The systemic nature of critical infrastructure protection using a medium sized company as the case study

Jeffery Sewell

Edith Cowan University

Follow this and additional works at: https://ro.ecu.edu.au/theses_hons

Part of the Information Security Commons

Recommended Citation


This Thesis is posted at Research Online.
https://ro.ecu.edu.au/theses_hons/1119
Edith Cowan University

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study.

The University does not authorize you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following:

- Copyright owners are entitled to take legal action against persons who infringe their copyright.

- A reproduction of material that is protected by copyright may be a copyright infringement. Where the reproduction of such material is done without attribution of authorship, with false attribution of authorship or the authorship is treated in a derogatory manner, this may be a breach of the author’s moral rights contained in Part IX of the Copyright Act 1968 (Cth).

- Courts have the power to impose a wide range of civil and criminal sanctions for infringement of copyright, infringement of moral rights and other offences under the Copyright Act 1968 (Cth). Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.
The Systemic Nature of Critical Infrastructure Protection using a Medium Sized Company as the Case Study

By

Jeffery Sewell

Student Number: 992960

A dissertation to be submitted in partial fulfilment of the requirements for the degree of

Bachelor of Science Honours
(Communications & Information Technology)

Faculty of Computing, Health and Science
School of Computer and Information Science,
Edith Cowan University,
Perth, Western Australia

Supervisor: Professor W. Hutchinson

October 2007
USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.
COPYRIGHT AND ACCESS DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

(i) incorporate without acknowledgement any material previously submitted for a degree or diploma in any institution of higher education;

(ii) contain any material previously published or written by another person except where due reference is made in the text; or

(iii) contain any defamatory material.

Signed...

Date.....

......
Abstract

Critical infrastructure can be defined as privately and publicly run organisations such as energy systems, water systems, transportation, telecommunications, emergency services, banking and finance.

The critical infrastructure (CI) on which society relies is now dependent on the interconnected communication networks the information age has spawned. With the evolution of the information age, not only has the communications landscape changed dramatically, the security landscape has changed too. With information technology being so ubiquitous, it has created new underlying concerns about the systems now reliant on them.

The reliance and complexity of these interconnected systems has increased vulnerabilities confronting critical infrastructure. This means old risk based assessment models cannot fully satisfy the needs of the contemporary world.

This research intends to understand the impact to Western Australia's critical infrastructure in the event of an information system failure in a company that is part of Western Australia's critical infrastructure supply chain.

The results of this research were a failure in the information system in the company investigated (The Coventry Group) would not have a catastrophic effect on Western Australia's CI supply. This conclusion is due to the redundancy the Coventry Group has built in their standard operating procedures through the use of manual procedures, which aims to minimize the disruption an information system failure causes to their customer service levels.
Contents

Abstract 2

Chapter One: Introduction 7
  1.1 Introduction to the Problem 7
  1.2 Overall View 7
  1.3 Introduction to the Coventry Group 8
  1.4 Research Question 10
  1.5 Significance of the Study 10

Chapter Two: Literature Review 12
  2.1 Introduction 12
  2.2 Security Complexity Due to Technological Advance 12
  2.3 Emergence of New Threats 13
  2.4 Studies by Alternative Theorists 19
  2.5 The Need for Further Investigation into this Field 21
  2.6 Conclusions 22

Chapter Three: Research Methodology 23
  3.1 Theoretical Framework 23
  3.2 Design 24
  3.3 Procedure 28

Chapter Four: Results 30
  4.1 Introduction 30
  4.2 Transformation 30
  4.3 Clients 32
  4.4 Owners 34
  4.5 Worldview 36
  4.6 Output 39
  4.7 Efficiency, Effectiveness and Efficacy 42
List of Diagrams
Soft System Model used in the Investigation into the Systemic Nature of Critical Infrastructure Protection using a Medium Sized Company as the Case Study 27

List of Tables
Table 4.1
Participant Perceptions of Services Supplied by the Coventry Group 30
Table 4.2
Participant Perceptions of Entities Affected by a Coventry Group Information System Outage 32
Table 4.3
Participant Perceptions of how Information Services Outages are Rectified within the Coventry Group 34
Table 4.4
Participant Occupations Summarized 36
Table 4.5
Participant Roles from within the Coventry Group’s Information Services Department 36
Table 4.6
Participant Roles within the Coventry Group but Outside of the Information Services Department 37
Table 4.7
Participant Roles Outside of the Coventry Group 38
Table 4.8
Participant Perceptions Summarized of how they would be Affected In the Event of the Coventry Groups Information System Failing 39
Table 4.9
Participant Perception of how Efficiency, Effectiveness and Efficacy would be measured in an Ideal System
Chapter 1: Introduction

1.1 Introduction to the Problem

This research is about examining the systemic nature of CI protection using a medium sized company as the case study. The importance of CI to society is highlighted by TISN (2004, p. 1) who defines CI as:

Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly affect the social or economic well-being of the nation, or affect Australia’s ability to conduct national defence and ensure national security

Dearth (2001) includes sectors such as telecommunications, transportation, energy generation, water and sewerage systems, emergency services, essential government services, banking and financial systems. As CI covers so many different areas, the services it supplies are vulnerable to disruption by various means. Threats to CI include natural disasters, supply chain failures, military strikes, terrorist and cyber attacks.

1.2 Overall View

Auerswald, Branscomb, La Porte and Michel-Kerjan (2005) sees the challenge of critical infrastructure protection as being multifaceted requiring a variety of responses. He theorises that market mechanisms and engineering design both have roles, but neither is sufficient. Adding to the complexity, in today's electronically networked environment, some security specialists believe cyber threats are just as real as physical threats. When considering CI security, all these threats need to be considered.

Underlying the running of the CI is information. For example, electricity providers need to know how close to capacity their active systems are, so blackouts are not caused. Water suppliers need to know how full their dams are, so decisions can be made on how much water can be supplied to the community. If a part breaks down in
a piece of equipment that is essential in CI supply, the supplier needs to know where to source them. To provide this information, infrastructure is reliant on computers and networks to provide this data and to maintain the integrity of a system.

Research into CI vulnerabilities by organisations including the U.S. Presidents Information Technology Advisory Committee (PITAC), the National Infrastructure Plan by the Department of Homeland Security (DHS) and the U.S Department of Commerce conclude that CI is reliant on networked computer systems. The papers by the U.S Department of Commerce, PITAC and the DHS also maintain the reliance CI has on the interconnected world of networked computer systems, creates the emergence of a significant threat to CI. A well planned attack on a CI provider’s computer system may disrupt another area of CI system, as they may be interconnected or reliant on each other.

Pye and Warren (2007) see the aim of government policy is to ensure continued supply of infrastructure through identifying and implementing protective safeguards. The result of this is much of the literature has been focussed on a macro level, looking at policies required to secure CI services. Tyrell (2001) notes governments are the major stakeholder in CI security which can also attribute why research into CI security has taken such a high level view.

The gap in the research in the area of CI security looking at how the failure in one node in the CI network, would effect the overall CI supply is the area this research intends to fill. The example used in this research is the Coventry Group; which is a mid sized company that supplies parts to repair equipment used in various sectors of Western Australia’s CI.

1.3 Introduction to the Coventry Group

The Coventry Group is a Western Australian owned and based company with its head office being based in Morley, Perth. Incorporated in 1936, the Coventry Group started as an automotive part supplier but has diversified into other markets such as fasteners, fluid systems, gasket manufacturing and hardware. The Coventry Group has a presence in every state and territory in Australia and overseas in New Zealand.
There are approximately two thousand two hundred employees and one hundred and fifty branches in the Coventry Group, with Western Australia making up thirty-six branches and eight hundred staff. Geographically, the Coventry Group has branches that go north to Port Headland, south to Albany, and east to Esperance and Kalgoorlie in Western Australia.

The Coventry Group can be seen as a small node in Western Australia’s CI network and resides in the supply chain area of this network. Spare parts are supplied by the Coventry Group and are used to repair equipment used in providing services within Western Australia’s CI. The Coventry Group’s parts are used in a variety of different applications within Western Australia’s CI network.

Through their fastener range, the Coventry Group’s products are utilized in areas of infrastructure including:

- Energy providers (nuts and bolts holding gas pipelines, water pipelines and electrical infrastructure together)
- Rail network (fasteners in rail lines, fasteners used to service trains)
- Housing and construction (roofing fasteners, screws in doors, fasteners in construction equipment such as cranes)
- Shire councils (nuts and bolts used to repair council equipment like bridges, fasteners that allow road signs to be displayed)
- Transportation (studs in wheel ends, bolts in axle housings, suspensions and mountings used by trucks, trailers and earthmoving equipment)
- Mining applications (fasteners to bolt together offshore drill rigs for gas supply, mining heads and frames, mining mills)
- Mechanical repair (fastener used in mechanical repair for service vehicles involved in CI maintenance).

The Coventry Group’s automotive division provides car parts, equipment items, consumables, light and heavy truck and trailer parts and division that services the mining and industrial sectors.
Automotive parts supplied by the Coventry Group automotive division touch many of the same areas as the fastener division but predominately are used to repair service vehicles used by CI providers such as vans and utilities. Consumables supplied by the Coventry Group are varied and range from different grades of oil (e.g. automotive, diesel and hydraulic oil), bags of rag, kitty litter to clean up workshop spillages, brooms, shovels and safety gear (safety glasses, hi-visibility and protective clothing).

Coventry’s equipment department provide complete units used in workshops such as electrical generators, diagnostic equipment, ramps and hoists. The mining and industrial department buys in goods for mining companies which varies from a windscreen for a road roller, fencing wire to secure areas to whole conveyor systems. There is also a specialist truck division within the Coventry Group, which provides engine, gearbox, differential, suspension, wheel end and trailer parts.

Cooper Fluids are involved in supplying hydraulic, pneumatic, fluid transfer and lubrication products to Western Australia’s mining, construction and transport industries.

The Coventry Group maintains many major contracts with suppliers involved in Western Australia’s CI. Mining companies are very important to the Coventry Group with large contracts are held with Rio Tinto, Pilbara Iron (a division of Rio Tinto), Worsley Alumina and Alcoa.

1.4 Research Question

The research question related to this study is:

What systemic effect can the failure of the information systems of a medium size component supplier have on the integrity of the critical infrastructure of Western Australia?

1.5 Significance of the Study

Western Australia is geographically isolated with large companies making up the major nodes in Western Australia’s CI network. Examples of major CI providers in
Western Australia include the Water Authority, Synergy, Alinta Gas, various port authorities and local councils. Servicing these large nodes are many small to medium sized companies.

Research into Australia’s CI by Pye and Warren (2006) suggest modelling Australia’s CI is required to understand the interdependencies that exist between CI providers. They maintain this would allow for the identification of risks, threats and vulnerabilities to Australia’s CI.

This study intends to investigate the resilience and redundancy that exists in Western Australia’s CI network by studying a small to medium sized company that is part of this network. Understanding the impact of the failure of a node within Western Australia CI supply chain and the impact this has on the rest of Western Australia CI network is the purpose of this study.

The significance of the study is to add knowledge in the area of CI protection, by investigating the perceived consequences of a failure to a CI supplier's information system that forms part of Western Australia’s CI network, to this network. Another significant aspect of this study is to understand if there is resilience and redundancy in this network.
Chapter Two: Literature Review

2.1 Introduction

The literature reviewed sees the threats to CI as being many and varied with threats including natural disasters, terrorist attacks, cyber threats, internal threats, geographical proximity, network theory, population growth and government policy. The literature relating to CI protection presents some recurring themes including:

- Security is becoming more difficult with technology advances not less
- The emergence of new threats, coupled with the complexity of information infrastructure are making previous and current models for assessing threats and vulnerabilities to CI outdated
- The need for further investigation into this field.

2.2 Increased Security Complexity Due to Technological Advance

CI security is becoming more complex due to the inter-opera ability of multiple technologies and the rapid advancement of technology (Anderson, 1999a). Traditional risk models have become outdated as almost all risk assessment methods today do not provide a method to accurately assess the threats facing a large networked environment. Sobelman (1998) sees the sharp advancement of technology is making CI security more difficult, as the basic time unit used to measure technological advantage is drastically shrinking. Choi (2004) refers to Moore's Law which proposes the rate of processor power, doubles every eighteen months. Information theory suggests, more information means increased uncertainty which increases the rhythm and speed of threats (Seebeck, 2004). With technology changing so fast, new security risks evolve quickly and securing CI becomes more difficult.

Conway (2003) observes the link between cyber terrorism and the broader issue of terrorism is not understood by CI security strategists. As a result of this, he sees the policy response required by governments to secure CI has failed to include both terrorist and cyber attacks in their CI security strategies.
2.3 Emergence of New Threats

Cobb (2003) adds another dimension to the argument that traditional risk models are outdated as he sees defence strategies as still being based on the conventional, visible, state based symmetrical attacks. Symmetrical warfare involved large scale military invasion and occupation of territories, with strategic CI being attacked and defended. Recent terrorist attacks such as the Madrid (2004), London (2005) and Bali (2005) terrorist bombings have occurred using unconventional warfare strategies, away from traditional terrorist hot spots like Northern Ireland, Columbia and the Basque region. Asymmetrical attacks are being launched from western societies, accessed via non nation state means, allowing them to be harboured in sympathetic communities and to be organised in a dispersed fashion. By augmenting international flows of all kinds, globalization has given prospective terrorists greater cover and the ability to create larger economic consequences from their attacks (Enders & Sandler, 2005). Terrorists concealed in these communities are able to move swiftly, accessing the resources they require launching their terrorist attacks. Cole (2006, p. 5) sees CI as being prime targets for terrorist attacks and states: "Al Qaeda has threatened to attack what Osama bin Laden calls the 'hinges' of the world's economy, that is, its critical infrastructure."

Asymmetrical terrorist attacks leave a lighter footprint than traditional conflict, as the terrorist do not seek to occupy territories or control CI (Seebeck, 2004). Tactics such as suicide attacks, which is typically a non western behaviour make launching a counter attack difficult for Western forces. Western defences are still geared towards defending against slow moving, visible or static targets (Danskine, 2005).

The US National Security Strategy of 2002 was to “disrupt and destroy terrorist organisations by: denying further sponsorship, support, and sanctuary to terrorists by convincing or compelling states to accept their sovereign responsibilities” (The Whitehouse, 2006, p. 5). This policy was enforced when America reacted to the September 11, 2001 attacks, by launching a state based attack against Afghanistan, as America believed Afghanistan were sympathetic to al Qaeda and provided sanctuary for al Qaeda operatives. Armistead (2004) suggests security policy has not changed in light of these new threats and postulates that new security models need to be developed, due to the emergence of these new threats facing CI.
Collins and Reed (2005) see that Australia's security policies have closely followed the United States of America. Australia's government policy on CI protection has also mirrored the United States of America approach according to Cobb (2003). Research by Armistead and Malone (2004) found that since the 2001 terrorist attacks on the United States, Australia has only tinkered with existing defence structures to combat the emerging terrorist threat. Their research found in comparison, America has made a significant overhaul of their national security machinery since the September 11, 2001 attacks. During this period both countries have made amendments to their counter terrorist policies and their CI protection policies. The USA has been consistently ahead in their pace, priority and the resources they have provided to implement changes to CI protection.

