Towards an evaluation and protection strategy for Critical Infrastructure

Submitted in partial fulfilment of the
requirement of the degree of

Master of Science
of Rhodes University

Jason Howard Gottschalk

July 2015

Abstract

Critical Infrastructure is often overlooked from an Information Security perspective as being of high importance to protect which may result in Critical Infrastructure being at risk to Cyber related attacks with potential dire consequences. Furthermore, what is considered Critical Infrastructure is often a complex discussion, with varying opinions across audiences.

Traditional Critical Infrastructure included power stations, water, sewage pump stations, gas pipe lines, power grids and a new entrant, the "internet of things". This list is not complete and a constant challenge exists in identifying Critical Infrastructure and its interdependencies.

The purpose of this research is to highlight the importance of protecting Critical Infrastructure as well as proposing a high level framework aiding in the identification and securing of Critical Infrastructure. To achieve this, key case studies involving Cyber crime and Cyber warfare, as well as the identification of attack vectors and impact on against Critical Infrastructure (as applicable to Critical Infrastructure where possible), were identified and discussed. Furthermore industry related material was researched as to identify key controls that would aid in protecting Critical Infrastructure.

The identification of initiatives that countries were pursuing, that would aid in the protection of Critical Infrastructure, were identified and discussed. Research was conducted into the various standards, frameworks and methodologies available to aid in the identification, remediation and ultimately the protection of Critical Infrastructure. A key output of the research was the development of a hybrid approach to identifying Critical Infrastructure, associated vulnerabilities and an approach for remediation with specific metrics (based on the research performed).

The conclusion based on the research is that there is often a need and a requirement to identify and protect Critical Infrastructure however this is usually initiated or driven by non-owners of Critical Infrastructure (Governments, governing bodies, standards bodies and security consultants). Furthermore where there are active initiative by owners very often the suggested approaches are very high level in nature with little direct guidance available for very immature environments.

Acknowledgements

To my wife, Talia, for all the support and sacrifices you made during my masters, without you I would have never completed it. Thank you for always believing in me.

To my children, Harry and Emily, thank you for always understanding. To my parents for always pushing, guiding and instilling a desire to always do better. To my brother Grant, thank you for all your support and guidance.

To Brent, thank you for your guidance and support. KPMG, thank you for your support.

To my supervisors: Barry Irwin thank you for all your guidance, support and patience. Alapan Arnab, thank you for your guidance and the healthy doses of debate.

To all my friends and family, thank you for being patient with my absence.

Table of Contents

List of Figures

List of Tables

List of Acronyms

CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure protection
CIP	Critical Infrastructure Protection
DDOS	Distributed Denial of Service
HIV/AIDS	Human Immunodeficiency Virus/ Acquired Immune Deficiency Syndrome
HSPDIC	The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
ICS	Industrial Control Systems
ICT	Information Communication Technology
ISA	International Standard Associaition
NIPP	National Infrastructure Protection Plan
OECD	Organisation for Economic Co-operation and Development
PCS	Process Controls Systems
PLU	Programmable Logic Units
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCADA	Supervisory Control and Data Acquisition
Y2K	Year 2000

Chapter 1

Introduction

Critical Infrastructure is often overlooked from an Information Security perspective as being of high importance to protect, with the perceived risk and impact often being described as being minimal. Critical Infrastructure includes the likes of power stations, water and sewage pump stations, gas pipe lines and power grids. Some of this infrastructure is operated utilising legacy technology such as Supervisory Control and Data Acquisition ("SCADA") technology which enables control over infrastructure (including monitoring and collecting data from systems that control and/or monitor a process sometimes remotely).

Legacy Critical Infrastructure by default was segregated from other systems due to propriety protocols being used to control and monitor devices predominantly over serial based communications (sometime RF where cable was not a viable option). However, since the early 1990's many of these devices have been migrated to Ethernet-based IP communications and as such, have limited security controls which in an IP-based environment is paramount (The Centre for the Protection of National Infrastructure, 2011). Due to nature of the Infrastructure and the often remote location, there is often a requirement for it to accessed

remotely. The implementation of connectivity is often without the implementation of essential security controls (for example firewalls, 2-factor authentication), which is paramount since inherently this infrastructure was designed without adequate security controls due its previous "by default" segregation.

The risk to Critical Infrastructure has long been on the agenda of developed economies with countries like United States leading the world in research and potential mitigation of security related risks (Wenger, Metzger, & Dunn, 2004) . An interesting study was performed by the US Government on the US water infrastructure as to understand the risks and potential impact of Cyber attacks on Critical Infrastructure. The analysis noted the potential for remote attacks on pump stations to easily result in the potential shutdown of these pumps (causing on average half a million people to lose access to running water per pump station). Since most pumps are custom built, it may take anywhere from a few months to a year to repair (since the attack resulted in physical damage resulting from continuous switching on/off). The analysis also identified the potential risk that the loss of power to key water systems may result in the release of untreated sewage water back into the ecosystem (Meinhart, 2006).

Cyber attacks are a reality and requirement to protect Critical Infrastructure cannot be ignored. A key challenge however is identifying Critical Infrastructure through assessments as well as identifying critical dependencies to classify infrastructure as critical. Furthermore assigning risk is always a challenge in the context of Cyber related attacks not to mention the almost certain question that one is challenged with as to why this is only now becoming an issue.

The paradox of what is deemed to be Critical Infrastructure to one individual may be different to another. In this context one should consider the nature of the service that the infrastructure provides and the potential impact the loss there-of would result in, which should form the basis for deciding the ultimate classification. Furthermore the nature of threats that could impact Critical Infrastructure may include Hacktivism, Cyber Warfare and Cyber Crime. To this point the Emerging Cyber Threat Report of 2008 (Ahamad, Amster, Barrett & Cross, 2008) suggests that Cyber Warfare is one of the top five risks to Information Security with targets strongly focused on Critical Infrastructure.

One must consider that legacy utility infrastructure by design utilised technology that was proprietary in design, using predominantly protocols and connectivity topologies that by default resulted in the environments being segregated from the general IT infrastructure. With the evolution of utility infrastructure, the situation has changed considerably with the migration to IP based technology utilising standard network topologies/protocols. This may have resulted in Critical Infrastructure being exposed to the Internet or general networking environment without the implementation of adequate controls to mitigate potential risks.

In developing economies, funding for Information Security initiatives is already under funded, and by design single points of failure (for example, limited sources of electricity supply and generation) already exist, highlighting the potential for the loss of key infrastructure being a reality. For developing economies, such as those in Africa and Asia, this will have significant and far reaching consequences, especially in the context of supplying basic services to populations that reside within. Running water and electricity are generally considered a luxury and ensuring that these basic services are provided is the focus rather than securing them from potential Cyber Attacks, which as a possible risk to supply is simply a non-starter (Akuta, Monari, & Jones, 2011; Cassim, 2011). One should also consider the every constant Information Security skills shortages that the market is experiencing, such as in South Africa (Wall, 2006).

1.1. Objectives of this Research

The core objective of this research was to aid in the awareness for the protection of Critical Infrastructure as well as create a hybrid framework that facilitates a feasible approach to identifying and classifying infrastructure as critical.

The hybrid framework should include the ability for organisations to identify potential threat vectors that they may face, consideration for appropriate controls as well as include a risk based approach to identifying security deficiencies.

In order to substantiate the validity of developed framework, key aspects would be applied to an organisation and validated through the use of a relevant case study. For the research,

existing risk methodologies/frameworks for the assessment of Critical Infrastructure will be adapted. An existing approach (high level methodology) that has been proposed for accessing a countries susceptibility to an attack on its Critical Infrastructure, NIPP (Homeland Security, 2013) will be evaluated and modified for suitability in the context of immature environments.

Control consideration should include controls that should fall within the scope of public domain (cyber related legislation, adherence to international cyber treaties, national Computer Security Incident Response Team) as well as suggest, where feasible and at a high level, compensating controls for controls that are absent.

To provide context to the risks facing Critical Infrastructure, example of Cyber related attacks including Cyber Crime and Cyber Warfare will be identified and discussed.

1.1.1. The core objectives

The core objectives of this research were to:

- Provide context for what is considered to Critical Infrastructure and why it is now at risk
- Identify the overlap between Critical Infrastructure and Critical Information Infrastructure
- Identify key attacks on Critical Infrastructure in the context of Cyber Warfare and Cybercrime
- To identify methodologies applicable to the protection of Critical Infrastructure in the context of immature environments
- Propose activities that will enable the protection of Critical Infrastructure in the context of the proposed methodology, including the identification of appropriate activities per phase of the methodology
- Identify at a high level, appropriate controls for protecting Critical Infrastructure.

1.2. Scope and Limits

The scope of the research specifically excludes:

- The identification of specific Critical Infrastructure
- The identification of a mandatory complete list of security controls

- Proving the hybrid framework through the use of case studies and/or interviews

1.3. Document Structure

The below list is a summary of the key sections found in this documents as well as a brief summary of the chapter content:

- Chapter 2 (Literature Review) – During this chapter the definition of Critical Infrastructure is discussed along with key Cyber related events that have impacted Critical Infrastructure.
- Chapter 3 (Critical Infrastructure Assessment Framework) – A hybrid framework for the protection of Critical Infrastructure is discussed as well as expansion of key areas of the framework
- Chapter 4 (Framework case study simulation) – The hybrid framework is applied to a Telecommunication company as to illustrate application
- Chapter 5 (Conclusion) – This chapter concludes the paper and reflects on the achievement of the stated research objectives including the future proposed extensions to the research.
- Chapter 6 (References).

Chapter 2

Literature Review

2.1. What is Critical Infrastructure

This chapter discusses the constant challenge of how and what to define as Critical Infrastructure. How different nation states view and classify infrastructure is examined along who is responsible for doing so.

One would state that roads, highways, dams, power grids and telecommunications (to name a few) at high level should be considered critical however in certain instances failure of infrastructure may affect some but not others. To this end how does one define what is Critical Infrastructure? A good analogy can be borrowed from the US office of Homelands Security (Theron & Bologna, 2013) who said: *"The assets, functions, and systems within each Critical Infrastructure sector are not equally important. The transportation sector is vital, but not every bridge is critical to the Nation as a whole".*

The challenge with identifying Critical Infrastructure is also further complicated by the fact that infrastructure has dependencies and interdependencies with other Critical Infrastructures

with many of these interdependencies driven by IT systems - suggested to be classified as ICT (Luiijf, Burger, & Klaver, 2003).

The inability to identify what Critical Infrastructure is stems from the lack of understanding of what is vital to a country's inhabitants. This is a view further shared by many including researchers Luiijf et al. (2003) who suggest that the Netherlands do not have a "crisp" definition either. Luiijf et al. (2003) set about attempting to define the Netherlands Critical Infrastructure and suggested the definition being the "services defining minimum quality levels". This transitioned the discussion to a political level surrounding what a country's inhabitants expect as a "minimum" which resulted in the following five key indicators being identified:

- National and International law & order
- Public Safety
- Economy
- Public heath
- Ecological environment.

Luiijf et al (2003) engaged with government departments responsible for the previously identified indicators, requiring them to complete questionnaires per potential vital product/service. Of the analysis of data resulting from 50 questionnaires, they concluded that the energy sector, human-oriented services like drinking water, food and health services, telecommunications and transport sectors scored highly. However of particular interest and considerably of most importance is the conclusion that the above services are supported by information and communications technology making them particularly susceptible to attacks of a Cyber nature.

The research generally suggests that Critical Infrastructure also be categorised according to the following criteria within the context that certain services may have an immediate impact (due to key interdependencies) that could (after a certain amount of time) have an irreversible affect (for example electricity supply):

fast impact with slow recovery services, e.g. water quality
slow impact with slow recovery, e.g. shipping,
fast impact and fast recovery, e.g. telecommunications
slow impact with fast recovery
very fast impact and very fast recovery, e.g. emergency communications

***Table 1 - Recovery Classification* - (Luiijf et al., 2003)**

Moteff & Parformak (2004) issued a report for the United States Congress on the "Definition and identification of Critical Infrastructure and Key Assets" which suggested that the "ambiguous or changing list of Critical Infrastructure" could lead to "inefficient use of limited homeland security resources". This report was aimed at highlighting the changes and possible development of the definition in light of the debate and shift from public policy as well as the movement from "infrastructure adequacy to infrastructure protection".

The report discusses various mandates and policy trends relating to the classification of Critical Infrastructure. An interesting perspective provided by this report, was how the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets ("HSPDIC") defined the following categories of Critical Infrastructure as well as the responsible department for ensuring its protections (refer to Table 2).

Department
Dept. of Commerce - Information and Telecommunications
Dept. of the Treasury - Banking and finance
Environmental Protection Agency - Water supply
Dept. of Transportation - Aviation, Highways, Mass transit, Pipelines, Rail, Waterborne commerce
Dept. of Justice/FBI - Emergency law enforcement services
Federal Emergency Management Agency - Emergency fire service Continuity of government services
Dept. of Health and Human Services - Public health service, including prevention, surveillance, laboratory services and personal health services
Dept. of Energy - Electric Power ,Oil and gas production and storage

***Table 2 - Critical Infrastructure protection ownership* - (Moteff & Parfomak, 2004)**

2.2. Critical Information Infrastructure

The terms Critical Infrastructure ("CI") or Critical Information Infrastructure ("CII") are often used and can easily be interchangeably, although there is a distinct difference between the two definitions (Mboneli & Herbst, 2010). Often initiatives for the protection of Critical Infrastructure or Critical Information Infrastructure ("CII") are phrased Critical Information Infrastructure Protection (the same would apply for Critical Infrastructure Protection).

The context for the additional terminology of CII is due to the evolution of risks that face the Protection of Critical Infrastructure which has evolved substantially from physical risk to that of the greatest risk being damage to Critical Infrastructure through ICT related vulnerabilities (Military Operations Research Society, 2010).

The introduction of the term Critical Infrastructure Information Protection ("CIIP") refers to the *"communications or information service(s) whose availability, reliability and resilience are essential to the functioning of a modern (national) economy, security, and other essential social values"*(Willke, 2007). This would suggest that services such as telecommunications, power distribution and water supply (to mention a few) would be included.

The challenge is trying to make a distinction between CIP and CIIP, as similarities and overlaps exist. The definition strives for a distinction that suggests where major ICT exists with a significant interdependency with ICT infrastructure it be classified as a subset of CIP but under the terminology CIIP (Bologna, 2005), a view further supported and evolved by researchers Mboneli & Herbst (2010). Furthermore they suggest that any ICT infrastructure at the core of Critical Infrastructure be classified at CIIP (Rome & Bloomfield, 2010).

2.3. Critical Information Infrastructure Protection

To appropriately define the scope of what would encompass CIIP, specifically what would be required to be protected, the requirement to discuss the different instances of actual equipment/infrastructure that may form part of CIIP protection is vital. Terms often associated with Critical Infrastructure such as SCADA, Industrial Control System ("ICS") and Information Communications Technology ("ICT") Infrastructure will be discussed in the context of Critical Infrastructure.

It is also important to understand the subtle differences between SCADA and ICS infrastructure as it relates to Critical Infrastructure, as well as the challenge of where ICT Infrastructure would lie within the ambit of CIIP. Security researcher Byres suggests that SCADA is rather a subset of ICS and that ICS would be the specific term used when referencing the automation of industrial systems, whereas SCADA would refer to controls systems that "span a large geographic area", although it must be considered all most Critical Infrastructure has components of SCADA, PCS and ICS (Byres, 2005).

It is further suggested by Byres (2005) that these systems were developed during an era where the micro controller did not exist and often PCS utilised mechanical pneumatics to create logic. In contrast, SCADA systems utilised transistors and radio to achieve same, resulting in different terminology since the underlying technology was vastly different (Byres, 2005).

An obvious evolution is that Critical Infrastructure is now being bridged with communications infrastructure for the purpose of remotely managing and monitoring infrastructure. Furthermore, Critical Infrastructures is now becoming interdependent through common communications infrastructure which has resulted in common infrastructures as well as that common communication infrastructure being considered critical (Fernandez & Fernandez, 2005; Luiijf et al., 2003).

Clemete (2013) suggests that the relationship between the private and public together with the incentives and pressures are, and will continue to drive the evolution of infrastructure being digitally connected. However the result of this evolution is also changing the risk profiles that interconnectivity brings, requiring larger Cyber budgets and stronger policy adoption.

2.4. ISA 99

The greatest challenge to understanding the design of Critical Infrastructure is that the "rules of engagement" differ to that of a standard IT Environment. The ISA 99 provides a standardised classification for discussing infrastructure across the architecture topology stack. Researcher Forster provides a summary of the different devices within the typical ICS environment, according to ISA 99, as summarised below:

- Level 0 - Controllers and I/O's that would reside at level 0 and would communicate to end point devices
- Level 1 – This would include Real-time controllers and I/O's which would encompass TCIP/IP controllers, PLC's and other control network devices
- Level 2 – This would include components such as supervisory controls, Operator HMI SCADA workgroup/domain operating systems and applications
- Level 3 – Components such as advanced Control and Advance Applications (specifically non-critical control applications) Workgroup and network domains with mirrored databases. 3rd party networks may also terminate at this level
- Level 4 – This is the business LAN/Enterprise network level. A distinction is made where no direct connection between the industrial networks and business LANs is made (Forster, 2012).

Forster suggests the use of the ISA 99 standard introduces 'zones' and 'conduits', which provide an easily understandable framework to most IT Security individuals. Furthermore it creates logical areas that for the segmentation/isolation of key sub-systems.

2.5. Critical Infrastructure Protection in the South African Context

Mboneli & Herbst (2010) identify three key Legislative acts that relate specifically to the protection of Critical Infrastructure or more specifically the protection of CIIP in South Africa:.

- The Electronic Communications Security Pty (Ltd) (Act 86 of 2002) discusses the creation of a government agency named "Comsec" with the sole responsibility of ensuring that critical electronic communications are protected and secured through co-ordinated research and development of communications security , products and services (The Presidency, 2003). Furthermore the Act defines communications infrastructure to include computers systems and programmes as "organs of the state".

- The Electronic Communications and Transaction Act 25 of 2002 mandated within Chapter 9, that critical databases must be registered with the relevant government organisation including who the administrators of the database are, its location and the type of data that it stores.
- The National Key Points Act 102 of 1980 of particular internet in regards to Critical Infrastructure Protection. It was passed during the height of unrest during Apartheid South Africa (1970's) where the government were concerned that acts of sabotage directed at national infrastructure with the aim in causing the country/economy to collapse. The Act never resulted in any list of National Key points being publicly defined until the Right2Know Campaign (de Wet & Benjamin, 2015) forced the South African Government to produce the list. The list included oil refineries, airports and power stations, to mention a few (Pothier, 2013).

The National Key Points Act 102 of 1980 is quite similar to that of USA patriot Act (Moteff & Parfomak, 2004) which allows the Government to do what is required to protect Critical Assets with a special mandate. Researchers Mboneli & Herbst (2010) suggests that the above Acts mandate responsibility that falls within three completely disparate national government departments. The above Acts touches on aspects of Critical Infrastructure protection with one single government entity being responsible for driving the requirements/agenda for a programme for protecting Critical Infrastructure, something that is quite mature in the United States and most European countries (Rome & Bloomfield, 2010).

Mboneli & Herbst (2010) views are shared by many in the academic environment including Von Solms who suggests that the greatest threat to Critical Infrastructure in South Africa will stem from Cyber related attacks. Ellefsen & Von Solms (2012) suggest that a centralised and co-ordinated Cyber Security Policy will be critical as a starting point to protecting Critical Infrastructure (Ellefsen & Von Solms, 2012).

The lack of clear direction relating to what is considered Critical Infrastructure is one challenge however the criteria upon which Infrastructure is deemed to be critical is paramount. Njotini argues that a framework for the protection of Critical Infrastructure is important but warns that the "adoption of a one-size-fits-all framework" would suggest that Critical Infrastructure could be protected through a "tickbox" exercise (Njotini, 2013).

If one focuses specifically on where the greatest Critical Infrastructure interdependencies exist then it could be argued that if attacked it would result in the greatest impact.

2.6. Critical Infrastructure Evolution

During the mid 1990's the United States of America started to evolve the definition of Critical Infrastructure from the previously very strictly termed "with respect to the adequacy of the nation's public works" which resulted in defining Critical Infrastructure Protection in the context of Homeland security, largely due to growing thread of international terrorism (Moteff, Copeland, Fischer, Ave, & Washington, 2003).

While the above does not strictly describe a movement towards the inclusion and reference of ICT related components in the overall definition of Critical Infrastructure, it was eventually acknowledged by Decision Directive Number 63 which was passed by the then president Bill Clinton on May 22, 1998. The directive specifically included a reference for the definition of Critical Infrastructure which included "*those physical and cyber-based systems essential to the minimum operations of the economy and government."* (Moteff et al., 2003).

