Key Procurement Topic

CIPS KNOWLEDGE

Supply Chain Security Management

... It's essential to have a disciplined process in place to identify, prioritise, and manage the wide range of risks that can impact your supply chain, Dittman

CPD HOURS 1

CIPS members can record one CPD hour for reading a CIPS Knowledge download that displays a CIPS CPD icon.

Introduction

A number of developments over the last decade highlighted the importance of supply chain security management. There has been a series of catastrophic events with implications for societies and economies across the globe (Closs and McGarrell, 2004). For example, in 1999 a major earthquake hit Taiwan affecting the country's semiconductor production capacity and telecommunications manufacturing industries for several consecutive months. Hurricanes in the US Gulf coast led to instability in oil supplies and prices due to damage to petroleum refineries and transportation infrastructure. Some recent non-natural disasters with economic implications include power grid failures and computer viruses (Autry and Bobbitt, 2008; Business Continuity Institute, 2011).

Disruptions to key operations can ripple throughout the supply chain and be particularly devastating. This applies particularly to just-in-time or similar supply chain models (Closs and McGarrell, 2004). Supply chain disruptions can result in a "devastating impact on shareholder value". Evidence shows that an average 40% decline in share price can occur due to supply chain disruptions (Dittman et al., 2010).

Recently, the International Standards Organisations (ISO) updated the 28,000 series of standards on supply chain security management. The series includes provisions to (1) establish, implement, maintain and improve a security management system, (2) assure conformity with security management policy, (3) demonstrate such conformity, (4) seek certification/registration of conformity by an accredited third party organisation, or (5) make a self-determination and self-declaration of conformity. According to ISO, the ISO 28,000 "will increase the ability of organisations in the supply chain to effectively implement mechanisms that address security vulnerabilities at strategic and operational levels, as well as to establish preventive actions plans".

Increasing attention has been paid to the notion of supply chain security orientation (SCSO) which represents an enterprise-wide attitude reflecting focus on supply chain security management (Autry and Bobbitt, 2008). To facilitate the culture of security management and to engage and educate workers, SCSO suggests that full top management support of processes is essential (Autry and Sanders, 2009).

Definition

Supply chain security management is the "application of policies, procedures, and technology to protect supply chain assets … from theft, damage, or terrorism and to prevent the unauthorised introduction of contraband, people... into the supply chain" (Closs and McGarrell, 2004).

Successful application

Building of supply chain security cannot be isolated from other business processes and requires cross-functional team collaboration, global focus on the end-to-end supply chain, contingency planning and crisis management, and a shift in thinking about a vertically integrated supply chain to outsourced business models (Closs and McGarrell, 2004). To maximise supply chain security management, both large and small firms should seek to develop a supply chain security orientation (SCSO) (Autry and Bobbitt, 2008).

Steps to successful application

1. Preparation and planning: establish predetermined procedures for replacing critical assets or personnel in preparation for unforeseen damaging or disruptive events. Consider formalised business processes (written policies/procedures), training, and worker empowerment to handle disruptions.
2. Security-related partnership: evaluate existing relationships with suppliers (and customers), focusing on communication between supply chain partners (i.e. security, product visibility, and forecasting), the use of contractual agreements, and the sharing of risks and rewards.
3. Organisational adaption: focus on physical enhancements (e.g. construct facilities and networks with enhanced security) as well as establishing alternative business systems (e.g. alternative distribution channels, shipping modes) and replication of critical assets which would allow a quick return.
4. Security-related communications and technology: implement up-to-date technology such as RFID, global positioning systems, and transportation management systems to detect potential weaknesses in supply chains.

Autry and Bobbitt (2008)

Hints and tips

- Ensure that every process in the supply chain is examined and recorded by all participants who also need to understand their roles in supply chain revival in case of emergency, disaster or disruption (Autry and Bobbitt, 2008).
- It is advisable to acquire appropriate (or re-assess existing) insurance policies during the preparation and planning process (Autry and Bobbitt, 2008).
- Companies should pay more attention to second tier suppliers: approximately 40% of disruptions occur below the direct/first tier supplier level (Business Continuity Institute, 2011).
- Where relevant, a secure supply chain should guarantee shipment integrity by: (1) not allowing any biological or chemical agent to be introduced to the product, (2) not allowing any illegal commodity to be intermingled with the shipment, (3) not allowing the replacement of the product with an illegal commodity or person and (4) not allowing the shipment to be used as a weapon (Autry and Bobbitt, 2008).
- Effective communication between buyers and suppliers is essential in aligning security goals (Autry and Bobbitt, 2008).

Potential advantages

- Employees in SCSO firms are thought to be more concerned with reducing the probability and impact of disruptions between the firm and its supply chain partners (Autry and Sanders, 2009).
- Given that worldwide cargo theft is estimated at over US$50b annually, there is a strong business case for effective SCSM from a traditional asset protection and shipping perspective (Closs and McGarrell, 2004).
- As many as 25 different parties may be involved in the worldwide movement of containers, for example, buyers, sellers, inland freighters, shipping lines, customs officers, financiers, government (Russell and Saldanha, 2003). As such, supply chain security should be a high priority.

Potential disadvantages

- Despite the evidence that companies are increasingly devoting resources and attention to security efforts, there is little academic research on the firm-level impact of destructive/disruptive events on the supply chain (Autry and Bobbitt, 2008).
- It is not always straightforward to demonstrate the return on investment (ROI) provided by supply chain security management investments, for example, the direct benefits from increased employee training (Closs and McGarrell, 2004).
- The cost of upgrading supply chain security management may be a barrier for smaller companies (Closs and McGarrell, 2004).