Mimicking the United States response to CI security is not practical policy for Australia according to Pye and Warren (2006). This is due to the situational differences between the two countries that include:

- Australia is a large island continent.
- Minimal sharing or reliance on external infrastructures and services located or provided from outside the national border.
- CI is spread over large geographical areas with limited populations in remote regions of the country.
- Largely immune from foreign critical infrastructure incidents, although this is not entirely the case from a cyber perspective.
- Due to remoteness, there is potential for early warnings regarding externally based incidents and perhaps isolation from the effects thereof, but Australia is not itself immune from the effects of externally originating incidents and nor can be expected to totally contain internally based incidents.

Not all threats are malicious, accidents, errors of omission and natural disasters all need to be considered when planning CI protection. Though there is much paranoia around the terrorist and cyber threats posed to CI security, literature on CI protection
considers threats such as natural disasters, supply chain failure, internal threats, government policy and population growth.

Supply chain vulnerabilities could also be used by terrorists to advance their causes. Thibault, Brooks and Button (2006) investigated the vulnerabilities in the USA’s maritime transportation supply chain. Vulnerabilities found in their research included using shipping containers or vessels to smuggle personnel or weapons (nuclear, biological, and conventional) into the U.S., using merchant ships, such as liquefied natural gas tankers, as weapons against port cities or critical maritime infrastructure and disrupting marine routes preventing the importation of critical items such as food and equipment into the country.

Cole (2006) suggests a vulnerability existing with energy suppliers because of the demands developing countries such as China and India are placing on their resources. Over the summer months of 2007 in Perth, Western Australia’s energy supplier Synergy, placed advertisements asking electricity consumers to lower consumption during peak periods, in the hope of avoiding loss of supply because of an overloaded power grid. These advertisements suggested this was caused by Perth’s rapid growth in population.

Population growth to certain geographical locations may also provide a threat to CI. Meade and Abbott (2003) found that coastal communities’ populations were increasing, as was property development in these areas. They assert that coastal areas are more vulnerable to natural disasters such as storms, flooding and tsunami and believe any natural disasters affecting CI in coastal communities, would affect greater portions of the population, as this is where people are choosing to live.

The threat of natural disaster disrupting CI supply also needs to be considered by security strategist. With the advent of global warming, Stavros (2005) remarks that many scientists believe, that the instances of natural disasters such as drought, hurricanes and tsunamis will become more common. The ABC (2007) reports that the drought the eastern states of Australia are currently experiencing may be the result of global warming. One of the threats this natural disaster may cause to Australia’s CI is the Snowy hydro – electricity scheme not being able to supply electricity, because of
the lack of water in the rivers that feed the hydro electricity plant there. According to Engineers News Record (2006), the discussions on CI security in America has expanded from terrorism to natural disasters, due to the impact that hurricanes Katrina and Rita had on America’s CI. According to Stavros (2005) the threat natural disaster poses to CI is increasing and needs to be planned for by security strategists and engineers.

Government policy can also be seen as a threat to CI security. Eosco and Hooke (2006) argue the extensive damage caused by Hurricane Katrina to New Orleans was due to government policy. They see damage caused by this natural disaster stemmed from decades, if not centuries, of public and private decisions with respect to land use, building codes, and the development and protection of CI.

The lack of ICT policies in developing countries is also seen as a threat to Western countries CI according to Burkhart and Older (2003). They argue loose ICT policies in developing countries can allow terrorist organizations such as al Qaeda to use the Internet for covert communicate means. These covert operations could include planning attacks on CI, using coded communication methods.

Another threat government policy has to keeping CI secure is balancing the need for security and the requirement to keep information flowing. Sobelman (1998, p. 2) states: “a nation’s ability to both produce and utilize information and protect its information assets becomes synonymous with securing its national security.” In general, things that have value to your business should be protected. The protection offered to these assets should be in proportion to the value of the item. Having too much security creates an unnecessary expense and causes decreased accessibility to those that are authorized to get access. There is a need to evaluate and balance the level of exposure with the criticality of what is being protected (Plant and Machinery, 2005).

Security strategies need to consider information flow when forming security policies. The lack of information flow could pose a threat to a CI supply, so ensuring the right information is available to the right people at the right in CI systems is an important consideration for security analysts.
Research by the TISN (2004) found that up to ninety percent of Australia’s CI is privately run. Because there is so much reliance on the private sector to provide CI services, government policy needs to consider the competing needs for corporate efficiency and the requirement to protect CI. The responsibility for setting goals rests primarily with the government, but the implementation of steps to reduce the vulnerability of privately owned and corporate assets depends primarily on private-sector knowledge and action. Although private firms uniquely understand their operations and the hazards they entail, it is clear that they currently do not have adequate commercial incentive to fund vulnerability reduction. For many, the cost of reducing vulnerabilities outweighs the benefit of reduced risk from terrorist attacks as well as from natural and other disasters (Nussbaum, 2005). The case of the January 2004 train crash in South Carolina where nine people were killed and a further fifty-eight were hospitalized, as reason why both private enterprise needs to remain profitable and public safety need to be considered when forming policy on CI security (Auerswald, et al, 2005).

Reduced investment can lead to deterioration in infrastructure and possible declines in safety, supply and optimum performance as no organisation has an infinite amount of funding (Wilson & Norris, 2006). Kilgour and Levy (2005) point out the Chernobyl nuclear reactor accident, was a result of deteriorating infrastructure at that plant.

Government policy relating to the freedom of information is seen as another threat to CI according to Ahmad, Fah, Ruighaver and Teo (2004). They note that the law in some countries requires CI information such as design diagrams of engineering equipment unique to CI, to be available in the public domain, for competitive reasons. Protecting CI is becoming more difficult with information related to key engineering and functional specifications of a CI system being made freely available in the public domain.

An area of CI security often overlooked is that vulnerability at a lower functional level of a network or a system undermines safeguards at higher levels (Brown & Odom, 2001). A system is only as strong as its weakest link, with many critical infrastructures being highly-interdependent on other CI and their networks. They see
any physical constraint on the system as being a point of vulnerability. To understand where the independencies exist in Australia's CI, Pye and Warren (2006) suggest modelling Australia's CI is required, allowing for the identification of risks, threats and vulnerabilities to Australia's CI.

Buchanan (2002) notes research into networks in natural, social and technological settings has found their underlying architecture is incredibly similar. Analysing the underlying architecture of networks in the natural, social and technological settings is important in understanding why protecting weak points in a network is important. One way to describe how weak points are important to network architecture is via social networks.

Social networks are comprised of nodes which are connected to other nodes with degrees of differing strengths. Some nodes interact with each other regularly, forming a strong link between the two nodes, some nodes interact less frequently and some are connected via another node. These less frequent interactions form weak links or ties within the network, however are still connected and influence the network (Granovetter, 1973). Watts and Strogatz (1998) applied a mathematical formula to work out how many links it takes to reach another node in a network, which allowed them to understand how well connected a network is. They theorised the less the degree of separation between the nodes the quicker it is to reach nodes within a network.

The possible impact of one node being removed is that all the connectors that are attached to this link, whether they have a strong or weak link to the node being removed, may be affected. This may result in the node possibly being removed from the network. The more highly connected the node that is removed, the greater the number of nodes will be affected. As other nodes are affected, the flow on affect in the network is that secondary extinctions occur, which sees some nodes losing their connections altogether and becoming totally isolated, so removed from the network (Buchanan, 2002).

Because of this network structure, Anderson, (1999b) suggests government agencies or commercial organisations should not expect there to be a hardened, secure
backbone minimum information infrastructure they can depend on, as the needs are too geographically and functionally diverse.

The structure of networks and the impact of destroying a highly connected hub within the network present another risk to CI security, which is via internal attacks. Lewis (2002) sees that a degree of sophisticated inside knowledge is required to identify what action is likely to cause the most harm to infrastructure, which hackers could only achieve via social engineering.

Investigations into sabotage of computer systems in various CI sectors concluded that though much money is spent on securing systems from outside threats, sixty to seventy percent of crimes committed on information systems running CI are from internal sources (Randazzo, et al, 2004 and Lynch, 2006). They concluded internal attacks on CI organizations cost CI suppliers more than those perpetrated by outsiders, results which are consistent found in research on cyber attacks in other sectors.

2.4 Studies by Alternative Theorists

The literature review introduced threats to CI such as natural disasters, geographical proximity, terrorist attacks, cyber threats, internal threats, network theory, population growth and government policy. Not all theorists subscribe to the belief that these emerging threats are creating any greater threat to CI protection than had previously existed.

Though many press reports contend that natural disasters are increasing due to global warming, not all scientists and theorists agree. Stavros (2005) points out that natural disaster such as hurricane scale storms have actually fallen in some places, including the region near Australia. Supporting the argument made by Stavros, is a study done by Meade and Abbott (2003) for the Office of Science and Technology, which concluded claims that a dramatic rise in the numbers and intensities of hazards are not generally supportable.

Koprowski (1998) explains that because of the complex nature of CI technologies, cyber attack poses a relatively small threat to CI and uses power plants as an example
of CI technology to highlight his point. Koprowski (1998) explains that shutting power plants requires manual processes such as opening circuit breakers and to lower the set points. Lowering set point levels at which they are transmitting power requires a user to be on site and these processes cannot be solely done on a computer. Access to areas where these manual processes are performed requires authenticated access, such as smart card access.

Matthew and Shambaugh (2005) see that though individual nodes within a network may be reached and destroyed, an extensive and almost inconceivable multi nodal attack would be required to totally disable a network. Lewis (2002) believes that the threat posed by terrorist attack to CI is overstated. He sees terrorists wanting to make an immediate impact and use violence, terror, bloodshed to grab attendant headlines, with most CI attacks not being able to produce these types of headlines.

According to Goodno (2005) there is little evidence of malicious behaviour bringing down CI systems and includes that hackers that have broken into CI information systems have not been able to cause any major damage or shut down any systems run by these systems. He points out that these hackers have at the most, been ‘pests’, with legal systems only having imposed small fines on them. The greatest risk posed to information systems is not from hackers but from targeted, well planned and co-ordinated state sponsored attacks (Busby, 1999).

Helping the alternative theorist’s arguments is the difficulty in getting accurate figures on the incidence or degree of cyber attacks. Governments are reluctant to release this information as they view this data as too sensitive and private companies are not willing to give out information on the attacks to their organisations as this may affect their business value (Smith, 1998).

Though government investigations such as the Presidents Information Technology Advisory Committee (PITAC), the National Infrastructure Plan by the Department of Homeland Security (DHS) and the U.S Department of Commerce have acknowledged Smith (1998), Browning (1997), Goodno (2005) and Koprowski (1998), a recurring theme in these reports is the need for further investigations into CI protection.
2.5 The Need for Further Investigation into this Field

The literature on CI vulnerabilities presents security as being the identification and management of risk with proper and accurate threat assessments allowing security experts to predict future vulnerabilities and mitigate damages. Investigations into CI security concludes that this process has historically tended to be reactive and event driven. Literature on CI protection argues that with the emergence of the information age and terrorist attacks, threat assessment needs to be a more dynamic process and to work in quicker response cycles.

New security models need to be developed, due to the emergence of these new threats facing CI and a lesson from the 9/11 attacks one security analysts lacked imagination in assessing the vulnerabilities their infrastructure faced. Terrorists have been able to innovate when launching their terrorist attacks. The 9/11 attacks were mounted by a small unsophisticated group, from caves in one of the most backward countries in the world, using garden variety means of public transport against the worlds only super power, with the most powerful and sophisticated military force in history (Cobb, 2003).

A well planned attack on a CI provider’s computer system may disrupt another area of CI system, as they may be interconnected or reliant on each other, research by the U.S Department of Commerce, PITAC and the DHS has found. TISN (2004) suggests the reliance CI has on the interconnected world of networked computer systems has created a new significant threat to CI and urge that the independencies in Australia’s CI need to be understood and defined.

Pye (2006) and Warren (2006) see CI protection as being an all hazards approach that accommodates interdependencies between business sectors, jurisdictions and government agencies. Thibault, Brooks and Button’s (2006) research into America’s maritime supply chain found that one node could have a ripple effect into many other areas not directly related just to America’s maritime activities such as food and equipment supply. Brown and Odom (2001) found that vulnerability at a lower functional level of a network or a system, undermines safeguards at higher levels.
2.6 Conclusions

Information from the literature review indicates what data is available on CI security and the impact this will have on the research. Dearth (2001) sees any investigation into CI security needs to consider private and confidential data around an organisation's procedures and vulnerabilities as information in this realm is sensitive as it relates to securing essential services and security. This may prove difficult to obtain from direct sources such as public or private organizations in charge of critical infrastructure on their vulnerabilities. By investigating how supply chain failures would affect a CI provider, there would be no need to ask questions that relate to sensitive areas of CI security.

Literature examining Australia’s CI security by Cobb (2002) and Armistead and Malone (2004) and has largely centred on government policy and what policies they perceive are required to ensure CI security in this country. The gap in the literature around the failure of a node in Western Australia’s CI is the area to which this investigation intends to add knowledge.
Chapter 3: Research Methodology

3.1 Theoretical Framework

The philosophical approach to this study is constructivist. A constructivist approach tries to understand how knowledge is constructed through people’s perceptions. Qualitative research explores attitudes, behaviour and experiences and has been used to effectively create models to analyse vulnerabilities in systems previously (Dawson, 2002).

Kane and Del Mistro (2003) observed that though science had made advances in foundation sciences such as physics, engineering and chemistry, similar progress has not been achieved in more complex areas such as psychology. This had meant fields such as sociology, political science and management did not possess a useful body of theory to solve the problems in these fields.

Checkland (1999) observed that in the social sciences virtually all knowledge gained is heavily meaning-bearing and in the management of social situations, goals are often obscure. Jackson (1992) sees the need to challenge traditional positivist/quantitative orientations, to help managers deal with and understand the extreme complexity of the systems they seek to control. Soft systems methodology was primarily developed by Checkland as a response to the failings of positivist/quantitative approaches.

Ackoff (1987) sees organisational problems as being poorly defined and with stakeholders interpreting problems differently. A soft system approach allows a practitioner to understand the system they are analysing as a collection of worldviews of reality. These worldviews provide a framework which help structure the analyst’s impression of the problem and allow these perceptions to be modelled. The problems can be represented as they are perceived by the different stakeholders and then be represented in a model.

Soft system methodology, though often described in a linear fashion, is a flexible tool to gain knowledge and understanding from individuals and to generate action from a group (Kane & Del Misto, 2003). Dick (2006) sees soft systems analysis useful to analyse social systems such as organisations. Soft system approaches attempts to
view the world holistically, seeing whole bodies linked with whole bodies (Checkland, 1999). Reisman and Oral (2005) add that the role of soft systems models is to identify and solve the right problem. Using this soft system approach will allow the interdependencies in Western Australia’s CI network related to the Coventry Group and a failure within this node, to be better understood.