The question as to why the movement to specifically include cyber related components in the definition can be answered through the examination of the evolution in the advancement of technology. Critical Infrastructure was previously segregated from other systems using propriety protocols to control and monitor devices predominantly over serial based communications (sometimes RF was utilised where serial cable was not a viable option) as depicted in Figure 1 (The Centre for the Protection of National Infrastructure, 2011).

Between International Standard Association ("ISA") 99 levels 3 and 4, the SCADA environment was not logically or physically connected to the Enterprise environment (refer to Figure 1).

Where systems were located over georgraphically despearant locations, POTS (Plan Old Telephone Services) lines utilised analog connecitvity to connect infrastructure allowing control from a centralised point while still predominantly achieving a segregated environment from the enterpise environment.

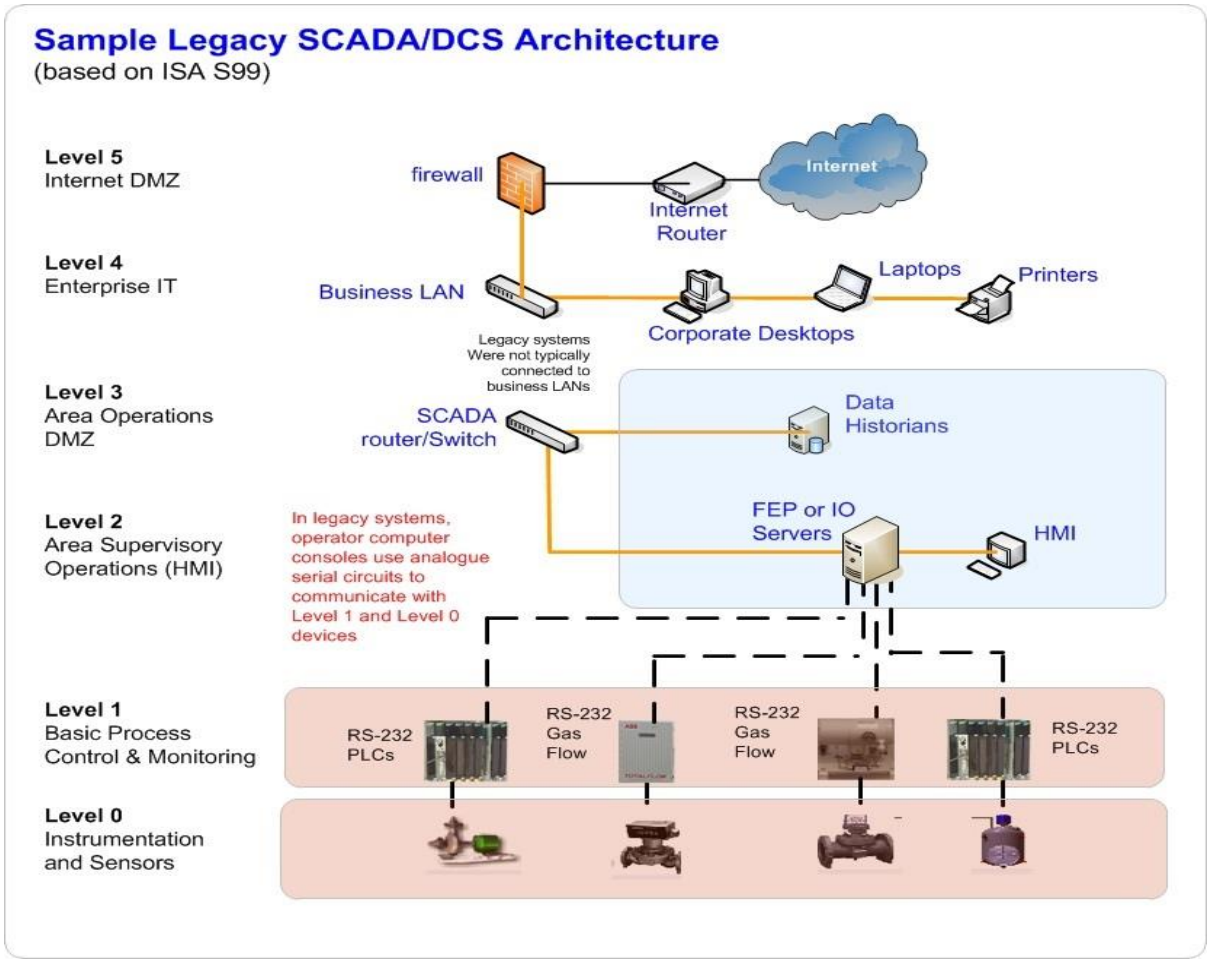


Figure 1 – Sample Legacy SCADA/DCS example **(Pollet, 2011)**

Therefore, traditional serial based equipment would require an attacker to obtain physical access to the equipment in-order to attack it. This is contrary in Ethernet-based IP environments where devices can be accessed externally and generally through common networks.

Since the early 1990's, many of these devices (at ISA 99 Level 1 & 2) were migrated from serial communications to Ethernet-based IP communications, introducing vulnerabilities into the environment since in IP-based environments, communications can be routed and sent to an external environment i.e. the internet (The Centre for the Protection of National Infrastructure, 2011). Compounding the issue further is that many vendors simply encapsulated the serial protocols within TCP/IP wrappers without consideration for authentication or the encryption of communications.

With the movement from serial to IP based communications, the model of one master to one slave topology has largely been eradicated, allowing for a one master to multiple slave environment. This design would introduce a greater risk should compromise to the master occur. Furthermore, the bridging of one master to multiple slave environments would further "bridge" traditionally segregated environments.

This situation has been further aggravated (Miller & Rowe, 2012) by the fact that Critical Infrastructure control systems have been carelessly connected to the internet without the necessary perimeter controls. Critical ICT Infrastructure ecosystem (specifically SCADA and ICS related systems – refer to Section 2.3 for explanations on SCADA/ICS) traditionally does not include the necessary security controls and never included development with requirement of testing code for security related vulnerabilities.

It has been shown that SCADA related infrastructure has been easily exploited utilising "proof-of-concept exploit code", with researchers and industry experts suggesting that malware will be specifically written to target SCADA related infrastructure, something that was shown to be very viable and effective in the Stuxnet incident (Constantin, 2013).

Another key factor is that ICT related systems are becoming increasingly embedded in Critical Infrastructure and are able to control key aspects of its operation which is relatively new and as a result of "pervasive computerisation and automation of infrastructures over several decades" (Rinaldi, Peerenboom, & Kelly, 2001). Rinaldi et al. (2001) suggests that the "reliable operation of modern infrastructure depends on computerised control systems, from SCADA systems that control electric power grids, to comprised systems that manage the flow of railcars and goods in the industry". These interdependencies are driving the potential for extreme impact on the inhabitants of country should a failure occur with communications infrastructure that has interdependencies.

Another key and relatively new factor is extensively discussed by researcher Luiijf who describes the importance that technology itself has become as a critical element in day to day living. In support of this, the Dutch Cabinet released a memorandum (Luiijf & Klaver, 2000) entitled "the digital delta" which suggests that the high level of ICT integration in society makes the functioning of that society dependant on telecommunication systems and suggests the importance of ensuring the securing thereof. In support of this statement a recent report

from the Dutch government suggests "serious disruptions to the ICT-based infrastructures could, increasingly, lead to a similar situation after a number of hours, given that our society is becoming increasingly dependent on chain processes such as electronic payment, logistical just-in-time systems" (H. Luiijf & Klaver, 2000).

Researchers Luiijf et al. (2003) believes that ICT integration into everyday life ensures that we are "increasingly dependent on the underlying infrastructures", which is illustrated by the hype and panic surrounding the millennial Y2K issue. It was further suggested that while the public thinks the Y2K issue was a *"storm in a tea cup",* problems were still experienced and actually had nothing been done the impact would have been significant.

2.7. Critical Infrastructure at Risk

The threat to Critical Infrastructure could potentially arise from various types of scenarios and types of transgressors. These would range from acts of Cyber Crime to acts of Cyber Terrorism (refer to Section 2.7.1 and 2.7.3 for definitions).

During the introduction it was positioned that Critical Infrastructure was previously segregated by default from other environments through the use of propriety protocols and most importantly, physical and logical separation from production environments. With the Critical Infrastructure context largely evolved to an environment where ICT infrastructure is mostly embedded in all aspects of Critical Infrastructure, as well as the transition of technology itself becoming critical, the risk from Cyber related attacks on Critical Infrastructure cannot be ignored.

The risk to Critical Infrastructure has long been on the agenda of developed economies with countries like United States leading the world in research and potential mitigation of security related risks. As referred to earlier in the introduction, the study performed on the US water infrastructure system in 2006 by the US Government, illustrates the potential impact Cyber events may have (The United States Government, 1997).

Developing economies are preoccupied with unemployment, HIV/AIDS, traditional crimes and other social issues and the inability to re-direct resources to focus on the

prevention/detection of Cyber related attacked on Critical Infrastructure will ultimately result in successful attacks on Critical Infrastructure being a reality (Cassim, 2011). The International Energy Agency ("IAEA") indicated that by 2035 developing economies will account for 40 percent of total global nuclear power generation by 2035, mostly being driven by increased demand for "clean" power and an abundance of it (Banks & Massy, 2012). Compromised Nuclear power stations would certainly introduce significant and catastrophic consequences for a country and its inhabitants.

To further conceptualise Cyber-attacks we will explore key events across two key domains, namely Cyber Crime and Cyber Warfare.

2.7.1. Cyber Crime

The term Cyber Crime is defined as the use of electronic means to commit crimes (Criminaljusticedegreehub.com, 2013), however for the definition to be applied correctly, illegal activities must have been specifically committed using an electronic device such as a notebook, tablet and/or phones) connected to a network and/or the Internet. Cyber Crime may manifest itself in many different forms and may often include extortion, cyber-stalking, reputational damage (through website defacing), information theft, hacking, Denial of Service attacks, phishing attacks, software piracy and credit card fraud, not to mention a combination of the above and more (Criminaljusticedegreehub.com, 2013; Fick, 2009).

A typical act of Cyber Crime, Hacktivism, has a very strong political motive utilising digital tools to make a political statement. The word Hacktivism is created from two other words, Hack and Activism, which can be interpreted as meaning "*the use of computers and computer networks as a means of protest to promote political ends*" (Mateski et al., 2012). Traditionally, these acts were performed utilising DDoS attacks causing the disabling of website servers through overloading. The concept was that of a *"virtual sitting"* with the distinguishing fact of intent being "disruptive rather than destructive" (Casserly, 2012). Accordingly, and on a strict interpretation, Hacktivism should inevitably be politically motivated and utilise the *minimum* required digital tools to make a political statement (of protest).

Cyber terrorism is a significantly more aggressive form of Cyber Crime with strong political objectives often funded directly or covertly by a country state. The term can be further conceptualised as "unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in the furtherance of political or social objectives"(Sproles & Byars, 1998).

In the context of Africa and more specifically South Africa, the improvement in the availability of high speed broadband connectively and the relatively low maturity of the users accessing the Internet (Cassim, 2011) has resulted in Cyber-crime becoming rampant in South Africa. Recent reports indicate that South Africa has the third highest number of Cyber-crime victims behind Russia and China (Mohapi, 2013) and is the second most targeted country, with 1 in every 170.9 e-mails identified as phishing attacks and 67.8% of all South African e-mail traffic is considered as SPAM (Rosewarne, 2013).

The South African Cyber Threat Barometer 2012/3(Rosewarne, 2013) report indicates that Cyber Crime in South Africa is estimated to have cost the country R2.65 billion and while there is an expected recovery, an estimated R662.5m would not (Rosewarne, 2013). This same report identified that common vulnerabilities are being exploited and with unemployment growing these people may become soft targets for syndicates (IT News Africa, 2013).

A prime example illustrating the potential impact Cyber Crime could potentially have on Critical Infrastructure would be the July 2008 attack on the JSE stock exchange which resulted in network downtime that lasted almost an entire day. The loss of the trade differential amounted to over R7 billion (Du Toit, 2008).

2.7.2. Cyber attacks on Critical Infrastructure

The earliest reported Cyber incident affecting Critical Infrastructure dates back to 1982. The disruption was caused by a Trojan which was "planted" in a SCADA system that controlled the Siberian Pipeline which affected systems resulting in a significant explosion (Miller & Rowe, 2012).

In 1992 a disgruntled ex-employee hacked into Chevron's emergency alert system and re-configured it to crash. It was only detected when an emergency arose relating to the release of noxious gases which required the system to be invoked. The potential failure may have resulting in citizens living across 22 states in America being put at risk (Miller & Rowe, 2012).

In June 2000 computer systems belonging to the Maroochy Shires Council in Australia was compromised by a disgruntled employee, Vitek Boden, who hacked into the sewage system and released millions of litres of raw sewage into the ocean (Abrams & Weiss, 2008).

Some of the most prevalent cases of Cyber-crime involve act of Hacktivism with the *Season of S0wnage* illustrating our Critical dependence on some internet related services. This occurred in 2011, affecting the Sony Corporation which stemmed from Sony's litigation against George Hotz after he successfully managed to "*jailbreak"* the Sony Playstation 3 (in the context of the Internet being considered Critical Infrastructure, the attack on Sony is considered appropriate for discussion since it resulted in the downtime of the Sony Gaming Network which services an extensive user base). Hotz succeeded twice, however on the second attempt he incurred the legal wrath of the Sony Corporation. As a result Sony Corporation commenced a legal battle against Hotz. During the ensuing legal battles, the California District Court granted Sony Corporation a subpoena providing them with access to the IP addresses of anyone who had downloaded "jailbreak" instructions (Kushner, 2012).

As a result of the litigation, Sony Corporation invoked a hornet's nest of hatred, attracting the attention of Hacktivist groups Anonymous, and subsequently LulzSec (an offshoot group) both of whom took exception to Sony Corporation's actions. The jailbreaking of the Playstation 3 was soon to be the least of their concerns. Anonymous initiated Operation Sony (OpSony) with the objection of *"help out this young lad, and to protest against Sony's censorship"* (Kumar, 2011). Shortly thereafter, both Sony.com and Playstation.com were attacked using DDOS attacks resulting in the loss of key services, with Anonymous taking credit for the attacks, and posting a YouTube video *Leave Fellow hackers like geohot alone*[*1] (Stoeffel, 2012).

[1] http://www.newyorker.com/magazine/2012/05/07/machine-politics

By June 2011, Sony was subject to numerous attacks, which resulted in Playstation service downtime and disclosure of personal customer information. A key attack vector that resulted in the disclosure of personal information was through a simple (almost embarrassing) SQL injection exploit (Schwartz, 2011). Losses to the Sony Corporation resulting from Hacktivism are estimated by them to be in the region of $170 million. The losses also take into account the costs associated with the breach of customer data, as well as the network outage. Besides these costs, Sony's actual share price dipped by 3.7% (GamePolitics.com, 2011).

2.7.3. Cyber Warfare

When trying to identify acts of Cyber Warfare researcher Ragnarsson (2010) suggests utilising Mcafee (Dewalt, 2009) four key attributes for classifying a Cyber Attack as Cyber warfare:

1. Source – Was the attack carried out or supported by a nation-state?
2. Consequence – Did the attack cause harm?
3. Motivation – Was the attack politically motivated?
4. Sophistication – Did the attack require customised methods and/or complex planning?

While the above criteria may be a guideline it is not necessarily an exact science since the appeal of using Cyber related attacks is that one is able to mask the true source of the attack therefore making it inherently challenging when trying to identify the source. More specifically the source may not always be a nation-state nor may it be possible to link the activities back to a nation-state (ISIS or Boko Haram as an example).

George Heron, former chief scientist for McAfee, believes that attacks on Critical Infrastructure are not isolated events and that Critical Infrastructure will continue and increasingly become targets of enemy nations especially from previously (or currently) considered hostile countries (BusinessWorld, 2009).

In support of this, the Georgia Tech Information Security Centre Emerging Cyber Threat Report of 2009 (Ahamad et al., 2008) identified Cyber Warfare as one of the top 5 risks to Information Security and if one considers the contributing factors to this type of attack being attractive, namely its low cost to initiate attacks, lack of key defences, plausible deniability

and lack of rules of engagement for conflicting nations, the reasoning behind Heron's thinking becomes apparent.

At the 2012 International Conference on Cyber conflict, researchers presented a study on the susceptibility of countries Critical Infrastructure by correlating a country's Internet-infrastructure level *vs.* its ability to deal with Cyber threats and the steps already taken by countries to defend against potential threats on Critical Infrastructure. The key findings from this report were that developing economies were increasing their Internet connectivity faster than developed countries and drew a direct correlation between the potential for Cyber threats on Critical Infrastructure and the density of Internet access within that country (Keren & Elazari, 2012). While the study indicated that while perhaps developed economies Critical Infrastructure was more likely to be the target of Cyber attacks, it was somewhat offset by the countries Cyber defence initiatives. Of most interest was the countries that had the lowest Internet-infrastructure had generally no measures in place to protect Critical Infrastructure.

Probably the most publicised Cyber Warfare attack affecting Critical Infrastructure is that of the Stuxnet and Duqu which are often viewed as SCADA "game changers" in that they were specifically designed to compromise SCADA devices and more specifically, certain types of PLC's (Farwell & Rohozinski, 2011), which are devices that monitor inputs and based thereon, will affect other devices to perform activities(Advanced Micro Controllers Inc, 2014) .

2.8. Cyber Warfare attacks on Critical Infrastructure

As discussed during Section 2.7, the Stuxnet worm was specifically designed to attack a PLU through the exploitation of the Siemens default password that was hardcoded into the device and was used to access Windows workstations that operated the control application. The worm searched for "*frequency-converter drives"* which were specifically manufactured by Fararo Paya in Iran and Vacon in Finland and *"altered the frequency of the electrical current to the drives causing them to switch between high and low speeds".* The continual switching caused *"the centrifuges to fail"* (Miller & Rowe, 2012). Through various sources it is thought that this attack originated from the Israeli and the United States governments (Kushner, 2013)

Another interesting example which speaks to the concerns of the US army relating to clean water infrastructure. In November of 2011 there was an attack on a water pump facility at the Springfield water utility that originated from an IP Address located in Russia. The Department of Home Land Security played down the risk but soon after that a similar facility was compromised in Houston (Neil, 2011).

Sections 2.8.1-3 discuss examples of Cyber Warfare where attacks on Critical Infrastructure are explored for purpose of illustrating the how the attacks affected the onset of the war and how the availability of Cyber as a medium of attack have evolved the art of warfare.

2.8.1. Cyber Warfare in Estonia

Estonia, while a small country consisting of 1.4 million citizens has established a strong and efficient online e-services portfolio with 97% percent of bank transactions occurring online with significant internet penetration across 60% of the country's population with the country significantly dependant on the internet since the government operates a virtually paperless environment (Herzog, 2011). A further illustration for their adoption of technology is that the ability of citizens to vote electronically during the 2007 elections, which 5.5% of the voters did (Kozlowski, 2014).

In 2007 Estonia fell victim to Cyber Warfare attacks affecting e-services including three of the country's six news agencies, two of the largest banks specialising in online transactions, key e-services as well as the parliamentary e-mail servers. The attack resulted in credit card and automatic tellers being unable to complete transactions for several days. It is suspected that the attack was in in retaliation to the removal of a Bronze statue erected by Russia during the liberation after World War II (Traynor, 2007). The removal thereof was seen as disrespectful to the Russian soldiers who fought against the Nazi's however a sign of oppression to the Estonians (Kozlowski, 2014).

The attacks on the above key e-services were delivered through DDoS attacks originating from IP addresses all over the world. While the early attacks originated from the Russian owned IP addresses and perhaps more incriminating IP addresses owned by Russian State

institutions, the European Commission and NATO technical experts were unable to conclude on the available evidence pointing toward the incrimination of Russia. This inability to trace the attacks is largely due to the use of globally dispersed hosts and virtually un-attributable botnets (Herzog, 2011). Investigation was further complicated by the lack of support by the Russian government perhaps indicating there direct involvement in the attacks (Ruus, 2008).

The Estonians were perhaps better equipped to deal with the Cyber attack than would have probably been expected however it was still necessary to engage with the government CERT's of the Finland, German, Israel and Slovenia to restore operations (Kozlowski, 2014). More specifically a public and private sector agreement was utilised in an attempt to defend the Cyber Infrastructure from the attacks. Even with the additional support from these countries, the attacks could not be fully defended against without a full counter-attack required to obtain control of the situation which was already into its 3rd week of operation.

Of particular interest is that this attack clearly illustrated the reliance on Critical Information Infrastructure and a "bridge" to various key support services.

