·供应链·

"911"后美国公司对于供应链安全管理的新思考

New Thoughts about Supply Chain Security after 9-11

李 婷，刘胜春 (云南财经大学，云南 昆明 650221)

LI Ting, LIU Sheng-chun *(Yunnan University of Finance and Economics, Kunming 650221, China)*

摘 要：简单介绍"911"后供应链的安全管理面临的问题，对安全策略在供应链中的重要性进行了分析；其次分六个步骤对如何对供应链进行安全管理提出了一些方法，对供应链企业进行安全具有一定的指导作用；将实施供应链安全管理措施对供应链中各成员的影响概括为三类。这样的分类能够让企业在具体执行供应链安全措施的实践中，对企业及企业外部操作环境所产生的直接或非直接影响，有一个较为全面的认识。

关键词：供应链；供应链管理；安全

中图分类号：F273.7 文献标识码：A

文章编号：1002-3100 (2008) 03-0119-03

Abstract: Before Sept.11, 2001, the question "what is supply-chain security" would surely have brought out the more traditional areas of risk management——natural and man-made disasters; equipment and infrastructure failures; regulatory requirements; loss prevention; geopolitical events and personnel strikes. Today, especially after the attacks of Sept. 11, supply chain security has taken on a whole new level of meaning and immediacy. It's now a primary consideration that needs to be addressed as comprehensively as any other part of running the business. Accordingly, it needs to undergo the same rigorous economic analysis as any other key activity. This paper discusses the problem of supply chain security from five aspects: it starts from brief introduction; and then, discusses the importance of security strategy within the supply chain; next, six steps of conducting security management are analyzed; fourth, the impacts of conducting supply chain security management on different members within supply chain are categorized into three category; finally, all the discussions are brought to an natural conclusion.

Key words: supply chain; supply chain management; security

1 关于安全策略在供应链中的重要性的分析

在2001年美国"911"事件发生之前，当人们问起什么叫做供应链安全的时候，一般提到的往往是诸如人为或自然灾害；设备和基础设施故障；行业标准的变更调整；损失预防；地理政治事件以及工人罢工这类传统的风险管理。但是在今天，特别是在"911"事件发生之后，供应链安全这一问题被赋予了更新也更直观的意义，企业在商业运作的过程中，在考虑其它重要问题时，也应该将供应链安全问题放在首要位置策划；同样道理，如同企业其它的关键经济活动一样，供应链安全也需要进行严格的经济分析。

事实上，大部分的公司曾经遭遇过供应链的中断破坏。美国麻省理工学院将供应链被破坏的情况分为了6种情形。类型如表1所示：

供应链在本质上很容易受到破坏的攻击，当中的任何一个部分发生故障都有可能导致整个网络的瘫痪。供应链的受攻击性表现了供应网络中各个单位相互依存的特性。供应链安全中的各个要素分属于不同的机构或是联合体，跨国的供应链安全管理则需要成员之间更多的合作，然而仅靠每个机构内部独立的安全防范意识是远远不足的，Deloitte的调查研究结果表明，各个行业中仅仅只有百分之四的成员认为他们在本行业安全检查这个问题上做

收稿日期：2007-08-08

作者简介：李 婷(1979-)，女(白族)，云南昆明人，云南财经大学商学院物流管理系教师，澳大利亚悉尼大学物流管理硕士，研究方向：物流网络及供应链管理；刘胜春(1971-)，男，云南昆明人，云南财经大学商学院，讲师，日本大阪产业大学物流与供应链管理方向工商管理硕士，研究方向：供应链管理与电子商务。

表1 供应链被破坏的类型[①]

破坏的类型	具体描述
供应的破坏	供货商发出的物料发生了延迟甚至不可得，导致公司由于物料投入短缺而生产瘫痪
交通的破坏	交通基础设施的延迟甚至不可得，导致进货及出货物流都无法移动货物
设施的破坏	车间设施、仓库及办公设备的延迟甚至不可得，妨碍了操作继续进行的能力
飞机的破坏	集装箱及货物完整性的破坏，导致货物遗失或被掺杂（可能是由于盗窃或是出于其它犯罪目的，例如在集装箱内夹带军火走私）
信息交流的破坏	发生在公司内部或外部的信息或通讯基础设施的延迟甚至不可得，导致无法对操作进行协调和实施转运
需求的破坏	下游的延迟或破坏会导致需求暂时甚至永久的流失，因此影响到整个公司的上游