Checkland (1999) sees often an outcome of undertaking a soft system approach to a problem is to gain a better understanding of a problem, rather than finding a solution to the problem. This research intends to understand the systemic effect of an information systems failure in a medium size component supplier will have on the integrity of the CI of Western Australia from a number of different perspectives. Using the internalized system models from the participant’s mind, a better understanding of the perceived vulnerabilities that exist in this node can be constructed, as can the social and political environment these systems operate in.

### 3.2 Design

Gregory (1993) suggests that soft system models attempt to create an ideal system to solve a problem. This intended research does not propose to create an ideal system to secure Western Australia’s CI. The intention of this research is to understand the systematic effect a node in Western Australia’s CI would have in Western Australia’s CI supply.

This has meant that the textbook approach to soft system methodology has had to be altered to understand this problem. The first stage of this investigation comprised data collection, through interviews, observations and studying the standard operating procedures used by the Coventry Group. Participants were to describe the situation by asking six descriptive questions. Model soft systems methodology does this by asking a series of questions which form the mnemonic known as CATWOE. The CATWOE questions used in classic soft systems methodology are:

- The clients of the system; who does the system serve?
- The actors in the system; who carries out the transformations in the system?
• The transformations in the system; what does the system do between input and output?
• The weltanschauung (worldview) which makes the system meaningful; what are the underlying assumptions made making the system meaningful?
• The owners of the system; who or what can close the system down?
• The environment of the system; what does the system take for granted? (Checkland and Scholes, 1999)

To help understand the overall research question, interviews were conducted using a specific set of questions derived from soft system methodology, specifically the CATWOE instrument. The questions used in this research were slightly changed in some instances, to allow the research questions to be answered. By using this design, the analyst can understand what is being affected (question 1), who is being affected (question 2) and how they are being affected (question 5). The enquiry also intends to understand how the system can be restored and if the resources to restore the system are readily available (question 3). Checkland and Scholes (1990) describe the measurement of success of a system can be done by finding out the efficacy, efficiency and effectiveness of any proposed system (question 6).

The participants were asked to provide a description of problem through the use of following CATWOE questions:

1.) “What services and products does your company provide? (What area of CI is being affected?)” This question can be matched to the CATWOE question; “The transformations in the system; what does the system do between input and output?” and aimed to find out what would be affected if there was an information system failure in the Coventry Group. The consequence of parts not being supplied was not an aim of this question.

2.) In the event of an information system failure in the Coventry Group who would be affected both inside and outside Coventry’s? What services do these entities provide? This question can be matched to the CATWOE question; “The
clients of the system; who does the system serve?” Question 2 was asked to find out who and what would be affected in the event of system outage.

3.) Who would be involved in rectifying any system outage? What extra resources would they need? Would these be readily available? This question can be matched to the CATWOE question; “The owners of the system; who or what can close the system down?” This question aimed to understand how the system can be restored and if the resources to restore the system are readily available.

4.) What worldview /perspective are you taking? (E.g. supplier, customer, internal staff member at Coventry’s) This question can be matched to the CATWOE question; The weltanschauung (worldview) which makes the system meaningful; what are the underlying assumptions made making the system meaningful? Question four was designed to find out the participants perspective.

5.) How would your products and services be affected in the event of the Coventry Groups information system failing? (E.g. how would output be affected?) This question wanted to find out how the participants would be affected.

6.) How would the efficiency, effectiveness and efficacy be measured in any proposed system designed to cope with critical failures? (E.g. what KPI’s are used? Lead times, fill rates etc) Question six intended to find how the participants would measure the success of a system that would be implemented to rectify an information system outage.

Diagram 1 below has been included to help the reader understand how the soft system model has been altered for this investigation.
From these questions, it is possible to define the area of concern, which is known as the ‘root definition’. A “root definition” allows the practitioner to understand the organisational activity that occurs within the system boundaries. The root definition also defines what is agreed and what is resolved as well as any other associated issues. This ‘root definition’ will allow the practitioner to understand the following “A system for the benefit of ....run by.... to achieve....from the perspective of....within the constraints of....and controlled by...”
A mind map can be created from this ‘root definition’ to conceptualise the answers provided in the investigation. This conceptual model is not a representation of the real world; it is a conceptual model of the internalized views held by the participants interviewed.

3.3 Procedure

As the Coventry Group supplies spare parts to repair equipment used in Western Australia’s CI supply, the population sampled for this study had to have knowledge of the systems they were being asked about. It is necessary in this investigation that participants are familiar with the systems and services used by the Coventry Group. The participants would also be required to understand how Western Australia’s CI would be affected if the services the Coventry Group offered failed.

To gain this information for this inquiry a judgement sampling design was used. Judgement sampling is considered as a non-probabilic sampling design and involves the choice of subjects who are in the best position to provide the information required. Having themselves gone through the experiences and processes, they might have expert knowledge, and perhaps be able to provide good data or information to the researcher. Judgement sampling designs are used when a limited category of people have the information that is sought (Sekaran, 1992). The population sampled in the interview process were staff from within the Coventry Group, customers of the Coventry Group and suppliers to the Coventry Group.

A disadvantage of using this sampling method for this research was the participants are selected on the basis of their expertise about the subject being investigated. This affects the ability to generalize about the sample, as it does not provide a true sample of the population. Although judgement sampling may curtail the ability to generalize about the findings as the consisted sample of experts who were conveniently available, sometimes it can be the only viable sampling method for obtaining the type of information that is required from very specific pockets of people who possess the knowledge and can give the insight sought. Depending on the nature of the topic, it may be the only meaningful way to investigate. As this research needs to gather data about CI services, the participant’s sampled need to be familiar with either the
systems they are using, equipment they are running and parts they are sourcing. This makes judgement sampling a valid sampling method for this investigation.

Mentioned in the design section, a root definition needed to be derived to understand the issues that would be caused in the event of an information system failure within the Coventry Group and the effect this would have on Western Australia’s CI supply.

Interviews were conducted face to face, over the telephone or via email. Visits to various locations to observe business processes within the Coventry Group and to understand more thoroughly how processes are impacted in the event of a system outage. The questions asked in the research were matched to the CATWOE questions. Results of these interviews are included in Appendix 1.

The investigation aimed to understand how parts supply to sectors of Western Australia’s CI would be affected in the event of an information system failure in a parts company that supplied parts to repair equipment used in Western Australia’s CI. The questions aimed to find what services would be affected and how, in the event of an information system outage, how would the system be restored and how long this would take, any biases in answers and how an ideal system to restore an outage would be measured.

The next phase in the study involved collating all the answers and grouping them together. A root definition was then created and a mind map was constructed to conceptualise the answers provided. This conceptual model used to analyse the systemic effect an information system failure in the Coventry Group would have on Western Australia’s CI so the results of this investigation could be detailed.
Chapter 4: Results

4.1 Introduction

The themes from the interviews conducted are summarized into tables related to the question. Each question is divided by a title, which provides an overview of the CATWOE instrument the question is related to and then the question. Appendix 1 has the full list of participant’s answers, grouped by participant for cross referral.

4.2 Transformation

The transformations in the system; what does the system do between input and output?

Question 1

What services and products does your company provide? What area of CI is being affected?

Table 4.1

Participant Perceptions of Services Supplied by the Coventry Group

<table>
<thead>
<tr>
<th>Response</th>
<th>Participant/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fastener, automotive, mining &amp; industrial supplies are services and products being supplied</td>
<td>1,2,3,5,6,7,8,9,10, 11,13,14,15,17,18</td>
</tr>
<tr>
<td>Items specific to supplier are services and products being supplied</td>
<td>10 &amp; 13</td>
</tr>
<tr>
<td>Supply of credit to customers are services and products being supplied</td>
<td>4</td>
</tr>
<tr>
<td>Services and products specific to customer are services and products being supplied</td>
<td>12 &amp; 16</td>
</tr>
</tbody>
</table>

A theme from the answers to question one was that the parts the Coventry Group supplies to Western Australia’s CI is varied, so many different areas could be impacted. The items supplied to Western Australia’s CI suppliers from the Coventry Group ranged from cleaning goods, automotive parts used in maintenance vehicles up to mining infrastructure such as refining, milling and crushing equipment.
The participant’s perceptions of products supplied by the Coventry Group to Western Australia’s CI provided by participant’s responses can be generalised by the following list:

- Fasteners
- Automotive parts
- Mining supplies
- Industrial supplies
- General equipment
- Adhesives
- Cleaners
- Oils
- General consumables
- Protective clothing
- Truck and trailer spare parts

Answers supplied by suppliers to the Coventry Group (10 and 13), focussed on the products their company supplied the Coventry Group which were electrical parts, bearings, various truck and trailer parts (10) and engine parts, dewatering vehicle parts, lighting tower parts and portable generator parts (13). Answers from CI suppliers that are customers of the Coventry Group stated they supplied services in alumina refining (12) and a shipping port (16) to Western Australia’s CI.

Participant 4 was an accounts receivable officer in the Coventry Group indicated another service the Coventry Group provided to Western Australia’s CI providers was the provision of credit to CI suppliers so they could purchase goods.
4.3 Clients

The clients of the system; who does the system serve? Who and what would be affected in the event of system outage?

Question 2

In the event of an information system failure in the Coventry Group who would be affected both inside and outside Coventry's? What services do these entities provide?

Table 4.2

Participant Perceptions of Entities Affected by a Coventry Group Information System Outage

<table>
<thead>
<tr>
<th>Response</th>
<th>Participant/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coventry Group staff at head offices and branches and external entities such as customers and suppliers would be affected an information system failure in the Coventry Group</td>
<td>1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 14, 15, 17, 18</td>
</tr>
<tr>
<td>Suppliers not receiving purchase orders would be affected an information system failure in the Coventry Group</td>
<td>10 &amp; 13</td>
</tr>
<tr>
<td>Specific organisations affected would be affected an information system failure in the Coventry Group</td>
<td>12 &amp; 16</td>
</tr>
</tbody>
</table>

Answers provided in answers 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 14, 15, 17 and 18 saw that internal (Coventry Group staff at head offices and branches) and external entities (customers and suppliers) as being entities affected by a Group information system failure. Suppliers to the Coventry Group stated that purchase orders from the Coventry Group would not be received so parts would not be supplied (10 and 13). Customers of the Coventry Group (12 and 16) answers saw themselves as only being affected by a system outage and these customers were Alcoa (12) and the Esperance Port (16).
The second part to this question asked “What services do these entities provide?” The participant perceptions of CI services provided by entities affected by a Coventry Group information system outage are listed below:

- Mechanical services
- Mining services
- Building services
- Transport services
- Engineering services
- Port services such as the loading and unloading of ships that carry various cargo including minerals and produce
- Refining of alumina
- Shire services
- Earthmoving
- Farming

Answers to this question provided from participants 5 and 15 introduced a theme that was also seen later in the investigation in question five, which was the perception that the Coventry Group’s image would be more affected by an information systems outage, rather than a threat to CI services.
4.4 Owners

Who are the owners of the system; who or what can close the system down?

Question 3

Who would be involved in rectifying any system outage?

What extra resources would they need?

Would these be readily available?

Table 4.3

Participant Perceptions of how Information Services Outages are Rectified within the Coventry Group

<table>
<thead>
<tr>
<th>Response</th>
<th>Participant/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information system issues are resolved at a first level initially, if required escalated to a second level of support. Second level support is normally managed by an external provider. Service level agreements are in place with external providers, ensuring outages are rectified within a specified time frame.</td>
<td>1, 3, 6, 7, 8 &amp; 9</td>
</tr>
<tr>
<td>Information system issues are resolved by the Coventry Group’s Information Systems Department.</td>
<td>2, 4, 5, 10, 11, 12, 13, 14, 15, 16, 17 &amp; 18</td>
</tr>
</tbody>
</table>

This question aimed to understand how the system can be restored and if the resources to restore the system are readily available, in the event of an information system failure. The answers to these questions varied and seemed dependent on the participant’s occupation.

Participants that are employed by the Coventry Group’s Information Systems department (1, 3, 6, 7, 8 and 9), saw that any information system outage would be handled initially at a first level support, by in-house by full time Coventry Group staff. If the issue could not be rectified through first level support, the issue would then be escalated to second level support. Incidents raised to second level support are normally resolved by an external supplier to the Coventry Group. Service level
agreements the Coventry Group has with outside suppliers are constructed so faults are rectified within a certain time frame. Service level agreements with external service providers are negotiated to reflect the potential impact an outage to a service has on the business. The more critical the fault reflects the response time that is agreed, which is also reflected as being a higher cost. Service level agreements are created in this manner to mitigate the risk of a lengthy system outage occurring to the Coventry Group.

Participants who did not work in the Coventry Group Information Systems department (2, 4, 5, 10, 11, 12, 13, 14, 15, 16, 17 and 18) did not provide the same depth with their answers; they saw system outages as being rectified only by the Coventry Group’s Information Systems Department.

A reason why this perception is held by the respondents not employed by the Coventry Group’s Information Systems Department is because they have no visibility of how an information system outage is rectified within the Coventry Group. When there is an information system outage in the Coventry Group, a communication is sent from the Information Services Department notifying internal and some external stakeholders (such as users of the company’s electronic catalogue) of this system outage. The details of a system outage are normally described at a fairly high level by the Coventry Group Information Services Department. Once services have been restored, a communication is once again sent out by the Coventry Group Information Services Department, notifying users that the affected services have been restored and are once again available. Users outside the Group’s Information Systems Department would have no idea how these issues are rectified unless this is done by the Coventry Group’s Information Systems Department.
4.5 Worldview

What viewpoint is the participant answering from.

Question 4

What worldview/perspective are you taking? E.g. supplier, customer, internal staff member at Coventry’s.

Table 4.4

Participant Occupations Summarized

<table>
<thead>
<tr>
<th>Response</th>
<th>Participant/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant from the Coventry Group, employed by the Information Services Department</td>
<td>1, 3, 6, 7, 8 &amp; 9</td>
</tr>
<tr>
<td>Participant from the Coventry Group not employed by the Information Services Department</td>
<td>2, 4, 5, 11, 14, 15, 17 &amp; 18</td>
</tr>
<tr>
<td>Supplier to the Coventry Group</td>
<td>10 &amp; 13</td>
</tr>
<tr>
<td>Customer of the Coventry Group and CI supplier in Western Australia</td>
<td>12 &amp; 16</td>
</tr>
</tbody>
</table>

Of the twenty interviews sent out, eighteen were received back. The jobs chosen in from within the Coventry Group’s Information Services Department are detailed in table 4.5.