2.8.2. Cyber Warfare in Georgia

The conflict within Georgia related to two specific provinces, South Ossetia and Abkhaza, which resulted in the province of Ossetia attacking other provinces of Georgia. Georgia responded to the securing parts of Ossetia while at the same time Russian was moving forces to protect the sovereign rights of South Ossetians which resulted in extensive fighting between Russian and Georgia (Markoff, 2008).

Of particular interest to this incident is the suggestion by the Georgian National Security Council chief Eka Tkeshelashvili that Georgia was invaded by Air, Sea, Land and now a fourth avenue, that of "Cyberspace" (Shachtman, 2009). More specifically it was the first time that the relationship between conventional warfare and Cyber-attacks was visible, illustrated by the fact that conventional warfare did not attack Georgian electrical infrastructure but rather left that to be attacked through Cyber. Kozlowski further suggests that the preparation for the attack must have taken proper planning since the access to attack

tools and co-ordinated instructions could not have been prepared in one day (Kozlowski, 2014).

The attacks resulted in over $300 million of damage to civilian infrastructure (International Crisis Group, 2008) with actual Cyber attacks directed to specifically as interfere with the Georgian Governments ability to distribute information during the invasion. This was achieved through introducing large amounts of data which essentially overloaded Internet communications. Besides a disruption in communications, it also resulted is the national bank disconnecting itself from the Internet for almost 10 days (The United States Government, 2009), causing a significant delay in electronic transactions..

It has also been suggested that an organised crime unit, RBN must have had direct involvement, since it has strong ties to the Russian Government. Russia's involvement is further supported by New York Times reporter, Morkoff (2008), who reports that many security researchers agree that Russia was responsible cyber-attacks on Georgia.

The US Cyber Consequences Unit (Gorman, 2009) recently found evidence that supports the notion that common Microsoft software was "refashioned" into Cyber "weapons" with co-ordination occurring through common social media platforms Twitter and Facebook resulting in co-ordinated attacks using Botnets (The United States Government, 2009).

An interesting report by Major William Ashmore of the US Army (2008) suggests that Georgia IT infrastructure was not very advanced, so the attackers easily have caused the Denial of Service attack which resulted in their banking, media and government websites being blocked, halting communications both internally and externally. Websites for foreign ministry and the National Bank were hacked, resulting in the pictures being added of Adolf Hitler and the then Georgian President.

Furthermore Ashmore suggests that they attack on Georgia were more supplicated than those on Estonia as they involved the use of SQL injection combined with Denial of Service attacks. Furthermore, while it not unusual for cellular towers to be targeted during a conflict there Internet Infrastructure was specifically targeted during the on-line Cyber-attacks (Borchard, Fox, Long, Mcveigh, & Moodie, 2008).

2.8.3. Cyber Warfare on Kyrgyzstan

In 2009 the main internet servers were attacked using Denial of Service attacks which resulted in key websites and country specific e-mail being rendered in-operable. During the attacks, at least 80% percent of the internet communications were disabled, mostly through the penetration of two of Kyrgyzstan's four Internet service providers (Jenik, 2009). This resulted in over 80% of external communications being lost and since Kyrgyzstan's online services are quite limited, it resulted in limited direct impact to country.

2.9. Critical Infrastructure protection

The controls required to protect a Critical Infrastructure are not significantly different from the security controls one would implement as of part general IT infrastructure security however one must consider the scale, efforts and importance to protecting Critical Infrastructure. Critical Infrastructure has components that are sensitive in nature and generally affect large geographic areas, something which general Information Security professionals would not be accustomed to.

It is important to be note that Zero day vulnerabilities in Critical Infrastructure may be more prevalent since awareness and focus on securing Critical Infrastructure is fairly immature resulting in significant impact for organisations and countries alike (refer to Section 2.6).

Below are some of the different approaches to protecting Critical Infrastructure including consideration for specific controls and organisational units that may aid in the protection of Critical Infrastructure (some of which are incorporated into the Section 3 of the proposed framework for the protection of Critical Infrastructure).

2.9.1. NIPP

The National Infrastructure Protection Plan ("NIPP") for the United States (Homeland Security, 2013) suggests a risk framework devised of the following key phases which was a directive from US Government with the objective of ensuring a defined and centralised approach to the protection of Critical Infrastructure. What is important to highlight is that NIPP was formed from the input obtained through the collaboration between private and

government counterparts, which was deemed to be paramount to ensuring national Critical Infrastructure security and resilience.

NIPP suggests three key elements of Critical Infrastructure (physical, cyber and human) must be specifically identified and integrated through all the stages of the framework.

The framework has five key stages identified which are explored in a generic context:

1. Set Goals and Objectives – Goals and objectives should be clearly defined and generally include indicators which are tangible in nature. This will ensure outcomes are measurable to determine success
2. Identify Infrastructure – Some key challenges in the identification of infrastructure exists some of which were discussed earlier. In the context of Critical Infrastructure it is paramount to ensure that all critical and interpedently infrastructure is identified
3. Assess and Analyse Risks – During this phase of the risk management, Critical Infrastructure risk should be assessed accordingly to Threat, Vulnerability and Consequence
4. Implement Risk Management Activities – Based on the outcome of the previous phase, risk mitigation procedures should be performed based criticality, costs of remediation and the benefit of risk mitigation. NIPP suggest the following key activities:
5. Measure Effectiveness – Protecting Critical Infrastructure is costly but required. The ability to measure the success of the implemented activities is key to ensuring budget renewal. NIPP suggest a "integrated and continuing cycle" that evaluates the achievement of goals and ensures learning and the adaption during and after simulations and incidents (Homeland Security, 2013).

2.9.2. OECD

The Economic Co-operation and Development ("OECD") is an international organisation that was established in 1960 and has 30 active member countries which focuses on promoting policies that drive the resolution of global challenges relating to Critical Infrastructure.

Njotini (2013) notes that the OECD promotes the Protection of Critical Infrastructure, more specifically it recommends that member countries implement a framework that achieves the OECD Security Guidelines for Protection Critical Information Infrastructure (Hyslop, 2007).

Njotini expands on the OECD criteria for Critical Infrastructure Protection through the identification of 4 key high level framework sections: *prevention, detection, response and recovery* (OECD, 2008). He suggests no real importance to the order of framework/elements although indicates that "elements builds on the other".

Njotini suggests that prevention should proceed detection and it could be argued prevention is superior to detection but these should be seen as parallel streams stream of equal importance, which will be discussed further in the research.

Njotini's (2013) elaborates further of the OECD elements to protecting Critical Infrastructure:

- Prevention – Ntjotini suggests that the real-time prevention of attacks on Critical Information Infrastructure is a non-negotiable. The Marsh report (which is a report commissioned by the United States President on protecting Critical Infrastructure) suggests the it would be costly and irresponsible to wait for disaster to affect Critical Infrastructure before implementing the necessary remediation to prevent attacks (The United States Government, 1997).
- Detection – The OECD indicates that a framework should incorporate parameters to identify and classify the risk of attacks to Critical Information Infrastructure. Where possible the ability to detect and report must be automated.
- Response – Ntjotini suggests that procedures and measures should be developed and established to ensure responses are rapid and achieve effective collaboration. This could possibility be achieved through the use of CERT's and CSIRTS's. Njotini refers to the G8 principles, which offers principles that will aid in the ability to respond to events affecting Critical Infrastructure which could be considered in the context of good practise.
- Recovery – OCED describes incident recovery measures to aid in the recovery of CII's. Ntjotini suggests that incident recovery measures can potentially establish the extent of the attacks and provide insight into attack trends which may enable improved intelligence to forecast future threats.

2.9.3. Key controls in the protection of Critical Infrastructure

The consideration of key security controls that may aid in the protection of Critical Infrastructure may be thought to be illusive in nature. To some security professionals it may seem very complicated and poorly articulated and one only has to search the Internet to understand why. Control descriptions are poorly defined (controls are described at a very high level and seldom specific to the challenges in protecting Critical Infrastructure) and existing methodologies are rather audit focused and less descriptive/prescriptive in the specification of controls that may aid in the protection of Critical Infrastructure. The illustrative example may be the control statement/objective that Critical Infrastructure is required to be logically segregated from the enterprise environment or that all Critical Infrastructure is required to be monitored. At a high level, a valid statement although how does an organisation achieve this and are there not specific best practises that should be adhered to in context of the above.

Onstott describes four key domain areas under which controls for Protecting Critical Infrastructure from Cyber related attacks should be focused on, namely, Continuous Monitoring, Configuration Management, Vulnerability Management and Patch management. At a quick glance one would reach the conclusion that those domains are not new nor would they be new to most organisations (Onstott, 2014). They challenge is that most organisations are failing to ensure that the design and operation of controls under those domains are operating effectively.

Typical control definition challenges across the domains could include:

1. Continuous Monitoring – Collecting logs from an environment is the easy part of Continuous Monitoring, however the value in this type of control is obtaining exception reporting that easily identifies issues relating to the monitoring team.
2. Configuration Management – The ability to not only ensure consistent configuration of infrastructure but also the ability to monitor changes to infrastructure.
3. Vulnerability Management – Vulnerability scanning may not be performed sufficiently frequently, resulting in vulnerabilities being left exposed. Of greater concern is that vulnerability management should simply not be about scanning the environment for

vulnerabilities but include the identification and remediation of vulnerabilities prior to systems being promoted to production. Consider the introduction of training for developers and administrators focused on common security vulnerabilities applicable to the work being performed.

4. Patch management – Patches are not applied timeously and very often vendors are slow to approve patches. In the context of Critical Infrastructure, release cycles to address vulnerabilities may be slow, leaving organisations vulnerable. As such organisations should consider virtual patching to ensure faster patching cycles as well as the consideration of compensating controls, like an IPS (Onstott, 2014).

Critical Infrastructure vulnerabilities that are identified would generally fall within the Technical, Management or Operational control domains with controls across these domains either pre-existing (with design deficiencies) or not at all.

The controls required to protect Critical Infrastructure may not be significantly different from the security controls one would implement as of part general IT infrastructure security. It is important to be note that Zero day vulnerabilities may be more prevalent since awareness and focus on securing these devices/systems is fairly immature (Zorz, 2012). Listening to vendor suggestions is not always the answer with some vendors having even suggested leaving ICS connected directly to the Internet (Mimoso, 2013). One should also consider that some of the vulnerabilities may be specific to the corporate environment which may be introducing risk into the ICS environment.

There is extensive research available discussing the merit of certain key technical and administrative controls and across various security professionals there are some commonalities which has been summarised in Table 3. Sources include researcher Watts who focused on vulnerabilities within the Electrical Utility environment, John Pollet who operates an expert consultancy firm in the field of ICS security and security researcher Fernandezs (Fernandez & Fernandez, 2005; Pollet, 2011; Watts, 2003).

Standard Technical Controls	Standard Administrative Controls
VPN access into CI should incorporate a separate login as well as a 2-factor authentication	Obtain management support by showing ROI for improved security controls
Passwords changes every 90 days with sufficient password complexity and IP-enabled instrumentation having adequate authentication configured with a password/PIN along with the requirement for configuration changes to be performed over serial console cable (although this has other associated risks) (Fernandez & Fernandez, 2005; Pollet, 2011)	Implement strong policies
Physical shielding of cables. Patch panels, multiplexing data streams and encryption of data flowing between the nodes and hosts should be applied to all wireless connections. LAN devices should also be configured to limit the data rate (Fernandez & Fernandez, 2005; Pollet, 2011).	Implement procedures to protect Critical Cyber assets in the security perimeter
Avoid non-UNIX based operating systems	Periodic review of computer accounts and physical access rights
Ensure aggressive patching cycles (Fernandez & Fernandez, 2005; Pollet, 2011)	Intrusion detection processes
Utilise external and internal firewalls & DMZ's as well as host based firewall/IDS software	Monitoring controls producing exception reporting
Disabling of unauthorised or unused computer accounts and physical access right, as well as unused network services and ports	

Table 3 - Control Summary (*Watts, 2003;Fernandez & Fernandez, 2005; Pollet, 2011*)

2.9.4. Advanced controls and additional control considerations

The controls suggested in Section 2.9.3 are fairly standard in nature and should be considered as mandatory in environments where protection is critical. The Pacific Northwest Nation Laboratory (PNNL) recommends key progressive security controls which are based on the premise of explicitly trust and deny all otherwise, which is particularly useful in the context of Critical Infrastructure (Viveros, 2012) which are usually very specific and controlled environments. PNNL progressive controls include:

1. Dynamic Whitelisting – Provides the ability to deny unauthorised applications and more importantly Active X controls, Java scripts and code. This would work on the premise of only allowing pre-approved applications and scripts from executing on a system
2. Memory Protection – This would be a more advanced version of whitelisting but would be specifically focused at a memory level.
3. File Integrity Monitoring – Any file change, addition, deletion, renaming, attribute changes, ACL modification, and owner modification is reported which would include network shares. While this may seem a very useful control, it must be considered for environments where little change is expected, otherwise the alerts would be overwhelming and unmanageable.

4. Read Protection – Read is only authorised for specified files, directories, volumes and scripts resulting in all other attempts being denied. This control may easily achieved in Unix environment rather than a Windows environment, however the principals are sound (Viveros, 2012).

In addition to the above, the below are controls are suggested by myself in conjunction with the controls described in Section 2.9.3 which are largely based on my experience of remediating Critical Infrastructure:

- Development of server and infrastructure baseline standards
- Creation of Critical Infrastructure related awareness training for the entire organisation. Including specialised security training for Critical Infrastructure engineers, as well as development and training in CIRT response procedures
- Critical Infrastructure network infrastructure should be physically segregated with entry achieved through Thin Client functionality (Jump Servers)
- Centralised logging of all Critical Infrastructure with exception reporting that is capable of detecting and reporting suspicious behaviour
- Yearly penetration testing and auditing of the environments adherence to defined policies and standards.
- Implement monitoring with exception reporting
- Implement active IPS linked to the monitoring
- Implement adequate logical segregation across key environment
- Ensure not critical systems are exposed to the internet unless achieved through VPN technology with two factor authentication (even then it should be limited to low risk interfaces).

To focus on Real time monitoring, company Riptech highlights real-time intelligent monitoring of ICS systems as a common deficiency as environment generate extensive quantities of data flooding Security resources resulting in the inability to recognise attack attempts (Riptech, 1999) .

Monitoring as a control is something that requires careful planning through a gradual systematic ramp-up to the monitoring of systems and events. If one considers the zones as

defined by ISA 99, monitoring requirements at each level should be defined as the requirements will be significantly different.

Prevention is always better than cure and as such controls designed and implemented should predominantly focus preventing compromise with monitoring controls being seen strictly as a compensating control.

2.10. Cyber Incident Forensic Readiness

Fick (2009) discusses the importance of Cyber forensic readiness in mitigating the risks associated with Cyber attacks/breach. He further describes cyber forensic readiness as the ability of an organisation to maximise the use of digital evidence to:

- Reduce the time taken to respond to an incident
- Maximise the ability to collect admissible evidence
- Minimise the length/cost of a cyber-incident investigation
- Reduce incident recovery time
- Prevent further losses.

The motivation for being forensically ready is well described above however the drivers in the context of Critical Infrastructure protection are somewhat different due to the impact of the associated risks should possible disruption materialise (Watts, 2003). One should also consider that digital forensics skills are in short supply within a standard IT context (Rosewarne, 2013) and it should be similar if not worse within a CI context due its specialised nature.

The Centre for the Protection of National Infrastructure in the USA defines the following key scenarios where a forensic readiness programme would be beneficial (Centre for protection of national infrastructure, 2005):

- gathering of evidence legally that will be admissible in court without interfering with business operations
- acquisition of evidence focusing specifically on incidents and disputes
- facilitating the investigation in a manner that ensures the costs are in proportion to the perceived “cost” of the incident
- minimising the interruption to the business as a result of the investigative activities

- ensuring that evidence makes a positive impact on the outcome of any potential legal action
- ensuring compliance with legislation.

Furthermore consideration for a successful readiness programme will have positive bi-products since the skills and tools may be common to operational troubleshooting, recovering of data, monitoring for operational issues, problem solving and achieving compliance and performing due diligence (Kent et al., 2006).

As further motivation, one should consider the challenges that organisations face in defending themselves against Cyber related threats, something well-articulated by CounterTack (2012) who performed a survey across 100 IT executives responsible for security at companies with $100m or more in revenue. Of notable interest from the survey were the 50 hours per month spent on average by responder studying malware to identify attack vectors, the inability to gather real-time attack intelligence due to the lack of technical skills as well as the inability to analyse information through the use of analytic tools. This should be overwhelmingly concerning since 84% of responders were vulnerable to Advanced Persistent Threats.

Having a forensic readiness program in its most basic form will not prevent a pending Cyber Attack however it would certainly aid in the potential to detect a possible attack since the environment required to achieve this would largely be common across the requirement for Forensic readiness. This provides an opportunity to combine the objectives of being ready from a Forensics as well as a Cyber resilience perspective, achieving the ability to drive an end-to-end strategy.

2.11. Summary

During Chapter 2, Critical Infrastructure is defined and context provided in terms of scope of Infrastructure that may be considered Critical. The drivers for protecting Critical Infrastructure were discussed including the identification of motivations from various countries and organisations to protect Critical Infrastructure. Context was also given to some of the attacks that have occurred against Critical Infrastructure, ranging from Cyber Crime to Cyber Warfare.

In Chapter 3, various approaches available to organisations to protect Critical Infrastructure are discussed with the objective of creating a hybridisation approach to identifying, remediating and protecting Critical Infrastructure.

Chapter 3

Critical Infrastructure Assessment Framework

This chapter discusses researched frameworks and methodologies for identifying Critical Infrastructure, their vulnerabilities, as well as going about remediating the vulnerabilities while ensuring the process is iterative in nature. The drivers for this hybrid framework, in context of the challenges facing Critical Infrastructure (as discussed during this chapter), include the challenge that existing frameworks generally fall into two categories, either very high level in nature or very detailed within a very specific sector relating to the protection of Critical Infrastructure.

The NIPP Risk Management Framework (as shown in Figure 2) (Homeland Security, 2013) forms the basis for the proposed framework since the key phases are high level in nature, but provide sufficient generic guidance as to the key order of phases applicable to protecting Critical Infrastructure. It was never developed to provide specific direction for key activities, leaving activities largely open to interpretation and in very immature environments would be substantially less effective.

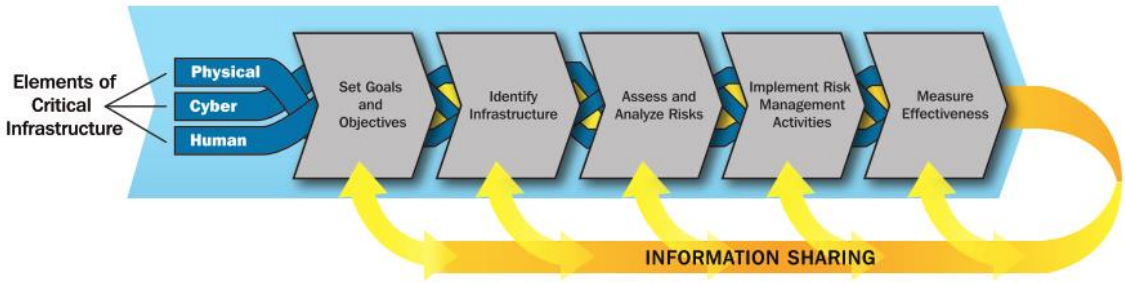


Figure 2 - NIPP Risk Management Framework **(Homeland Security, 2013)**

The key phases for the hybrid framework are detailed below in Figure 3 and within each of the subsequent sections, the scope and suggested activities are discussed with the objective to achieve a holistic approach to identifying, preventing, detecting and responding to the risks associated with a potential Cyber related attacks on Critical Infrastructure. The use of "best of breed" methodologies and approaches provides an opportunity to develop a framework that is universally applicable.

