Development of a Supply Chain Management Security Risk Management Method: A Conceptual Model

Matthew Warren and Shona Leitch
Deakin University, Melbourne, Victoria, Australia
mwarren@deakin.edu.au
shona@deakin.edu.au

Abstract: This paper continues the prior research undertaken by Warren and Leitch (2009), in which a series of initial research findings were presented. These findings identified that in Australia, Supply Chain Management (SCM) systems were the weak link of Australian critical infrastructure. This paper focuses upon the security and risk issues associated with SCM systems and puts forward a new SCM Security Risk Management method, continuing the research presented at the European Conference of Information Warfare in 2009.This paper proposes a new Security Risk Analysis model that deals with the complexity of protecting SCM critical infrastructure systems and also introduces a new approach that organisations can apply to protect their SCM systems. The paper describes the importance of SCM systems from a critical infrastructure protection perspective. The paper then discusses the importance of SCM systems in relation to supporting centres of populations and gives examples of the impact of failure. The paper proposes a new SCM security risk analysis method that deals with the security issues related to SCM security and the security issues associated with Information Security. The paper will also discuss a risk framework that can be used to protect against high and low level associated security risks using a new SCM security risk analysis method.

Keywords: critical infrastructure, security risk analysis and supply change management

1. Introduction

Prior research undertaken (Warren and Leitch, 2009), presented a series of initial research findings identifying that within Australia, Supply Chain Management (SCM) systems formed the weakest link of Australian critical infrastructure. One of the issues facing Australia is that the majority of critical infrastructure resides under the control of the business sector and certain aspects (such as SCM systems) are distributed entities. This proves to be a very important factor when you look at areas such as food distribution.

Researchers (Pye et al, 2005) have identified that Supply chain, value chain, demand chain, critical chain, and supply network are key description terms in relation to SCM. These terms are used somewhat interchangeably in the literature to refer to a conceptual chain of cooperating business partners that facilitates the bi-directional flow of information and goods and services to which it adds cumulative value from raw materials to the consumer (Pye et al, 2005).

The common areas that IT is used in conjunction with SCM systems are (Warren and Hutchinson, 2000):

- *Managing information about demand.* Providing on-line information from customer service, sales support, etc. to the required business area or customer.
- *Managing physical flow of goods.* Provide on-line information to aid production planning, procurement, inventory management, etc.
- *Managing financial flows.* The ability of financial organizations to supply suppliers and customers with detailed financial information on-line.
- *Order management.* Being able to assist the order management cycle by offering on-line cost estimation and pricing, on-line order planning and order generation, on-line order billing and account/payment management, etc.

In a Australian context, the Food Chain Assurance Advisory Group (the Food Chain Group) forms part of the of the Australian TISN (Trusted Information Sharing Network), overseeing critical infrastructure protection. The primary aim of the Food Chain Group has been to improve the security of the agriculture and food supply chain in the changed global security environment. The existing food safety and security systems and food regulatory arrangements are primarily aimed at preventing and detecting natural or accidental risks. The new challenge is to ensure these systems are now capable of responding to the new increased potential for acts of deliberate and malicious intervention including cyber based activities (FCIAAG, 2007).

This paper proposes a new Security Risk Analysis model that deals with the complexity of protecting SCM critical infrastructure systems and also put forwards a new approach that organisations can apply to protect their SCM systems.

The importance of SCM systems from a critical infrastructure protection perspective will be discussed and the proposal of a new security risk analysis method that can be used to protect SCM systems will be introduced. The proposal of an initial SCM security risk analysis method that deals with the security issues related to SCM security and critical infrastructure protection will include a risk framework that can be used to protect organisations against high and low level associated security risks. A number of case studies to illustrate the new SCM security risk analysis method will be used to show the method's effectiveness. The paper will also discuss the difficulty in linking high and low level associated security risks.

The conclusion of this paper will end with a discussion about the next stage of the research and some of the key variables that need to be identified for future research.

2. USA response to supply chain security

In response to the security situation following September, 11th, 2001, the USA government has identified this as a potential security risk in relation to supply chain security and the importing of goods into the USA. In response to the situation of September 11th, the US Customs and Border Protection (CBP) developed the Customs-Trade Partnership Against Terrorism (C-TPAT).