Table 4.5

Participant Roles from within the Coventry Group’s Information Services Department

<table>
<thead>
<tr>
<th>Role</th>
<th>Participant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warehouse Management System Consultant</td>
<td>1</td>
</tr>
<tr>
<td>System Administrator</td>
<td>3</td>
</tr>
<tr>
<td>Communications Engineer</td>
<td>6</td>
</tr>
<tr>
<td>Database Administrator</td>
<td>7</td>
</tr>
<tr>
<td>Server Analyst</td>
<td>8</td>
</tr>
<tr>
<td>System Administrator for the Tandem System</td>
<td>9</td>
</tr>
</tbody>
</table>

These participants were chosen to help understand how the different information services departments and systems within the Coventry Group are affected by a system outage and how long and what is required to get these systems up and running again.
The systems that were investigated were the Oracle E-business Applications Suite, Discoverer Reporting application and the electronic parts catalogue (known as I Store) used by customers and businesses on the Oracle system (System Administrator and Database Administrator), Cov Parts legacy system (System Administrator for the Tandem System), Windows applications, email, Electronic Data Interfaces (EDI), payroll and anti virus (Server Analyst), communications services such as telephones, faxes and the Internet (Communications Engineer) and the warehouse management system for the Distribution Centre (Warehouse Management System Consultant).

Coventry Group staff interviewed but whose roles were outside of the information systems department are detailed in table 4.6.

Table 4.6
Participant Roles within the Coventry Group but Outside of the Information Services Department

<table>
<thead>
<tr>
<th>Role</th>
<th>Participant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement Officer Overseas Buying</td>
<td>2</td>
</tr>
<tr>
<td>Accounts Receivable Officer</td>
<td>4</td>
</tr>
<tr>
<td>Assistant Accountant</td>
<td>5</td>
</tr>
<tr>
<td>Customer Service Representative Coventry Fasteners</td>
<td>11</td>
</tr>
<tr>
<td>Business Development Manager</td>
<td>14</td>
</tr>
<tr>
<td>Branch Manager</td>
<td>15</td>
</tr>
<tr>
<td>Storeman</td>
<td>17</td>
</tr>
<tr>
<td>Coventry’s Parts Interpreter</td>
<td>18</td>
</tr>
</tbody>
</table>

The areas these roles were in were finance (accounts receivable and accounting departments), procurement (Procurement Officer Overseas Buying), sales (Customer Service Representative Fasteners, Business Development Manager, Branch Manager, Storeman and Coventry’s Automotive Parts Interpreter) and warehousing (Storeman). These roles fit into CI as the sales staff supply the items to the customers who are repairing the equipment that is being serviced, the procurement department as this department sources the goods and the accounting departments as they provide credit
to the customers running CI and pay the suppliers who the parts to repair broken CI equipment are sourced from.

Roles chosen outside of the Coventry Group were from suppliers (Mack Trucks and All Light) and customers (Alcoa and Esperance Port Authority).

Table 4.7

Participant Roles Outside of the Coventry Group

<table>
<thead>
<tr>
<th>Role</th>
<th>Participant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier of Truck Parts from Mack</td>
<td>10</td>
</tr>
<tr>
<td>Alcoa Purchasing Officer</td>
<td>12</td>
</tr>
<tr>
<td>Supplier of engine parts from All Light</td>
<td>13</td>
</tr>
<tr>
<td>Esperance Port Authority Purchasing Officer</td>
<td>16</td>
</tr>
</tbody>
</table>

The suppliers were chosen to understand how parts supply to the Coventry Group is affected when there is an information system failure. The customers were chosen as they are from different sectors in Western Australia’s CI and to understand how they are impacted when the Coventry Group has an information system failure.

The range of participants interviewed are involved in supply chain activities within Western Australia CI supply and range from the sending of parts to the Coventry Group from an external source (external suppliers), the processing of various transactions such as sales, purchasing, despatching, receivals and finance roles within the Coventry Group (internal roles within the Coventry Group), maintaining various information systems within the Coventry Group and customers receiving goods from the Coventry Group (customers).
4.6 Output

What does the system or services output?

Question 5

How would your products and services be affected in the event of the Coventry Groups information system failing? E.g. how would output be affected?

Table 4.8
 Participant Perceptions Summarized of how they would be affected in the Event of the Coventry Groups Information System Failing

<table>
<thead>
<tr>
<th>Response</th>
<th>Participant/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information system outage not causing a major disruption to</td>
<td>11, 12, 13, 14, 15,</td>
</tr>
<tr>
<td>trade</td>
<td>16, 17 &amp; 18</td>
</tr>
<tr>
<td>Information system outage causing a major disruption to trade</td>
<td>1, 2, 3, 4, 5, 6, 7, 8,</td>
</tr>
<tr>
<td></td>
<td>9 &amp; 10</td>
</tr>
</tbody>
</table>

This question polarised participant’s views the most. A theme from answers from participant’s 11, 12, 13, 14, 15, 16, 17 and 18 indicated there would be no great disruption in the event of an information system failure in the Coventry Group. The participants that held this perception were engaged in the buying or selling of parts as either an internal sales role, a supplier of parts to or customer of the Coventry Group. Staff that held internal sales roles within the Coventry Group (11, 14, 15, 17 and 18) indicated that manual procedures would be used to ship orders in the event of an information system failure. The roles these perceptions were provided were;

- Customer Service Representative at Coventry Fasteners (11)
- Supplier of engine parts (13)
- Business Development Manager (14)
- Branch Manager (15)
- Storeman (17)
- Coventry’s Parts Interpreter (18).

The responses in interviews 11, 12, 13, 14, 15, 17 and 18 saw the manual processes as just taking a little longer, with the biggest impact being the item missing a local
delivery run. Participants interviewed internally and eternally stated if there was any issue in getting a part due to a system failure the customer generally shops around and procures the item from one of Coventry’s competitors (11 and 12). The Coventry Group’s main competitor in automotive are AMCAP, Super Cheap Autos and Repco; in fasters the main competitor is Blackwood’s.

The views of staff directly involved in the selling and buying of goods contrasted with answers from the Information Services Department, a purchasing officer from the Overseas Buying Department and an assistant accountant, who viewed an information systems failure as being more catastrophic. The response from interview 2 (Procurement Officer Overseas Buying) and 5 (Assistant Accountant) may have been due to staff in these roles not having manual procedures to fall back on in the case of an information systems failure in the Coventry Group. This especially is the case for the assistant accountant who relies on an EDI interface to check that suppliers have been paid the correct amounts they are owed. The Procurement Officer Overseas Buying was placing orders on overseas suppliers, orders which take months to arrive into Australia. As he is not placing time critical orders, he does not utilize a manual purchase order back up system which other areas of the Coventry Group use.

In answers 1 to 10, the perception was that if the system was not available, the Coventry Group would not be able to do any transactions. The answer from interview 10 by parts supplier Mack Truck is contrasted with that of another supplier All Light in response 13, who sees no impact on supplying parts to the Coventry Group if there is an information system failure in the Coventry Group. Allight stated that they primarily supply goods to the Drivetrain branch within the Coventry Group, with this branch having a manual back up procedure in case of an information system failure. Once the system does come back, another system purchase order can be generated and referred to the manual purchase order.

Mack use a web based interface with the Coventry Group, so all their orders are placed using this method, so the Coventry Group would need to have at least a web link available to order parts from Mack Trucks.
Staffs that held the perception an information system would mean the Coventry Group could not trade held the following positions;

- Warehouse Management System Consultant (1)
- Procurement Officer Overseas Buying (2)
- System Administrator (3)
- Accounts Receivable Officer (4)
- Assistant Accountant (5)
- Communications Engineer (6)
- Database Administrator (7)
- Server Analyst (8)
- System Administrator for the Tandem System (9)
- Supplier of Truck Parts from Mack (10).
4.7 Efficiency, Effectiveness and Efficacy

How the participants would measure the success of a system that would be implemented to rectify an information system outage.

**Question 6**

How would the efficiency, effectiveness and efficacy be measured in any proposed system designed to cope with critical failures?

**Table 4.9**

Participant Perception Of how Efficiency, Effectiveness and Efficacy would be measured in an Ideal System

<table>
<thead>
<tr>
<th>Response</th>
<th>Participant/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of sales being the primary measure</td>
<td>1, 3, 4, 11 &amp; 14</td>
</tr>
<tr>
<td>Time down being the primary measure</td>
<td>2, 6, 8, 16 &amp; 18</td>
</tr>
<tr>
<td>Impact on customer service being the primary measure</td>
<td>15 &amp; 17</td>
</tr>
<tr>
<td>Having to but off alternate supplier being the primary measure</td>
<td>12</td>
</tr>
<tr>
<td>Items being supplied being the primary measure</td>
<td>16</td>
</tr>
<tr>
<td>Loss of data being the primary measure</td>
<td>7</td>
</tr>
<tr>
<td>Speed of recovered system being the primary measure</td>
<td>5</td>
</tr>
</tbody>
</table>

Responses 1, 3, 4, 11 and 14 saw the loss of sales as the primary measure to assess how effective a proposed system designed to cope with critical failures would be measured. Time down was seen as critical in answers 2, 6, 8, 16 and 18 saw time down as more important. The effect on customer service was the most important measure in answers 15 (Branch Manager) and 17 (Storeman). The two customers that responded had different perspectives on an outage.

The customers remarked that what was important was getting parts from the Coventry Group in a timely fashion. Alcoa (12) responded that the greatest impact to them was creating more unplanned purchase orders, as other suppliers outside Coventry’s would be used. The Esperance Port Authority (16) saw a bigger issue if the Distribution Centre in Perth did not send the goods, as this would cause greater delays to them rather than a manual docket being used in the event of an information system failure. Both customers did not perceive an information system failure within the Coventry
Group as having a major impact on their services as they could get the items on a manual invoice or procure the items from another vendor.

This observation is consistent with answers provided in 11, 13, 14, 15, 17 and 18 in question five which all mentioned that manual processes are used to supply goods when there is an information system failure. This indicates staff involved in selling goods or customers procuring goods does not see an information system failure group within the Coventry Group as a big issue in regards to Western Australia’s CI supply.

Respondent 7, a Database Administrator saw the loss of data as being the key measure and the assistant accountant saw the speed of the system once it was brought back up as the primary measure. He remarked the system is normally slow after an outage; the system was inefficient after an outage.

4.8 Transformations Summarized

This section aims to define what are the transformations in the system that generate a product or a service and how are they achieved? What can also be derived is how well are they performing and to avoid coming to early conclusions about what is important.

- (Transformation) the supply of spare parts to customers in various industries. The goal is providing the correct item to the customer the first time. This is done by interpreting the requirement, picking and shipping the item via various means
- The actors are staff, customers and suppliers of the Coventry Group
- The owners include shareholders and Coventry Group staff
- The environment: business locations within the Coventry Group, Coventry Group customers and Coventry Group suppliers. The customer’s environments include CI in various locations, workshops and external providers who they may have service agreements with to maintain their equipment
- The weltanschauung may involve company prosperity, rival competitors, profit margins and incorrect descriptions of items from customers leading to the wrong item being supplied by the Coventry Group, which may lead to an angry response from the customer.
4.9 Root Definition

A 'root is a well- defined statement about the area of concern, its activities and components. The ‘root definition’ formed from the participants answers to the questions posed is;

A system run for the benefit of Coventry Group’s customers and shareholders, run by Coventry Group staff to achieve spare parts and equipment supply to customers from the perspective of various spare parts, fastener and equipment supply within the constraints of part and equipment availability and controlled by nominated Coventry Group staff or third party providers.

The root definition derived has a very narrow focus on the Coventry Group, rather than the whole CI network. This can be seen in the root definition where the Coventry Group’s systems have been mentioned, but no mention of Western Australia’s CI network. The respondents did not perceive what a loss of parts and equipment supply would mean to this network overall. A reason why this narrow focus has been derived is the respondents in their day to day activities are focussed solely on their jobs; they have no visibility of how the items they are supplying, fit into the overall network.

In the case of the participants who responded that were engaged in selling, buying or supplying spare parts, their focus is on interpreting the customers description of the item required, this is what they are paid to do and the organisation has ingrained the belief if sales are going well, the company is doing well and the staff will be rewarded. When a customer rings up for an item, the detail of the piece of equipment that is broken down is provided. The respondents are just focussed on providing this item, if they have done that they have done their job. The only time a parts interpreter needs to think beyond this is when the customer has not asked for a related as part of an order e.g. if a customer has requested a bolt they would need a nut to fasten it, sometimes a customer may just ask for the bolt and not the nut. The parts interpreter needs to ask the customer if they need the nut to go with it.

The customer generally does not give the parts interpreter visibility of where the item fits in the whole CI network, unless this has been communicated to them by one of
their managers and the customer procuring the goods needs the items to be sent on the next available freight carrier.

The suppliers to the Coventry Group have a similar worldview, as they are also supplying parts to a customer. The customers interviewed were purchasing officers, whose main goal is to procure an item to get the equipment that is out of service repaired as quickly as possible. If the item is causing major inefficiencies then the purchasing officer may then gain knowledge of the importance of an item to the whole network. These perceptions are modelled in Appendix Three.

4.10 Conceptual Modelling

When a soft system analysis is normally conducted, a conceptual model of an ideal system is normally created. In the design section (section 3.2) it was stated this research did not intend to create an ideal model as the system was being deconstructed, to help understand the implications of a catastrophic failure in a node of Western Australia’s CI. The results also presented a very narrow view of the overall network; making the creation of an ideal conceptual model not meaningful.

An ideal system in the parts supply node of Western Australia’s CI can still be attempted (refer Appendix Four.). The ideal system would be a system that ensures the right item is interpreted, picked and shipped to the correct destination every time a piece of equipment in Western Australia’s CI network breaks down. This system may not be achievable when considering factors such as superseded items, varying equipment, logistic company’s delivering items and human activities within the system, such as varying degrees of knowledge and competencies. A desirable element for this system would be to contain a method to help actors in the system understand where the item that has been requested, fits into the whole CI network in Western Australia ideal system would need to provide this information.

The criteria for choosing and deciding what goes into this system would also be done. It should be understood that not all the actors would agree on everything or have the same power in making the decision. The question about efficiency, effectiveness and efficacy that measures any proposed system designed to cope with critical failures
gave an insight into the respondent’s perceptions of what an ideal system would contain. The results from the interview highlights this with the two most common perceptions being the loss of sales and time down the system the two most common themes in... Items not being supplied were the primary measure by one of the customers who was interviewed. One reason for this result was fourteen out of the eighteen participants were Coventry Group employees who say an information system failure as a threat to their jobs. The real issue with CI supply is getting the parts to the customer so the equipment can be repaired and brought back into service.
Chapter 5: Discussion of Results

5.1 Introduction
The data gathered using soft systems methodology aim to capture participant’s perceptions rather than being scientific in nature. These participant perceptions are collected to help the investigator understand the problem situation better when soft system modelling is used in research. This section of the paper compares what the participant’s perceptions were to what occurs in the real world and also links these perceptions to issues raised in the literature review.

