2007

Commercial Critical Systems and Critical Infrastructure Protection: A Future Research Agenda

Matthew J. Warren
Deakin University,

Shona Leitch
Deakin University,

DOI: 10.4225/75/57a83862befa7
Originally published in the proceedings of the 8th Australian Information Warfare and Security Conference, Edith Cowan University, perth Western Australia, 3rd-4th December, 2007

Commercial Critical Systems and Critical Infrastructure Protection: A Future Research Agenda

Matthew J. Warren and Shona Leitch

School of Information Systems,
Faculty of Business and Law,
Deakin University,
Burwood, Victoria, Australia, 3217.

mwarren@deakin.edu.au and shona@deakin.edu.au

Abstract

Secure management of Australia's commercial critical infrastructure presents ongoing challenges to owners and the government. Although it is currently managed through high-level information sharing via collaboration, but does this suit the commercial sector. 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 of the critical infrastructure such as Supply Chain Management (SCM) systems are distributed entities and not a single entity. The paper focuses upon the security issues associated with SCM systems and critical infrastructure protection.

Keywords

Critical infrastructure protection and Supply Change Management.

INTRODUCTION

The aim of the paper is to evaluate how Australia is protecting its NII (National Information Infrastructure) and CII (Critical Information Infrastructure) in terms of developing strategies and implementing national policies from a corporate viewpoint, NII (National Information Infrastructure) and its relationship with Supply Chain Management Systems (SCM). The NII runs the day-to-day life of Australians, operates gas and electricity supplies, banking and finance sectors, airports and transports, defence forces, telecommunications and government departments.

A key factor is the concept of CII and how that relates to Australia/. CII is the subset of the NII that has a national importance. Many of these aspects are related to corporate organisations and as such government cannot have complete control and must instead try to influence corporations to correctly manage these aspects of the NII and CII.

Within Australia, an annual national Computer Crime and Security Survey is undertaken to assess the sort of computer crime occurring within Australia. An earlier AusCERT survey (AusCERT, 2004) identified that organisational ignorance of criticality status could potentially undermine the reliability and security of Australia's CII, as these organisations are utilising the NII without realising their risk liability. The latest AusCERT survey (AusCERT, 2006) showed that of the sample, only 34% of the organisations had indicated that they were part of the CII, which is a lower percentage that one would expect. Therefore organisational ignorance of criticality status could potentially undermine the reliability and security of Australia's CII, as these organisations are utilising the NII without realising their risk liability.

AUSTRALIA'S CRITICAL INFRASTRUCTURE

Historically, much of Australia's infrastructure was originally owned and operated by the public sector at the federal, state and local government levels (Smith, 2004). However the majority of Australia's critical infrastructure has now been privatised and is under private sector ownership. Consequently, protecting Australia's critical infrastructure now requires a high level of cooperation between all levels of government and the private sector owners. Hence, the federal government has developed a policy for critical infrastructure protection that focuses broadly on addressing the following strategies (Australian Government, 2004):

Distinguishing critical infrastructures and ascertaining the areas risk;

Aligning the strategies for reducing potential risk to critical infrastructure;

Encouraging and developing effective partnerships with state and territory governments and the private sector;

Advancing both domestic and international best practice for critical infrastructure protection.

The Trusted Information Sharing Network (TISN) is a forum in which the owners and operators of critical infrastructure work together by sharing information on security issues which affect critical infrastructure (TISN, 2007). TISN requires the active participation of CIP owners and operators of CIP infrastructure, regulators, professional bodies and industry associations, in cooperation with all levels of government, and the public. To ensure this cooperation and coordination, all of these participants should commit to the following set of common fundamental principles of CIP (TISN, 2007). These principles are (TISN, 2007):

1. CIP is centred on the need to minimise risks to public health, safety and confidence, ensure economic security, maintain Australia's international competitiveness and ensure the continuity of government and its services.

2. The objectives of CIP are to identify critical infrastructure, analyse vulnerability and interdependence, and protect from, and prepare for, all hazards.

3. As not all critical infrastructure can be protected from all threats, appropriate risk management techniques should be used to determine relative severity and duration, the level of protective security, set priorities for the allocation of resources and the application of the best mitigation strategies for business continuity.