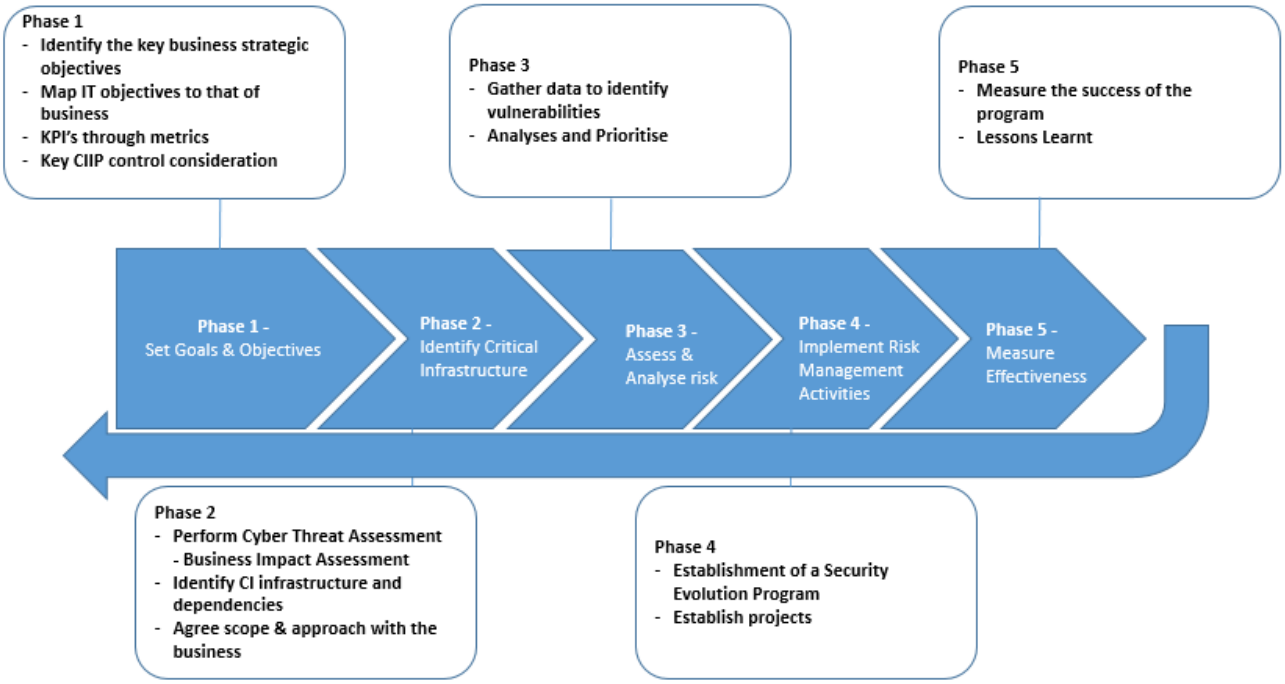


Figure 3 - Proposed Hybrid Framework (After NIPP Framework)

In developing the hybrid framework consulting firm Deloitte (Godfrey, 2008) advise that a framework that achieves a successful approach to security transformation should consider the following key challenges:

- The framework that will be used to define and measure progress against strategic objectives

- The current maturity of the organisation's security capabilities
- The desired state and how representative of the organisation it is
- Process that the organisation will follow to achieve its desired future state
- How will the organisation ensure successful delivery of its transformation.

The activities within the proposed framework are developed with the above in mind however to specifically achieve the following:

- Interactive in nature
- Scalable to suit organisations with varying levels of maturity
- Top down approach, linked to key business processes
- Applicability across various environments.

Furthermore, the scope of activities were chosen to ensure that value is derived from the security assessments and the approach increase the probability of identifying infrastructure related vulnerabilities and in the context of Critical Infrastructure, one must consider that the ability to remediate instrumentation and Level 0 devices (discussed in Section 2.5.1) would be challenging as reliance on vendors would be key. As such consideration if made by focusing on production and server assessments since administrators are generally in a better position to remediate/mitigate vulnerabilities.

The NIST Guide to ICS Security Recommendations of the National Institute of Standards and Technology indicates the importance of developing a "compelling business case" as the first step in implementing a Cyber security program for Critical Infrastructure (Stouffer & Scarfone, 2011). The consideration for this could be included at the completion of Phase 1 and should achieve business buy-in and support prior to beginning Phase 2 if required (refer to Section 3.4).

3.1. Phase 1 - Set goals and objectives

The NIPP framework suggests that Critical Infrastructure owners should identify objectives and priorities for Critical Infrastructure Protection that align to sector objectives. Consideration of the above should be performed in context of the operational and risk environment in conjunction with available funding. NIPP also suggests the consideration for resourcing is key although this is also rather a function of budget and while resources take time to on-board, budget constraints in most instances would be the greater challenge.

During Phase 1 of framework the above objectives from NIPP would remain however this phase should define detailed activities building upon what exists within the NIPP framework. The following key activities are proposed to achieve the phase objectives, which is largely based on the philosophy of a "balanced scorecard" approach to ensure that the protection of infrastructure is aligned to those of the businesses objectives. This aids in avoiding misalignment in terms of what IT is protecting and ensures businesses buy in. One should also consider that the triad of security priorities differ between General IT and that of Critical Infrastructure. Pieth (2004) suggests the priorities and objectives, as depicted in Figure 4 (used as a visual indicator), are at opposites across the environment.

Figure 4 - Security Goals and Priorities **(Pieth, 2004)**

With the above context in mind, Phase 1 ultimately sets the foundation for establishment of a transformation program, with the following key activities being suggested to achieve this:

1. Identify the key business strategic objectives (Section 3.1.1)
2. Map the business objectives to the key ICT objectives (Section 3.1.2)
3. KPI's through metrics (Section 3.1.3)
4. Consideration of key controls relevant to CIIP domains (Section 3.1.4).

3.1.1. Identify the key business strategic objectives

The protection of Critical Infrastructure from a technology perspective is something that should not be driven as a "point in time" exercise but should be iterative in nature and largely driven by the business through defined strategic objectives for service delivery to customers.

It has been suggested that IT is no closer to assisting Business in achieving its goals than twenty years ago, with alignment to business being at the forefront of concerns for IT executives (Moteff & Parfomak, 2004). ISACA suggests that the balanced scorecard "translates strategy into action to achieve goals with performance measurement" (IT Governance Institute, 2005).

The balanced score card was originally developed by Kaplan and Norton (US Office of Personal Management, 2014) and was used specifically to drive business strategies based on measurement through the use of KPI's to ascertain the success of the businesses performance against the defined strategies. Recently the balanced scorecard has been adopted for use to ensure alignment of IT to the businesses strategic objectives, something which has been an industry challenge since IT became the enabler (Saull, 2003).

A suitable approach to completing a balanced scorecard would be through specific workshops with key business and IT representatives during which the key sections of the balanced scorecard would be completed. During the workshops it is suggested (through my industry experience) that the key artefacts that would be completed would be:

- An IT Balanced Scorecard aligned to the identified Strategic Objectives of the Business
- Identification of key COBIT control measurements for protecting Critical Infrastructure.

For all intensive purposes this activity could be overlooked and one could move directly to making assumptions relating to the security controls that the business expects IT to achieve however the purpose of this activity is to avoid assumptions. IT must engage with Business to ensure expectations are understood but more importantly, this provides an opportunity for Business to understand the Cyber related risks against Critical Infrastructure and obtain their support from the beginning of the initiative.

In the realm of IT Governance, the IT Balanced Score Card is central to strong governance and specifically aims to:

- Ensure IT is aligned with the business in terms of its specific strategic objectives
- Ensure that IT is an enabler to business, deriving maximum business value from the IT spend
- IT resources are used responsibly
- IT risks are managed and mitigated appropriately with awareness and evolvement with business.

The principles of the balanced scorecard are to identify the businesses strategic objectives across the following four categories (Saull, 2000) as illustrated in Figure 5 (an example is given for illustrative purposes):

1. Financial – The financial objectives of the organisation as it relates to profit and loss
2. Customers – The focus of the company's operation in relationship to ensuring positive customer poster
3. Internal Business Process - What are the key business processes that are paramount to business

4. Learning and Growth – What are key areas that business is required innovate to improve.

Balanced scorecard sector	Efficiency	Effectiveness
Financial results (i.e. business value)	• Channel costs • Channel profitability	• Online contribution (direct) • Online contribution (indirect) • Profit contributed
Customer value	• Online reach (unique visitors as % of potential visitors) • Cost of acquisition or cost per sale (CPA / CPS) • Customer propensity to defect	• Sales and sales per customer • New customers • Online market share • Customer satisfaction ratings • Customer loyalty index
Operational processes	• Conversion rates • Average order value • List size and quality • Email active %	• Fulfilment times • Support response times
Innovation and learning (i.e. people and knowledge)	• Novel approaches tested • Internal e-marketing education • Internal satisfaction ratings	• Novel approaches deployed • Performance appraisal review

Figure 5 - Example of an IT Balanced Scorecard **(Badger, 2010)**

3.1.2. Map IT objectives to that of business

As discussed during Section 3.1.1 the focus of IT should be specifically aligned to enabling the business to achieve its strategic objectives. Researchers Ahuja and Goldman introduce the concept of an Info-Sec Balanced scorecard with the purpose of specifying specific security objectives to meet the business objectives (Ahuja & Goldman, 2009). They strongly believe that by doing so, Information Security Alignment is achieved by ensuring alignment between the Business, IT and Information Security.

Table 4 depicts the proposed alignment between the different balanced scorecards:

	Business Balanced Scorecard	IT Balanced Scorecard	InfoSec Balanced Scorecard
Financial Perspective	Provide a good return on investment of IT - enabled business investments.	Improve IT's Cost-efficiency and its contribution to business profitability	Security should be used as an enabler to reduce cost and reduce complexity
Customer Perspective	Establish service continuity and availability	Reduce solution and service delivery defects and rework	Ensure security is incorporated in the design of services to reduce customer related breaches
Internal Perspective	Provide compliance with external laws, regulations and contracts.	Ensure that critical and confidential information is withheld from those who should not have access to it	Ensure security control achieve confidentiality, Integrity and availability
Learning and Growth Perspective	Acquire and maintain skilled and motivated people	Acquire and maintain it skills that respond to the IT Strategy	Ensure key security awareness is a priority of training

Table 4 – Interpreted IT Balanced Scorecard Mapping to Business Scorecard **(Ahuja & Goldman, 2009)**

The development of the Information Security component of Balanced Scorecard could be viewed as an evolution on the standard IT balanced scorecard and considered on the second iteration on the framework.

IT's strategic objectives would essentially form the basis of the objectives for performing the initiative using the hybrid framework. The development of a business case to justify the initiative may be optional and developed as required since it may not always be relevant (budget and approval may have already been granted). If it is required, the mappings performed during the balanced scorecard could be used as drivers for motivation. The development of metrics (as discussed during Section 3.1.3) would be used to measure the overall success of the program to achieve the businesses strategic objectives.

3.1.3. KPI's through metrics

Metrics enable the measurement of performance, ultimately identifying measurement of success or failure for security initiatives (Fleming & Goldstein, 2012). It should be considered common sense that if proper metrics are not established upfront how can the success of an initiative be measured.

Fleming and Goldstein suggest that metrics should measure reduction in Critical Infrastructure incidents and the damage caused by these incidents. Characteristics of metrics may be that they are quantitative, universally acceptable, obtainable, repeatable and time based in nature (Abbadi, 2006). While there may be specific metrics that are required to measure the success of this initiative, one should recognise that metrics probably already exist within the organisation in a form of security reporting. Where this does exist, it should be considered for inclusion within this initiative.

Security metrics, should be designed to measure the derived benefit from the implementation of key security controls since it creates an opportunity for business to directly measure the benefit it derives from its IT Security investments, as well as enabling IT to communicate effectively with Senior Management (Ponemon Institute LLC, 2013). Furthermore it enables senior management to be part of the process in dealing with Information Security risks that should result in enabling the ability for the business to make key decisions in accepting or mitigating the identified risk (Tashi & Ghernaouti-Hélie, 2007).

Researchers Tashi and Ghernaouti-Hélie (2007) suggest that security metrics be aligned to organisational objectives, relevant to their current issues and quantifiable with associated costs.

The process of presenting metrics should occur through three key phase as suggested by research (Wang, 2005):

- collection
- validation
- processing.

The actual creation of metrics is often achieved through the review and consolidation of logs collected from the environment. OWASP suggests identifying tools capable of collecting the appropriate logs as well as the appropriate IT team members who should be responsible for producing the necessary reports for IT management (OWASP, 2006). Reports that are heavily worded in IT jargon are usually not well received by senior business management and therefore it should be the responsibility of a manager to ensure the reports are easily understood and displayed in a manner that relays the actual business risk.

For this activity two main categories of metrics are envisaged, new metrics developed to measure the success of the initiative at hand and adoption of existing metrics that could be used to provide metrics to measure overall performance.

Researcher Payne suggests developing agreed baselines and improvement targets for the metrics and even use best practise/peers to ensure that targets are realistic and achievable (2006). For the purposes of identifying the appropriate security metrics, it is suggested to refer to the SANS Top 20 security controls as a base for identifying the metrics for which Stimac's examples could be selected as an appropriate base to work from. (Cain & Couture, 2011; Stimac, 2013).

Even when establishing a "baseline" it must consist of defined measurable criteria. Some examples of metrics could include (Stimac, 2013):

- Number of incidents causing unavailability of critical services
- Number of incidents causing the loss of critical data
- Number of detected incidents
- Number of identified vulnerabilities

- Vulnerabilities that could not be remediated in 30 days.

3.1.3.1. COBIT based metrics

Another approach to metrics is the use of the COBIT framework, which could also be used to show control maturity through year to year measuring (another form of metrics). Through the use of the balanced scorecard, COBIT generic IT goals (Figure 6) could be mapped directly back to the Business objectives and as such by default the applicable IT Processes/COBIT control domains (have specific control descriptions across various levels of maturity) would be identified.

	IT Goals	Processes									
1	Respond to business requirements in alignment with the business strategy.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1
2	Respond to governance requirements in line with board direction.	PO1	PO4	PO10	ME1	ME4					
3	Ensure satisfaction of end users with service offerings and service levels.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13		
4	Optimise the use of information.	PO2	DS11								
5	Create IT agility.	PO2	PO4	PO7	AI3						
6	Define how business functional and control requirements are translated in effective and efficient automated solutions.	AI1	AI2	AI6							
7	Acquire and maintain integrated and standardised application systems.	PO3	AI2	AI5							
8	Acquire and maintain an integrated and standardised IT infrastructure.	AI3	AI5								
9	Acquire and maintain IT skills that respond to the IT strategy.	PO7	AI5								
10	Ensure mutual satisfaction of third-party relationships.	DS2									
11	Ensure seamless integration of applications into business processes.	PO2	AI4	AI7							
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	PO5	PO6	DS1	DS2	DS6	ME1	ME4			
13	Ensure proper use and performance of the applications and technology solutions.	PO6	AI4	AI7	DS7	DS8					
14	Account for and protect all IT assets.	PO9	DS5	DS9	DS12	ME2					
15	Optimise the IT infrastructure, resources and capabilities.	PO3	AI3	DS3	DS7	DS9					
16	Reduce solution and service delivery defects and rework.	PO8	AI4	AI6	AI7	DS10					
17	Protect the achievement of IT objectives.	PO9	DS10	ME2							
18	Establish clarity of business impact of risks to IT objectives and resources.	PO9									
19	Ensure that critical and confidential information is withheld from those who should not have access to it.	PO6	DS5	DS11	DS12						
20	Ensure that automated business transactions and information exchanges can be trusted.	PO6	AI7	DS5							
21	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	PO6	AI7	DS4	DS5	DS12	DS13	ME2			
22	Ensure minimum business impact in the event of an IT service disruption or change.	PO6	AI6	DS4	DS12						
23	Make sure that IT services are available as required.	DS3	DS4	DS8	DS13						
24	Improve IT's cost-efficiency and its contribution to business profitability.	PO5	DS6								
25	Deliver projects on time and on budget, meeting quality standards.	PO8	PO10								
26	Maintain the integrity of information and processing infrastructure.	AI6	DS5								
27	Ensure IT compliance with laws, regulations and contracts.	DS11	ME2	ME3	ME4						
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	PO5	DS6	ME1	ME4						

Figure 6 - IT Goals mapped Processes **(IT Governance Institute, 2007)**

For illustration purposes DS5 of COBIT 4.1 is discussed below:

DS5 – Ensure System Security

Within DS5 there are 11 high level control objectives. Generally all may be applicable to most organisation but it must be noted that they are high level Control Objectives which still require an organisation to design the actual control implementation.

An example taken directly from COBIT 4.1 is DS5.5 - Security Testing, Surveillance and Monitoring, suggests the following control objectives:

- Test and monitor the IT security implementation in a proactive way
- IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained
- A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.

While considering the above objectives, the organisation would implement actual controls (designed specifically to their environment) to achieve the above. Yearly those controls would be audited against the high level control objectives and the following maturity level from COBIT would be utilised for assessing maturity of the implemented controls:

- **Level 0 - Non-existent when** the organisation does not recognise the need for IT security
- **Level 1 - Initial/Ad Hoc when** the organisation recognises the need for IT security
- **Level 2 - Repeatable but Intuitive when** responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator, although the management authority of the co-ordinator is limited
- **Level 3 - Defined when s**ecurity awareness exists and is promoted by management and IT security procedures are defined and aligned with IT security policy
- **Level 4 - Managed and Measurable when responsibilities** for IT security are clearly assigned, managed and enforced
- **Level 5 - Optimised when** IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives.

Since COBIT is universally accepted, it provides a recognised and mature option to define controls, measure control maturity and utilise them as metrics to measure success or failure.

3.1.4. Key CIIP control consideration

Control metrics discussed during Section 3.1.3 would be measured off controls existing within a particular environment requiring controls to exist and to be measured. Controls form a key component in the protection of Critical Infrastructure and the identification of key controls will aid in the protection there-of. During Section 2.9.3, various security controls were considered in the context of protecting Critical Infrastructure. Since controls may vary in suitability across various environments, the identification there-of should be prescriptive. As such, the list in Section 2.9.3 is prescriptive in nature and should be seen in the context of minimum baselines applicable to most environments.

During Section 3.1.3, the use of Balanced Scorecard in conjunction with COBIT's generic IT Processes also provides the opportunity to define high level control requirements. Note that it is high level in nature compared to the prescriptive controls in Section 2.9.3. During this activity consider the identification of such key controls as a guidelines during subsequent phases.

3.1.5. Phase 1 Summary

During this phase a number of key foundational activities would have been performed. The deliverables that should have been completed would have been the IT Balanced Scorecard which should have enabled the identification of the businesses strategic objectives and aided in aligning IT objectives (operational and security), an essential component to the success of any initiative.

The identification of potential controls if aligned to the Balanced Scorecard would be "fit for purpose" and ultimately provide measurable metrics to indicate project success or failure. The consideration of security controls that will enable the protection of Critical Infrastructure should be seen as descriptive and not prescriptive in nature, since at this stage it would be premature to dictate specific controls, especially since no existing controls would have been reviewed.

In summary, once all phases of this framework have been completed, success or failure will need to be measured. Using the above, consider the balance between using existing metrics and developing new metric to measure success or failure.

3.2. Phase 2 - Identify Critical Infrastructure

During the Phase 1 (Section 3.1), the activities listed would have identified the businesses strategic objectives along with the IT's strategic objectives aligned to the business, with the option iteration in the identification of the InfoSec security objectives. As input to Phase 2, the Phase 1 objectives must drive the agenda in the identification of Critical Infrastructure.

Phase 2 is of strategic importance since the scope of the assessment and remediation will be defined. The process of how Critical Infrastructure is identified creates a direct opportunity to engage with Business, which if correctly facilitated will result in their involvement and ultimately their support of the initiatives going forward (Waters, 2007).

The activities for this phase strive to achieve a Top-Down approach that enables the identification of key business processes/services that will result in the identification of the underlying Critical Infrastructure required to be protected.

1. Perform Cyber Threat Assessment with Business and IT
2. Perform Business Impact Assessment using the Threat and Risk vectors identified
3. Identify Critical Infrastructure and key interdependencies
4. Agree scope as identified during the previous activity with the business.

The key artefacts for this phase are described below with the motivation and included activities described per activity:

- Cyber Threat modelling (Section 3.2.1)
- Business Impacts Assessment (Section 3.2.2)
- Identification of CII interdependencies (Section 3.2.3)
- Scope of CIIP assessment and remediation. (Section 3.2.4).

3.2.1. Perform Cyber Threat Assessment

The objective of the Threat assessment is to identify the potential threats applicable to CI whether they be natural, human or environmental, its causes and the potential impact on CI Confidentiality, Integrity and Availability (Dunn & Wigert, 2004). Risk and Threat assessments are usually performed in series however in context of this methodology the Threat assessment output is envisaged to be utilised as context to the Business Impact Risk Assessment discussed in the next Section.

The identification and vetting of the threat vectors (or actors) is not an IT responsibility but rather a joint responsibility between Business and IT. A key component of understanding the risks businesses faces through an attack on CI, is to understand where possible attacks may originate from. This will provide the ability to better understand and analyse the potential threats, while associating potential threats with potential consequences (Mateski et al., 2012).

Potential "threat actors", depicted in Figure 7, are referenced by Von Solms (2013) to include cyber threat sources such as Foreign Intelligence Services, disgruntled employees, extremist Organisations, hacktivists , organised Crime Groups and investigative journalists. The European Union Agency for Network and Information Security published threat landscape suggests threats to corporations include Competing Corporations, Cybercriminals, Employees, Hacktivists, Nation states and Terrorists (ENISA, 2013).