5.2 Perceptions Matched to Reality
The perceptions gained from participants during this investigation found if the Coventry Group was removed from the network, the network would still be intact. The results from this inquiry indicated that there is enough redundancy resilience in the network to ensure the continuation of CI supply in the event this node was removed from this network.

Though the Coventry Group is the preferred supplier to many CI suppliers in Western Australia, there are various other local suppliers that supply the same product range and brands, with similar levels of parts expertise in their organisations. The Coventry Group may be the preferred supplier for many of these CI suppliers; these customers also hold accounts with other parts suppliers, who are also able to provide parts vital in repairing equipment used in Western Australia’s CI supply chain. If a supplier does not hold an account with a rival supplier to the Coventry Group, items can be bought in on a cash on delivery basis or bought in using another supplier’s account. Participants who were interviewed and involved in selling and buying parts within this network, indicated if one supplier could not supply an item, the customer will contact other suppliers to source an item.

When the perceptions were compared to what actually occurs, the perceptions and the reality matched. The perception from participants involved in selling and buying parts was if the information system in the Coventry Group was unavailable, manual processes are invoked to allow a continuation of services. This is the case in reality.
When the information system is down, branches revert to manual invoice books named Proforma Invoice Books to ship items to customers, there are manual purchase books used to procure items from suppliers and manual stock sheets that hold the location of each item kept in a branch are printed off in hard copy and kept in branch locations. Each branch has a file containing standard manual operating procedures in the instance of an information system failure.

The customer’s perception also matched reality, if an item is not available in the required time frame from the Coventry Group, the customer shops elsewhere. Alcoa pointed to the fact they maintain a spreadsheet of possible suppliers of parts they require in their refineries to reference, when a preferred supplier is unable to fulfil an order.

5.3 Network Redundancy and Resilience

There is also resilience in the system around the time it takes to get the system back up and running. The Coventry Group’s Information Services Department has service level agreements with suppliers to get systems back up in the instance of an information system outage. Within the Coventry Group a major information system outage is considered to be a couple of hours. The service levels are set, so that the majority of information failures can be rectified quickly and the system brought back up.

A comparison can be created between the Coventry Group being removed from Western Australia’s CI network and buying a book on the Internet. If the customer had traditionally bought their books online from Amazon, but if Amazon was removed from the World Wide Web, customers would need to use another online vendor to supply their books. Other online book vendors such as Dymocks and Angus and Robertson have access to the same supply chains that Amazon do, such as publication houses and logistic systems used to deliver books. Users would have to become accustomed to going to a different address to procure their books, using a different interface and possibly having search results listed in a different order.
If the Coventry Group was removed from Western Australia’s CI network, customers would simply move to other suppliers. As with the online book shop analogy, users may experience a period of discomfort using another supplier for various reasons. The customer may have formed a relationship with a specific customer service representative, delivery driver or sales representative in the Coventry Group that is familiar with the equipment the customer is using. The new supplier may have delivery runs may be not suit the customer’s requirements as well as the times used by the Coventry Group. The layout of invoices and statements may be different from the Coventry Group’s making reading and reconciling these documents more difficult. The items that the customer requires could still be sourced and equipment vital in providing CI services.

The resilience and redundancy in this network does create other implications. The first repercussion of the inbuilt resilience of the system is the interdependence of the system; this means people can go anywhere to procure their parts. A result of this interdependence is that people in this network do not see themselves as part of a wider system; they are only focussed on their role and their organisations role, which are the sale of parts and the continued profitability of the organisation.

This resilience has implications on the entire network. Organisations may not stock items which are vital in ensuring CI supply, only parts that are fast moving lines that will ensure profits will be stocked. As the participants do not see their place in the system, they will take no action to prevent the loss of parts supply to CI equipment. The overall network affect of not having these items is a risk to CI supply. From a theoretical network perspective, the break down of supply parts equipment to CI infrastructure can be interpreted as a cascading network failure.

An implication of this network analysis is the need of efficient relational risk management strategies to be designed. This redundancy can already be seen in some sectors of this node where contracts are kept with the Coventry Group and customers providing CI services. These contracts ensure vital parts required for keeping equipment running that provide CI services are stocked over a specified period, ensuring the contract between customer and supplier is kept binding.
Viewed from a theoretical network perspective, the nonlinearity of networks is vital in influencing the risk and the value of corporations, since the dynamics of information age companies are not smooth and linear, but rather disruptive and nonlinear (Kemper, n.d.). If adequate supplies of parts vital in servicing Western Australia’s CI, are not perceived by stakeholders as vital in maintaining the organisations profitability, these items may not be readily available in Western Australia. This would then alter the entire dynamic of Western Australia’s CI network.

The results in this investigation showed removing a mid sized company from Western Australia’s CI network would not affect the network. Though there appears to be a high degree of resilience and redundancy in this node of Western Australia’s CI network, do other areas of this network have the same resilience and redundancy?

Cases that illustrate the resilience and redundancy existing in CI networks are the speed at which the networks that were attacked in the 9/11, Madrid and London terrorist attacks (Matthew, et al, 2005) recovered. It was feared after the 9/11 attacks on the World Trade Centres in the USA, which were seen as a major hub for financial trading in the western world, the western world would plunge into a recession or depression. Though these terrorist attacks showed how vulnerable each node is in a network are to attack, they were not successful in bringing down the western worlds technological networks and financial systems or driving the west out the Islamic world.

In the literature review the similarities in network structure in the natural, social and technological worlds was presented, as was the importance of maintaining the integrity of networks. Granovetter (1973) theories relating to the existence of weak points or connectors in network structures, the role they play in connecting different nodes within a network and the possible impact of their removal on the network were highlighted in the literature review.

To illustrate his theories on the impact the removal of nodes in a network can influence an entire network where Granovetter used social networks to contextualize his findings. He stated that different nodes or links exist in network architecture, with these links being able to be considered as either strong or weak links. An example he
provided of a strong link in a social network were links between family members, good friends or people, who spend a lot of time together, like work colleagues or people who belong to the same associations such as sport clubs. Weak links or ties can be defined as acquaintances, or friends of friends. When the strong link is removed from a network there was little effect on the degrees of separation in a network, or the time taken to reach other nodes within the network. When a weak link was removed, the degrees of separation increased dramatically. He saw weak links serving the same function as bridges and roads do for travellers. These weak links are used to reduce the distance to any point within a network, making it quicker to reach another node within a network, as roads and bridges do for travellers. The use of weak links or connectors allows a network to be brought together as a whole, regardless of the size or amount of nodes in a network. Though many theorists had discounted the importance in network structures of weak or connector links, Granovetter saw these nodes or links as vital in a network continuing to function as a whole.

Granovetter theories poses the question of “what would happen to the integrity of Western Australia’s CI network if a node was removed?” as different nodes and links also appear in Western Australia’s CI network. These nodes can be seen in, but not limited to power generation, transport systems, emergency services, water supply and financial services. An example of the rearrangement of a network structure in the natural world leads us into the importance of maintaining network integrity and structure.

To turn water into ice, the cells in water simply rearrange their order. The molecular structure of each individual cell in ice is exactly the same as water, the structure of the cells or the network is all that changes when water becomes ice (Buchanan, 2002). A conclusion drawn from this investigation into the systemic effect the failure of the information systems of a medium size component supplier can have on the integrity of the critical infrastructure of Western Australia, found that the removal of the Coventry Group would have no great impact on Western Australia’s overall CI supply due to the redundancy and resilience that appears to be in this network.

The example of the rearrangement of cells or nodes in a network, turning water in ice provokes further discussion on this finding. If all that is required to turn water into ice
is to arrange the structure of cells in a network, wouldn’t the removing of a node such as the Coventry Group from Western Australia’s CI network change the structure of this network? Buchanan (2002) argues that by removing nodes in a network, nodes were faced the risk of loosing their connections to the network, becoming totally isolated and removed from the network. If the rearrangement of cells in water causes such a dramatic change as turning into water into ice could changes in Western Australia’s CI network potentially also cause issues with CI supply that are not readily identifiable?

Physics’ Albert, Jeong and Barabasi (2000) did further testing on the removal of nodes within a network; to understand what affect this has on a network. These physics’ see two types of network architecture in existence; random and scale free networks. Random networks are characterised by nodes being randomly linked together, with nodes having about the same number of connections as other nodes in the network. They provide the early Internet as being an example of a random network, as computers were linked together on a network in an unsystematic fashion. The other common network structure these physics’ perceive is what they term a scale free network.

Scale free networks are characterised by having well connected nodes known as hubs that are linked to a large number of nodes. Using the World Wide Web as an example, Google is a well connected hub on the World Wide Web, as this hub is linked to millions of other pages on the World Wide Web. A hub can also be seen in the Coventry Group too, as Distribution Centres are part of this organisations supply chain. Distribution Centres in the Coventry Group are used to receive in stock for the whole of a region from the organisations external suppliers and then distributes items to branches as they are required.

These physics’ conducted a series of tests to help them understand how the redundancy and resilience in the two different networks they identified were affected when nodes were removed. Both networks had redundancy built in (there are multiple paths to other computers within the network), with the same amount of computers and links between them.
These physics launched attacks on two different computer networks. The first test looked at the affect a random failure had on the two networks. This kind of failure could be brought about by an attack that was launched in an uncoordinated manner, or when computers breakdown in a network. The second test involved launching an attack in a more sophisticated and targeted manner, at the most highly connected hubs within the network.

The results from first test using the uncoordinated attack method on the random network found that when 28 percent of the elements were destroyed in the network, the network had collapsed into a collection of tiny, isolated subnetworks, even though 72 percent of computers were still up and running. Even though this random network had redundancy built allowing access to nodes within the network via various different paths, it fell apart quickly in the face of an uncoordinated assault. The scale free network managed much better in the face of the same attack. When the scale free network was attacked and half the nodes were removed, the network was still able to remain as an integrated whole, instead of shattering like the random network.

The second test using the highly coordinated attack was then launched, targeting key hubs in the network. The result of this type of attack on the scale free network found that destructing 18 percent of elements in network splintered the entire network into tiny fragments. The result of this sophisticated attack was the network was left fragmented into little, remote, non-functioning pieces. Surprisingly, the random network, which had splintered easily in the face of an uncoordinated attack, took longer to fragment in the face of a coordinated attack.

These physicists concluded from these tests that the highly connected hubs acted as glue within the network, holding the network together. They theorised that uncoordinated attack targets done in a random manner almost always knocks out unimportant elements that have few links, while missing the well connected hubs. Removing the well connected hubs proved to create the most damage to the networks attacked in these experiments.

What implications does this have for security strategists? The example from the natural world shows that changes in network structure can radically alter a networks
strength and form. The tests by the physics’ see that redundancy is not enough in a network, the well linked hubs within a network need to be protected. Recent terrorist attacks have been successful in attacking nodes within networks. The literature presented recent attacks such as 9/11, the Madrid, Bali and London bombings as being examples of these terrorist attacks. The literature also referred to theorists who believed these terrorist attacks posed a new threat to western societies, one their defence structures are not prepared to defend against.

The use of scale free networks in the western world has made it easy for terrorist organisations to attack and destroy individual nodes within these networks. However, the structure of these free scale networks that define the western world, could also provide strength in defending them.

5.4 Network Architecture

It is argued by Matthew and Shambaugh (2005) that existence of hubs in these networks aids the co-ordination and efficiency of defence. They sees the increased organisation, high level of coordination these free scale networks allow, provide the structure for western nations to mobilize their forces to defend and counter attack terrorist organisations. Mentioned earlier in this section was that search engine can be seen as key hubs on the World Wide Web, allowing the coordinate the efficient retrieval of information. By using free scale network structures, western forces are able to efficiently coordinate their defence resources and to launch counter attacks. By remaining in these network centric formations, he sees terrorists lacking the ability to efficiently coordinate their resources and maintain a sustained and successful attack on the west.

To promote his theory, Matthew and Shambaugh (2005) cite parallels in the organization structure used by current terrorist organisations and the structure used to lead forces during the medieval crusades. During the crusades, the Catholic Church brought together a diverse range of people, unified by common beliefs and values of recovering the holy lands. They see the crusades failed to have any success in recovering the holy lands over two centuries due to the lack of coordination and hierarchical structure that existed throughout these campaigns. Matthew and
Shambaugh (2005) also see terrorist groups also attempting to tie a diverse range of people together, often from dispersed geographical locations under a unified belief. By terrorist groups organizing themselves in dispersed, network centric structures, they risk having the same failure the leaders of the crusades experienced which was due to a lack of co-ordination and strong leadership. The co-ordinated structure the west uses distributed, can be seen in their response to the 9/11 terrorist attacks, where a “war on terror” was launched against terrorist organisations. Part of this “war on terror” was an invasion of Afghanistan by the USA and its allies as they identified al Qaeda’s key hubs residing here.

Recent reports estimated that about two-thirds of al Qaeda leaders have been either killed or captured. This result of this co-ordinated attack on al Qaeda key hubs has been to severely limit the amount of command and control that al Qaeda’s highest echelon can exercise over its far-flung cells (Gerges & Isham, 2003). Though terrorist can organise and launch attacks from various locations and attack nodes in targeted networks, the western world’s structure allows a coordinated mass to be assembled and mobilized. By organizing themselves in this manner, the west is able to remove highly influential hubs and cells in terrorist networks. Cells in the terrorist network may no longer see themselves being protected, in the face of these co-ordinated responses by the west, in the network centric structures they organized themselves into. If the terrorists cannot see themselves being protected by this network, cells may no longer feel mobilized to support al Qaeda’s principles.

5.5 Terrorist Attacks and Critical Infrastructure

The literature presented theories from analysts that the emergence of terrorist attacks has created a greater threat to CI? Enders and Sandler (2005) studied the instances of terrorist attacks pre and post 9/11 and found that the basic time series (e.g. the all-incident series, bombings and incidents with casualties) displayed no changes after 9/11. Incidents had remained at their low pre-9/11 levels but the nature of terrorist acts had changed. Previously complex hostage-taking missions and assassinations, sometimes yielding only a single victim, had characterised terrorist’s attacks. Terrorist attacks post 9/11 have been characterised by bombings to a far greater extent than ever before. They observed by making attacks appear to be random, terrorists have
threatened a larger audience and increased the public’s anxiety. This has a consequence on security strategists, as the targeted society must try to protect a wider range of vulnerabilities.

Apart from invading Afghanistan, another response by defense forces to the 9/11 terrorist attacks has been the tightening of security at airports, embassies and other attractive targets. As Enders and Sandler (2005) study points out, this response has had positive and negative impacts on security. Their study concluded that though there has not been an increase in attacks since these new security strategies have been put in place, there has been an increased reliance on bombings. Bombing attacks are easier to launch and can cause more damage than assassinations and hostage missions terrorists previously relied on. They also note that terrorists are quick to change their tactics, switching from intended targets that have been recently fortified to relatively softer targets. This indicates defence strategists in the west are focussed on protecting the key points within their networks and deflecting attacks to the weaker points in the network.