Performance monitoring

- Quality control measures: help to ensure that correct quantity, quality and value are achieved (Autry and Bobbitt, 2008).
- ROI: supply chain security investments will require senior organisational figures to demonstrate return on investment (Closs and McGarrell, 2004).
- Supply chain security skills gap analysis: help to evaluate areas where staff require additional training (Lysons and Farrington, 2006).

Case studies

Following the aftermath of the Katrina hurricane, Cisco released more than $1b into supply chain recovery but realised that the company could not see where the product was or its financial impact. As a one of its responses, Cisco developed a crisis management dashboard. It is used for 25 product families, accounting for more than half of Cisco's revenue. Using the Business Continuity Planning (BCP) for these products and Google Earth software, the dashboard can display the potential disruptive threat on a global basis leasing to potential savings of up to US$1m (Gartner, 2010).

A survey of 559 organisations across 62 countries and 14 industries found that 85% of companies experienced at least one supply chain disruption in 2011. Adverse weather and unplanned IT and telecommunications outages were the first and second causes respectively, with cyber-attacks ranked third in the financial sector (Business Continuity Institute, 2011).

Pace, a hard disk manufacturer, announced that its profits would be reduced by £5.9m after severe flooding affected its supply chains in Thailand in 2011. As a result, the company's HDD line suppliers have experienced difficulty in forecasting pricing and capability (Supply Management, 2011).

Further reading

CIPS Source Downloads

CIPS Australia: Opening the way to successful risk management in procurement and supply

CIPS: Risk assessment template

Manchester Business School: The role of risk in environment. Related supplier initiatives

CIPS: Supply Chain Management

CIPS: Supply Chain Management and Networks

Web Resources

The EC's new communication on the security of the supply chain.

Occupational accidents in supply chain

Harvard Business Review: Supply chain risk

Pfizer pressures UK government over supply chain security

Survey results on supply chain vulnerability

Print Resources
Supply Chain Risk: A Handbook of Assessment, Management and Performance (International Series in Operations Research & Management Science) ISBN **978-0387799339**

Supply Chain Risk Management: Vulnerability and Resilience in Logistics ISBN 978-0749463939

Managing Risk and Resilience in the Supply Chain ISBN 978-0580607264

The Definitive Handbook of Business Continuity Management ISBN **978-0470670149**

Supply Chain Risk ISBN 978-0754639022

References

Autry, C.W. and Bobbitt, L.M. (2008) Supply Chain Security Orientation: Conceptual Development and a Proposed Framework. International Journal of Logistics Management, Vol. 19(1), pp. 42-64.

Autry, C.W. and Sanders, N. (2009) Supply Chain Security: A Dynamic Capabilities Approach. In G.A. Zsidisin and B. Ritchie, (Eds.) Supply Chain Risk: A Handbook of Assessment, Management, and Performance. Springer: New York.

Battles, W. (2008) Port of Houston Authority Achieves ISO 28000 Certification for Security Efforts. ISO Management Systems, pp.23-26, November-December.

Business Continuity Institute (2011) Business Continuity Institute Survey on Supply Chain Failure. November.

Closs, D.J. and McGarrell, E.F. (2004) Enhancing Security Throughout the Supply Chain. Special Report to the IBM Centre for the Business of Government. Washington, DC.

Dittman, J.P., Slone, R. and Mentzer, J.T. (2010) Supply Chain Risk: It's Time To Measure It. Harvard Business Review. 5 February.

Gartner (2010) Case Study: Cisco Addresses Supply Chain Risk Management. 17 September.

Lee, H. and Whang, S. (2003) Higher Supply Chain Security with Lower Cost: Lessons from Total Quality Management. Research Paper Series. Graduate School of Business, Stanford University.

Littman, J. (2003) Thwarting the Perfect Crime. Electronic Business, Vol. 29(4), pp. 50-54.

Lysons, K. and Farrington, B. (2006) Purchasing and Supply Chain Management. Pearson Education: Essex, UK.

Monczka, R.M., Handfield, R.B., Giunipero, L.C. and Patterson, J.L. (2009) Purchasing and Supply Chain Management. South-Western Cengage Learning: Mason, OH.

Russell, D.M. and Saldanha, J.P. (2003) Five Tenets of Security-aware Logistics and Supply Chain Operation. Transportation Journal, Vol. 42(4), pp. 44-54.

Supply Management (2005) Buyers Learn From Terror Attacks. [online] Available at: www.supplymanagement.com/news/2005/buyers-learn-from-terror-attacks/?locale=en. [Accessed 22 December 2011].

Supply Management (2011) Thailand Floods Cost Hard Disk Manufacture £5.9m. [online] Available at: www.supplymanagement.com/news/2011/thailand-floods-cost-hard-disk-manufacturer-59-million/ [Accessed 22 December 2011].

Video

Global supply chain security
https://www.youtube.com/watch?v=8ubqsWM9D30

CIPS KNOWLEDGE

CIPS Group Easton House, Easton on the Hill, Stamford, Lincolnshire, PE9 3NZ, United Kingdom
T +44 (0)1780 756777 F +44 (0)1780 751610 E info@cips.org

CIPS Africa Ground Floor, Building B, 48 Sovereign Drive, Route 21 Corporate Park, Irene X30, Centurion, Pretoria, South Africa
T +27 (0)12 345 6177 F +27 (0)12 345 3309 E infosa@cips.org.za

CIPS Australasia Level 8, 520 Collins Street, Melbourne, Victoria 3000, Australia
T 1300 765 142/+61 (0)3 9629 6000 F 1300 765 143/+61 (0)3 9620 5488 E info@cipsa.com.au

CIPS Middle East & North Africa Office 1703, The Fairmont Hotel, Sheikh Zayed Road, PO Box 49042, Dubai, United Arab Emirates
T +971 (0)4 327 7348 F +971 (0)4 332 5541 E mena.enquiries@cips.org

www.cips.org