 테러위협을 차단하기 위해 공급사슬 파트너 및 정부당국과 긴밀한 협조체제를 구축하는 한편, 공급사슬의 가시성을 개선하고, 복원성을 높임으로써 테러공격으로 인한 물류시스템의 혼란에 대비하여야 한다.

1. 공급사슬보안의 요소 및 범위

공급사슬 보안은 개별기업의 노력만으로 그 효과를 충분히 발휘하기 어렵다. 물품의 조달에서 생산·판매 및 인도에 이르는 공급사슬상 모든 활동은 상호 연계되어 있기 때문에 개별기업 차원에서 확고한 보안시스템을 구축하였다 하더라도 공급 네트워크를 구성하는 여러 단계 중 어느 한 곳이라도 보안상의 허점이 발생하는 경우에는 공급사슬 전체가 보안위험에 노출되게 된다. 따라서 물류보안은 개별기업 차원이 아닌 전체 공급사슬 네트워크의 관점에서 다루어져야 한다.[19]

Manufacturing Institute and Stanford University, July 2006.

보안위험은 여러 요인들의 상호작용에 의해 야기된다. 가령, 컨테이너는 밀수, 불법이민, 대량살상무기의 밀반입 등에 이용될 가능성이 높다. 컨테이너 선박은 그 자체로서 테러공격의 타깃이 될 수 있고, 테러공격을 위한 무기나 수단으로 이용될 수 있으며, 선박의 등록 및 소유관계에 있어서 투명성의 결여는 테러분자들이 선박을 범죄적인 목적에 악용할 수 있는 소지를 제공한다는 점에서 보안위험을 초래할 가능성이 있다.[20] 컨테이너운송은 전체 공급사슬 활동 중 일부 영역에 지나지 않는다. 도로 및 철도, 항공운송을 비롯하여 항만이나 공항설비 등 물리적 시설 등도 보안위협으로부터 자유로울 수 없다. 생산, 운송, 보관, 하역에 관여하는 공급사슬 당사자들 역시 테러행위에 직접 혹은 간접적으로 개입할 수 있다는 점에서 공급사슬보안의 주요 대상이 된다. 따라서 기업들은 공급사슬 파트너 및 정부기관과 함께 물품의 입고에서 운송과정을 거쳐 소비자의 손에 인도되기까지 공급사슬상의 모든 지점에서 보안사항을 감시하고 안전을 확보하기 위해 상호 협력해야 한다.[21]

Hamilton[22]은 계획에서부터 실행 및 통제에 이르기까지 모든 단계에서 핵심적인 역할을 수행하는 것은 인간이기 때문에 기술적인 요소에만 의존하여서는 결코 효과적인 보안을 달성할 수 없다고 한다. Wiederin[23]은 일련의 과정, 정책, 절차 및 인적요소, 그리고 최신 보안기술이 상호 작용하여 완전한 보안을 제공한다고 한다. 이렇듯 효과적인 보안관리를 위해서는 내부와 외부의 다양한 영역과 위험요소들을 고려하는 전체적이고 포괄적이며 통합적인 접근방식을 요한다.[24]

한편, 공급사슬상 어느 한 지점에서 보안상의 문제가 발생하면 그 효과는 공급사슬 전체로 확산될 수 있다. 따라서 공급사슬상 어느 단계에서 발생한 보안상의 결함을 그 다음 단계에서 방어할 수 있도록 보안시스템을 계층적으로 유

19) James B. Rice, Jr & Federico Caniato, “Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains”, MIT Center for Transportation and Logistics, August 8, 2003, p.27.

20) 2003년 기준으로 약 5400대의 상선이 약 6만개의 항구에 기항하고 국제적으로 거래되는 화물의 90% 가량이 해상컨테이너를 이용한다. 그 중 약 2% 정도만이 목적지에 도착한 후 물리적인 검사를 받는다고 한다.(M. Van de Voort, *et al., Improving The Security of the Global Sea-Container Shipping System,* RAND Europe Report, MR-1695-JRC, 2003)

21) Ravi Sarathy *op. cit.*, p.31.

22) CR. Hamilton, The case for holistic security: The integration of information and physical security as an element of homeland security, 2004(www.riskwatch.com/Press/Holistic_Security_10-03.pdf)

23) S. Wiederin, D. Wurster, RS Hoefelmeyer and T. Phillips, The true meaning of security, 2002 (www.rrtidd.com/webQuest/shared/true%20Meaning%20of%20Security.pdf)

24) Vinh V Thai & Devinder Grewal, The Maritime Security Management System: Perceptions of the international Shipping Community, Maritime Economics & Logistics, 2007. 9., p.129.

지할 필요가 있다. 여러 보안기능들이 복합적으로 연결되어 상호 지원해주는 다중 보안시스템은 개별 보안요소가 그 기능을 완벽하게 수행하지 못하더라도 다른 요소들을 통해 그 결함을 보완할 수 있기 때문에 어느 단일 계층에서 보안상의 허점이 발생하더라도 그로 인하여 보안시스템 전체가 붕괴되지는 않으며, 테러행위를 지연시키거나 그 효과를 경감시키는 효과가 있다.[25]

1.1 생산장소

생산장소에서 발생하는 보안문제는 제품의 부당한 변경(tampering) 혹은 대체(substitution)가능성 등으로 이는 고객의 불만을 야기하고 신제품의 출시나 제품의 가용성을 지연시키거나 방해하는 한편, 기업의 책임 및 평판에도 영향을 미칠 수 있다. 생산하도급자와 같은 조달파트너와 관련하여 채용과정에서의 면밀한 심사를 하고 제조설비에 대한 접근통제절차를 확립하며, 보안사항의 위반을 막기 위한 제조공정의 심사뿐만 아니라 파트너와의 신뢰관계를 구축하는 조치들은 보안사고로 인한 공급사슬의 혼란을 경감하는데 도움이 된다.