These findings indicate that Albert, Jeong and Barabasi (2000) theory that the key to overall network security, redundancy and resilience is to protect the key hubs that reside in the network. If terrorists are forced to target ‘softer’ targets, less damage should occur to the network, keeping the network intact.
Chapter Six: Conclusion

6.1 Introduction

The research question related to this study is:

What systemic effect can the failure of the information systems of a medium size component supplier have on the integrity of the critical infrastructure of Western Australia?

The research found an information system failure in the Coventry Group would not have a catastrophic effect on Western Australia’s CI supply. This conclusion is due to the redundancy the Coventry Group has built in their standard operating procedures through the use of manual procedures, which aims to minimize the disruption an information system failure causes to their customer service levels.

The Coventry Group has had to devise manual procedures because the legacy Cov Parts system that has recently been replaced by the Oracle 11i E-business Suite, had to be shut down regularly so system maintenance or stock takes could be performed. Maintenance work and stock taking occurred most commonly on weekends, branches still needed to trade, which led to manual processes being created to enable branches to trade when system outages occurred. Though labour intensive, the manual processes still allows an item to be ordered and despatched from a Coventry Group branch in the event of an information system failure and is a process most staff are familiar with.

6.2 The Coventry Group and Critical Infrastructure

A hub and spoke distribution network is utilized within the Coventry Group. This hub and spoke distribution method requires a distribution centre to carry the majority of the stock and the branch stock levels are replenished from these DC’s. The Coventry Group has an automotive distribution centre (at Morley with approximately one hundred thousand stock kept items worth $13 million) and a fastener distribution centre at Welshpool (approximately $4 million in stock).
Coventry Group branches hold smaller inventory values and stock items grouped by category (for example with the oil category, all oil is held in the same area of the warehouse, for items in the gearbox category, all gearbox items are kept in the same area). This makes it easier for staff to find items when there is an information system failure occurs in branches. An information system failure has a greater effect when a distribution centre is disrupted because of the amount of parts that are stocked and extra distance and time it takes to get to the warehouse.

Most large contracts the Coventry Group handles involving CI suppliers are done from their distribution centre, though some are handled at branches because of their geographically proximity to some sites. An information system failure would impact the customers who deal with distribution centres the most, which CI suppliers in Western Australia predominately do.

The main implication of a computer system failure is the time it takes to ship an item. For a local customer this may mean goods may miss a local delivery run, for a country customer this may mean the goods may miss the overnight freight run via truck or air freight, though this would mainly occur to orders that are phoned through late in the day. Physically checking stock and despatching an item on a manual invoice is an overhead to efficiency and customer service, especially in a large distribution centre, but not a reason to prevent an item that has been flagged as critical by a customer from being despatched.

If the inefficiency caused by a computer outage is contrasted with the delays caused by a vital component not being available, the effect of a system outage in the Coventry Group can be placed in a better perspective. The example of the non availability of a bearings can illustrates this point.

Bearings can be found in various applications used by Western Australia’s CI suppliers. Just a sample of the equipment that requires bearings to function includes:

- Centre bearings used on shafts that pump water out of Western Australia’s dams
• Bearings used in mills, heater heads and crushing machines used in refineries, mining and farming

• Mechanical applications such as engines, gearboxes, differentials, differentials, power take offs, pumps and wheel bearings in applications that make up the state’s transport infrastructure such as ships, ferries, buses, trains, rollers, tractors, earthmoving equipment, trucks, trailers and service vehicles.

Bearings can come in many different configurations and sizes. There are ball bearings, tapered roller bearings, sealed and unsealed, shielded and unshielded, bearings with or without circlip grooves, ones with different clearances e.g. C1, C2, C3 clearance (clearance in bearings is the space between each ball bearing, the bigger the clearance the better heat dissipation, so bearings with greater clearances should have a longer life) and spherical roller bearings to name a few different configurations. Bearings come in different sizes depending on their application, ranging from a tiny 6000 bearing that could be found in a fishing rod or in roller skates to giant bearings used in crushing machines.

The Customer Service Representative Coventry Fasteners, Business Development Manager and Branch Manager remarked that contracts to provide parts to many CI suppliers are put up for tender every year. One of the major factors in keeping contracts with these suppliers is fill rates (refer Appendix 2) with the supplier. These fill rates are monitored and the suppliers must maintain a specified level of supply over the length of the contract to keep the contract binding.

The bearing example highlights why fill rates are an important measure for customers providing CI services. In the case of a breakdown where a particular piece of equipment supplying CI services required a special sized bearing, the equipment may not be able to be used. This would be dependent on the nature of the breakdown. If the computer system was down and the special sized bearing is on the shelf, the bearing could be sent out on a manual docket.
Even if the item was not available off the shelf, and the item could be located, a manual purchase order could be raised on a supplier that had the item in stock, so the item could be supplied in an emergency.

If the item was not available, the options to supply the bearing take much longer to get the item supplied. When the Coventry Group is not able to supply a bearing from one of their Western Australian branches, other possible suppliers in Western Australia would be contacted and the item bought in and sent out to the customer. If no local suppliers were able to supply the component, the supplier of the item would need to be contacted to find out the availability of the item ex east. The bearings the Coventry Group sell are sourced from suppliers such as Timken (based in Ohio with a distribution centre in Melbourne), FAG (based in Germany with a distribution centre in Sydney) and Koyo (based in Japan with a distribution centre in Sydney). The item if available from the eastern states would be able to be despatched on an overnight air freight delivery unless the freight could be sent on a flight on the same day. By not having the item on the shelf or another local supplier having the item, there would most likely be a days down time at least.

If the item was not available from an eastern states location, the item would need to be freighted from an overseas location. Lead time quoted for overseas air freight is usually one week for emergency air freight orders. This is mainly due to the time it takes for an item to be cleared through customs.

An item that was not available from an overseas location would then have to be manufactured and depending on the engineering specifications of the item such as size and finish of the bearing, the time to manufacture the item may take months. In the very worst case scenario in the event of an information system failure within the Coventry Group, an item available off the shelf may miss a local delivery run or an overnight freight run. Items may also miss these despatch methods because of human error, so in the worse instance, the item may take a couple of days longer to get to its destination. If an item cannot be sourced in Western Australia, the best case scenario is a same day or overnight airfreight, to air freight ex overseas to having to be manufactured.
The type of equipment used in Western Australia’s CI and the availability of parts to repair the equipment is another issue that would need to be considered. There is redundancy built into the parts market when an item is not available. An example can be found using a fastener as an example. Fasteners are identified by such criteria as diameter, length, thread and finish. When a fastener was not available that was a certain diameter in width and length, a fastener that was longer could be used provided there was enough space to fit the fastener into. If there was not enough room, the longer fastener could be cut down and if a mild steel bolt was used, a high tensile nut would be used to fasten the piece of equipment. If there was no mild steel bolt, a high tensile bolt could be used and cut down and a button used to allow the nut to be put on. Just because the identical part is not on the shelf, there is a number of ways an item could be provided to allow the job to be finished.

There are other parts that are not as easy to work around to get a piece of equipment repaired as used in the fastener example. To use an example from truck parts a gearbox part not being available. All American trucks except Mack (who have their own running gear), use running gear supplied by another party. Ford, Stirling, Kenworth and International trucks can use engines supplied by Cummins, Caterpillar or Perkins, gearboxes supplied Eaton-Fuller or Spicer, axles supplied by Meritor, Eaton or Spicer and clutches supplied by Eaton. If any of these components broke down they would be able to be sourced from a number of local suppliers, not just from the Coventry Group’s truck division, Drive Train. If an item was critical to servicing Western Australia’s CI, but not available off the shelf locally or ex east, vehicles running this gear would have a number of other options.

If a gear was broken off a transmission and could not be sources in Australia, rather than having the vehicle off the road while the item was flown in from overseas or a new gear cut, the owner could get another gearbox of the same or different make to replace it. This could be done quite easily as long as the output ratio of the gearbox was similar to the one it was replacing, could handle the engine torque and could fit in the chassis rails of the truck. If the gearbox was longer or shorter, the driveline could be lengthened or shortened and if the holes for the bell housing did not match up on the flywheel, new holes could be redrilled. This may be an expensive way to get a
vehicle on the road again, but may be cheaper if was costing more to have the vehicle out of service.

If the truck was a Volvo, Mercedes Benz, Mack, Mitsubishi, Iveco or a Scania the parts for these trucks would be harder to source. These makes use original equipment parts which means the most parts are available as genuine only, so the replacement parts would need to be brought from the same place the vehicle was bought from, as there are not many alternative suppliers such as aftermarket suppliers of these parts. So there would be an onus on the fleet and equipment divisions that buy equipment that services Western Australia’s CI to buy units that have readily available parts supply or have the most inbuilt redundancy in their parts supply.

The participants indicated the CI suppliers did not care how they got their parts if it was from a parts person using a computer or a manual process, just as long as they got their parts in a timely manner. This worldview was also mirrored by Coventry Group sales staff.

6.3 Research and the Literature Reviewed

The literature reviewed presented the theory that vulnerability at a lower functional level of a network undermines safeguards at higher levels. The concept of weak links as important components in networks and the affect they have to network integrity was presented to develop this theme further.

The case study highlighted that parts availability was the key in maintaining and running equipment was essential in the continuation of CI production in Western Australia. CI suppliers need to be aware of the type of equipment they are running, their interdependence on the whole network and what parts and services are critical to ensure the equipment is in continuous service. The CI suppliers need to know if a piece of equipment was not available, would other CI services they provide be affected.

Another theme presented in the literature was that the most important assets should be secured; trying to stretch security across every node in a network is often not
achievable. CI protection is good example to illustrate this theory, as CI protection often requires networks which are stretched over vast geographical distances, to be secured. Does a gas pipeline in the northwest of Western Australia supplying gas to only a small population require the same protection as a section of pipeline that provides Perth with gas? Because of these vast distances, security strategists need to understand where the vital assets are in the network.

6.4 Further Research

This research concluded that an information system failure within the Coventry Group was unlikely to cause a major impact on Western Australia’s CI supply due to the redundancy inbuilt into this network. This redundancy can be seen by the use of manual back up procedures the Coventry Group has in its standard operating procedures and the redundancy that is intrinsic in parts supply. A simulated test on a two differently configured computer networks was conducted by Albert, Jeong and Barbasi (2000) concluded that building redundancy into a network is not enough, protecting the key hubs within a network was more important to keep the network functioning.

The strength that is offered in network in structures is the multiple pathways or alternative in the event of an attack against the network. This can be seen in the structure of networks where connectors or bridges are used to connect nodes within a network. Insights into the theory of complex interdependence suggests that even the network structure decreases the vulnerability interdependence of each node by providing it with alternative pathways to stay connected or navigate within the network, the network structure also increases the sensitivity interdependence of each node. This is due to each tying others into actions taken by or against others in the network (Keohane & Nye, 1977). Though this architecture provides resilience and redundancy within a network, individual nodes are still vulnerable to attack.

Network structure needs to be considered when CI protection formulating policies on security. To reduce vulnerability to CI in the USA, Anderson, et al. (1999b) recommended information infrastructures that are so important in maintaining CI
supply need to be given special thought, perhaps in the form of special hardening, redundancy, rapid recovery or other fortification or recovery instruments.

If research into network architecture has concluded an intelligent attack on key hubs within a network is able to cause major disruptions, rather than just random attacks to any part of the network, where would these disruptions need to target and how they impact the rest of a network? Further research into Western Australia’s CI could investigate where these critical hubs lie in Western Australia’s CI supply, or where are the choke points?

To use the parts supply example used in this research, if a gear critical to the unloading of ships was not available for an extended and ships were not able to unload, what impact would this have on Western Australia’s CI supply? Would certain foodstuffs not be available, certain medicines, certain heavy machinery vital to Western Australia’s supply chain activities? If a major arterial road was destroyed and along with a fleet of machinery used to repair roads, what consequence would this have on Western Australia’s CI supply? If a specially engineered part was not available to pump water from dams what would be the consequences elsewhere, would fires be able to be fought by the fire department, would agricultural activities cease, would drinking water be available, would disease spread due to the reduced hygiene? The USA’s overall electrical power grid is comprised of three sub-networks known as interconnections. One provides power to the eastern part of the USA, another to the west of the Rocky Mountains with Texas having their own sub-network (Buchanan, 2002). Is Western Australia’s power supply dependent on a major hub supplying this states energy? Are these power services provided by third parties and how secure do they keep their systems and equipment?

The critical dependencies lie in Western Australia and how would the failure of one node affect the rest of the network is worthy of further investigation. These are the relationships that would need to be investigated to fill in the gap in the research in the area of CI protection.

Human factors such as attrition rates in an organisation could also be further investigated, given the competitive labour market that exists today. Currently the
Coventry Group has a thirty percent attrition rate throughout the group and the automotive division in Western Australia has forty seven unfilled jobs in their workforce of six hundred staff. With such an attrition rate a lot of the tacit knowledge held in the organisation about parts that fit specialized equipment used by CI customers is lost. A greater risk to CI provider is the wrong part being sent out, especially to a remote location or ordering an item off a staff member that has not got the experience to know where to source an item from. The time it takes to source the item or to resend the item will mean the piece of equipment will be broken down longer than the inefficiency caused by an information system failure, as highlighted by the bearing sourcing example used in the previous section.

Contract agreements made between customers and suppliers are another area that could be further investigated. If an item the CI supplier new had the potential to break and would cause the shut down of a specific piece of machinery, the contract would between the Coventry Group and the CI supplier would need to ensure critical items would be available “off the shelf” at all times throughout the contract period. This would also mean that the maintenance departments in CI providers would need to be familiar with the key components that run the infrastructure they provide. There are many items in the Coventry Groups inventory that can only be sold to certain customers because of these contract agreements. If a customer brought new equipment, once again contracts would have to be revised to ensure components that were essential in the maintenance and running of the equipment were stocked.

The ability of the Coventry Group’s competitors to supply parts to Western Australia’s CI suppliers in the event of the Coventry Group not being able to supply parts is another area that could be further researched. This research could investigate if the Coventry Group for whatever reason were not able to ship any goods from their locations, would other parts suppliers have enough parts to ensure CI supply was maintained in Western Australia.

Further studies could be undertaken into an information system failure within The Office of Shared Services (OSS). OSS was established on 1 July 2005 to provide business services to general agencies of the Western Australian Government (excluding Health and Education & Training) and has 102 agencies on its umbrella
and 46,000 users. As the research undertaken in this investigation was aimed at a mid-sized company, research into the OSS system would fill the gap in knowledge related to an information system failure in a large organisation within Western Australia that is involved in CI services.

An idea presented in the literature review was around the similarity of the network architecture is present in different environments. Examples presented in this paper have been from the technological, natural and social environments. Research into the structure and of networks that exist in different environments and the defense mechanisms used to protect these networks, would add knowledge into the area of infrastructure security.
References


Plant Engineering, 59(4), 37-38.