Figure 7 - Potential Threat Actors **(International Telecommunications Union, 2011)**

Understanding and applying threats metrics is often considered a rather immature practise, rather in overzealous measurement or none at all (Mateski et al., 2012). While the process of performing a Threat Assessment may not be an exact science, it should be seen as iterative and something is always better than nothing especially if it aids in awareness and acknowledgement for the initiatives at hand.

Van Solmns (2013) suggests the followings two key activities key in performing a Threat Assessment:

1. **Estimate the Actors Capability** – This would be focused specifically on an External Threat Assessment and would consider an Actors ability to exploit vulnerabilities to breach security in the context of a worst case scenario
2. **Estimate the Threats Actors Motivation** – This would consider factors driving motivation to breach security in the context of using the worst case motivation of any influencing Threat Source.

Across Actor Capability and Maturity, Von Solms (2013) suggests the following levels of risk and motivations that be considered when performing the threat modelling:

	Capability	Motivation
Level 0	Opportunistic attacks	No interest in attacking the system
Level 1	Opportunistic attacks	May casually investigate or attack a system if exposed to it, but not by design
Level 2	Some IT knowledge and resources for basic attacks (including the use of free malware, non-zero type attacks)	Actor will attempt to attack the system; but one person attack; part-time
Level 3	Considerable IT knowledge however actors lack the capability and resources to implement sophisticated attacks	Focused on the system; full-time attacker; with support from part-timers
Level 4	Very capable with the resources to execute sophisticated attacks using zero-day exploits involving significant customisation	Attack system frequently or constantly; several people; bribe or coerce
Level 5	Sophisticated attacks, well-funded and resourced.	Absolute priority employing detailed research in conjunction with social engineering, bribery and coercion

Table 5 - Capability/Motivation **(Von Solms, 2013)**

Figure 8 describes the associated risk rating by combining the motivation and capability level to identify the potential actors over threat potential (refer to specific diagrams through use of figure numbers):

Motivation Level	Capability Level				
	1	2	3	4	5
0	Negligible	Negligible	Negligible	Negligible	Negligible
1	Negligible	Negligible	Low	Low	Moderate
2	Negligible	Negligible	Low	Moderate	Substantial
3	Negligible	Low	Moderate	Substantial	Severe
4	Low	Low	Moderate	Severe	Severe
5	Low	Moderate	Substantial	Severe	Critical

Figure 8 - Threat Table Measurement **(Von Solms, 2013)**

In completion of this phase all threats actors would be rated against the above risk matrix as to identify possible threats actors used in the subsequent phase. Ensuring business involvement is key in achieving buy in as well as accuracy in performing the threat modelling and it is suggested that the modelling be performed through workshops with key stakeholders represented by Business and IT (Paul, 2013).

3.2.2. Business Impact Assessments

The Business Impact Assessment is adopted from Business Continuity Management leading practise (IBM, 2014). Is was specifically selected since it has a strong business focus and provides a *top down* approach in identifying Business/IT dependencies.

The Business Impact Assessment provides two direct outputs:

- Provide the identification of the key business processes and their underlying dependency on IT, while identifying assets that require the greatest level of protection (IBM, 2014)
- Provide insights into the planning of responses to various cyber related situations (Scarfone, Grance, & Masone, 2012).

The common activities (at a high level) that occur in completing the Business Impact Assessment are:

- **Identification** of key processes per department. This would include identifying the Recovery Time Objectives ("RTO") for each key processes (RTO is how long a process can be down before an unacceptable amount of impact is experienced). The type of impact will be categorised either as Financial, Infrastructure related, HSEQ and Reputational/Legal

- **Mapping** and the identification of key systems/infrastructure that support key business processes/services and the defined RTO's that would be identified
- **Process** dependencies are identified with external/internal departments/organisations.

These activities provide the context for identifying, at a high level, the key business processes and services, as well as the businesses reliance from a system/service perspective. There is much research available suggesting methodologies aiding in the identification of Critical Infrastructure, however many of these focus specifically on identifying interdependencies within Critical Infrastructure and between externally dependant infrastructures.

The above approach is tangible and feasible in quickly identifying an organisations Critical Infrastructure through the identification of key processes/services that are underpinned through technology. During Section 3.2.3, the activities performed during this section will form the basis for the final activities for Phase 2.

3.2.3. Identify CI related infrastructure and dependencies

The CIIP handbook provides various approaches to identifying Critical Infrastructure (which are discussed in more detail during this section) and what is critical during this phase is to not exclude key infrastructure as this may result in infrastructure with vulnerabilities being potentially exploited.

During this phase business dependencies should be mapped to systems/infrastructure as to identify Critical Infrastructure. To achieve this, it is suggested to utilise the ISA 99 stack to identifying infrastructure that may potentially be at risk. Consideration for the use of the ISA 99 topology structure for the identification of Critical Infrastructure provides a structured approach for infrastructure identification. It is suggested to specifically exclude Level 0 infrastructure since it may be possible and more beneficial to secure from Level 1 upwards while potentially logically securing Level 0. As such Level 0 devices should be specifically excluded from the scope of the assessment.

By establishing the "link" between key business processes/services that business provides and Critical Infrastructure aligned to ISA 99 stack, potential high risk business dependencies

are quickly identified. Figure 9 depicts the presentation of the interdependencies using the ISA 99 approach as discussed in this Section.

Substantiating risk for the environment will be performed during the subsequent phases during which vulnerabilities are identified. The costs of securing infrastructure .vs the potential impact is something that will aid in the exclusion of the scope items.

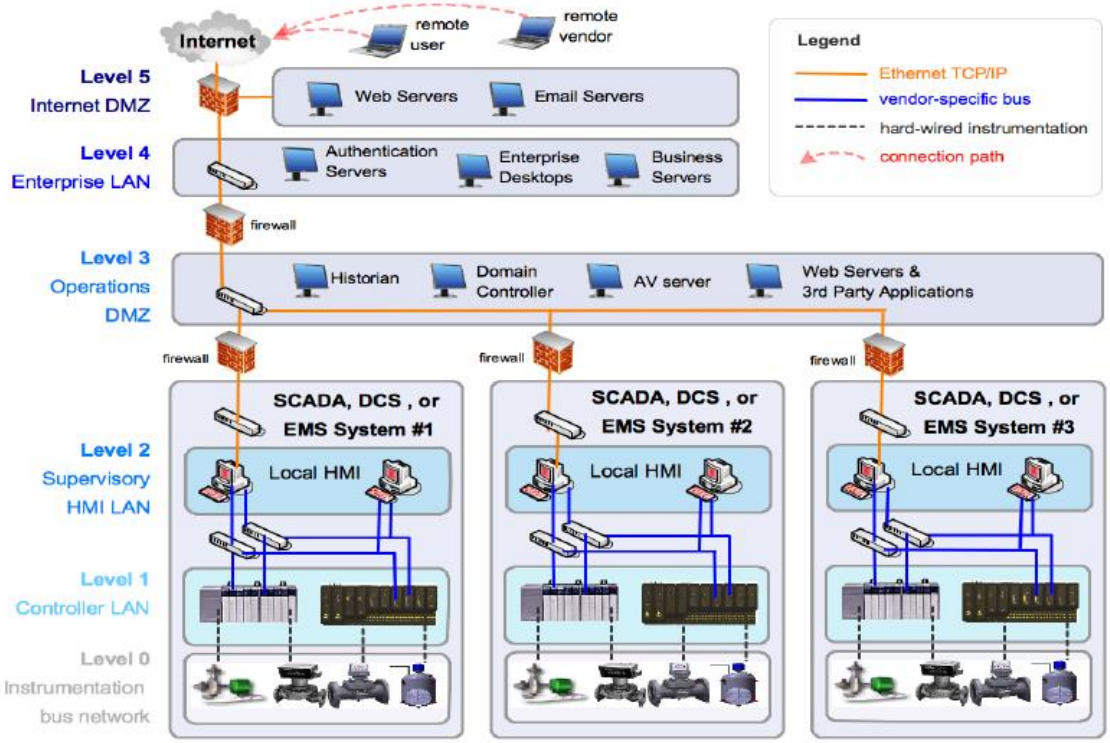


Figure 9 - ISA 99 Stacked Level Approach **(Pollet, 2011)**

There are other approaches to identifying Critical Infrastructure including the VAF framework (see Figure 10) as well as many other as discussed in CIIP handbook (Dunn & Wigert, 2004).

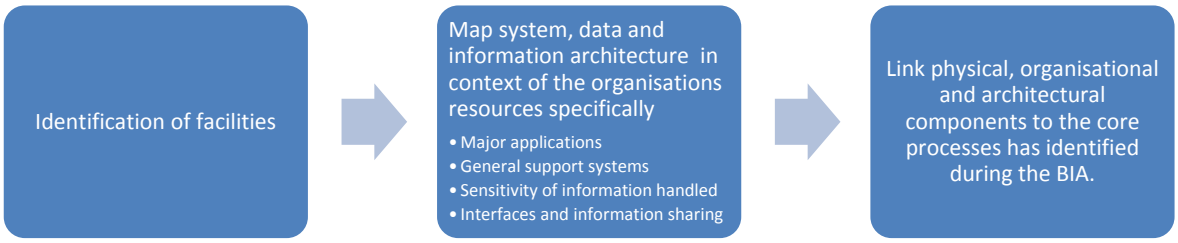


Figure 10 - CIIP Handbook - Identifying Critical Infrastructure**(Dunn & Wigert, 2004)**

The approach suggested (aligned to ISA99) for use in this framework would achieve the same results as the VAF framework and those suggested in CIIP, since they follow a similar logical

flow but are obviously aligned to the above activities. Figure 11 displays the mapping of key business processes to that of key applications (refer to Section 3.2.2) which in turn is mapped to underlying infrastructure. This would aid in the identification of the scope for Phase 3 and require detailed topology diagrams to identify all infrastructure for inclusion within.

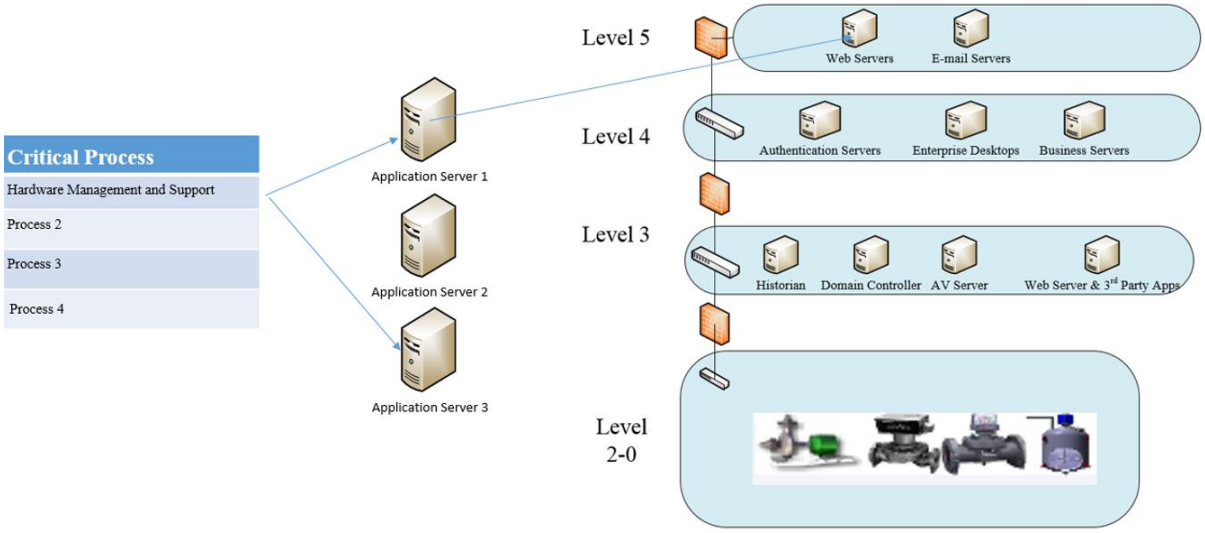


Figure 11 - Example of Process to Infrastructure Mapping

3.2.4. Agree scope and approach with the business

Having identified the Critical Infrastructure scope that will form the scope for Phase 3 (Section 3.3), the actual scope and approach for the assessment should be agreed assessment (to be performed during Section 3.2.5) with the business. Pieth (2004) suggests that budgets are generally the determining factor as to scope and approach of the assessments however suggests the following hierarchy of activities:

- Operational risk assessment
- Lab assessment
- Component testing
- Technical documentation review
- Functionality and configuration review
- Production assessment
- Technical documentation review
- Staff interviews
- Functionality and configuration review
- End-to-end penetration assessment.

While the above approach is aligned to ICS environments which by discussion/definition are well suited to Critical Infrastructure, it follows a risk based approach which is illustrated by the consideration of Lab assessment testing (item two on the list) before penetration (items ten on the list, the motivation for performing this test last is discussed in Section 3.3.2).

During Phase 3 (Section 3.3) an approach should be considered that is fit for purpose to the environment being evaluated and as such Pieth's guidelines should be used only as guideline and not as the *de facto* approach.

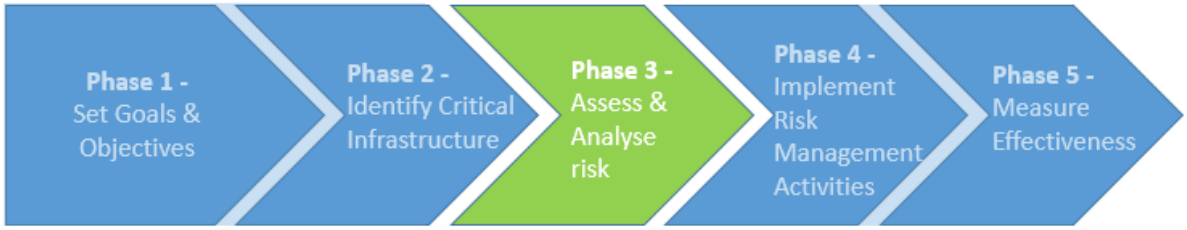
3.2.5. Phase 2 Summary

The outcome of the activities during the Phase 2 would have produced the following key artefacts:

- Cyber Threat modelling including the identification of actors
- Business Impacts Assessment, identifying key business processes that may be affected by a Cyber Attacks on CI
- Identification of CI interdependencies
- Scope and approach to assess CI during the subsequent phases.

Phase 1 and 2 activities have most been discovery in nature, with the aim of identifying the scope and approach for following Phase, *Assess & Analyse risk*. The bulk of the activity will now take phase during the Phase 3.

3.3. Phase 3 - Assess and analyse risk



This phase is dedicated to identifying vulnerabilities/deficiencies associated with the in scope Critical Infrastructure. The intention is to identify vulnerabilities and substantiating the risks associated with relevant vulnerabilities. One would be testing controls that would generally fall within the Technical, Management and Operational control domains.

The term vulnerabilities would be utilised for issues of a technical nature, with deficiencies rather describing Operational/Management related issues. Controls across these domains will either directly or indirectly contribute to the security posture of the environment, with a key objective being the ability to identify the security risks associated within the scope of Critical Infrastructure (and supporting systems) as identified during Phase 2 (Section 3.3).

Dunn and Wigert (2004) suggest that a risk assessment should analyse the probability of loss/damage resulting from potential threats. The consideration for the materialising of threats should be considered in context of the existing vulnerabilities/deficiencies and should achieve coverage across what could go wrong (scenario), the likelihood and the subsequent consequences (impact).

In answering *what can go wrong* (scenario) one would have to understand where the security vulnerabilities exist impacting the Confidentiality, Integrity and Availability of infrastructure as a result of potential deficient controls. This will require one to assess the likelihood of what vulnerabilities may be exploited as well as the consequences that may arise.

The CIPP handbook (The United States Government, 2000) suggests five examples of vulnerability assessment frameworks/methodologies for assessing Critical Infrastructure. The two selected from the CIPP handbook are United States Department of Energy ("DoE", refer to Section 3.3.1) and Vulnerability Assessment Framework ("VAF", refer to Section 3.3.2)

since they both provide extensive audit program guidelines (audit procedures enabling the identification of control weaknesses) which are modular in nature and are suitable for hybridisation.

During this section positive elements are selected from each methodology to provide an improved approach. One must consider again that this is merely a guideline and the user may substitute alternate options the approach.

3.3.1. VAF Framework

The VAF framework (Pieth, 2004) was developed by Critical Infrastructure Assurance Office and selected for hybridisation with the DoE vulnerability framework specifically for it objective of ensuring that Critical Infrastructure vulnerabilities were identified for both cyber related risks, traditional physical risks and its suitability for use by large government organisations as well as small government departments with no prior experience in infrastructure vulnerability assessments (Marwick, 1998).

The VAF framework consists of 3 high level phases of which the 2nd and 3rd phases are chosen as key high-level sub phase activities for use during Phase 3:

Figure 12 - VAF Framework **(Homeland Security, 2013)**

3.3.2. DoE framework

The scope of activities within the Assessment and Post Assessment phases were selected as guidelines within the specific VAF activity headings (*Gather data to identify vulnerabilities* & *analyse and prioritise vulnerabilities*) since their activities are well described enabling easier activity identification. The Figure 13 illustrates the DoE's scope to performing its Assessment and Post Assessment activities.

The DOE's *Pre-Assessment phase* have been mostly covered during Phase 1 and 2 (sub section 3.1 & 3.2), specifically the *Define objectives and Scope of Assessment* having been covered during Phase 2, and is therefore excluded. The *Establish Information Protection Procedures* would be specifically covered during the Phase 4 (sub section 3.4) and one would challenge the benefit of performing that activity now since we are yet to establish the potential vulnerabilities and associated risks and impacts. The *Identify and Rank Critical Assets* activity would largely have been achieved but from a business perspective through the identification of the process/service RTO's and subsequent mapping to ISA 99 level 4 (and below) Critical Infrastructure stacks, with underlying infrastructure specifics very much absent at this stage.

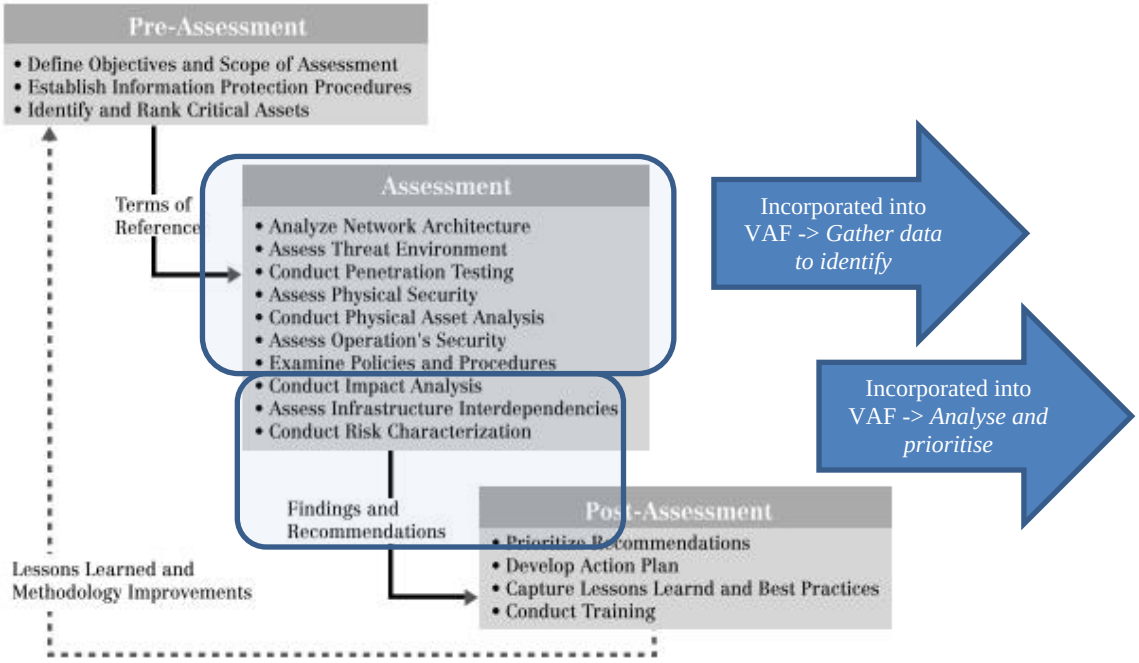


Figure 13 - DoE Framework **(Dunn & Wigert, 2004)**

For the activities listed under the DOE's *Post Assessment* phase, one would envisage many of these activities (namely Lessons Learnt, Best practise developed and Training Conducted*)* would best be performed during Phase 4 (Section 3.4) since the ability to develop "fit for purpose" content may only be realised after remediation activities are completed. It should also be noted that some recommendations may actually not be feasible and alternate recommendations may need to be agreed.