1.2 제품

제품과 관련된 보안의 문제는 제품의 컨테이너 적재과정 감시, 컨테이너 적입 후 봉인 등의 과정을 통한 컨테이너의 무결성 확보, 운송 중 컨테이너에 적입된 내용물의 변경시도 감시, 도착 후 컨테이너의 무결성 검증 등이다. 컨테이너 봉인과 컨테이너에 부착된 센서와 같은 신기술은 운송 중 컨테이너화물의 변경을 제어하는데 도움이 된다.

1.3 공급사슬 파트너 및 중개업자

C-TPAT와 같은 보안프로그램은 공급사슬 당사자들이 보안관행을 공유하도록 함으로써 공급사슬 보안의 표준을 설정하고, 보안규정의 준수를 점검하며, 이를 통해 신속절차와 같은 인센티브를 제공한다.

1.4 운송노드 및 운송인

화물보안을 위해서는 센서, 엑스선, 감마선, 방사능 감시, 자기장을 이용한 침입탐지 등의 보안기술들을 활용한 컨테이너 화물의 적격심사와 의심대상 컨테

25) Making the Nation Safer - The Role of Science and Technology in Countering Terrorism Committee on Science and Technology for Countering Terrorism of the National Research Council, The National Academies Press, 2002, p.214.

이너화물을 선별하여 현물검사를 실시할 필요가 있다. 컨테이너 적격심사의 목적은 핵물질이나 화학무기와 같은 위험화물을 검사하기 위한 것이다.[26] 항만보안은 관찰뿐만 아니라 이미지를 수집하고 분석하며 위협을 탐지할 수 있는 고정 혹은 이동식 카메라로 이루어진 지능형 영상(intelligent vision)을 통한 감독과 함께 접근통제를 통해 이루어진다.

1.5 인력

공급사슬의 매 단계마다 인력이 개입되기 때문에 공급사슬에 참여하는 모든 개별 당사자들의 신원을 보장하기 위한 보안조치들이 필요하다. 이는 선적전 송하인의 점검에서부터 적재 및 출하 단계에 개입하는 당사자들, 그리고 컨테이너 화물에 접근하는 당사자들의 감시에 이르기까지 포괄적인 보안조치가 필요하다. 다만, 개별 당사자들의 프라이버시와 정치적인 고려가 균형을 이루어야 한다.

1.6 정보보안

공급사슬의 안정성 및 성과는 정확한 공급사슬정보의 확보 및 처리에 의존한다. 정보보안의 목적은 공급사슬정보에 대한 접근을 통제함으로써 정보의 위조 및 변조를 방지하고 공급사슬 정보의 기밀성을 높이는데 있다. 최근 정보보안을 위해 활용되고 있는 RFID 태그와 관련한 문제는 RFID 태그에 저장된 정보를 삭제하고 변경하는 해킹시도를 어떻게 방지할 것인가 하는 것이다. RFID 태그의 무결성이 확보되지 못하는 경우 태그에 저장된 정보의 신뢰성이 떨어져 RFID 태그를 활용한 정보보안의 효력이 상실되게 된다.[27]

2. 보안위험의 예방

공급사슬 보안시스템을 구축함에 있어서 최대의 쟁점은 공급사슬의 효율성을 그대로 유지하면서 보안사고를 효과적으로 예방할 수 있는 방법을 모색하는 것이다. 이에 대하여 전사적 품질관리(TQM: Total Quality Management)의 원리를 적용하면 보안사고를 예방하고 그 효과를 경감하는 동시에 공급사슬의 효율을 높일 수 있다고 한다.[28]

---

26) Ravi Sarathy *op. cit.*, p.34.
27) *Ibid.*, p.35.
28) Hau L. Lee and Michael Wolfe, "Supply Chain Security without Tears", *SCMR*, Jan/Feb, 2003, p.14.

전사적 품질관리는 제품품질개선의 중심이 검사에서 예방으로 발전한 것으로 많은 기업들은 교육, 조직 전체의 협업, 설계개선, 공정변동 축소 등의 과정을 통해 검사비용과 제품의 하자를 획기적으로 줄이고 생산효율을 그대로 유지하면서 품질을 개선하는 것이 가능하다는 것을 경험하고 있다. 이러한 원리는 공급사슬관리에 적용되어 공급사슬상 보안위험을 줄이는 동시에 공급사슬의 효율을 높일 수 있는 대안을 제시할 수 있다.

9/11 테러사건 이후 일부 국가에서 항만과 국경에서 화물, 컨테이너 및 운송수단의 검사를 강화하자는 목소리가 높아지고 있으며, 심지어 수입화물에 대한 전수검사를 실시하자는 의견도 제기되고 있다. 하지만, 이러한 문제해결방식은 검사비용을 증가시키고, 물류정체를 심화시켜 물류시스템의 효율을 떨어뜨리고 공급사슬을 불안정하게 만든다. 이는 결국 재고비용을 증가시키고 화주 및 고객에 대한 서비스 수준을 떨어뜨리는 등 공급사슬 전반에 걸쳐 부정적인 영향을 미칠 수 있다. 전사적 품질관리의 관점에서 공급사슬보안은 보안사고 발생으로 인한 혼란을 수습하기 위한 대책을 강구하는 차원에서 논의되기 보다는 공급사슬상 보안위협을 사전에 탐지하고 이에 신속하게 대응함으로써 보안사건을 미연에 예방하고 그 파장을 최소화할 수 있는 시스템을 구축하는데 초점이 맞추어져야 한다. 가령, 검사비율을 늘리기 보다는 공급지에서 이루어지는 예방프로그램과 사전선별작업을 개선함으로써 위험도가 높고 의심이 가는 소수의 선적화물에 검사작업을 집중시키면 검사작업의 효과를 높일 수 있다. 정부에서 주도하는 일부 보안조치들은 이러한 방향으로 진행되고 있다. 그 대표적인 예가 C-TPAT와 CSI 프로그램이다.