4. The responsibility for managing risk within physical facilities, supply chains, information technologies and communication networks primarily rests with the owners and operators.

5. CIP needs to be undertaken from an 'all hazards approach' with full consideration of interdependencies between businesses, sectors, jurisdictions and government agencies.

6. CIP requires a consistent, cooperative partnership between the owners and operators of critical infrastructure and governments.

7. The sharing of information relating to threats and vulnerabilities will assist governments, and owners and operators of critical infrastructure to better manage risk.

8. Care should be taken when referring to national security threats to critical infrastructure, including terrorism, so as to avoid undue concern in the Australian domestic community, as well as potential tourists and investors overseas.

9. Stronger research and analysis capabilities can ensure that risk mitigation strategies are tailored to Australia's unique critical infrastructure circumstances.

The Food Chain Assurance Advisory Group (the Food Chain Group) forms part of the TISN. 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 (FCIAAG, 2007).

SUPPLY CHAIN MANAGEMENT

Supply Chain Management (SCM) involve the flows of material, information and finance in a network consisting of suppliers, manufacturers, distributors and customers (Lee, 2000) and is one area that can be effectively adapted to eBusiness, especially if the Internet is used for the exchange of business information (Lucian et al, 2002).

SCM is defined by the Global Supply Chain Forum (Lambert and Cooper, 2000) as the integration of key business processes from end user through original suppliers that provides products, services and information that add value for stakeholders. Cooper et al (1997) argue that the supply chain management evolves through several stages of increasing intra- and inter-organizational integration and coordination. In a very broad sense and

implementation, it spans the entire chain from initial source (supplier's supplier, etc) to ultimate consumer (customer's customer, etc.).

As SCM technologies have developed in complexity, so to have the risks that are posed to the businesses that employ them (Vasiu et al, 2002). Smith et al (2002) intimate some of main risks that businesses are exposed to when doing business on the Internet:

- Current software engineering techniques do not produce systems that are immune to attack;
- Organisations do not have the expertise to defend their systems against attack;
- Cyberspace legislation lags behind current attack trends;
- Little evidence to suggest improved security since organisations are continually playing 'catch-up' with routinely discovered vulnerabilities;
- Current security tools only address piecemeal technical aspects of security whereas information security is a holistic issue; and,
- System administration is difficult to manage due to continuous system patching.

The attraction of utilising the convenience of the Internet for communication interconnectivity between SCM partners can expose these businesses to security risks and vulnerabilities that if breached, will compromise the security of the entire SCM, thus placing other businesses involved with the SCM are at risk.

SUPPLY CHANGE MANAGEMENT AND PRIOR SECURITY RESEARCH

In terms of SCM security there has been prior research undertaken by the research team in relation to SCM and electronic fraud. This research is important because the security risks associated with CIP SCM cannot be considered in isolation. If a key SCM system is compromised by traditional fraud then the impact could have a national impact and could also be an indicated of more serious security issues associated with that SCM

It is extremely difficult to put hard figures on the incidence of SCM electronic fraud. The explanations are lack of awareness that fraud has occurred and under-reporting. The last one is due to fear of loss of goodwill (Vasiu et al, 2002), pessimism regarding the apprehension of attackers, dissatisfaction with the outcomes of previous criminal proceedings and a common preference to take administrative action and attempt to recover losses without criminal charges .

Benbow (1992) identifies five types of fraudsters:

- the opportunist: having the ability and knowledge to manipulate accounts;
- the habitual claimant: using many different names to commit fraud time and time again;
- the patient claimant: perpetrating the same fraud time and time again;
- the providers: volumes of fraudulent transactions by providers can easily be committed; and
- the organized gang: large organized gangs running complex frauds.

According to Di Nicola and Scartezzini (2000), the more complex the context in which fraudsters operate, the more professional experience they require and the broader organizational structures they need in order to commit their crimes. Large-scale crimes need organization to better achieve results and to reduce risks. Criminals need detailed information on techniques and practices in order to assess opportunities and risk.

The three electronic fraud methods are:

- *Input* ("*data diddling*" or "*number fudging*"): the fraudster dishonestly enters false data, suppresses, or amends data as entered (a variant on common false accounting). It is the most common computer crime

(Vasiu et al, 2002) and can be committed by anyone having access to normal data-processing functions at the input stage.