The aim of the C-TPAT strategic plan is designed to (CBP, 2004):

- Improve security of a significant percentage of shipments to the United States;
- Provide benefits and incentives to private sector companies that meet or exceed C-TPAT supply chain security criteria and best practices; and
- Concentrate CBP's inspectional resources and capabilities on higher risk shipments.

Organisations can apply to become member of the C-TAPT program, which offers a number of benefits including (CBP, 2004):

- A reduced number of inspections and reduced border wait times;
- A C-TPAT supply chain specialist to serve as the liaison for validations, security issues, procedural updates, communication and training;
- Access to the C-TPAT members through the Status Verification Inter face;
- Self-policing and self-monitoring of security activities;
- Certified C-TPAT importers are eligible for access to the FAST lanes on the Canadian and Mexican borders;
- C-TPAT certified highway carriers, on the Canadian and Mexican borders, benefit from their access to the expedited cargo processing at designated FAST lanes. These carriers are eligible to receive more favorable mitigation relief from monetary penalties;
- C-TPAT certified Mexican manufacturers benefit from their access to the expedited cargo processing at the designated FAST lanes.

The US Customs and Border Protection were integrated into the Department of Homeland Security (DHS). DHS undertook a review of SCM security and developed a number of new strategic principles in relation to Supply Chain Security; these are (DHS, 2007)

SO-1: Provide for end-to-end supply chain security by building trusted relationships and assisting trading partners and the trade community with enhancing their security systems.

SO-2: Provide incentives and benefits for supply chain partners who enhance their supply chain security, while recognizing that some benefits (e.g., increased security resulting in reduced cargo loss and/or reduced costs of doing business) are trade-driven issues.

SO-3: Advance security by promoting the development and implementation of international standards.

SO-4: Increase the availability and use of appropriate data in order to maintain complete awareness of the supply chain activities and target Department resources to the highest risk movements.

SO-5: Utilize and provide WMD (Weapons of Mass Destruction) detection systems at ports of origin and entry, in order to provide for a defense in depth, layered system.

SO-6: Expedite movement of low-risk shipments through the supply chain, while maintaining a level of detection such that even low-risk shipments are screened for high-consequence threats (e.g., WMD detection).

SO-7: Provide clear communications with the trade community and our international trading partners in order to facilitate recovery efforts.

SO-8: Ensure that data gathered during normal operations is also sufficient to allow for the management of resumption activities following a supply chain disruption.

SO-9: Promote technological development of detection systems which increase the probability of detection, decrease "false positive" detections, and expedite processing times in order to promote rapid trade movement.

SO-10: Leverage key nodes in the supply chain to provide for specific scanning, screening, and inspections activities in order to detect and deter illicit use of the supply chain.

SO-11: Develop systems which automate and expedite the use of Department resources.

SO-12: Provide, or support development of, a robust cargo security system that will withstand a supply chain disruption, and rapidly resume pre-incident or near pre-incident status.

SO-13: Provide for a flexible, standardized response mechanism which includes processes to facilitate trade resumption in short and long term recovery operations.

SO-14: Promote development of modal-specific technologies and systems to ensure security of cargo while in transit.

SO-15: Leverage agreements with foreign partners to facilitate investigative activities related to the detection of illicit material in the supply chain.

3. Research update

Prior research by the authors has focused on looking at the development of security risk analysis models and their applicability to SCM systems. This research has been presented at previous European Information Warfare Conferences (Leitch and Warren, 2009). This prior research proposed the use of OII – SRA (Organisational Information Infrastructure – Security Risk Analysis) method to protect SCM systems. The OII-SRA method is concerned about CII protection (Busuttil and Warren, 2002, Busuttil and Warren, 2004, Busuttil and Warren, 2005, Warren and Busuttil 2007). Analysis by the researchers has identified that the OII-SRA is only focused on security at the process level and relies upon a consensus decision making process in relation to security decisions. Theoretically this may seem an appropriate method but in reality would be considered unworkable; therefore the researchers have looked at alternative ways of protecting CII systems.

The authors reflected upon the security requirements of SCM and the associated level of security risks and have developed a conceptual model that represents this view point; this is shown in Figure 1.