As such the following hybrid approach to Phase 3 is suggested:

- **Gather Data to identify vulnerabilities**
  - Analyse Network Architecture
  - Assess Threat Environment
  - Conduct Penetration Testing
  - Assess Physical Security
  - Conduct Physical Asset Analysis
  - Assess Operation's Security
  - Examine Policies and Procedures
- **Analyses and Prioritise**
  - Conduct Impact Analysis
  - Assess Infrastructure Interdependencies
  - Conduct Risk Characterization.

3.3.3. Gather and Identify Vulnerabilities

The *Gather and Identify Vulnerabilities* is the first activity envisaged for Phase 3. The ability to achieve "quick wins" are discussed for key domains and procedures, as aligned to the activities within Gather and Identify Vulnerabilities, which as per the hybrid approach consists of the list of testing within the DOE Assessment phase (refer to Section 3.3.2)

Both the DoE and the VAF framework provide audit based questions that are sufficiently generic to be applicable to most environments which can be used as guidelines for audit activities (Department of Energy, 2002; Pieth, 2004).

During Section 3.3.3.1, challenges to key areas of testing are discussed with guidelines aimed in reducing the risk in identifying CI vulnerabilities considering that many of this systems are live and impacting the operational environment is not an option as a result of testing.

One should consider that testing on live CI can potentially affect the availability of the systems resulting in failure or a system "unknown state". Pieth suggests that prior to exploiting a vulnerability, CI administrators should fully understand the context of the issue

and the ability to segregate that component from the main system or the ability to test the exploitation of vulnerability in a lab environment should be considered. Consideration for the ISA 99 infrastructure stack in context of where the greatest risk lies should form the basis of the testing strategy. Working on a Level 0 bus (actual infield devices) may result in direct production issues as those devices are very sensitive to the network traffic and be more susceptible for the testing performed. They are also generally better segregated from other networks and therefore testing at that level provides little value.

Breaking down the activities per level and halting the penetration test at the agreed level may reduce the risk around testing. It may also be prudent to involve the vendor during the assessments as device related vulnerabilities will need to be remediated by the vendor (as source code may not be available for debugging). Furthermore, Pieth suggests that by involving the vendor during the assessment they may be willing to share otherwise unavailable information making the assessment more successful (Gellings, Caskey, & Russell, 2010; Pieth, 2004).

3.3.3.1. Conduct Penetration Testing

A key consideration in the approach to improving ones overall security is from the Cyber Security Assessments of Industrial Control Systems Good Practice Guide which suggests that non-intrusive methods be utilised for assessing production ICS environments (Pieth, 2004).

To this point the DoE framework suggests the following 4 key activities during this phase:

- **Defining the rules of engagement (ROE)** – This would include establishing the scope of testing, start time & date, specific exclusions
- **Establishing a white cell** – This is essentially a team of "insiders" consisting of resources performing the testing as well as resources from the organisation. It provides an opportunity to ensure that key people within the organisation are aware of the test without letting anyone know since the ability to test the detection aspects of infrastructure could still be achieved this way
- **Designing and conducting the test (Methodology)** – This is an essential component of the actual penetration test. Deciding the scenario of attack is valuable for its potential to ensure the penetration test is a representation of a "real world" event. Types of scenarios

would include outside threats, Insider threats and associated 3rd parties. The activities within the methodology are discussed in further detail during this Section.

- **Writing the Final Report** – The greatest challenge with writing a suitable report is the ability to ensure that identified vulnerabilities are written in a manner that is suitable for business to understand as well as ensuring that the recommendations are fit for purpose and perhaps incorporate a staged implementation in the context of risk (should they be extensive in nature).

If an organisation is planning on performing a penetration test for the first time without having performed any vulnerability assessments, it may be prudent to first initiate a vulnerability assessment and remediate them prior to performing the penetration test. Furthermore, penetration testing is expensive since the resources are specialised in nature and the ability to perform these activities effectively internally would prove a challenge.

It should also be considered that a penetration test may introduce risk to the availability of systems especially in ICS type environments and as such vulnerability assessment will still identify vulnerabilities while reducing the risk associated with Penetration testing (Pieth, 2004).

Another key point to consider, is that most organisations can effectively perform a vulnerability assessment with existing in-house resources. Which also provides for a cost effective approach to identifying vulnerabilities and facilitates an environment where budget could rather be allocated for remediation. A concern against only performing a vulnerability assessment is that a vulnerability assessment report shows vulnerabilities and the potential risk of exploitation but in certain instances it does not in itself provide absolute confirmation (vulnerabilities with unknown exploits often found in applications) that vulnerabilities will lead to exploitation (resulting in doubt as the criticality identified). This could also be applied to penetration testing which in itself does not prove that every vulnerability was identified and every vulnerability was tested for the possibility of exploitation. It is a common view within the security community that support for a finding stemming from a successful exploit obtains more support than that of a vulnerability assessment.

Perhaps a perform middle ground would be an iterative approach to this challenge by having an organisation build towards full penetration testing. Based on my experience *Footprinting*

should be the first stage in identifying the potential target environments and in a penetration testing approach that has many iterations, (refer to Figure 14) foot printing activity preceding the actual exploitation is viable.

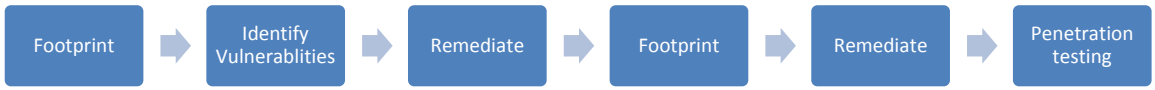


Figure 14 –Penetration Testing Methodology **(Gupta & Kaur, 2013)**

Penetration testing is generally an advanced skill performed by highly specialised individuals, who are very often in short supply (Rosewarne, 2013). Furthermore it is unlikely that many organisation have the ability to perform this aspect of technical testing in-house, as such it is advised to outsource this aspect of testing. Consideration of an outsourced providers who has experience in ICS related systems should be key especially in the context of the risks associated with the penetration testing of ICS systems.

Approaches to Penetration testing

When performing a penetration test on ICS environments it often suggested that grey box testing is most effective. Most organisations would prefer a "black box" type approach to the penetration testing as it traditionally meets "regulatory self-assessments requirements" however Pieth indicates that effective testing would require knowledge of the environment and as such one should "plan for the worst" and provide as much detail as possible or is feasible resulting in "grey box" testing (Pieth, 2004).

Pieth indicates that metrics are important to understanding or rather quantifying the risks associated with vulnerabilities and advocates the CVSS as a "standardised method of scoring vulnerabilities in a way that represents the risk to an individual organisation's unique environment". The CVSS framework is also free and provides additional tools which aid in risk rating vulnerabilities.

3.3.3.2. Examine Policies and Procedures

Effective Policies and Procedures are the foundation of any strong security environments. Researcher Fernandez (2005) identifies a number key security controls aimed to improve SCADA related infrastructure of which strong policies was the 2nd control encouraged.

The challenge with policies and procedures is that it will dictate the general security posture of the overall environment. Consider the lack of policies and standards relating to how servers are baselined within an environment. Baselines can be very subjective and as such configurations should be performed through the use of fit-for-purpose security baselines. This also provides a "yard" stick for vulnerability assessment/penetration testing phase as the ability to identify vulnerabilities that should have been resolved by the agreed security baseline often indicates the failure of key security processes.

The DoE describes seven key steps of which only critical key activities are considered and discussed below:

- Examination and review of the organisation document repository as to identify the policy and procedure gaps. Specific focus must be placed on the review of documents relating to Information Security related documents (acceptable use, information security, other related processes and procedures.
- A site visit should be performed to view the adherence to policies and procedures performed during business as usual activities with a view to identify additional policies and procedures that may aid to improve the overall security posture
- Interview key staff across demographics should be performed to gauge to adherence to policies and general awareness of their existence.

3.3.4. Analyse and prioritise

The final activity within Phase 3 – *Analyse and prioritise* will ultimately set the remediation scope for Phase 4 - Implement Risk Management Activities (refer to subset 3.4). As per the hybrid approach, the objective for this activity is to review findings and make recommendations through the following key activities:

- Conduct Impact Analysis
- Assess Infrastructure Interdependencies
- Conduct Risk Characterization.

During these activities recommendations should consider that since most environments are live, the ability to implement remediation actions may be limited and heavily dependent on maintenance windows. Furthermore specifically with CI, vendors would need to be engaged to discuss the remediation's and ensure that any potential changes will not impact CIA and as well as SLA's. The biggest challenge to these activities are understanding the infrastructure interdependencies & assessing the risk, as such these two activities are expanded.

3.3.4.1. Assess Infrastructure Interdependencies

DoE describes the assessment of Infrastructure Interdependencies as "physical and electronic (cyber) linkages" with the focus on the identification of Critical Infrastructure that supports critical facilities. It creates the context for identifying infrastructure that may have greater direct impact/dependencies on other processes/infrastructure/organisations which in itself is often CI's greatest weakness – making this activity vitally important (Collier & Lakoff, 2008). Identifying interdependencies has always been a challenge due to the very often complex environments and their breadth of reach (Jiaotong, 2009).

There are many suggested approaches to identifying CI interdependencies with the PreDict Interdependency Analysis (Refer to Figure 15) approach providing a simple yet effective manner in identifying interdependencies (specifically where Cyber world and physical meet) (Dunn & Wigert, 2004). The actual interdependency model is quite simplistic but that in itself is valuable and represents interdependencies in a grid format with different levels of detail that could be utilised with individual Critical Infrastructure components mapped to depict their interdependencies.

Another dependency mapping approach suggested by CIIP, is the *Process and Technology analysis* approach as depicted in Figure 16. This approach follows a 4 layer approach to dependency mapping – Core Functions, Infrastructure, Information & communication infrastructure and a sector based view. It differs from the Predict approach, in that it incorporates a more detailed mapping of dependencies (almost as much detail as the approach suggested in Figure 11).

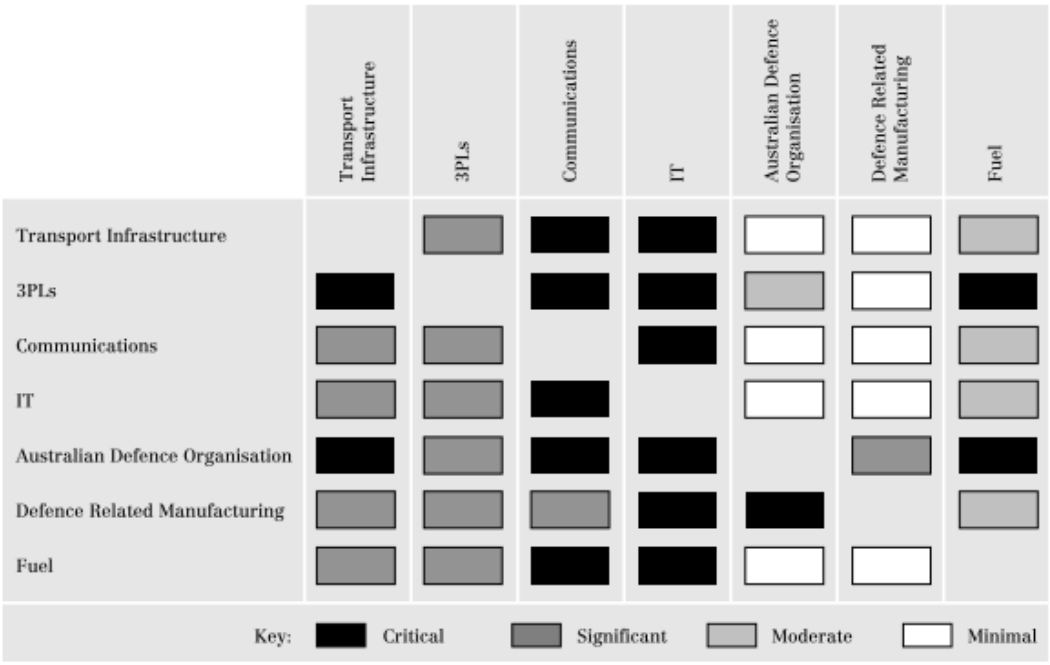


Figure 15 - The PreDict Interdependency Analysis **(Dunn & Wigert, 2004)**

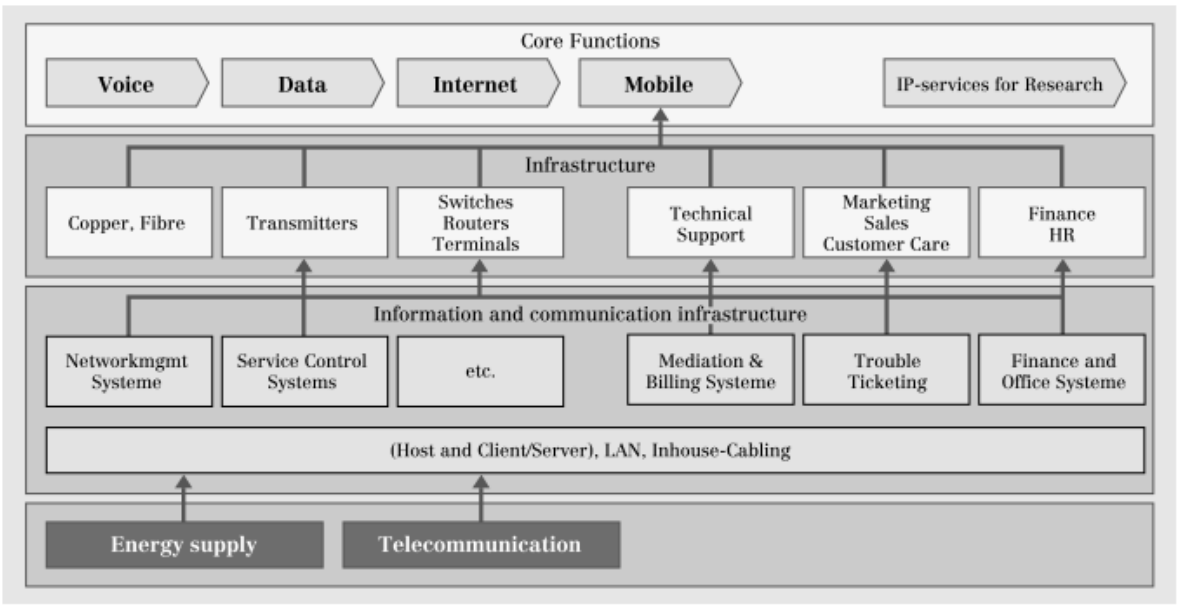


Figure 16 - Process and Technology analysis **(Dunn & Wigert, 2004)**

The Italian Cyber Security Report of 2013 (Marco, Arcuri, Baldoni, Ciccotelli, & Di Luna, 2013) considers six different dimensions to infrastructure interdependency analysis:

- Environment – condition of each environment
- Type of interdependencies – Physical, cyber, geographic and logical
- State of operation – effect during normal operating hours, times of disruptions or during repair
- Infrastructure characteristics
- Type of failures – whether interdependencies could be the cause of failure
- Degree of connexion – number of interdependencies which may create the intensity for failure.

The incorporation of the above dimensions into either of the suggested approaches may aid in fully understanding the characteristics of CI dependencies enabling a deeper understanding of the challenge at hand. One must considers that one of the suggested approaches may be more applicable to an organisation and as such the framework provides this flexibility based on the requirements.

In summary consider the Process and Technology approach (refer to Figure 16) for complex environment with Predict(Dunn & Wigert, 2004), refer to Figure 15, for simpler environments. Utilise the Italian Cyber Security reports (Marco et al., 2013) suggested dimensions where applicable within either approach.

3.3.4.2. Conduct Impact Analysis & Risk Characterisation

Impact Analysis and the Risk Characterisation as per the DoE framework were independent activities occurring at different phases through the approach. We have combined the activities to occur in a parallel manner as well as conduct them as part of the *analyse and prioritise* phase.

The context for this activity is to ensure that all potential technical, operational and management related deficiencies identified have an appropriate risk and potential impact rating so that a roadmap can be developed during Phase 4 (Section 3.4).

DoE suggests that the impact analysis should help to estimate the impact that a potential outage may have and suggests this as the "introduction" to *risk characterization*. DoE

mandates the use of quantitative formulas to estimate the impact however in the context of Critical

Infrastructure, dependency risks should also be considered and that may be challenging to identify the quantitative estimates (refer to Figure 17 for an example of the DoE Risk Characterisation). Ultimately the exercise results in the weight of expenditure to mitigate the vulnerability vs the risk (Department of Energy, 2002).

Recommendation Descriptions	Implementation Cost (SK)[4]	Implementation Time(weeks)	Change in Operating Cost ($k/yr)[b]	Attractiveness of Asset	Consequence Level	P_B	P_a	S_B	S_A	Technical & Cultural	Infrastructure Dependency

Figure 17 - DoE Risk Characterisation **(Department of Energy, 2002)**

The DoE risk characterisation framework is comprehensive and aids in objectively prioritising the recommendations resulting from the assessment. The framework builds upon the preceding phases using the specifically identified vulnerabilities, organisation specific threats (as developed during Section 3.2.1), and potential impacts when combining the two.

While security related risk criteria are quite specific, it is valuable to align the risk rating to those of the organisation's Enterprise Risk Framework ("ERF") ratings. This facilitates for the universal understand for the potential risks. Furthermore the ERF rating will be aligned to the financial losses applicable to either level of risk.

ENISA's approach to national level Risk Assessments is depicted in Figure 18, which provides an alternate approach to achieving *Conduct Impact Analysis & Conduct Risk Characterisation* objectives. Vulnerabilities are covered in a technical and non-technical manner along with the discussion of threats, although these are limited to Cyber related in nature and therefore by default exclude the *force majeure* type events.

This approach may prove more applicable since it considers key outputs created during the previous phases (Threats –Section 3.2.1 & Vulnerabilities –Section 3.3.3) and is less quantitative in nature, which may be more valuable in immature environments.

One of the suggested approaches by ENISA as to the creation of scenarios, is the UK's approach which suggests scenarios based on casualties, fatalities, economic harm, social disruption and psychological impact (Trimintzios & Gavrila, 2013).

The risk assessment would consider all inputs (as per Figure 18) as to understand the true risks associated with vulnerabilities identified, while taking into account the impact/likelihood of the scenarios materialising.

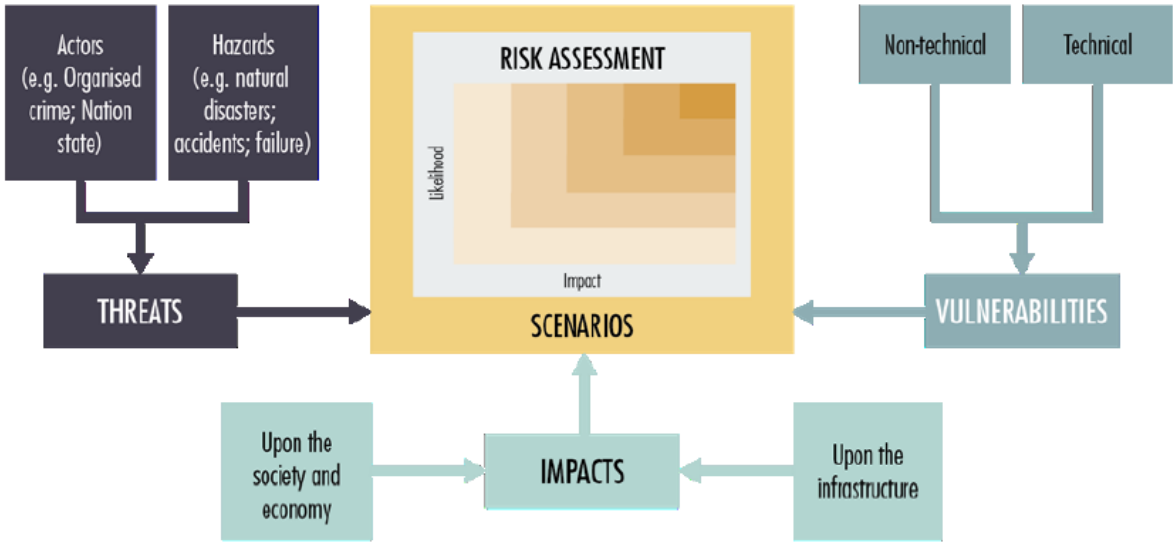


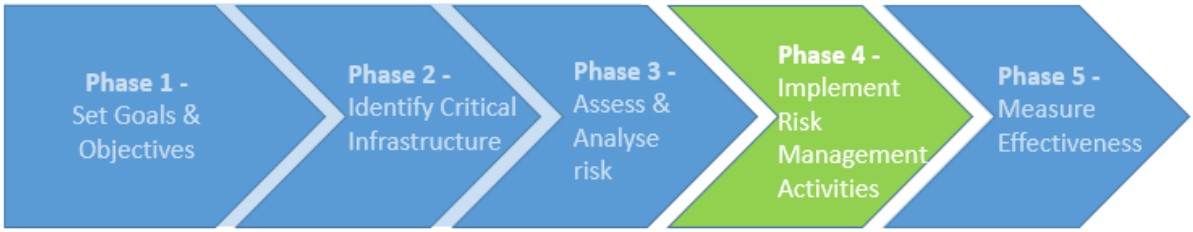
Figure 18 - ENISA National Level Risk Assessment **(Trimintzios & Gavrila, 2013)**

Regardless of which approach is chosen, they activities are key since they provide important context to Phase 4 (Section 3.4) which includes the development of a remediation roadmap. The risk and impact ratings created during the above activities will help ensure the roadmap correctly prioritises based on risk.