Bibliography


Appendices

Appendix 1: Interview Answers Grouped by Participant
Appendix 2: Vendor Performance Chart
Appendix 3: Mind Map of Coventry Group Supply Chain
Appendix 4: Model of CI Node Coventry Group Resides In
Appendix 1: Interview Answers Grouped by Participant
## Appendix 1
### Interview Answers Grouped by Participant

In the tables below are the answers from the interviews. These answers have been grouped by participant. The first table references the question number to the question. The tables following this have the participant’s answers.

<table>
<thead>
<tr>
<th>Question Number</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>What services and products does your company provide? (What area of CI is being affected?)</td>
</tr>
<tr>
<td>2</td>
<td>In the event of an information system failure in the Coventry Group who would be affected both inside and outside Coventry’s?</td>
</tr>
<tr>
<td></td>
<td>What services do these entities provide?</td>
</tr>
<tr>
<td>3</td>
<td>Who would be involved in rectifying any system outage?</td>
</tr>
<tr>
<td></td>
<td>What extra resources would they need?</td>
</tr>
<tr>
<td></td>
<td>Would these be readily available?</td>
</tr>
<tr>
<td>4</td>
<td>What worldview/perspective are you taking? E.g. supplier, customer, internal staff member at Coventry’s</td>
</tr>
<tr>
<td>5</td>
<td>How would your products and services be affected in the event of the Coventry Groups information system failing? (E.g. how would output be affected?)</td>
</tr>
<tr>
<td>6</td>
<td>How would the efficiency, effectiveness and efficacy be measured in any proposed system designed to cope with critical failures?</td>
</tr>
<tr>
<td>Participant Number 1</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Question Number</strong></td>
<td><strong>Response</strong></td>
</tr>
<tr>
<td>1</td>
<td>Automotive spare parts, so mainly transport, mining and council maintenance vehicles</td>
</tr>
<tr>
<td>2</td>
<td>External and internal customers (internal customers are branches that have parts sent to them from the DC) Suppliers</td>
</tr>
<tr>
<td>3</td>
<td><strong>Who would be involved in rectifying any system outage?</strong> Oracle Business as Usual Support Team for oracle related issues Coventry Groups Server Team for other issues Dematic they supply the conveyor system at the distribution centre Datanet (for support around the picking and despatching scanners) <strong>What extra resources would they need?</strong> Oracle Support may need someone to restart a database. These resources are readily available as they are full time employees of the Coventry Group Coventry Groups Server Team may need to get an external supplier to start an application. These resources are readily available as they are full time employees of the Coventry Group</td>
</tr>
</tbody>
</table>
4  Warehouse Management System Consultant

5  Unable to supply goods from a Distribution Centre. Branches and customers have items despatched from a distribution centre and each state has a distribution centre

6  Sales would be the primary measure

   There would be a temporary loss of sales and the potential for ongoing lost sales because a customer gets upset with Coventry’s service

   The amount of returns could also be a measure, because items are sourced elsewhere because it took longer for Coventry’s to send out the part than a competitor because the system was down
<table>
<thead>
<tr>
<th>Question Number</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fasteners, tools, protective clothing, general equipment, loctite, hand cleaner</td>
</tr>
<tr>
<td>2</td>
<td>Customers, suppliers, staff in branches</td>
</tr>
<tr>
<td><strong>What services do these entities provide?</strong></td>
<td>Mining, critical infrastructure, building, transport, engineering</td>
</tr>
<tr>
<td>3</td>
<td><strong>Who would be involved in rectifying any system outage?</strong></td>
</tr>
<tr>
<td></td>
<td>Oracle Business as Usual Support Team, as no suppliers using an EDI interface</td>
</tr>
<tr>
<td><strong>What extra resources would they need?</strong></td>
<td>Only require the Oracle application to work.</td>
</tr>
<tr>
<td><strong>Would these be readily available?</strong></td>
<td>As there is a full time business as usual support team, these are readily available</td>
</tr>
<tr>
<td>4</td>
<td>Procurement Officer Overseas Buying</td>
</tr>
<tr>
<td>5</td>
<td>Purchasing officer can’t order parts, so could not send an order</td>
</tr>
<tr>
<td></td>
<td>There are no manual purchase order books to order parts. An email can be sent advising a supplier the system is down but the suppliers need an order number due to supplier contracts</td>
</tr>
<tr>
<td>6</td>
<td>Time down and speed of the system after a failure (the system is normally slow after a breakdown)</td>
</tr>
<tr>
<td>Participant Number 3</td>
<td>Question Number</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>6</td>
</tr>
<tr>
<td>Participant Number 4</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>---</td>
</tr>
<tr>
<td><strong>Question Number</strong></td>
<td><strong>Response</strong></td>
</tr>
</tbody>
</table>
| 1                    | Supply of credit to customers involved in critical infrastructure  
This would allow customers involved in CI to purchase items to keep parts of CI maintained and functioning  
Customers from CI are in mining, transport, councils |
| 2                    | Customers could not order any goods, customer account balances would be wrong if manual orders had been taken, customers may have been supplied items when they were on credit hold.  
Internally branches would not get orders; sales staff could not process sales orders. This would affect accounting, as no revenue would be generated. |
| 3                    | **Who would be involved in rectifying any system outage?**  
The Information Services Department would need to be contacted to rectify an outage  
What extra resources would they need? Would these be readily available? |

What services do these entities provide?  
Mining, transport, industrial
The Information Services Department is responsible for most IS functions and there is a full time support team available. Not sure who the support team contacts otherwise, bank maybe for accounts receivable?

<table>
<thead>
<tr>
<th></th>
<th>Accounts Receivable Officer</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Could not provide credit to our customers</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Loss of customers, loss of sales, time the system was down</td>
<td></td>
</tr>
<tr>
<td>Question Number</td>
<td>Response</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Automotive and industrial parts</td>
<td></td>
</tr>
</tbody>
</table>
| 2               | Suppliers  
|                 | Sales staff  
|                 | Customers  
|                 | Shareholders  
|                 | Stock market (investors may think the company has liquidity problems) |
| 3               | **Who would be involved in rectifying any system outage?**  
|                 | Coventry Group Information Services Department or Corporate Online  
|                 | **What extra resources would they need?**  
|                 | **Would these be readily available?**  
<p>|                 | The Desk bank help desk may need to be run; there is a specialist resource for the Coventry’s account, so readily available |
| 4               | Assistant Accountant |
| 5               | Suppliers could not be paid, this leads to Coventry’s being put on stop credit by the suppliers |
| 6               | Speed needed to get the system back up e.g. if the system is down one day that would be ok, if it was a week, there would be big problems especially for stock levels of fast moving items |</p>
<table>
<thead>
<tr>
<th>Question Number</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Automotive parts, industrial parts, mining supplies</td>
</tr>
<tr>
<td>2</td>
<td>Staff in the Coventry Group and external stakeholders e.g. customers, suppliers</td>
</tr>
<tr>
<td>3</td>
<td><strong>Who would be involved in rectifying any system outage?</strong></td>
</tr>
<tr>
<td></td>
<td>Dependent on the outage, could be Iinet (for the Internet), Datanet (for scanners), Macquarie (phones), Terrius and Cisco (hardware). The Coventry Group Communications Team could rectify this at a first support level e.g. if a cable was unplugged this could be rectified at first level support</td>
</tr>
<tr>
<td></td>
<td><strong>What extra resources would they need?</strong> This is dependent on the fault. Could require a communications engineer, hardware engineer. If the supplier could not fix at a second level, they raise this to another level internally.</td>
</tr>
<tr>
<td></td>
<td><strong>Would these be readily available?</strong> Service level agreements mean these services are readily available</td>
</tr>
<tr>
<td>4</td>
<td>Communications Engineer</td>
</tr>
<tr>
<td>5</td>
<td>If there are interdependencies between applications there could be no orders received (if the telephone was down), no Internet would mean no Oracle so know transactions would be performed on the application so no sales, purchasing etc.</td>
</tr>
<tr>
<td></td>
<td>No internet would also mean any email orders</td>
</tr>
<tr>
<td>6</td>
<td>Time down would be the main measure</td>
</tr>
<tr>
<td></td>
<td>Cost could also be the main measure. The reason for this is if there was a redundant link (which there is not) there would need analysis of how much this redundant link costs and how often it was used, so a cost needs analysis would be needed</td>
</tr>
<tr>
<td>Question Number</td>
<td>Response</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>1</td>
<td>Automotive, mining &amp; industrial supplies</td>
</tr>
</tbody>
</table>
| 2               | Employees, customers, suppliers.  
**What services do these entities provide?**  
Employees: servicing our customers & processing transactions regarding sales etc.  
Customers who supply different services e.g. mechanical, critical infrastructure maintenance  
Suppliers |
| 3               | **Who would be involved in rectifying any system outage?**  
This is dependent on the outage. Oracle business as usual is able to resolve hardware, UNIX and application issues on the “live hardware”. Disaster recovery is outsourced to IBM.  
**What extra resources would they need?**  
Service/support from any services which are outsourced by us.  
The disaster recovery is maintained by IBM. IBM are required to get the disaster recovery up in four hours.  
**Would these be readily available?** There are service level agreements, so these resources are readily available |
<p>| 4               | Database Administrator |
| 5               | Unable to maintain continuity of the application(s) used by the business to perform transactions |
| 6               | Loss of data |</p>
<table>
<thead>
<tr>
<th>Participant Number 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question Number</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>
| 2                 | Internally: All employees who rely on computers  
                      Externally: customers, suppliers, dealers, I store users (I Store is the company’s electronic catalogue) |
| 3                 | **Who would be involved in rectifying any system outage?**  
                      Internally would be the Server analyst for Intel and Windows based boxes.  
                      Externally:  
                      Microsoft looks after the servers  
                      Computer Associates (CA) resolve issues around EDI interfaces and help desk software such as the Beagle application  
                      CDM for hardware under licence or out of warranty hardware  
                      Talent2 resolves payroll issues  
                      Axiant would be involved in restoring the right fax application  
                      Alphawest resolve network issues and issues with Office Scan software  
                      Trend would be used to resolve any issue around the anti virus software  
                      **What extra resources would they need?**  
                      **Would these be readily available?** |
This is dependent on the outage. Some issues can be resolved at first level support, some need to be escalated to second level support. There are service level agreements that require any suppliers to resolve an outage within a specified time period.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Server Analyst</td>
</tr>
<tr>
<td>5</td>
<td>If the domain control fails, users will not be able to log into their computers, so there would be no processing done on any applications. On the front end there are smaller issues such as loss of access to the web services, file services and print services.</td>
</tr>
<tr>
<td>6</td>
<td>How quickly it takes for DR activated</td>
</tr>
<tr>
<td></td>
<td>How much data was lost on the file servers</td>
</tr>
<tr>
<td></td>
<td>How many orders were lost for the EDI servers</td>
</tr>
<tr>
<td></td>
<td>How many orders were lost for the fax server</td>
</tr>
<tr>
<td>Question Number</td>
<td>Response</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>1</td>
<td>Customer facing and background functionality for daily sales, accounting and inventory for CP, CA, CS, FL and UQ (these are the business units still on the legacy system)</td>
</tr>
<tr>
<td>2</td>
<td>Internal group and branch customers accessing CovParts for work. This would have an indirect effect on customer service</td>
</tr>
</tbody>
</table>
| 3               | **Who would be involved in rectifying any system outage?**  
Tandem System Support (myself, -f/t) and/or CovParts Application Support (Lois Parsons, -p/t availability).  
**What extra resources would they need?**  
**Would these be readily available?**  
Extra resource may include HP Hardware and Software support plus engineer support; -these are all contracted and accessible. System support may also require ad hoc assistance from p/t contractor Rod Carter or other f/t IS Staff. |
| 4               | System Administrator for the Tandem System |
| 5               | The Tandem server relies heavily on network stability. EU PC functionality is required but these failures would be localised |
| 6               | System availability  
Application availability |
<table>
<thead>
<tr>
<th>Question Number</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Meritor differential parts, trailer parts, Eaton Fuller gearbox parts, Hella electrical parts, Narva electrical parts, BPW trailer parts, some Mack genuine parts, Timken bearings, Hendrickson suspension parts, Horton engine fan clutch parts (cools the engine)</td>
</tr>
</tbody>
</table>
| 2               | As a supplier, Mack would not receive any orders for parts  
Also Coventry’s customers won’t get parts as they would not be able to be ordered from the supplier (Mack)  
Services are mainly transport and logistics |
| 3               | Who would be involved in rectifying any system outage?  
What extra resources would they need?  
Would these be readily available?  
The purchasing department at the Coventry Group would contact their Information Services department for issues with the Oracle system  
Oscar at Reynolds and Reynolds would be contacted for the Mack online EDI interface which is web based  
Currently no interface exists between the Oracle system at Coventry’s and the Mack EDI system |
| 4               | Supplier of Truck Parts from Mack |
| 5               | No purchase orders would be received from Coventry’s, so no truck parts supplied |
| 6               | Mack would check their Cognos system to check how much the Coventry Group was spending (normally $200,000 a month)  
Emergency daily sales orders could not be processed  
E.g. if there was a breakdown and an emergency order had to be placed on a supplier, this could not be done and the vehicle would remain down. The customer may be forced to another supplier who could order that part from the original
equipment supplier.

The greatest effect would be to gearbox breakdowns (purchased from Eaton in Melbourne), clutch parts (purchased from Eaton in Melbourne), differential breakdowns (Meritor in Melbourne) and suspension breakdowns (Hendrickson in Melbourne).