최근 미국은 수입화물검사의 효과성을 높이고 그 영향을 줄이기 위해 타국정부와 협력을 강화하고 있다. 이러한 일환으로 시행되고 있는 것이 CSI 프로그램이다. 이 프로그램은 선별 및 검사작업을 화물이 발생하는 선적항에서 수행하는 것으로 하자발생의 근본원인을 찾아내어 품질을 개선하고자 하는 전사적 품질관리기법과 그 맥을 같이한다. CSI 프로그램은 선별 및 검사작업의 일부를 선적항으로 이동함으로써 테러사고의 위험을 감소시키고 안정적인 화물의 흐름과 예측가능성을 보장해준다.

또한 최근 미국세관에서 채용한 자동표적시스템(ATS: Automated Targeting System)은 사전선적정보와 송하인 및 유사선적화물에 대한 과거 이력정보를 바탕으로 수많은 수입화물들을 선별하는데 사용되고 있다. ATS 기술은 선적화물의 급증이나 새로운 공급원으로의 단순한 이동, 운송경로의 변화 등 변동사항을 탐색한다. 대부분의 사전심사 및 검사대상 후보자들은 이러한 결과를 토대로 선

정된다. 이와 함께 ATS를 통한 사전심사를 개선하기 위한 조치로 24hour rule을 시행중인 바, 이에 따라 선적화물의 상세한 정보가 선적되기 24시간 전에 미국세관에 전자적으로 제공되지 않는 경우 당해 컨테이너의 유입이 금지되고 과징금이 부과된다. 이 규칙은 ATS를 통한 선별검사의 창구를 제공할 뿐 아니라 수상한 컨테이너에 대해서 선적 전 검사를 실시할 수 있도록 기회를 제공한다.

C-TPAT 프로그램은 공급사슬상 모든 당사자들이 전체 공급사슬의 무결성을 보장하기 위한 정책, 계획 및 절차들을 실행하도록 함으로써 운송과정에서 화물의 변조위험을 낮추고, 광범위한 모니터링을 통해 불법거래를 방지하도록 하는 등 보안사고의 예방활동에 중점을 두고 있다. 이는 자율규제(voluntary) 프로그램으로 항만 및 국경이동과정에서 신속한 통관절차를 보장해 주는 등 참여기업들에게는 다양한 인센티브가 주어진다.

한편, 2002년 10월 착수된 SST(Smart and Secure Tradelane)는 미국항구에 입항하는 컨테이너를 대상으로 최신의 자동화된 추적, 탐지, 보안기술을 적용하고자 하는 산업계의 조치로 운송중인 컨테이너의 잠재적 변조를 식별하여 격리시키는 것을 목적으로 한다. 이러한 효과적인 절차통제는 최종검사과정의 지연을 방지하고 화물의 신속한 흐름을 보장할 것이다.

3. 보안사고에 대한 효과적인 대응전략

지금까지의 논의는 주로 공급사슬 보안사고의 예방에 초점이 맞추어졌다. 하지만, 일단 사고가 발생한 경우에 대비하여 그 피해를 경감하기 위한 전략도 필요하다. 건전한 공급사슬관행은 보안상의 문제에 대한 대응할 수 있는 올바른 방법을 제공해준다. 이하에서는 보안사고의 효과를 경감하기 위해 기업이 취할 수 있는 전략들을 제시한다.

3.1 광범위한 추적 및 모니터링(Comprehensive Tracking and monitoring)

보안사고는 공급사슬상의 구조적인 결함으로 발생하는 경우가 많으며 어느 시점에 갑작스레 발생할 수도 있고 점진적으로 발생할 수도 있다. 어느 경우든 사고는 의외의 경우이거나 예상치 못한 경우가 대부분이다. 복잡하게 얽혀있는 글로벌 공급사슬 시스템의 구조상 위기의 징후를 탐지하기가 쉽지 않고, 설사 탐지가 가능한 경우라 하더라도 그 상황을 제대로 파악하기가 어렵다. 기업들은 대부분 위험의 징후를 인지하지 못한 채 사고를 방치함으로써 위기에 적절히

대응할 수 있는 시기를 놓치게 되고 위기에 직면하게 됨으로써 손실은 더욱 증가하게 된다.[29] 따라서 보안사고에 효과적인 대응하기 위해서는 보안사고 발생시 이를 즉시 탐지할 수 있는 능력이 요구된다. 통제할 수 없는 문제들은 신속하게 탐지되어야 하며, 문제의 정확한 소재 및 본질을 파악하여야 한다.

기업들은 공급사슬보안을 위해 선적화물, 재사용이 가능한 포장용구 및 운송수단에 대한 효율적이고 효과적인 모니터링 시스템을 도입하여야 한다. 또한 추적시스템은 여러 모순되는 사항들 중 우선순위를 정하여 이를 바로잡기 위한 적절한 조치를 취할 수 있도록 지원할 수 있어야 한다. 현재 화물의 발생지에서 최종 목적지까지 지속적으로 모든 선적화물을 모니터링 할 수 있는 시스템은 없지만 공급사슬 이벤트관리나 공급사슬 성과관리와 같은 기술들이 도입되면서 잠재적 사고를 감지할 수 있는 실시간 가시성 및 모니터링 역량을 제공하고 문제발생시 관련 당사자와 의사결정자에게 그 사실을 알림으로써 적절한 조치를 취할 수 있도록 지원한다.[30] 가시성 및 모니터링 시스템은 의사결정자에게 보안사고로 영향을 받는 특정 영역에 대한 구체적이고 정확한 정보와 함께 당해 문제의 규모를 제공할 수 있어야 한다.