3.3.5. Phase 3 Summary

Phase 3 objectives are to identify vulnerabilities and analyse them for remediation. A key activity for this phase was to quantify the risk associated with the identified vulnerabilities as well identify key infrastructure interdependencies, a key activity in reducing Critical Infrastructure interdependency risks. Furthermore, ensuring these activities were conclusively performed is key as anything that was overlooked will not be remediated during Phase 4.

3.4. Phase 4 - Implement Risk Management Activities



During the preceding phase, phase 3, vulnerabilities across various domains were identified and the priorities for remediation agreed based on the identified vulnerabilities. At a high level NIPP describes the following activity domains relating to this phase:

- Identify, Deter, Detect ,Disrupt and Prepare for Threats and Hazards
- Reduce vulnerabilities
- Mitigate Consequences.

The challenge with this phase if not what to do but rather how to go about doing it. Often remediation efforts are required to be performed in a stacked approach to ensure that they don't reoccur. An illustrative example would be vulnerabilities relating to patching. If a vulnerability assessment is performed and vulnerabilities are identified relating to patching issues, remediating the vulnerability by patching would be a point in time fix however as new patches are released, unless a patching process is implemented its likely vulnerabilities will re-occur. As such the Phase 4 activities differ from that of NIPP, DoE and VaF which specifically aim to remediate identified vulnerabilities in the scope of the initiative as a point in time exercise.

Security consulting firm Ciber suggests that it's "time for operationally mature security solutions that address multiple security risks with systemic fixes that permanently reduce risk" (Bassett, 2008). Organisations should appreciate that remediation is not an exact science and remediation may overrun in both time and budget. DoE suggests that remediation plans should include timelines, staffing assignments and associated budgets.

When developing roadmaps, a key consideration is that remediation activities may have interdependencies and efforts should be spent to try and identify them so prioritisation can be as accurate as possible. Consideration should also be given to focus on the quick wins that

provide improved risk reduction and improved security with the least amount of effort and cost.

The roadmap should attempt to go beyond this by setting about positive change in how security is embedded in the organisation which could be achieved through the establishment of a Security Transformation Program. As such Phase 4 objectives are as follows:

- Initiate a program to bring about the overall improved change in the Cyber Security posture
- Ensure that the security culture of the organisation changes
- Ensure the program is design and structured to achieve change with key strategic sub projects.

3.4.1. Establishment of a Security Evolution Program

The greatest challenge during remediation activities is for individual projects to lose momentum and to avoid this it may be required to establish a Security Evolution Program which is responsible for driving remediation activities through existing organisational structures.

Consideration of the challenges facing Security Transformation Programs would be valuable in ensuring success by not repeating the same errors. Consulting firm Deloitte (2008) suggests the following key challenges which Security Transformation initiatives face:

- Lack of common vision
- Lack of buy-in from stakeholders
- Immature delivery of capabilities
- Information overload.

To limit the potential for these risks to materialise the following key principles should be adhered to during the establishment of a program (Godfrey, 2008):

- A steering committee should be established consisting of key stakeholders from Business and IT. They should be responsible for on-boarding strategic resources, establishing the Project Management Structure, reporting guidelines, establish and prioritise the delivery of a roadmap

- A detailed charter should be established identifying the responsibilities, benefits and mandate of the program
- The consideration for the inclusion of external security consultants with key expertise would improve the success for the transformation initiatives, especially if existing skills within the organisation are lacking.

One should also consider that there will be various projects within the security transformation program. Remediation's can be viewed in the short term as to mitigate existing risks but in the long term to ensure control robustness. Controls requiring similar remediation or rather remediation involving the same root cause can be grouped together to form sub project. The objective of this activity is to work through the vulnerabilities identified and confirm an appropriate project home which ultimately will develop and remediate a solution within the sub projects.

Owners for each project within the program should be identified and should be required to report back to the program steering committee. The steering committee will ultimately be responsible for approving program budgets (which will consist of project budgets) and will be responsible for reporting back to executives on the progress of the program.

The associated risks and potential impact of the identified deficiencies should aid the steering committee prioritise project budgets and resources and agree the subsequent program timelines (and the detailed projects). The establishment of sub projects is discussed in Section 3.4.2.

3.4.2. Establish projects

Each project within the transformation program would have very different requirements and therefore require different skills. To ensure consistency is structure, reporting and quality, each project should align to an appropriate project governance structure.

A proposed project methodology (refer to Figure 19) was selected from the SANS institute since has a strong review component within it and is based on the established 4 step project methodology (Rodgers, 2002). It should also be noted that the approach suggested is generic where possible and may not be applicable to all project or initiatives.

Figure 19 - SANS Project Methodology **(Rodgers, 2002)**

3.4.2.1. Concept phase

The Concept phase is responsible for establishing the project along with the high-level scope. A key output in this phase is the development of a business case which is approved along with the creation of the project charter (It may not be always necessary to develop a business case due to the pre-existing program).

3.4.2.2. Requirements phase

The project requirements phase is key since it defines what the project must achieve. During this phase all stakeholders, business process engineers, and analysts must all be engaged with the project manager and IT as to define the requirements.

3.4.2.3. Analysis and Design Phase

From across the organisation engineers and business must engage with one another to work through the identified vulnerabilities and establish the required future state. If the remediation requires the implementation of tools then a Technical design specifications should be created.

3.4.2.4. Execution Phase

This phase is made up of 4 sub activities:

- **Build phase** – this phase sees the creation/modification or remediation of vulnerabilities. Persons with the appropriate skills should be developing a solution to ensure it meets the requirements
- **Test phase** – This would be the natural progression for the proposed remediation activity to transition into QA or a staging area. A full test plan (integration, system, regression, performance testing) will occur during this time
- **Implementation phase** – Once all testing is complete, the final remediation/initiatives are promoted to the production environment
- **Post Implementation phase** – During this phase the changes must be monitored, defects logged and resolved.

3.4.3. Phase 4 Summary

The ability to remediate environments is very often better achieved through an effective Security Transformation Program. Key is effectivity grouping the remediation of vulnerabilities into key projects within a Security Evolutionary Program. This provides a structured approach to implementing and monitoring remediation while providing structured and documented reporting to senior management.

3.5. Phase 5 - Measure effectiveness

The NIPP methodology describes the final phase as the process of "measuring effectiveness" as being a process that should evaluate the achievement of objectives through the measurement of the collected data as to assess progress of the objectives. During Phase 1 (Section 3.4), goals and objectives would have been established in the form of metrics. It was also discussed that the process of measuring metrics for success consists of the three phases, Collection, Validation and Processing. Phase 5 would be the process of validating and processing the metrics to measure the success of the program.

Besides measuring the success of the program during this final phase of the framework, with all remediation activities completed, it would an opportune time to ensure Lesson are Learnt from the program activities.

With this in mind Phase 5's objectives are to:

- Collect data and compare metric result as to measure the success of the program
- Ensure that lessons learnt from the program and its sub projects are recorded and incorporated into future efforts to ensure continuous improvements.

3.5.1. Measure the success of the program

Since the framework is designed to be iterative in nature, the first time it is completed certain metrics may only be measurable on the second iteration. If mature security metrics are pre-existing then it may be possible to validate and process to substantiate success at this point. Since most organisations struggle with validating and processing metrics to identify value, SANS institute researcher Payne suggests that often threats cannot be measured since it's the potential for harm combined with the fact that the practise of metric measuring is in the early stages of development making measuring success difficult (Payne, 2006).

Metrics traditionally would be gathered from vulnerability management systems such as Qualys and Nessus and since metrics originating from those system would generally be "moving targets" (based on the facts that these systems collect patching vulnerabilities) and as such of little value to measure success of this program.

Metrics would need to have been established during Phase 1 and if no data was collected, one would have to consider reverting back to basic metric analysis such as - the number of vulnerabilities remediated through route cause remediation versus a *point is time* remediation. This would require being creative with the metrics available and then substantiating remediation success. While very basic in nature it still provides an opportunity to measure the success of the program.

A critical aspect of reporting on the metrics is ensuring what happens directly thereafter, as successes and failures should be learnt from and utilised to improve the security posture. In Section 3.5.2 the activities around this sub phase are discussed.

3.5.2. Lessons Learnt

Reviewing the program, the activities and findings provides an opportunity to gather information that could benefit other programs/projects in the future. Lessons learnt may not always be positive in nature but may consist of undesirable results which one would want to avoid in the future (United States Government, 2015).

The CIO's office of the US Government describes lessons learnt as simply asking *"What worked well or what didn't work so well?"* (United States Government, 2015). NIPP describes lessons learnt as a positive influence to aid in adaption of risk management activities and objective of a program to incorporate lessons learnt (Homeland Security, 2013). Furthermore by applying lesson learnt through the application of corrective actions it may ultimately reduce vulnerabilities that exist within the environment (Homeland Security, 2013).

Establishing a Lessons Learnt exercise should ensure that something is always learnt from the experience. Where there is an opportunity for innovation, the approach should be documented and shared to ensure application and where possible processes improvement (United States Government, 2015).

During Section 3.5.1, the identification and review of metrics may include useful information for where the program/projects succeeded or failed. This will aid in ensuring that insight is achieved. The process of formalising lessons learnt could be achieved through a question style information sheet submitted to teams to discuss and report back on. Valuable insight could be documented and circulated among key persons (United States Government, 2015).

Metrics identified where favourable and non-favourable results were achieved could be used as topic points of questionnaires or workshops where the results are discussed among the project teams with outcomes documented and circulated.

The Project Management Institute endorses an approach by engineer Terrell (Michael, 2014) for an effective lessons learnt:

- Recognition for the need to have such a program
- Selecting a champion to oversee the program
- Ensuring the team member share in accountability
- Encourage and reward the support of the program
- Ensure effective communication of the results to the team.

3.5.3. Phase 5 Summary

Activities performed during Phase 5 ultimately aim to measure the success of the initiatives, specifically activities performed during Phases 2-4. The metrics identified during Phase 1 would ultimately be utilised to measure the success and would contribute to the lessons learnt.

How the lessons learnt are documented and circulated is almost secondary, what is key though is that the improvements identified are implemented. Depending on the extent, it may be necessary to formalise the remediations under suitable projects, depending on the extent of feedback received. Since the framework provides for continuous application and maturing of the organisation, the lessons learnt should be incorporated into the next iteration when applying the framework.

3.6. Summary

The proposed Framework is described as Hybrid in nature and should be seen as a guideline which organisations can follow and make the necessary changes or apply the appropriate exclusions based on their specific environments.

The activities across the various sections within the proposed framework aim to achieve the following defined objectives (defined at the beginning of Section 3):

- Ensure the approach is interactive in nature
- Scalable to suit organisations with varying levels of maturity
- Provides a top down approach, linked to key business processes
- Has applicability across various environments.

During Chapter 4, key activities of the proposed hybrid framework are applied as a simulation based on a fictitious organisation as to illustrate the applicability or rather suitability of the framework to achieve the above defined objectives. By applying key activities it provides further context to the value of the framework and potential improvements offered through the “hybrid approach”.

Chapter 4

Framework case study simulation

The purpose of the case study is to simulate the application of the framework against a typical organisation. The application of the case study covers key aspects of the hybrid framework, as shown in Figure 3, across the five phases.

Since many of the activities within the hybrid framework are extensive in nature, it is quite challenging to simulate all activities. Furthermore there may be better value in focusing on key activities that are simpler to illustrate but difficult for immature environments to execute on, making it suitable for the challenging foundational activities to form the basis of the simulation.

The key activities within the scope of case study are listed below per phase:

- Phase 1 – Set Goals & Objectives
  - Identify the key business strategic objectives
  - Map IT objectives to that of business

- Phase 2 – Identify Critical Infrastructure
  - Perform Cyber Threat Assessment with Business and IT
  - Perform the Business Impact Assessments
  - Identify CI infrastructure and key interdependencies
  - Agree scope & approach with the business
- Phase 3 – Assess & Analyse risk
  - Analyses and Prioritise
    - Conduct Impact Analysis
    - Assess Infrastructure Interdependencies

Please note that Phases 4 and 5 are specifically excluded from the scope of the simulation due to requirement to have detailed information in-order to provide valuable output for those phases.

4.1. Scenario

Open Telecom, a telecommunications provider servicing the SOHO and SME market has recently become the target of a Cyber attack that resulted in the failure of key services being delivered to customers. The impact of the Cyber attack resulted in a 5% drop in its share price as well as the invocation of penalties for inability to deliver key services which resulted in financial losses for the quarter. The telecommunications providers has over 3000 SME clients and manages the network infrastructure for South Africa's Top 100 companies.

Post forensic investigations were inconclusive due to the lack of available logging and monitoring information as well as the inability to confirm the validity of information that was collected. It is believed that the attack may not actually have been intended for Open Telecom but rather one of its customers. Open Telecom Board of Directors has mandated the CIO to perform a full evaluation on the environment and report back to the board on vulnerabilities identified and the plan for remediation. Figure 20 depicts the departmental structure of the organisation that will be used during the scope of the simulation.

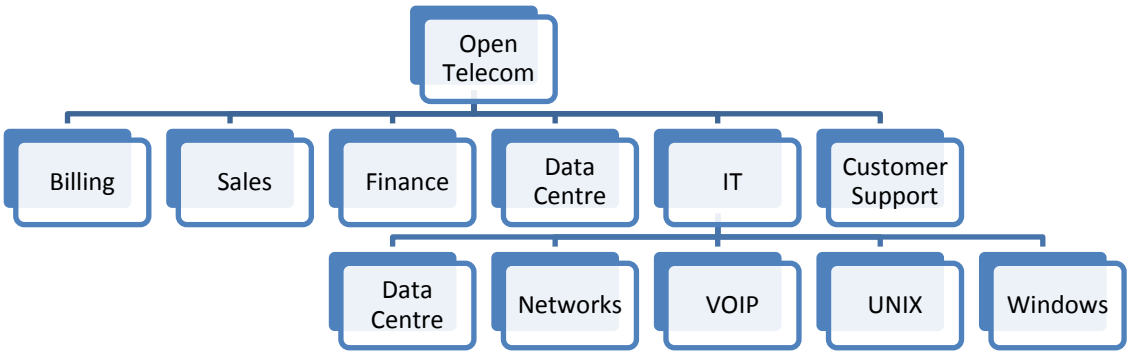


Figure 20 - Open Telecom Structure

4.2. Phase 1 – Set Goals and Objectives

Open Telecom's key strategic objectives as per its financial statement is:

- To provide market leading services to its clients
- Provide a positive return on investment in IT
- Improve customer service
- Achieve internal compliance and prompt mitigation of key risks
- Sustain growth with strategic investment
- Increase customers penetration of Internet Services
- Ensure improved redundancy of service offerings through service continuity and availability
- Create agility in the ability to respond to changing business requirements
- Recruit and retain skilled and motivated persons.

As per the hybrid approach, the businesses strategic objective will be applied to the balanced scorecard with the appropriate aligned IT objectives defined (refer to Figure 21). By combining the context of drivers as well as the business strategic objectives, the goals and objectives for the program can be defined.

Link Business goals to OpenTelecom Goals

Area	No.	Open Telecoms Business Goals	IT Objectives
Financial Perspective	1	Provide a positive return on investment in IT	Improve IT cost-efficiency and its contribution to buisness profitability
	2	Achieve internal compliance and prompt mitigation of key risks	Establish clarity of business impact of risk to IT objectives and resources
Customer Perspective	3	Improve customer service	Ensure IT service are available as required
	4	To provide market leading services to its clients	Improve IT cost-efficiency and its contribution to business profitability
	5	Ensure improved redundancy of service offerings through service continuity and availability	Ensure minimum business impact in the event of an it service disruiption or change
	6	Sustain growth with strategic investment	deliver projects on time and on budget, meeting quality standards
Internal Perspective	7	Ensure governance structures and policies are aligned with external governments requirements	Respond to governance requirements in line with the board direction
	8	Achieve internal compliance and prompt mitigation of key risks	Ensure proper use and performance of the applications and technology solutions
	9	Create agility in the ability to respond to changing business requirements	Define how business functional and control requirements are translated in effective and efficient automated solutions while ensuring IT agility
Learning and Growth Perspective	10	Recruit and retain skilled and motivated persons.	Aquire and maintain IT skills that respond to the IT Strategy

Figure 21 – Example of a Business/IT Mapped Balanced Scorecard

By reviewing defined IT objectives as well as the buisnesses strategic objectives in the context of the Cyber attacks and recent downtime experienced, the goals and objectives are suggested to be:

- Understand the threat landscape facing Open Telecom
- Identify material vulnerabilities and remediate
- Identify infrastructure that is not maintained according to policies and procedures
- Ensure the infrastructure is implemeted to achieve high availability through fault tollerance.

4.3. Phase 2 – Identify Critical Infrastructure

During phase 2 and within the scope of the scenario, the hybrid frameworks chosen activities are to:

- Perform Cyber Threat Assessment with Business and IT
- Identify CII infrastructure and key interdependencies.

Sections 4.3.1 - 4.3.5 detail the output of the above two activities.

4.3.1. Phase 2 – Perform Cyber Threat Assessment with Business and IT

Potential Cyber threat sources facing Open Telecom were presented to key representative of Business and IT for the purpose of discussing the relevance of the presented Cyber threat sources as well as discussion for inclusion of additional Cyber threat sources. The output from the workshop included a threat assessment based on the motivation and capability of potential threat sources. An overall Threat Risk rating, as per Figure 22, was applied to each potential threat source as well as a motivation.

The Motivation and Capability descriptions as per Table 5 (Section 3.2.1) were utilised for the workshops. The weightings identified, as illustrated in Figure 22, are illustrative in nature only. The Threat Risk Rating was achieved through the use of the table as per Figure 8 (Section 3.2.1.).

Threat Source	Motivation	Capability	Threat Risk Rating
Disgruntled employees	1	2	Negligible
Extremist Organisations	3	3	Moderate
Hacktivists	4	4	Severe
Nation States	1	1	Negligible
Corporations	2	2	Negligible
Organised Crime Groups	3	5	Severe
Customers of Open Telecom	3	4	Substantial

Figure 22 - Threat Risk Rating

Based on the results from the above threat assessment, customers of Open Telecom and Hacktivists were identified as posing the greatest risk to Open Telecom. Since Open Telecom provides Internet Connectivity and Managed Network services to its customer, one could understand how those two entities provide the greatest risk. Since Open Telecoms customers may be targeted the shared networks (key dependencies) would essentially affect Open Telecoms other customers should the attack be severe.

4.3.2. Phase 2 - Business Impact Assessment

The Business Impact Assessment would generally be performed in a workshop style format with a developed BIA template being projected and representatives from the department working together to complete it. As context to this phase, extracts from Business Impact Assessments are detailed per area (Section 3.2.2).

Process Name	Headcount per process	Process Description	Critical periods	Comments (regarding Days & Time)	Process Type
Hardware Support and Management	7	Business as usual activities relating to the maintenance, configuration, and repairing of hardware, operating systems and SAN storage nationally (Cape Town, JHB & Durban)	Every day is critical	This is key process and those servers not only support customers but also enable the operation of Open Telecoms.	Partially Automated

4.3.3. Phase 2 – Functional Breakdown

The functional breakdown would be performed for each department within Open Telecom and within in each department the key business processes would be identified and expanded as per Figure 23. Of key consideration is the *Headcount per process* that would be the number of persons involved in the process and the *process type* which relates to whether the process is automated or not (which will be important when identifying underlying dependency on systems with the consideration for manual process options).

Figure 23 - Functional Breakdown Example

4.3.4. Phase 2 – Business Impact Assessment

Figure 24 depicts the outcome of the Business Impact Assessment for the process as described in Section 3.3.2. Please note that the process impact would be considered across various impact categories. During Section 4.3.5 the underlying system dependencies are identified during which the critical impact, as defined by the Recovery Time Objective ("RTO"), will aid in establishing the criticality of Infrastructure.