One of the key problems in developing a risk analysis method is how to deal with the complexity involved with SCM security as shown in Figure 1. After a thorough assessment it was found that a risk method called ODESSA may be suitable (Warren, 2001). This method was originally developed to deal with the complexity of healthcare security risk but the authors believe that the flexibility of the ODESSA method can deal with security issues associated with SCM. In the following sections the authors put forward a new method ODESSA-SCM and also propose an initial conceptual model that will be the nexus for future development.

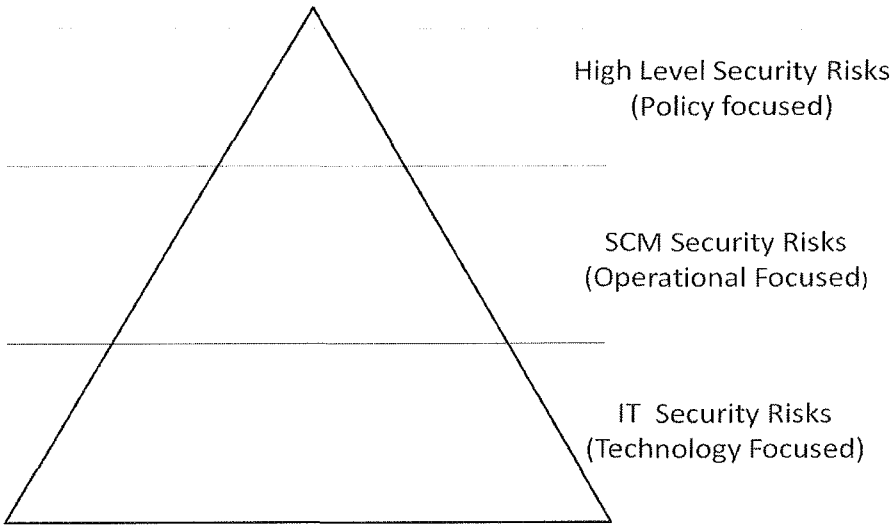

Figure 1: Conceptual model of SCM security risk

4. The rationale of ODESSA-SCM method

The rationale of ODESSA-SCM is that at a basic level, SCM organisations would have similar security requirements but beyond this basic level the security countermeasures are unique to each SCM organisation.

Within ODESSA-SCM, security is examined from the context of the whole SCM, with **the main factors that influence the whole SCM being considered**, which may range from the size of the SCM, organisations involved, to the sensitivity and type of data supporting the SCM.

These elements have been incorporated into a framework as shown in Figure 2. This diagram illustrates the steps involved (at a theoretical level) in determining the security requirements for a SCM.

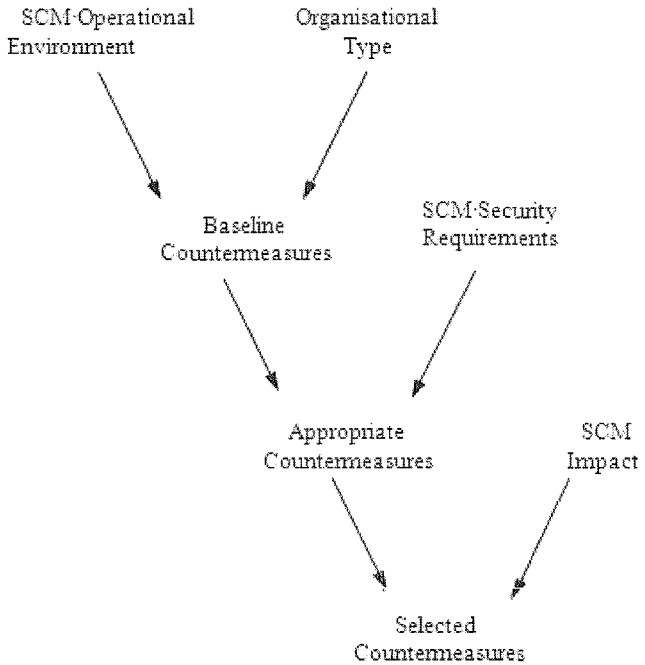

Figure 2: ODESSA-SCM methodology overview

The ODESSA system suggests three sets of security countermeasures.