3.2 공급사슬 가시성의 개선

공급사슬상에서 이루어지는 모든 활동에 대한 정확한 정보를 적시에 파악하고 이를 토대로 특정 사건이 공급사슬 전반에 미칠 영향을 예측할 수 있다면 기업은 조달·생산·물류 및 결제에 관한 보다 합리적이고 효과적인 의사결정을 통해 공급사슬 운영의 효율성을 높이는 한편, 사고발생의 징후를 미리 인지하고 문제점을 조기에 시정함으로써 보안사고로 인한 파장이 공급사슬 전반으로 확대되는 것을 방지함으로써 피해를 최소화할 수 있다. 반면, 가시성을 확보하지 못하면 기업의 전략적 목표에 적합한 공급사슬 계획의 수립 및 변화하는 공급사슬 상황에 대한 체계적인 대응이 어렵기 때문에 공급사슬 전반에 대한 가시성을 개선하는 일은 기업경영에 있어서 매우 중요한 요인이다.

가시성은 원자재의 조달에서 최종소비자에게 완제품의 인도에 이르기까지 공급사슬 프로세스 전반에 걸친 물자의 이동, 거래 및 사건의 발생을 감지하고 통제할 수 있는 능력을 의미한다.[31] 가시성은 공급사슬 내에서 실시간으로 발생하

29) Paul Barnes and Richard Oloruntoba *op. cit.*, pp.526~527.
30) Hau L. Lee and Michael Wolfe, *op. cit.*, p.17.
31) William Atkinson, "Gaining Supply Chain Visibility", *SCMR*, Vol. 5. Issue 6, Special Supplement, November, 2001, p.4.

는 정보에 대한 모니터링을 통해 공급사슬 프로세스 전반에 대한 완전한 시야를 확보하고 공급사슬 프로세스상의 문제를 미리 감지하여 공급사슬상의 변동에 선제적으로 대응함으로써 공급사슬 전반에 미치는 효과를 최소화 하는데 그 목적을 두고 있다.[32]

공급사슬 전반에 대한 가시성은 공급사슬상 물자의 이동경로 및 위치, 재고수준, 도착예정시간 등 적시의 정확한 정보를 바탕으로 재고수준의 감소, 리드타임의 변동발생률 감소, 생산성 향상, 품절발생률 감소, 도난방지, 수입자와 고객, 그리고 공급자와의 관계를 개선하는데 도움을 준다.[33] 기업이 공급자, 생산자, 운송서비스 제공자와 함께 공급사슬상 재고의 소재 및 형태(원자재, 부품, 재공품, 운송재고 및 완제품)에 대해 명확히 파악하고 있다면 공급사슬상 일정 영역에서 보안사고가 발생한 경우 즉각적인 운송루트의 변경, 생산계획의 수정, 생산자원의 재배치 및 생산능력의 조정 등 적절한 대응을 통해 공급부족으로 인한 공장가동 중단이나 고객의 불만을 최소화할 수 있도록 지원한다. 송하인은 선적화물에 다한 가시성을 확보함으로써 운송화물의 이동상태를 파악하여 선적지연, 배송착오, 손상 등의 문제가 발생할 경우 적절한 조치를 취할 수 있다. 뿐만 아니라 예측의 정확성을 높이고 공급사슬이 순조롭게 운영되도록 함으로써 재고비용 및 급송비용을 절감하는 한편 예외적인 상황의 발생가능성을 줄임으로써 관리비용을 절감할 수 있다.

정보의 가시성을 확보하기 위해서는 적어도 두 가지 요건이 필요하다. 하나는 사건중심(event driven)의 공급사슬 운영에 관한 정보이고 다른 하나는 공급자, 제조업자, 물류서비스 제공자, 고객으로부터 적시의 정확한 정보를 확보하기 위한 정보시스템의 통합이다.[34]

3.3 공급사슬의 유연성 및 복원성 확보

견고하고 복원력 있는(robust and resilient) 공급사슬 구조는 보안사고 발생시 공급사슬상의 혼란을 피하고 그 영향을 최소화하는데 도움을 준다. 견고한 공급사슬은 보안사고에 대한 취약성을 낮추고 복원성은 우발적인 사건이나 재난으로 불안정해진 시스템이 그 이전의 정상적인 상태로 복귀할 수 있는 능력으로[35] 공급사슬상 혼란이 발생하더라도 정상적인 상태로 신속하게 복귀할 수

32) Yossi Sheffi, “Supply Chain Management under the Threat of International Terrorism”, *IJLM*, Vol. 12, No. 2, 2001, pp.4~6.
33) Yossi Sheffi and James B. Rice, “A Supply Chain View of the Resilient Enterprise”, *Sloan Management Review*, Fall 2005, p.47.
34) Hau L. Lee and Michael Wolfe, *op. cit.*, p.14.

있도록 해준다.

복원성을 확보하기 위해서는 만약의 사태에 대비하여 기업의 생산능력 비축, 재고수준의 증가, 공급선 다변화 등 공급사슬상 낭비적인 요소를 어느 정도 용인하여야 하는 바, 이로 인해 공급사슬의 효율성이 떨어질 수 있다. 하지만, 보안위험에 대한 공급사슬의 취약성을 낮추고 공급사슬 구조를 유연하게 함으로써 수시로 변하는 시장상황에 보다 신속하고 효과적으로 대응할 수 게 된다.[36] 견고한 공급사슬은 공급사슬이 정상적으로 운영되는 상황에서는 비용절감, 고객만족 및 고객관계를 향상시키는 한편, 공급사슬 혼란이 발생하는 동안에도 공급사슬의 정상적인 운영을 지속할 수 있는 구조를 말한다. Tang[37]은 공급사슬구조를 견고히 하고 복원성을 높이기 위해 공급자 다변화, 전략적인 재고유지, 운송방식의 다양화, 그리고 모듈화 및 지연전략을 통한 제품의 다양성 확보 등의 전략이 필요하다고 하고 있다.