- *Program:* this involves either the creation of a program with a view to fraud or the alteration or amendment of a program to such ends. It is very difficult to discover and is frequently not recognized (Vasiu et al, 2002)). It requires computer-specific knowledge and high level access to computer databases and/or software (Vasiu et al, 2002), and for this reason, it is usually associated with insiders.

- *Output:* the fraudster dishonestly suppresses or amends data being output—very often linked with input fraud (e.g. suppressing or changing balance reports to hide misappropriated funds). The goal with this type of scheme is to conceal bogus inputs and also to prevent or postpone detection of such input fraud (Vasiu et al, 2002). This type of fraud is relatively unsophisticated and is concerned with the end product; because computer output is normally accepted as being accurate and genuine its authenticity is taken for granted.

The greatest concern present the frauds that involve manipulation of data records or computer programs to disguise the true nature of transactions, cracking into an organization's computer system to manipulate business information and unauthorized transfers of funds electronically

Based upon the research a conceptual framework (Vasiu et al, 2002) was developed that described the issues of electronic fraud within SCM, this is shown by figure 1.

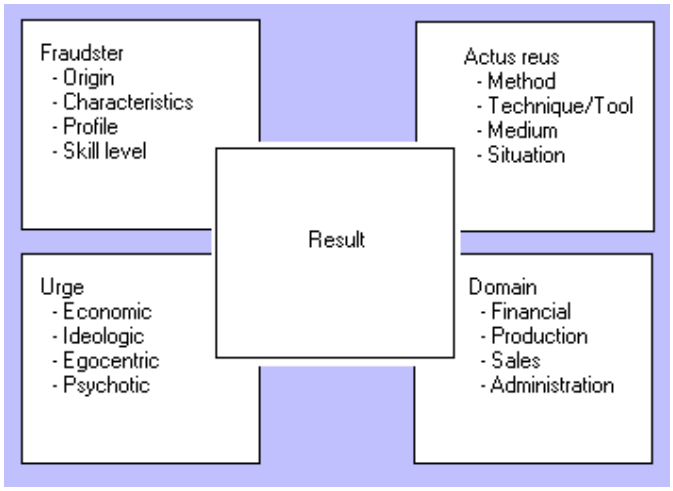

Figure 1: Conceptual framework of electronic Fraud within SCM

SCM CASE STUDIES

The following actual real life examples show the impact that failures within Australian SCM systems have had. The examples focus upon the state of Victoria, Australia.

Car Industry

The automotive industry is one of Australia's key manufacturing sectors and an important source of employment, and research and development. The increasing exposure of the Australian automotive industry to international competition has seen it develop to where it is now competing successfully in global markets. There is also a strong inter-dependence between the car makers and their suppliers, and strong linkages with the rest of the economy (Australian Bureau of Statistics, 2005).

In August, 2007, 200 workers from Melbourne based plastic parts supplier Venture went on strike in regards to $25 million in redundancy entitlements. They supplied the Australian Car Industry will many of the parts used in the car manufacturing process. As a consequence of the strike, 1850 assembly line

and engine workers at Ford's Victorian plants in Broadmeadows and Geelong were stood down without pay and all manufacting at those plants ceased (Herald Sun, 2007a; News.Com.AU, 2007).

The actions of a single car parts supplier caused all car manufacturing within the state of Victoria to cease for several weeks.

Power Supply

On 16th January, 2007, 4pm a power blackout impacted Victoria and left 200,0000 homes and businesses without electricity as well as disrupting Melbourne's public transport system and road network.

A bushfire at Benalla burnt a main power line cable between Victoria and New South Wales. The black out caused about 1,200 traffic signals across the Melbourne and Geelong metropolitan area to fail and the power failure interrupted the metropralition train systems within Victoria. SP AusNet eventually restored power to the Victorian - New South Wales interconnector powerline on the 17th January at 12:30 a.m. (Herald Sun, 2007b; The Age, 2007).

This examples shows how a failure of a critical service such as power can completelty disrupte the operation of a SCM.