Baseline Countermeasures

These represent the minimally acceptable security countermeasures for SCM organisations.

Appropriate Countermeasures

These represent the unique SCM security countermeasures. They are based upon a series of questions from which data sensitivity profiles are formed.

Selected Countermeasures

These represent the selected countermeasures from stages one and two that have been selected by the SCM organisation and reviewed.

4.1 Steps of ODESSA-SCM

The steps of ODESSA-SCM are described in the following section of the paper.

Step 1: Organisational Environment Assessment

This considers the **physical** environment in which the SCM assets are located which may affect the level of protection required. Table 1 gives examples of environmental considerations that may have to be considered.

Table 1: Organisational environments

Type	Options	Comments
Location	Inner City	Location may indicate risk of vandalism, and theft
	Outer City	Threats from fires from rural areas, increased chance of theft due to location
	Rural	Location may be at threat from natural disasters, e.g. bushfire
	Transnational	Risk of political or natural occurrence, e.g. war or pandemic

Step 2: Organisational Type

This stage relates to the different organisational types that exist within the SCM sector. The baseline security countermeasures are tailored to these different SCM organisations (e.g. giving advice to staff that may be using laptops in remote locations). The research included a comparison of past healthcare security reviews, which helped to form the baseline security needs for the different types as shown in Table 2.

Table 2: Organisational types

Type	Description
Regional Based SCM	A localised SCM environment, e.g. a manufacturing process being supplied by local suppliers
National SCM	A SCM that spans a national environment, e.g. food distribution;
Trans-Regional SCM	A SCM that services a region, e.g. SCM servicing the European Union market;
Global SCM	A global SCM, e.g. niche scenario a single provider supplying a global market.

Some of the organisational factors would trigger other forms of security protection, e.g. a global SCM would need to be compliant with US C-TAP security standards.

Step 3: Organisational Baseline Security

The concept of baseline within ODESSA relates to the minimal security levels requirements that an organisation should have installed (Warren, 1997). Examples of baseline security methods that could be applied include:

- AS/NZS ISO/IEC 27001:2006 – Security Techniques (AS/NZS, 2006);
- IT Sector Baseline Risk Assessment (DHS, 2009);
- ISO 28000 – Specification for security management systems for the supply chain (ISO, 2007).

Step 4: Organisational Requirements

At this stage the use of the data is considered and evaluated. Many SCM systems use similar sensitive data types which require the same generic security countermeasures, i.e. encryption of personal data.

Because of the nature of SCM systems, it is not possible to determine the usage of the data, but the sensitivity of the data can be considered. The sensitivity impacts of the data are:

- Denial: Denial of access to the information for different time periods;
- Destruction: Destruction of the information;
- Disclosure: Unauthorised disclosure of information;
- Modification: Accidental or deliberate alteration of data;
- Resilience: Ensuring the survivability and continuation of the SCM.

The data impacts are determined as percentages and these are converted to ratings, which are low, medium or high (low is equal to baseline security, and high the maximum protection that is offered). The sensitivity values and data types are determined by answering a series of security related questions, the results are then used to produce a security profile of the organisation under review. Figure 3 shows the steps involved in determining the organisational requirement.