3.3.1 유연한 소싱 전략

1980년대 이후 많은 기업들은 장기적인 관점에서 공급자와의 관계를 보다 확고히 하고 복잡한 공급자관계를 관리하는데 소요되는 비용을 절감하기 위해 공급자의 수를 축소함으로써 공급네트워크를 단순화하고 있다. 이러한 전략은 조달 및 생산비용을 절감할 수 있는 장점이 있지만 테러위협의 증가와 보안사고로 인한 공급사슬의 중단 등을 고려할 때 이러한 전략의 수정이 불가피하다. 따라서 기업들은 공급자 다변화, 역내공급자의 활용을 통해 보안사고로 인한 공급사슬 혼란 및 시장의 수요변화에 유연하고 신속하게 대응하도록 하는 한편 기존의 전략을 유지하면서 공급네트워크를 이원적으로 활용함으로써 공급사슬의 효율을 지속적으로 유지할 수 있다. 가령, Dell은 컴퓨터 프로세서와 메인보드의 경우 Intel, 그리고 운영시스템의 경우 Microsoft와 강력한 단일공급자관계를 구축하고 디스크 드라이브와 같은 기타 부품에 대해서는 다양한 공급업자를 활용하고 있으며, HP는 조달비용을 절감하기 위해 수요가 안정적인 대부분의 프린터를 싱가포르에서 생산하는 동시에 북미시장에 신속하게 대응하기 위해 캐나다 밴쿠버에 추가적인 생산설비를 갖추고 있다.[38]

---

35) Cranfield School of Management, *Creating Resilient Supply Chains: A Practical Guide*, report on behalf of the Department for Transport, 2003.
36) Ravi Sarathy *op. cit.*, pp.45~47.
37) Christopher S. Tang, "Robust strategies for mitigating supply chain disruptions", *International Journal of Logistics*, 9(1), March, 2006, pp.33~45.
38) Yossi Sheffi, *op. cit.*, pp.2~3.

3.3.2 제품 및 프로세스의 재설계

제조공정 및 제품 디자인에 있어서 규격화된 모듈을 사용하는 기업은 원자재 공급부족이나 조달상의 어려움에 유연하게 적응할 수 있으며, 시장에서 제품의 가용성에 심각한 영향을 초래함이 없이 우발적인 상황에 신속하게 대응할 수 있다. 또한 일부 제조업체들은 생산품목 및 선택사항의 수를 줄임으로써 수요예측의 어려움을 극복하고 있다. 선택사항의 축소는 위험의 분담을 보다 수월하게 하고 가변성을 낮추어 예측을 개선하고 전반적인 비용을 줄일 수 있다. Intel Systems Group은 2000여 종의 레지스터, 축전지, 다이오드 등을 35종으로 축소하여 비용을 절감하는 한편 조달절차를 간소화함으로써 수요변화 및 공급난에 유연하게 대처할 수 있는 능력을 가지게 되었다.[39] 생산프로세스의 표준화 역시 기업들의 생산능력을 점차 공동화시켜 특정지역에서 공급중단이 발생하는 경우 다른 지역의 공급자를 활용할 수 있다.

제품의 최종형태를 마지막 순간까지 보류하는 지연전략(postponement strategy)은 보안사건이 발생하여 특정 부품의 공급부족이 발생한 경우 최종형태를 변경하여 수요를 충족시킬 수 있다. 주문생산(build-to-order) 시스템은 공급잉여지역의 부품 및 반제품을 급격한 수요증가나 공급부족이 발생하는 지역으로 전용함으로써 수요와 공급의 불균형을 해소할 수 있다. 일례로 HP는 공통된 디자인과 부품을 사용하는 프린터를 세계 도처의 물류센터로 배송하되, 변압기와 전원공급장치, 사용자 매뉴얼 등은 각 지역별로 주문을 받아 고객의 요구조건에 맞게 변형하는 지연전략을 활용하였다. 이러한 방법을 통해 HP는 보편적인 프린터에 대한 총수요를 예측하고 지역별 특성 및 소비자의 요구가 다른 부품에 대해서는 개별적인 예측을 통해 재고비용을 줄이고 리드타임을 단축할 수 있었다.[40] 이렇듯 제품 및 프로세스의 재설계로 다양한 생산능력의 공유가 가능해지면서 생산의 유연성이 확보되고 수요의 급증이나 공급중단에 신속하고 유연하게 대응할 수 있다.

3.3.3 효율적이고 효과적인 재고관리

기업들은 JIT 및 Lean[41] 생산체제를 통해 지속적으로 재고를 감축하기 위해

39) Yossi Sheffi, “Resilience Reduces Risk”, *Logistics Quarterly*, Vol.12, Issue 1, March 2006, p. 13.

40) Yossi Sheffi, *op. cit.*, pp.4~6.

41) Lean은 모든 공정상의 낭비(waste)를 제거하고 공급사슬 프로세스를 최적화하여 속도와 흐름을 증진하기 위한 활동으로 도요타 생산시스템(Toyota Production System)에 그 뿌리를 두고 있다(Thomas Goldsby and Robert Martichenko, *Lean Six Sigma Logistics*, J. Ross, 2005, p.4).

노력해 왔다. 하지만, 9/11 테러사태 이후 기업들은 이러한 시스템 하에서 보안사고나 예상치 못한 사건이 발생시 공급프로세스가 쉽게 혼란을 겪을 수 있다는 점에서 문제를 제기하기 시작하였다. 일부 기업들은 JIT 생산방식이 지니는 많은 이점에도 불구하고 보안사고로 인해 운송시스템에 혼란이 야기될 경우에 대비하기 위하여 부품을 대량으로 주문하고 안전재고를 늘리고 있다.