RESEARCH FOCUS

The initial description of the research within the paper is the start of a new research project. The research will focus upon:

- identification of commercial critical systems within Australia and also other countries that have defined critical infrastructure systems;
- analysis of open source intelligence to identify security threats and risks that have occurred against commercial critical systems, e.g. potential security risks and threats that complex SCM systems could face;
- review of existing security approaches applied to SCM systems and whether they can be applied to protecting more generic commercial critical systems linked to critical infrastructure;
- review of traditional security risk analysis approaches to identify how traditional approaches could deal with complex security issues.

CONCLUSION

The security of the any SCM is only as strong as its weakest link and therefore it is incumbent upon the individual organisational partners that make up the SCM to be proactive in continuously improving their security measures and policies in order to effectively protect or indeed pre-empt any likely damage resulting from possible threats and vulnerabilities and their subsequent adverse effects on the functionality of the SCM. The issue with critical SCMs is any failure will not just impact the SCM partners but could have the possibility of impacting entire industrial sectors or impacting Australia as a whole.

REFERENCES

Australian Bureau of Statistics (2005) Australia's automotive industry - Year Book Australia - 2005, URL: http://www.abs.gov.au/AUSSTATS/ABS@.NSF/Previousproducts/1301.0Feature%20Article252005?opendocument&tabname=Summary&prodno=1301.0&issue=2005&num=&view= , Accessed 27th August, 2007.

AusCERT (2004), *2004 Australian Computer Crime and Security Survey*, AusCERT, Brisbane, Australia.

AusCERT (2006), *2006 Australian Computer Crime and Security Survey*, AusCERT, Brisbane, Australia.

AGD (Attorney General Department) (2004), *Critical Infrastructure Protection National Strategy*, [Online], Available from: <http://www.nationalsecurity.gov.au/> Accessed 10th November, 2004.

Benbow, G. (1992) 'The Criminal Element', *Computer Control Quarterly*, Vol. 10, Issue 4, pp. 19-21.

Cooper, M.C., Lambert, D.M. and Pagh, J.D. (1997) 'Supply Chain Management: more than a new name for logistics', *International Journal of Logistics Management*, Vol. 8, No. 1, pp. 1-14.

Di Nicola, A. and Scartezzini A. (2000) 'When economic crime becomes organized: the role of information technologies. A case study', *Current Issue in Criminal Justice - Journal of the Institute of Criminology*, University of Sydney, Faculty of Law, Vol. 11, n. 3.

FCIAAG (Food Chain Infrastructure Assurance Advisory Group) (2007), [Online],

http://www.tisn.gov.au/agd/WWW/tisnhome.nsf/Page/RWP894E5FDE8DBB8BC7CA25717000240E46, Accessed 15th July, 2007.

Herald Sun (2007a), Further Ford stand-downs looming, 28th August.

Herald Sun (2007b), Fires cause massive power cut, 16th January.

Lambert, D. M. and Cooper, M. C. (2000) 'Issues in Supply Chain Management', *Industrial Marketing Management*, 29, pp. 65-83.

Lee, H. L. (2000) 'Creating Value through Supply Chain Integration', *Supply Chain Management Review*, September/October 2000.

News.Com.Au (2007), Car industry strike set to go on, Auguest 29th, URL: http://www.news.com.au/story/0,23599,22325097-29277,00.html, Accessed 10th September, 2007.

Smith, S. (2004), *Infrastructure*, [Online], NSW Parliament, Available from:

<http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/0/C6389C30B0383F9ACA256ECF0006F610> , Accessed 10th November, 2006.

Smith, B., Yurcik, W., and Doss, D., (2002) Ethical Hacking: The Security Justification Redux, *Proceedings of the International Symposium on Technology and Society*, 6-8 June 2002, Raleigh, North Carolina, USA.

The Age (2007) Mass power outages hit state, January, 16th.

TISN (Trusted Information Sharing Network)(2007) About Critical Infrastructure [Online] TISN, Available from: http://www.tisn.gov.au/ Accessed, 15th July, 2007.

Vasiu L, Mackay D and Warren M.J (2002) A conceptual framework of E-fraud from an SCM perspective, 3rd International We-B Conference, Perth, Australia.

COPYRIGHT