了很完备的工作。因此，安全问题在整个供应链的运作过程中已经成为了一个很重要的问题。

在"911"事件之后，为了更好地解决供应链安全问题，美国海关发展了一个叫做C-TPAT的项目以促进公司和海关之间的合作。目标是让企业（生产企业、运输企业）成为值得联邦政府信赖的实体，从而能够更快地通过国境线，并将价值最终传递到他们的客户手上。

与此同时，企业也主动地采取了一系列行动来保护他们的供应链不受损坏，根据2004年的C-TPAT情况，企业对于C-TPAT的回应主要分为8种：

(1) 货物的安全管理：货物的安全管理包括监管和控制设施内部及外部的安全措施，例如信函的安全，门锁及钥匙的管理，内部及外部的报警系统管理。

(2) 人员访问的控制：禁止未经许可的人员靠近设施、运输工具、容器、飞机、船舶、卸货港以及集装箱区域。假如无法对人员访问进行控制，在其它方面需要采取额外谨慎的安全措施。

(3) 内部职员的安全管理：职员的安全管理是指在法律认可的范围内，对职员以及可能被雇佣的职员进行背景安全方面的检查。

(4) 员工安全意识培训教育：员工安全意识培训教育包括就安全政策的问题对员工进行教育培训，鼓励员工对违背安全政策的行为保持警觉，并且知道应该如何应对这些情况。

(5) 程序安全管理：程序安全管理确保了供应链中货物的位置有记录并且能够被证实。程序必须能够为货物在整条供应链中的安全提供保障。同时，程序安全管理中应该包含意外事故处理程序。

(6) 文件处理过程的安全管理：无论是电子文件或是手工文件处理过程的安全管理要确保信息的明确，同时也防止数据丢失以及错误信息的干扰。

(7) 贸易伙伴安全管理：贸易伙伴安全管理将供应链安全管理扩展到了上游供应商和下游客户领域。沟通、评估、培训以及改进是实施贸易伙伴安全管理的关键措施。

(8) 运输安全管理：防止未经授权的人员或货物进入供应链，包含了供应链中不同节点之间区域。

当一个公司计算实施安全管理、预防损失技术和管理控制的经费时会发现，这种投资的利远远大于弊，这些利益主要体现在：理顺了整个流通渠道，一些企业甚至因此减少了他们使用的供应商。这直接地降低了成本，并且对于采购货物的种类管理也有附加的好处。因为企业对于供应链安全给予了更多的关注，往常货物被盗情况也减少了。最后，效率的改善使得企业对于货物在供应链中的流动情况能够进行更好的追踪和监控，从而能够使之更快的到达客户手中。

2 如何对供应链进行安全管理

对于供应链的安全管理，企业应该更着重于预防而并非检查，并且应该有一个事前的流程控制。以下的几个步骤对于一个企业制定、斟酌并精良其供应链安全管理的计划有所帮助。

2.1 最大程度的提升整条供应链的可见度。

掌握供应网络的其余部分的信息能够使一个公司降低安全损坏的影响。当供应链中一个部分的损坏有扩大的趋势时，一个对于在供应网络中其它库存的位置和形式、其供应商的能量、生产商、运输服务商以及配送网络有着清晰理解的公司往往能够更有效的应对。这些信息能够使其迅速地重新运送物资，修改生产计划，重新布置生产资源并且调整生产量。

2.2 建立综合的追踪及监控系统。

一个有效的应对战略应该着眼于在安全损坏刚发生的时候就能够马上察觉。

任何失控的问题都必须被及时的发现，失控问题的确切位置及其性质也必须马上被隔离开来。在供应链安全这个问题上，企业需要在被运输的物资上，在可循环使用的包装材料以及运输工具上安装成本效率较高的监控系统。