일정한 서비스 수준을 유지하기 위해 안전재고를 일정수준으로 유지하는 것은 공급사슬상 리드타임의 변동에 대비하기 위한 것이다. 따라서 평균 리드타임을 줄이는 것 보다는 리드타임의 변동을 줄이는 것이 안전재고를 감축하는데 도움이 된다. 공급사슬의 불안정에 대비하기 위해 JIT 전략을 재검토할 필요가 있지만, 그렇다고 재고보유량을 늘리게 되면 그에 따른 비용도 만만치 않다. 따라서 기업들은 적정수준의 재고를 유지하기 위해 품절위험과 재고관리비용 간의 상충관계를 평가하기 위한 과학적인 재고관리기법을 도입하여야 한다. 이를 위해 보안사건과 관련한 공급중단의 위험을 파악할 필요가 있다. 하지만, 대부분의 전통적 재고관리시스템은 수요의 불확실성만을 다루고 있다. 따라서 기업들은 수요와 공급의 불확실성을 모두 커버할 수 있는 재고관리시스템을 개발할 필요가 있다. 이를 위해 재고를 이원적으로 관리할 필요가 있다.[42] 즉, 기업경영상 발생하는 예측상의 오류와 시장 환경의 변화에 대응하기 위해 일정 수준의 안전재고를 비축하는 한편, 테러위협 등 보안사고로 인한 공급사슬의 혼란에 대비하기 위해 전략적으로 비상재고(emergency stock)를 지정하여 이는 일상적으로 발생하는 수요변동에 사용하지 않고 공급사슬 혼란이 발생하는 최악의 경우에만 사용도록 하는 것이다. 전략적으로 유지되는 비상재고는 일상적인 수요예측에 관계없이 재고가 소진되는 즉시 보충되도록 관리하여야 한다. 이는 미국이 오일파동에 대비하여 전략적으로 오일을 비축하는 것과 유사하다.

기업들은 예측실패로 인한 위험을 분산하기 위해 재고를 집중시켜 관리하되, 보안상 일정 지역에 테러공격이 자행되는 경우 그로 인한 손해를 완화하기 위해 기업의 자산 및 인력을 분산시킬 필요가 있다. 또한 분산 배치된 재고를 중앙에서 통합하여 관리함으로써 재고관리비용을 절감하는 한편, 재고의 편중과 과부족을 해소할 수 있다.[43]

3.4 공급사슬 파트너 간 신뢰구축 및 협업

공급사슬에는 기업을 비롯하여 공급파트너, 정부기관, 그리고 유통업자 및 중

42) Yossi Sheffi, *op. cit.*, pp.3~4.
43) Hau L. Lee and Michael Wolfe, *op. cit.*, p.14.

개업자 등 많은 당사자들이 참여하게 된다. 복잡한 공급사슬 구조상 보안위험은 대부분 가장 취약한 연결지점에서 발생하기 때문에 공급사슬에 참여하는 모든 당사자들에게 보안에 대한 경계 및 주의가 요구된다. 기업들은 보안에 대한 부담을 덜기 위해 국제물류보안제도 및 기업의 보안요구사항을 준수하는 공급파트너를 선호하게 되고 안정적으로 물자를 조달할 수 있는 지역에 공급네트워크를 집중시킬 수 있다. 즉, 공급사슬 보안을 위한 공급네트워크의 구성에 있어서는 비용보다 공급사슬 당사자 간의 신뢰가 중요한 요소가 된다. 이와 함께 기업들이 보안을 강화하고 보안관련 솔루션, 투자, 기술, 정보, 실행 및 혜택을 공유하기 위해서는 공급사슬 전반에 걸친 협력이 필요하다. 기업들은 공급사슬보안의 관리 및 통제를 위한 프로세스와 규칙을 개발하고 당사자들에게 보안을 위한 일정한 역할과 책임을 할당하는 한편, 물류보안규정의 준수를 보장하도록 하는 등 공급사슬 파트너와 협력할 필요가 있다.[44]

이와 더불어 국경을 초월하여 이루어지는 글로벌 공급사슬활동의 특성상 기업은 지역 및 연방정부와 협력하여 효율적이고 효과적인 보안시스템의 달성을 위해 노력하여야 한다.[45] 정부는 주로 국경 및 보안설비 강화에 주력하고, 민간기업들은 화물보안, 공급사슬 파트너와의 협력, 그리고 인력에 대한 보안교육 및 훈련에 주력하는 것이 바람직하다. 공급사슬상의 보안을 개선하기 위한 민관협력프로그램은 공급사슬상의 취약부분을 발견하고 공급사슬 프로세스를 합리화하는데 도움이 되며, 공급사슬 당사자 간 의사소통을 촉진시키고 정부 및 참여기업이 핵심정보를 공유할 수 있도록 한다.[46] C-TPAT와 더불어 SST 및 OSC와 같은 공급사슬 보안을 위한 민관협력프로그램은 보다 시의적절하고, 정확하고 완전한 정보접근을 통해 기존의 비즈니스 프로세스를 단순화하고 보다 합리적인 의사결정을 도와줌으로써 상당한 재정적 효과를 볼 수 있다고 한다.[47]

3.5 공급사슬 보안 개선을 위한 조직구조 개편

공급사슬보안의 개선을 위해 기업은 보안시스템의 개발 및 실행과 관련하여 집중화와 분권화를 균형 있게 추진하여야 한다. 정보공유를 통한 조직 구성원들 간의 원활한 의사소통과 의사결정권한의 이양은 핵심 당사자들이 공급사슬 프로세스상의 문제를 사전에 감지하고 적절한 조치를 취할 수 있도록 함으로써

44) Ravi Sarathy *op. cit.,* p.47.
45) Yossi Sheffi *op. cit.*, pp.6~9.
46) David J. Closs & Edmund F Mc Garrell, Enhancing Security throughout the Supply Chain, IBM Center for The Business of Government, April 2004,, p.37.
47) Smart&Secure Tradelanes, Phase One Report, November 2003.