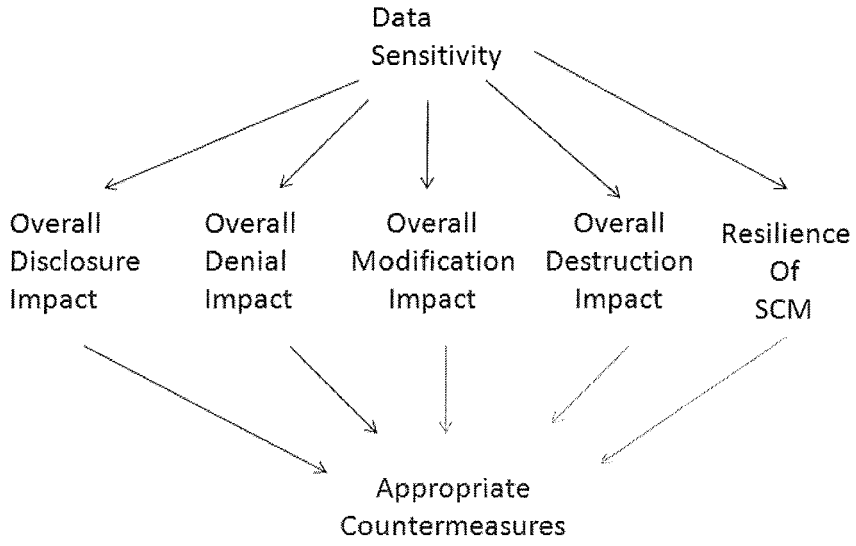

Figure 3: Data sensitivity model

5. Conclusion

In conclusion, this paper has built upon previous research that has highlighted the importance of the security issues of SCM and their importance to the critical infrastructure of a country.

A new security risk analysis method, ODESSA-SCM to protect against security SCM threats has been proposed by this paper. The next stage is to develop the model further with a number of SCM security scenarios from Australia and overseas. This will allow for a greater understanding of the complexity of SCM security and risks and also help to identify some of the unique risk issue that are SCM related.

Further research is still required to develop the ODESSA-SCM methodology and apply the ODESSA-SCM to other types of SCM critical infrastructure systems. The next stage of the research will be to validate the method using a number of real life case studies and help to develop security management strategies and approaches in order to protect Australian critical infrastructure.

References

Australian Bureau of Statics (2009) Report 3218.0 - Regional Population Growth, Australia, 2007-08, URL: http://www.abs.gov.au/ausstats/abs@.nsf/Products/3218.0~2007-08~Main+Features~Victoria?OpenDocument, Accessed 15/2/10.

Australian / New Zealand Standard (2006). AS/NZS ISO/IEC 27001:2006 Information Technology – Security Techniques – Information Security Management Systems – Requirements.

Busuttil, T. B. and Warren, M. J. (2002). A Conceptual Approach to Information Warfare Security Risk Analysis, 2nd European Conference on Information Warfare, London, UK.

Busuttil, T. and Warren, M. (2004) CIIP-RAM- A Security risk Analysis Methodology for Critical Information Infrastructure Protection, in Yves Deswarte, Frederic Cuppens, Sushil Jajodia, Lingyu Wang (eds), Information Security Management, Education and Privacy, Kluwer Academic Publishers, Boston.

Busuttil T.B , and Warren, M (2005) An Australian Risk Analysis Approach for Critical Information Infrastructure Protection, The 4th European Conference on Information Warfare and Security. Glamorgan, UK.

CBP (2004) Securing the Global Supply Chain Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan, US Customs and Border Protection.

DHS (2007) Strategy to Enhance International Supply Chain Security, Department of Homeland Security.

DHS (2009) IT Sector Baseline Risk Assessment, Department of Homeland Security.

FCIAAG (Food Chain Infrastructure Assurance Advisory Group) (2007), [Online], http://www.tisn.gov.au/agd/WWW/tisnhome.nsf/Page/RWP894E5FDE8DBB8BC7CA2571700040E46, Accessed 15th July, 2007.

International Standards Organisation (2007). Specifications for security management systems for the supply chain, IS0 28000:2007.

Pye G, Pierce J, Warren M.J & Mackay, D (2005) Supply Chain Security: the Need for Continuous Assessment, Supply Chain Practice, Vol. 7, Issue No. 1, UK.

Warren M.J (1997) A new hybrid approach for Risk Analysis, IFIP TC 11 WG11.1 - Information Security Management Conference, Copenhagen, Denmark.

Warren, M.J (2001) A Risk Analysis Model to reduce computer security risks among healthcare organisations, Risk Management: An International Journal, Vol 3, No 1, Perpetuity Press, UK.

Warren, M.J and Hutchinson W (2000) Cyber Attacks Against Supply Chain Management Systems, International Journal of Physical Distribution and Logistics Management, Vol 30, No 7-8, MCB Press, UK.

Warren, M. and Leitch, S. (2009) Supply Chain Management Security: The Weak Link of Australian Critical Infrastructure Protection. 8th European Conference on Information Warfare. Lisbon, Portugal.