The main criteria would be how much Coventry’s spent with Mack.
<table>
<thead>
<tr>
<th>Question Number</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fasteners and abrasives are the products sold by Coventry Fasteners. Coventry Fasteners have a number of contracts with mining companies including Alcoa, Pilbara Iron (Rio Tinto).</td>
</tr>
<tr>
<td>2</td>
<td>Every customer would be affected as unable to check price, unable to check stock and unable to check what’s on order with a supplier. The mining companies that have contracts with Coventry’s Fasteners are involved in mining and the refining of minerals they mine (supply fasteners for Alcoa’s refinery).</td>
</tr>
</tbody>
</table>
| 3               | **Who would be involved in rectifying any system outage?**  
**What extra resources would they need?**  
**Would these be readily available?**  
Log an incident with Coventry’s Information Service Department, no external providers need to be contacted as no suppliers use an EDI interface with Coventry Fasteners. |
<p>| 4               | Customer Service Representative Coventry Fasteners |
| 5               | Fasteners could not be supplied to customers. This would affect Alcoa’s refinery. The fasteners on the contract fit the heater heads, mill ends, basically everything in the refinery. If the items are on contract with Coventry Fasteners they have to buy from Coventry Fasteners. The Alcoa contract is for 600 to 800 lines in fasteners, but Alcoa do source also from Blackwoods (opposition company) if Coventry’s cannot supply. |
| 6               | Other measure lost sales over the month or how busy you are, if you are not busy customers may have gone to the opposition. The way to check if Alcoa had been affected is by number sequence, as if there is a big break in the number sequence, Alcoa have bought off another supplier. |</p>
<table>
<thead>
<tr>
<th>Question Number</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mining and the refining of alumina (mining and refining of aluminium is done in the eastern states)</td>
</tr>
<tr>
<td>2</td>
<td>The supply of parts to refinery and mines for Alcoa</td>
</tr>
<tr>
<td></td>
<td>Mining alumina is what services Alcoa provide</td>
</tr>
</tbody>
</table>
| 3               | Who would be involved in rectifying any system outage?  
|                 | What extra resources would they need?  
|                 | Would these be readily available? |
|                 | No EDI interface exists so email is used. There is no Business to business interface between Alcoa’s Oracle system and  
|                 | Coventry’s Oracle system |
|                 | If Coventry’s email failed they contact their Information Services department internally  
<p>|                 | If Alcoa’s email, fails then Alcoa’s Information Services is contacted |
| 4               | Alcoa Purchasing Officer |
| 5               | Advanced shipping notices would not be sent from Coventry’s. This would mean a receipt would not be created, so no paid vendor receipt is created, so no payment would be made when the payments terms were met. Coventry’s would eventually put Alcoa on stop credit as Alcoa would not have paid their bill from Coventry’s |
|                 | Excel spreadsheet is used to buy off, so as long as the spreadsheet is accessible, Alcoa know where to buy certain items |
| 6               | How many adhoc purchase orders were created is how this would be measured. Rather than buying off Coventry’s as their system was down, other suppliers would be used to procure items |</p>
<table>
<thead>
<tr>
<th>Question Number</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Engine parts for Perkins (Perkins engines are trucks, rollers etc), Alllight parts for lighting towers, Perkin Sabre engine parts (Sabre are marine engines), Godwin parts (Godwin are mobile dewatering vehicles), portable generator parts</td>
</tr>
</tbody>
</table>
| 2               | Alllight would not receive orders, so Coventry’s would not receive parts  
Coventry’s customers that would be affected are customers who use parts that Alllight supply  
Services would vary depending on what machinery was being operated |
| 3               | Who would be involved in rectifying any system outage?  
What extra resources would they need?  
Would these be readily available?  
As orders received from Coventry’s are via phone or fax, Alllight would contact their fax or phone providers.  
Alllight has an IT department based in Sydney and recently an IT staff member has started at Alllight in Perth  
Coventry’s would contact their own IT and communications providers |
| 4               | Supplier of engine parts from All Light |
| 5               | As purchase order numbers are rung through to Alllight and Drivetrain have a manual back up procedure in case of system failure, there is not a great impact when the system fails. Once the system does come back, another system purchase order can be generated and referred to the manual purchase order |
| 6               | After a month if no orders would be received, Alllight would be concerned that there was an issue with Coventry’s  
Coventry’s and Drivetrain (Drivetrain are a division of Coventry’s specialising in heavy duty truck parts) however are stocking a lot of fast moving items now, so only emergency orders for parts that are not stocked at Coventry’s would be affected. So it would take a while for Alllight to notice a major system outage at Alllight |
<table>
<thead>
<tr>
<th>Question Number</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fastener supplier</td>
</tr>
</tbody>
</table>
| 2               | Major contract customers with Coventry Fasteners would be affected  
Other customers won’t receive goods  
Internal staff at the Coventry Group  
Biggest issue would be a cash flow issue for the Coventry Group as Coventry’s would not get paid as contract customers won’t receive advanced notice of orders that are to be shipped  
Major contracts are with mining companies such as Pilbara Iron (part of Rio Tinto), Worsley and Alcoa who provide mining services |
| 3               | **Who would be involved in rectifying any system outage?**  
**What extra resources would they need?**  
**Would these be readily available?**  
Coventry IS department if the system failure is to do with Oracle  
Fax orders are the way orders are sent from major contracts, so the communications team if failure is related to the fax machine |
| 4               | Business Development Manager |
| 5               | Customers don’t get goods on time, major contracts could be at risk because contracts are measured on KPI’s such as lead times and fill rates  
Rio Tinto is currently upgrading their material numbers from the 25th of August to the 3rd of September, so their system has been down. Critical emergency orders are manually raised and sent through, so mitigating the risk of down time on critical machinery |
<p>| 6 | How are levels of customer service affected |
|   | Speed and accuracy of the system           |
|   | Fill rate off the shelf                   |
|   | Ability to retain major contracts         |</p>
<table>
<thead>
<tr>
<th>Question Number</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fasteners</td>
</tr>
<tr>
<td>2</td>
<td>Internal staff is affected the most. When the system goes down, internal staff gets the most harassment from customers waiting for goods as the manual system is slower than Oracle. Customers offer various services, Worsley are involved in alumina mining.</td>
</tr>
<tr>
<td>3</td>
<td>Who would be involved in rectifying any system outage? What extra resources would they need? Would these be readily available? Coventry’s would contact their internal Information Services Department. They have their own service levels internally.</td>
</tr>
<tr>
<td>4</td>
<td>Branch Manager</td>
</tr>
<tr>
<td>5</td>
<td>When the system crashes, the impact is more on us as a business as our customer’s perception of our service level is directly related to our profitability. Harder to get parts out on the manual system, so effects customers getting their parts.</td>
</tr>
<tr>
<td>6</td>
<td>KPI measured by Worsley (document sent with KPI’s)</td>
</tr>
<tr>
<td>Question Number</td>
<td>Response</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>1</td>
<td>Shipping port</td>
</tr>
<tr>
<td>2</td>
<td>Esperance Port would be affected. Service includes the loading and unloading of ships carrying various cargo e.g. nickel, wheat</td>
</tr>
<tr>
<td>3</td>
<td>Who would be involved in rectifying any system outage? What extra resources would they need? Would these be readily available? Coventry's would contact their internal Information Services Department. They have their own service levels internally.</td>
</tr>
<tr>
<td>4</td>
<td>Esperance Port Authority Purchasing Officer</td>
</tr>
<tr>
<td>5</td>
<td>Operations that involve Coventry's parts in Esperance Port Authorities operations, not critical to unloading of ships</td>
</tr>
<tr>
<td>6</td>
<td>Not a big issue as long as a manual docket can be provided with a price, that is all that is required for the Esperance Port to receive goods in, manual dockets are accepted. A bigger issue is parts not being supplied or parts not being sent from the warehouse in Perth to Esperance. This causes greater delays than the system being down as manual dockets are used.</td>
</tr>
<tr>
<td>Participant Number 17</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>--</td>
</tr>
<tr>
<td><strong>Question Number</strong></td>
<td><strong>Response</strong></td>
</tr>
<tr>
<td>1</td>
<td>Auto parts, truck parts, household goods, cleaners, oil, general consumables (fly spray etc)</td>
</tr>
<tr>
<td>2</td>
<td>Customers</td>
</tr>
<tr>
<td></td>
<td>Suppliers</td>
</tr>
<tr>
<td></td>
<td>Staff</td>
</tr>
<tr>
<td></td>
<td>Various services are supplied by customers such as the Shire, transport companies, earthmoving companies, mechanics, port authority, car dealerships, trade customers, retail customers, Co-operative Bulk Handling, farmers</td>
</tr>
<tr>
<td>3</td>
<td><strong>Who would be involved in rectifying any system outage?</strong></td>
</tr>
<tr>
<td></td>
<td><strong>What extra resources would they need?</strong></td>
</tr>
<tr>
<td></td>
<td>The Information Services Department are rung to rectify computer issues.</td>
</tr>
<tr>
<td></td>
<td><strong>Would these be readily available?</strong></td>
</tr>
<tr>
<td></td>
<td>Yes there is a permanent IS department at Coventry’s</td>
</tr>
<tr>
<td>4</td>
<td>Storeman</td>
</tr>
<tr>
<td>5</td>
<td>Manual procedures are used to ship items</td>
</tr>
<tr>
<td>6</td>
<td>Dependent on whom the customer is. Would be a different measure on who the customer was e.g. a transport company or mechanical workshop would be dependent on speed on getting items to customer as the vehicle would need to get back on the road.</td>
</tr>
<tr>
<td></td>
<td>For a retail customer this would be less of an issue as the job may be done on the weekend</td>
</tr>
<tr>
<td></td>
<td>Main measure is customer service as the customer does not care if the system is down, they just want their parts</td>
</tr>
<tr>
<td>Question Number</td>
<td>Response</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>1</td>
<td>Auto parts, truck parts, mining parts</td>
</tr>
<tr>
<td>2</td>
<td>Internal staff, customers and suppliers</td>
</tr>
</tbody>
</table>
| 3               | Who would be involved in rectifying any system outage?  
|                 | What extra resources would they need?  
|                 | Would these be readily available?  
|                 | Ring Coventry Group IS Department |
| 4               | Coventry’s Parts Interpreter |
| 5               | Manual docket used to get parts to customer |
| 6               | Time down |
Appendix 2: Vendor Performance Chart
## Vendor Performance - 2006

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Coventry Fasteners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plant</td>
<td>(All)</td>
</tr>
<tr>
<td>Buyer</td>
<td>(All)</td>
</tr>
<tr>
<td>Status</td>
<td>(All)</td>
</tr>
<tr>
<td>Agreement</td>
<td>(All)</td>
</tr>
<tr>
<td>Order Category</td>
<td>(All)</td>
</tr>
<tr>
<td>Order Type</td>
<td>(All)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Years</th>
<th>Month</th>
<th>Average of Days Delivery</th>
<th>% Late Items</th>
<th>% In Full</th>
<th>No. of Expedites</th>
<th>% Expedite Rate</th>
<th>No. of Invoice Discrepancies</th>
<th>% Invoice Discrepancies</th>
<th>No. of Receipt Exceptions</th>
<th>% Receipt Exceptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>Jun</td>
<td>5.9</td>
<td>16.0%</td>
<td>95.4%</td>
<td>19</td>
<td>14.5%</td>
<td>0</td>
<td>0.00%</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td></td>
<td>Jul</td>
<td>4.9</td>
<td>11.3%</td>
<td>98.8%</td>
<td>21</td>
<td>18.3%</td>
<td>1</td>
<td>0.87%</td>
<td>2</td>
<td>1.7%</td>
</tr>
<tr>
<td></td>
<td>Aug</td>
<td>5.3</td>
<td>9.1%</td>
<td>96.4%</td>
<td>32</td>
<td>19.4%</td>
<td>3</td>
<td>1.82%</td>
<td>2</td>
<td>1.2%</td>
</tr>
<tr>
<td></td>
<td>Sep</td>
<td>7.1</td>
<td>16.8%</td>
<td>98.3%</td>
<td>41</td>
<td>34.5%</td>
<td>5</td>
<td>4.20%</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td></td>
<td>Oct</td>
<td>5.7</td>
<td>16.3%</td>
<td>94.8%</td>
<td>39</td>
<td>22.7%</td>
<td>2</td>
<td>1.16%</td>
<td>2</td>
<td>1.2%</td>
</tr>
<tr>
<td></td>
<td>Nov</td>
<td>9.6</td>
<td>24.3%</td>
<td>95.6%</td>
<td>76</td>
<td>42.0%</td>
<td>3</td>
<td>1.66%</td>
<td>5</td>
<td>2.8%</td>
</tr>
<tr>
<td></td>
<td>Dec</td>
<td>31.5</td>
<td>81.1%</td>
<td>75.0%</td>
<td>104</td>
<td>63.4%</td>
<td>4</td>
<td>2.44%</td>
<td>30</td>
<td>18.3%</td>
</tr>
<tr>
<td>2006</td>
<td>Jan</td>
<td>16.2</td>
<td>71.3%</td>
<td>83.6%</td>
<td>82</td>
<td>67.2%</td>
<td>9</td>
<td>7.38%</td>
<td>14</td>
<td>11.5%</td>
</tr>
<tr>
<td></td>
<td>Feb</td>
<td>8.1</td>
<td>32.8%</td>
<td>90.4%</td>
<td>31</td>
<td>24.8%</td>
<td>17</td>
<td>13.60%</td>
<td>5</td>
<td>4.0%</td>
</tr>
<tr>
<td></td>
<td>Mar</td>
<td>9.3</td>
<td>34.3%</td>
<td>91.0%</td>
<td>38</td>
<td>28.4%</td>
<td>6</td>
<td>4.48%</td>
<td>6</td>
<td>4.5%</td>
</tr>
<tr>
<td></td>
<td>Apr</td>
<td>14.8</td>
<td>48.7%</td>
<td>86.7%</td>
<td>91</td>
<td>57.6%</td>
<td>9</td>
<td>5.70%</td>
<td>5</td>
<td>3.2%</td>
</tr>
<tr>
<td></td>
<td>May</td>
<td>9.5</td>
<td>42.4%</td>
<td>90.9%</td>
<td>78</td>
<td>47.3%</td>
<td>5</td>
<td>3.03%</td>
<td>5</td>
<td>3.0%</td>
</tr>
<tr>
<td>Grand Total</td>
<td></td>
<td>10.9</td>
<td>34.0%</td>
<td>91.0%</td>
<td>652</td>
<td>37.2%</td>
<td>64</td>
<td>3.66%</td>
<td>77</td>
<td>4.4%</td>
</tr>
</tbody>
</table>

*Note: Invoice discrepancies must exist for at least 24 hours to be captured.*
Appendix 3: Conceptual Model of Respondents Perceptions
Receive items and equipment to repair broken equipment from the Coventry Group.

Pay Coventry Group for items purchased.

Receive purchase orders from the Coventry Group and ship items back to the Coventry Group or direct to customers depending on the shipping instructions.

Coventry Group
Supplies system to stakeholders to allow transformations in the system such as sales processing to occur

Customers
Supply parts and equipment to customers

Internal Sales Staff

IS Department
Coventry Group IS Department contacted in the event of an information system outage. If Coventry Group IS Department unable to restore service, external provider contacted.

Staffs revert to manual processes in the event of an information system outage.

Suppliers
External IS provider contacted. Required to restore services in the time specified in the service level agreement.
Appendix 4: Conceptual Model of Critical Infrastructure Node
the Coventry Group Resides In
Model of the Critical Infrastructure Node the Coventry Group Resides In

**CI Equipment**
- Despatch goods to CI equipment in need of repair or servicing.

**Customers**
- Request items to be supplied to repair or maintain CI equipment to allow the continuation of CI services in Western Australia.

**Internal Sales Staff**
- Supply various CI services to Western Australia.
- Supply parts and equipment to CI suppliers in Western Australia.

**Coventry Group**
- Supplies resources such as staff, parts and equipment that allow CI systems in Western Australia to be repaired and serviced. These services allow the continuation of CI supply in Western Australia.

**Western Australia’s CI Customers**
- Supply various CI services to Western Australia.
- Purchase items from suppliers that are not in stock in the Coventry Group for the repair or maintenance of CI equipment.

**Suppliers**
- Supplies resources such as staff, parts and equipment that allow CI systems in Western Australia to be repaired and serviced. These services allow the continuation of CI supply in Western Australia.