보안사건에 신속하고 유연하게 대응할 수 있도록 한다. 이를 위해 기업은 보안책임을 담당할 최고보안담당 책임자(Chief Security Officer)를 지정하여 기업의 전략적 목표와 보안활동 간의 불균형을 시정하고 다양한 보안계획들을 조정·검증함으로써 테러공격 이후에도 기업 활동이 지속될 수 있도록 보장하는 한편, 교육 및 훈련을 통해 기업 구성원들의 보안의식을 높이고 보안에 대한 인식이 조직 전체로 확산될 수 있도록 분위기를 조성하여야 한다.

이와 함께 기업들은 보안사고로 시스템이 와해되는 경우에 대비하여 재고 및 공급처, 그리고 업무지식 및 비즈니스 프로세스에 대한 백업시스템을 구축할 필요가 있다.[48] 직원들의 업무지식은 대부분의 기업들에게 매우 중요한 자원이라 할 수 있다. 만약의 사태에 대비하여 잉여인력을 유지하기는 것은 어렵기 때문에 주요 업무프로세스를 문서화하여 언제라도 이용할 수 있도록 하여야 하며, 가능하다면 인력의 교차 훈련을 통해 부서 간 전용이 가능하도록 하여야 한다.[49] 이와 더불어 기업전반의 비즈니스 프로세스와 업무관행을 표준화함으로써 업무의 적응성과 정확성을 높일 수 있으며, 보안사고 발생으로 공급사슬의 운영상 차질이 발생하더라도 인력 및 프로세스를 유연하게 전용할 수 있다.

3.6 공급사슬 보안기술의 활용[50]

최근 컨테이너 보안, RFID 테그의 활용, 컨테이너 적격심사와 같은 보안기술이 점차 안정되어 가고 있다. 새로운 보안기술의 활용은 공급사슬 당사자의 식별 및 공급사슬 결절점에 대한 접근통제, 컨테이너의 안전한 적재 및 전자적하목록(electronic manifests)을 통한 검증, 컨테이너 내용물의 변조를 방지하는 봉인장치, 소프트웨어를 활용한 우범화물의 자동선별, 컨테이너화물의 적재과정을 추적하고 이동을 감시하는 GPS(Global Positioning System) 및 RFID 기술 등 여러 방면에서 공급사슬 보안시스템을 강화하는데 중요한 역할을 한다. RFID를 비롯하여 바코드, 전자봉인장치(electronic seal), GPS, 무선통신네트워크 등의 물류보안기술은 공급사슬 시스템과 연계하여 정보를 수집하고, 수집된 정보를 변환·분석하여 적절한 당사자에게 제공함으로써 선적화물의 무결성을 보장하고 운송 중 변조가능성을 낮추는 한편, 공급사슬의 가시성을 개선할 수 있다. 특히 RFID 기술은 자동침입탐지, 방사능 등 위험물질의 검색, 컨테이너의 위치

48) Yossi Sheffi *op. cit.*, p.4.

49) 세계무역센터에서 7000명의 직원을 거느리고 금융서비스를 제공하는 Solomon Smith Barney는 한순간에 이들을 모두 잃었다. 하지만 이 기업은 뉴저지에 있는 백업사이트와 일련의 백업프로세스를 가동하여 12시간 만에 다시 업무를 재개할 수 있었다.

50) Ravi Sarathy *op. cit.*, pp.47~48.

및 상태에 대한 실시간 무선송신을 통해 공급사슬 보안을 강화하는데 도움을 준다.[51] 미국 국토보안국(DHS: Department of Homeland Security)에 따르면 능동형 RFID(active RFID)를 장착한 컨테이너는 도착지에서 검사가 생략되고 즉시통관 대상이 된다고 한다. 이와 같은 조치는 운송시간의 단축과 재고수준의 감소효과가 있을 뿐 아니라 컨테이너의 보안상태나 내용물에 대한 검증이 용이해 통관절차가 신속히 이루어짐에 따라 위급상황에서도 공급사슬의 효율성을 지속할 수 있다는 점에서 많은 혜택을 제공한다.[52] 하지만 이러한 보안기술은 보안을 향상시키기 위한 유일한 방법도, 오류가 없는 절대 안전한 방법도 아니다. 보안기술은 전반적인 공급사슬의 재설계와 전체 공급사슬 및 업계, 정부 및 국제기구와의 협업을 통해 보완되어져야 한다.

Ⅳ. 요약 및 결론

9/11 테러사태를 계기로 공급사슬보안에 대한 중요성이 높아지면서 공급사슬 보안의 필요성에 대한 인식이 증대되고 있지만 공급사슬상 보안을 강화하기 위해서는 많은 비용과 노력이 소요된다는 점에서 기업들에게 부담을 안겨주고 있다. 특히, 공급사슬보안의 목적을 달성하기 위해서는 글로벌 소싱이나 JIT 생산 등 공급사슬의 효율성을 개선하기 위해 기업들이 추진해온 전략과 상충되는 부분이 많이 발생하기 때문에 기업들의 의사결정을 더욱 어렵게 하고 있다. 하지만, 공급사슬보안은 장기적인 관점에서 공급사슬의 안정성을 높여주고 불확실성을 낮춤으로써 비용을 절감하고 고객서비스를 개선하는 한편, 예상치 못한 변동상황에 대한 신속하고 유연한 대응을 통해 공급사슬의 복원성을 높임으로써 피해를 최소화할 수 있는 효과적인 방법들을 제공해 줄 수 있음을 여러 사례들을 통해 확인하였다. 따라서 공급사슬보안에 대한 투자는 공급사슬상 비용을 증가시키는 요인이기 보다는 공급사슬 프로세스를 더욱 효율적이고 효과적으로 개선함으로써 기업의 경쟁력을 높이기 위한 필수적인 요소임을 인식하여야 한다.