2.3 预防于根源。企业需要去采取那些"防止在装货前、装货中和装货后都在调整集装箱"的程序。这就要求对处理货物和靠近设施的人员进行详细彻底的检查。公司也同样应该谨慎地监控货物的流动以及整个的处理过程。

2.4 检查以及过程控制。采用不同的技术来选择应该受到检验的货物，首先采用自动目标系统来检查船只的历史数据，然后仅仅检查这些有异像的货物。

2.5 聘用及监控过程控制。有效的监控过程应该从对雇佣过程的监控延伸到包括对每个可以对货物靠近的雇员以及第三方服务提供商的持续的追踪。这就要求对任何那些对货物有充足知识，可以靠近货物并且意图摧毁安全系统的人进行小心的记录保存，在关键的时候警告公司有可能受到来源于这些人的威胁。与此同时，公司必须在雇佣环节对雇员进行尽可能警惕的背景调查。

2.6 建立一支强健的供应链安全管理队伍。在公司内部及外部服务供应商那里挑选出代表来参加供应链安全合作委员会。代表应该包括采购部门、信息技术部门、交通部门、法律部门、仓库管理部门及货物配送部门、损失预防部门以及保安公司、供货商、客户代理人、转运人及运输公司。所有这些部门都会受到某种程度的影响，同时他们本部门都有自己的安全标准，这些部门之间应该形成强大的交流及合作。

3 实施供应链安全管理措施对供应链中各成员的影响

安全管理战略对其成员来说制造了直接和非直接的影响。直接影响来自于恐怖袭击和恢复措施，包括人员伤亡、损坏、拥挤堵塞以及对商业活动和日常生活的破坏。因为安全应对措施的地理跨度、功能范围以及可能较长的持续时间，它产生了具有重要意义的间接影响，除了诸如提高成本、耽搁以及不可预见性这些负面影响，它也带来了诸如更高的安全性、改善了供应链的效率和效力这样的积极影响。对于其成员来说影响主要有：

3.1 增加了供应链中各企业的成本。对供应链安全管理的投资会增加成员的成本。总之，检验、筛选、预防措施、员工的教育以及对安全管理软件及技术的投资会非常昂贵。

3.2 在供应链中建立相互信赖的伙伴关系。严格的安全意识使得供应链关系更加复杂。企业可以真实的受益于选择能够在兼顾效力与效率的前提下保证供应链安全的供货商。他们可以通过在以下的几个关键活动中与能够达到严格要求的供货商建立值得信赖的安排，以获得较大的利益。这些活动分别是：选择在运输安全上比较谨慎的运输商，通过安全的码头运输，达到包装安全的要求并且提供关键雇员的背景信息。因此，供应链当中的各种关系将会变的比从前更加真实可信与紧凑简洁，从而达到整条供应链的安全管理。

3.3 改变供应链中公司的操作行为。以上的这些改变可能来源于政府行为，也可能来源于公司的战略决定。这些改变包括调整操作，例如之前提到的提前24小时提交载货单的规定，或者是新的集装箱检查制度，这些改变或许会在新制度的推广前先改变公司的正常操作行为。这些新的调整的行为要求供应链中的各个公司在安全管理方面加强与联邦政府及其它商会的协调与合作。

4 结 论

总而言之，供应链安全管理应该是公司总体风险管理项目中的一个重要部分，其目标应该是识别出供应链当中所有可能存在的破坏性行为，并且制定相应的应对措施及意外事故紧急计划。公司应该逐渐地理解在安全管理及预防损失方面投资的重要性，并且理解其短期及长期利益。

注：①源自：MIT research group on "Supply Chain Response to Global Terrorism", Sheffi, Rice, Fleck and Caniato (2003)。

参考文献：

[1] Peck, J. Supply-chain Security Slow to Go[M]. Traffic Word, Newark, 2002:10.

[2] Atkinson, William. Supply Chain Security a Concern in Post-9/11 World[J]. Apparel Magazine, 15432009, 2004,45(11):15.

[3] William, G. The Real Definition of Supply Chain Security[J]. The Journal of Commerce, 2003(11):13.

[4] Rice, J. B., Caniato, F. Building a secure and resilient supply network[J]. Supply Chain Management Review, New York, 2003,7(5):22.