공급사슬보안시스템을 구축함에 있어서 관건은 보안상의 목적과 효율성이라는 상충되는 이해관계를 조정함으로써 단기적으로 발생하는 비용과 장기적인 이익이 균형을 유지하도록 하는데 있다. 이를 위해서는 먼저, 공급사슬상 위험요인들을 식별하고 공급사슬을 구성하는 다양한 구성요소의 취약성을 평가하는

51) John F. Frittel *op. cit.,* pp.88~94.
52) Ravi Sarathy *op. cit.,* p.42.

작업이 선행되어야 한다. 이를 토대로 공급사슬의 효율성을 저해하지 않는 범위에서 보안사고를 효과적으로 예방할 수 있는 방법들을 모색하여야 한다. 이와 관련하여 전사적 품질관리의 개념은 공급사슬 보안의 문제에 효과적으로 적용될 수 있는 모델을 제공한다. 이와 함께 공급사슬의 가시성을 개선하고 복원성을 높이기 위해 기업의 조직구조 및 공급사슬네트워크를 개편하는 한편 공급사슬 당사자간 협업프로세스를 통해 보안사건 및 강화된 물류보안제도에 신속하고 유연하게 대응할 수 있도록 하는 노력이 필요하다.

참고문헌

1. Atkinson William(2001), “Gaining Supply Chain Visibility”, *SCMR*, Vol. 5. Issue 6, Special Supplement, November.
2. Banomyung Routh(2005), “The impact of port and trade security initiatives on maritime supply chain management”, *Marit. Pol. Mgmt.*, Vol.32. No. 1, pp.3～13.
3. Barnes Paul and Oloruntoba Richard(2005), “Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management”, *Journal of International Management*, pp.519～540.
4. Closs David J. & Garrell Edmund F Mc(2004), *Enhancing Security throughout the Supply Chain*, IBM Center for The Business of Government.
5. Cranfield School of Management(2002), *Supply .Chain Vulnerability*, report on behalf of DTLR, DTI and Home Office.
6. _____(2003), *Creating Resilient Supply Chains: A Practical Guide*, report on behalf of the Department for Transport.
7. Frittel John F(Nov. 2006). “Port and Maritime Security: Background and Issues, Military Technology”, pp.88～94.
8. Gillai Barchi Peleg, Bhat Gauri and Sept Lesley(July 2006), “Innovators in Supply Chain Security”, *The Manufacturing Institute and Stanford University.*
9. Goldsby Thomas and Martichenko Robert(2005), *Lean Six Sigma Logistics*, J. Ross
10. Hamilton CR. (2004), *The case for holistic security: The integration of information and physical security as an element of homeland security*, (www.riskwatch.com/Press/Holistic_ Security_10-03.pdf)
11. Hendrick, Kevin B. and Singhal R. Vinod (Spring 2005), “An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm”, *Production and Operations Management*, 14 (1), pp.695～711.

12. Lee Hau L. and Whang S. (2005), "Higher Supply Chain Security with lower cost: Lessons from total quality management", International Journal of Production Management, Vol.96, pp.289～300.
13. _____ and Wolfe Michael(2003), "Supply Chain Security without Tears", *SCMR.*
14. Rice James B and Frederico Caniato(2003), "Building a Secure and Resilient Supply Network", *SCMR*, 2003, pp.22～30.
15. _____(August 2003), "Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains", *MIT Center for Transportation and Logistics.*
16. Sheffi Yossi (2001), "Supply Chain Management under the Threat of International Terrorism", *IJLM*, Vol.12, No.2, pp.1～11.
17. _____(Maech 2006), "Resilience Reduces Risk", *Logistics Quarterly*, Vol.12, Issue 1, pp.12～14.
18. _____ and Rice James B. (Fall 2005), "A Supply Chain View of the Resilient Enterprise", *Sloan Management Review*, pp.41～48.
19. Sarathy Ravi(2006), "Security and the Global Supply Chain", *Transportation Journal*, Fall 45, 4, pp.28～51.
20. Shister Neil(Dec 2006), "The Business Case to Justify Security Investments", *World Trade*, Vol.19, No.12, pp.44～50.
21. Sodhi M.S.(Fall 2003), "How to do Strategic Supply Chain Planning", *Sloan Management Review*, pp.41～48.
22. Tang Christopher S. (March 2006), "Robust strategies for mitigating supply chain disruptions", *International Journal of Logistics*, 9 (1), pp.33～45.
23. Thai Vinh V & Grewal Devinder(2007), "The Maritime Security Management System: Perceptions of the international Shipping Community", *Maritime Economics & Logistics*, pp.119～137.
24. Van de Voort, M. *et al.*(2003), *Improving The Security of the Global Sea-Container Shipping System,* RAND Europe Report, MR-1695-JRC.
25. Wiederin S., Wurster D., Hoefelmeyer RS and Phillips T.(2002), *The true meaning of security*(www.rrtidd.com/webQuest/shared/true%20Meaning%20of%20Security.pdf)
26. Waters Donald(2007), *Supply Chain Risk Management*, KOGAN PAGE.

Abstract

A Study on the Supply Chain Security and Risk Management Strategies of Global Companies

Yang, Jung-ho*

Since the 9/11 terror attack, the event which caused supply chain disruption, supply chain security has becomes more important than ever before. Furthermore, such company's logistics strategies conflicting supply chain security as increased global sourcing, JIT manufacturing are increasing supply chain vulnerability.

It could burden for global companies to strengthen supply chain security because not only it requires additional investment cost but also changes of companiy's global logistics strategy. However, on the other hand, supply chain visibility and resilience can be improved through supply chain security. In addition, it allows companies to stabilize supply chain structure as well as rapid and flexible response to market demand.

The key issue is balancing between efficiency and supply chain security. To do this, identifying risk elements under the supply chain and assessing vulnerability of each supply chain components should be performed before developing efficient supply chain security management system without obstructing supply chain efficiency.

Key Words : Security Risk, Supply Chain Management, Supply Chain Risk Management

* Full-time lecturer, Department of International Trade, Sang-Ji University