Process name	Type of impact	0-4 hours	4-8 Hours	Failure up to 2 Days	< 1 week	< 1 month	> 1 month
Hardware Management and Support	Financial	Low	Low	Low	High	High	High
	Legal/ Regulatory	No impact	No impact	No impact	High	High	High
	Health and Safety	No impact	No impact	No impact	No impact	No impact	No impact
	Reputational	Low	Low	Medium	High	High	High
	Infrastructure	Medium	High	High	High	High	High
	Greatest impact	Medium	High	High	High	High	High
	RTO Required	4-8 Hours					

Figure 24 - RTO Table

4.3.5. Phase 2 – Identify CI related infrastructure and dependencies

The key system dependencies, as presented in Figure 25, represent the mapping of critical business processes to that of supporting systems that essentially can be deemed at *critical*. By mapping the key supporting system to the underlying infrastructure it now becomes possible to map Critical Infrastructure. Topology diagrams as suggested in Section 3.2.3 would probably be the easiest way to identify the supporting infrastructure by tracing from a Level 5 stack down.

System	Dependant Process	Process RTO	Internal Dependency	External Dependency	Required RTO	Required RPO
System 1	Hardware Management and Support	4-8 Hours	Customers, Internal Systems	Eskom, Telkom, Neotel	4-8 Hours	0-2 Hours
System 2	Hardware Management and Support	4-8 Hours	Customers, Internal Systems	Eskom, Telkom, Neotel	4-8 Hours	0-2 Hours
System 3	Hardware Management and Support	4-8 Hours	Customers, Internal Systems	Eskom, Telkom, Neotel	4-8 Hours	0-2 Hours
System 4	Hardware Management and Support	4-8 Hours	Customers, Internal Systems	Eskom, Telkom, Neotel	4-8 Hours	0-2 Hours

Figure 25 - Critical Dependency Mapping

Figure 26 represents graphically the mapping of critical process to the application stack and the infrastructure and from this, phase 3 scope will be defined.

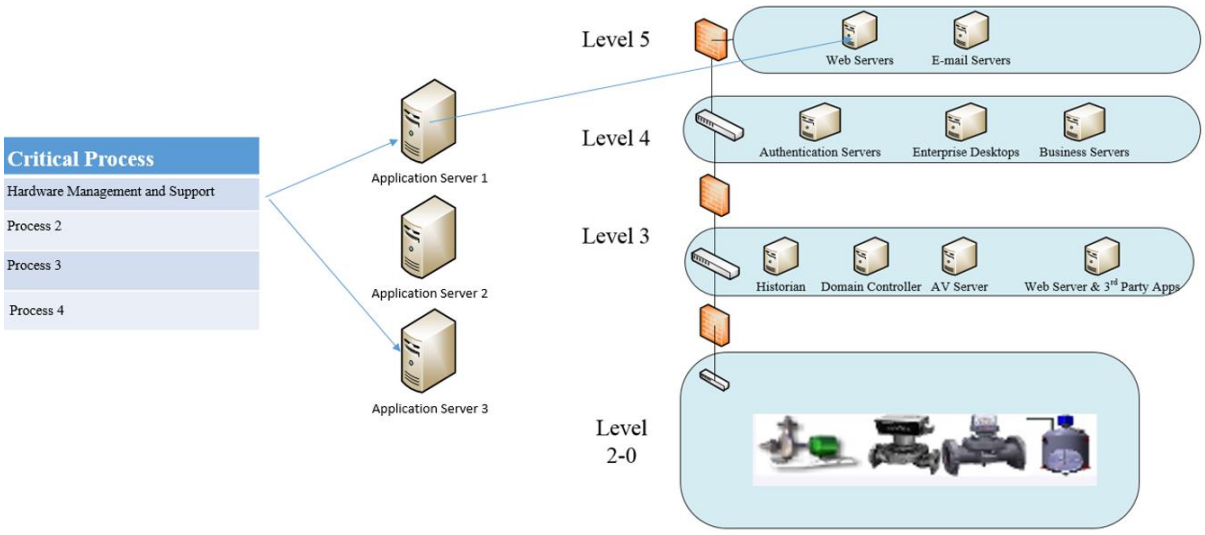


Figure 26 - Process to Infrastructure Mapping

4.3.5.1. Phase 2 - Agree scope & approach with the business

During Phase 2, the identification of critical processes, mapped to critical systems, mapped to critical infrastructure, would have aided in defining the scope that would now be discussed and agreed with the business. The benefit in this approach in the hybrid framework is that it provides a top down approach driven largely by business drivers, as opposed to bottom up that would traditionally be driven by business. Once the scope is agreed it provides the platform for Phase 3, the most critical phase, of the hybrid framework, which is essentially the gap analysis.

4.3.6. Phase 3 – Analyse and Prioritise

The key activities for Phase 3 are to:

- Identify key dependencies in Open Telecom's infrastructure based on its services/identification of infrastructure dependencies
- Conduct the Impact Analysis & Conduct Risk Characterisation.

4.3.6.1. Phase 3 - Assess Infrastructure Interdependencies

The application of the PreDict approach on Open Telecom maps the dependencies on processes to key applications as depicted Figure 27. Where this differs from the activities that produced Figure 26 (4.3.5) is that you are adding a dependency critical rating to each dependency. The output of this activity provides context to the criticality of the dependency which will be utilise during Section 4.3.6.2.

	Application 1	Application 2	Eskom	Telkom	Neotel
Hardware Management & Support	Critical	Significant	Moderate	Minimal	None
Process 2					
Process 3					
Process 4					
Process 5					
Process 6					

Figure 27 - PreDict application on Open Telecom

4.3.6.2. Phase 3 - Conduct Impact Analysis & Conduct Risk Characterisation

For this activity ENISA's National Risk Assessment is utilised, which was discussed during Section 3.3.4.2. To illustrate the application of inputs for simulation, the risk assessment will be performed a single instance.

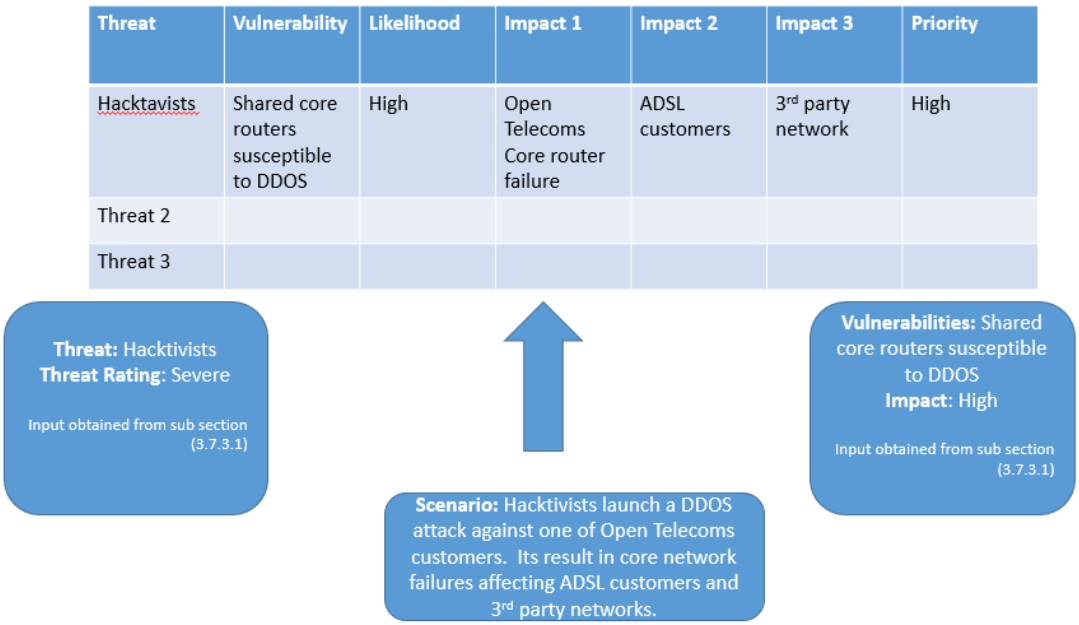


Figure 28 - Application of ENISA Risk Assessment

4.4. Summary

As discussed during Section 4.1, Phases 4 and 5 are specifically excluded from the scope of this simulation due to requirement to have detailed information from Phase 3 which would form the foundation to complete the deliverables for Phases 4 and 5.

Phase 4 and 5 would specifically deal with the development of a roadmap for remediation of identified vulnerabilities and ultimately enable the process of remediation, which in the above simulation would be challenging to illustrate.

Chapter 5

Conclusion

Critical Infrastructure is at risk and in order to protect it one needs to understand what is deemed as critical before it can be protected. Once it is known was is critical, it is important to understand what one is protecting it from. During the research traditional Infrastructure such as Electricity, Water and Airports was considered as Critical with a new entrant being the critical importance of the Internet.

The Internet as a new entrant into the category of Critical Infrastructure, is largely since Society has become very reliant on the Internet as tool for communications and of course Commerce's reliance on the internet to transact. The reliance on the Internet as a global communications network was identified as one of the greatest risks to Critical Infrastructure. The Internet provides the perfect medium for interconnecting Critical Infrastructure, managing Critical Infrastructure remotely and also the perfect platform to attack Critical Infrastructure.

The risk of attack on Critical Infrastructure is largely relevant now since the evolution of Critical Infrastructure communication from serial and dedicated communications lines to that

of an IP based network. Through the use of poorly implemented security controls, these IP based network have been exposed to the Internet.

To try and substantiate the risk that Critical Infrastructure faces, the threats and challenges were discussed through key case studies/real world examples including examples of Cyber Crime and Cyber warfare (refer to Section 2.6). Furthermore the definitions and motivations were discussed in the context of CI.

The awareness to protect CI of countries globally was identified through specific examples where developed economies have initiated steps through legislation and focus groups to drive the awareness and protection of Critical Infrastructure. Key examples of strong security controls were identified applicable to various sectors and industries (refer Section 2.9.3) including controls that are often found to be deficient in CI environments.

Understand the security control that should be implemented in CI is important, but identifying the deficient controls or rather the vulnerabilities within the environment is a critical challenge. Critical Infrastructure environments can generally span large geographic areas and one should also consider that some environments have key interdependencies on other environments and other environments on it. Therefore identifying vulnerabilities and testing for vulnerabilities may be very complicated and for first time assessments a daunting task.

5.1. Research Objectives

The core objectives of the research were achieved as follow:

Provide context for what is considered to Critical Infrastructure and why it is now at risk - During Section 2.1 context was provided as to what would be considered to be Critical ranging from water, roads, airports and the Internet. During Section 2.6 justification was provided as to why Critical Infrastructure is now as risk including examples of where the evolution of Critical Infrastructure has introduced risk.

Identify the overlap between Critical Infrastructure and Critical Information Infrastructure - The advent of the Internet as Critical Information Infrastructure through its

prolific use of it as a global network was discussed during Section 2.2 as well as in Section 2.7.

Identify key attacks on Critical Infrastructure in the context of Cyber Warfare and Cybercrime - Examples of Cyber Crime were discussed during sections 2.7.1 - 2.7.3 as well Cyber Warfare during sections 2.8.1-2.8.3, during which both instances included discussions surrounding the nature of the attacks and the consequences.

To identify methodologies applicable to the protection of Critical Infrastructure in the context of immature environments – The NIPP approach as well as the OECD approach to Critical Infrastructure protection was discussed during Section 2.9.1 and 2.9.2 respectively.

Propose activities that will enable the protection of Critical Infrastructure in the context of the proposed methodology, including the identification of appropriate activities per phase of the methodology - During Section 3 of research, a hybrid framework was developed based on various other frameworks relating to Critical Infrastructure protection. The framework was largely based on the NIPP framework for protecting Critical Infrastructure, however the detailed activities that one should conduct were quite high level and as such the framework identified key activities for key phases along with examples providing real life context to the application of the framework.

For certain sections extensive detail was provided and in many cases more than one approach to a phase was discussed. The framework (like all framework) should be seen as a continual evolving approach and users of the framework should substitute key activities for other activities should they feel improved suitability for their application.

Identify at a high level appropriate controls for protecting Critical Infrastructure - During Section 2.9.3 various key controls were discussed that would aid in the protection of Critical Infrastructure. The benefit of Cyber Incident Forensic Readiness was discussed in detail in Section 2.10.

5.2. Future Work

The framework should not be seen as final product but rather a work in progress. Areas that could be explored and developed further are as follows:

1. Critical Infrastructure dependency modelling could be improved and justified through real-life case studies
2. Collation of breach data among Critical Infrastructure would be insightful including root cause analysis
3. Development of specific Critical Infrastructure security metrics would be advantageous.

In closing, the research and the proposed framework provides a strong starting point for organisations that want to understand the importance of identifying and protecting Critical Infrastructure to do so. The framework is tangible and activities are well articulated for immature environments, potential controls aiding in the protection of Critical Infrastructure are discussed with the appropriate context.

References

Abbadi, Z. (2006). *Security Metrics What Can We Measure ? What is a " Metric ."* Retrieved January 19, 2014, from https://www.owasp.org/images/b/b2/Security_Metics-_What_can_we_measure-_Zed_Abbadi.pdf.

Abrams, M., & Weiss, J. (2008). *Malicious Control System Cyber Security Attack Case Study*. Retrieved December 14, 2014, from http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf.

Advanced Micro Controllers Inc. (2014). *AMCI : Tech Tutorials : What Is A Programmable Logic Controller (PLC)?*. Retrieved December 23, 2014, from http://www.amci.com/tutorials/tutorials-what-is-programmable-logic-controller.asp

Ahamad, M., Amster, D., Barrett, M., & Cross, T. (2008). *Emerging cyber threats report for 2009*. Retrieved December 23, 2014, from http://smartech.gatech.edu/handle/1853/26301

Ahuja, S., & Goldman, J. E. (2009). Integration of COBIT . Retrieved December 22, 2014, from https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2009-21.pdf

Akuta, E. A., Monari, I., & Jones, C. R. (2011). Combating Cyber Crime in Sub-Sahara Africa ; A Discourse on Law , Policy and Practice, (May), 129–137. Retrieved December 23, 2014, from http://www.interesjournals.org/full-articles/-combating-cyber-crime-in-sub-sahara-africa-a-discourse-on-law-policy-and-practice.pdf?view=inline

Ashmore, W. C. (2008). *Impact of Alleged Russian Cyber Attacks*. Retrieved November 21, 2014, from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA504991

Badger, D. (2010). *Posts about balanced scorecard on Duke does digital marketing*. Retrieved January 21, 2015, from https://dukedoesdigitalmarketing.wordpress.com/tag/balanced-scorecard/

Banks, J., & Massy, K. (2012). *Nuclear power in developing countries? Let's talk about it*. Retrieved September 20, 2013, from http://www.globalpost.com/dispatches/globalpost-blogs/commentary/nuclear-power-developing-countries-discussion

Bassett, ed. (2008). IT Security Operational Maturity : Why you need more than personal heroism and silver bullets. Retrieved December 15, 2014, from http://www.technologyexecutivesclub.com/Articles/security/op.php

Bologna, S. (2005). The need to improve local self- awareness in CIP / CIIP. In *IEEE International Workshop on Critical Infrastructure Protection 2005*.

Borchard, J., Fox, J., Long, T., Mcveigh, B., & Moodie, M. (2008). WMD Insights. *Defense Threat Reduction Agency*. Retrieved September 17, 2013, from http://cns.miis.edu/wmd_insights/WMDInsights_2008_03.pdf

BusinessWorld. (2009). *The Dangerous Web*. Retrieved September 19, 2013, from http://www.authbridge.com/media-centre/authbridge-in-news/print-coverage/152-the-dangerous-web.html?

Byres, E. (2005). *SCADA Security Basics: SCADA vs. ICS Terminology*. Retrieved July 31, 2014, from https://www.tofinosecurity.com/blog/scada-security-basics-scada-vs-ics-terminology

Cain, C., & Couture, E. (2011). *Establishing a Security Metrics Program*. Retrieved September 12, 2013, from http://www.sans.edu/student-files/projects/jwp-caincouture-whitepaper.doc

Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: Evaluating measures adopted by South Africa and other regional role players. Institute of Foreign and Comparative Law. Retrieved from http://www.jstor.org/stable/23253117

Clemente, D. (2013). *Securing "the homeland" - Cyber Security and Global Interdependence: What Is Critical?*. (K. S. Cavelty, Myriam Dunn; Kristensen, Ed.). Routledge.

Collier, S. J., & Lakoff, A. (2008). The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation.

Constantin, L. (2013). *Poor SCADA Security Will Keep Attackers and Researchers Busy in 2013*. *www.cio.com*. Retrieved September 19, 2013, from http://www.cio.com/article/724602/poor_SCADA_Security_Will_keep_Attackers_and_Researchers_Busy_in_2013

CounterTack. (2012). *A Cyber-readiness Reality Check*. Retrieved February 19, 2014, from http://www.countertack.com/a-cyber-readiness-reality-check

Criminaljusticedegreehub.com. (2013). *What is Cybercrime? at Criminal Justice Degree Hub*. Retrieved May 21, 2013, from http:/what-is-cybercrime/

De Wet, P., & Benjamin, C. (2015). *National key points: The list you weren't meant to see*. *Mail & Guardian*. Retrieved January 29, 2015, from http://mg.co.za/article/2015-01-22-national-key-points-the-list-you-werent-meant-to-see

Department of Energy. (2002). Vulnerability Assessment Methodology - Electric Power Infrastructure. Retrieved from htts://www.hsdl.org/view&did=439919.pdf

Dewalt, D. (2009). *Virtual Criminology Report 2009*. Retrieved September 19, 2013, from http://www.goodharbor.net/media/pdfs/VCR_2009_EN_VIRTUAL_CRIMINOLOGY_RPT_NOREG.pdf.

Du Toit, C. (2008). *JSE denies hacker attack*. *ITWeb*. Retrieved July 09, 2014, from http://www.itweb.co.za/index.php?option=com_content&view=article&id=9728

Dunn, M., & Wigert, I. (2004). *CIIP Handbook 2004*. (J. Wenger, Andreas;Metzger, Ed.). ETH - Swiss Federal Institute of Technology Zurich. Retrieved from

Ellefsen, I., & Von Solms, S. (2012). A Framework for the Implementation of a National CIIP Structure for Developing Nations. Retrieved September 19, 2013, from http://www.csir.co.za/dpss/docs/Ellefsen_Framework for Cyber Security Structure in Developing Nations.pptx.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23–40. doi:10.1080/00396338.2011.555586

Fernandez, J. D., & Fernandez, A. E. (2005). SCADA systems: vulnerabilities and remediation. *Journal of Computing Sciences in Colleges*, *20*(4), 160–168. doi:10.1109/MSPEC.2003.1222043

Fick, J. (2009). *Cyber crime in South Africa: Investigating and prosecuting cyber crime and the benefits public-private partnerships*. In *Council of Europe octopus interface conference cooperation against cybercrime* (pp. 10-1).

Fleming, M. H., & Goldstein, E. (2012). Metrics for Measuring the Efficacy of Critical-Infrastructure-Centric Cybersecurity Information Sharing Efforts. *Available at SSRN 2201033*.

Forster, K. (2012). Session 14 : Functional Security in a Process Environment. In *Session 14* of the 2012 Safety Control Systems Conference (pp. 1–9).

Gellings, C. W., Caskey, J. F., & Russell, B. D. (2010). *The Electricity Grid*. (C. Arenberg, Ed.) (Volume 40,.). National Academy of Engineering. Retrieved September 19, 2013, from http://www.nae.edu/TheBridge

Godfrey, K. (2008). Shifting gear. *Nursing Times*, *95*(11), 27.

Gorman, S. (2009). *Hackers Stole IDs for Attacks - WSJ*. *The Wall Street Journal*. Retrieved August 04, 2014, from http://online.wsj.com/news/articles/SB125046431841935299

Gupta, A., & Kaur, K. (2013). Vulnerability assessment and penetration testing. *International Journal of Computer & Communication Technology*, *3*(6-8), 71-74.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks : Digital Threats and Multinational Responses Revisiting the. *Journal of Strategic Security*, *4*(2), 49–60.

Homeland Security. (2013). *National Infrastructure Protection Plan*. Retrieved April 13, 2014, from http://www.dhs.gov/national-infrastructure-protection-plan

Hyslop, M. (2007). *Critical information infrastructures: Resilience and protection*. Springer Science & Business Media

IBM. (2014, May 6). *IBM - Business impact analysis*. IBM Corporation. Retrieved October 12, 2014, from http://www-935.ibm.com/services/nz/en/it-services/business-impact-analysis.html

International Crisis Group. (2008). *Russia vs Georgia: The Fallout*. Retrieved September 19, 2013, from http://www.crisisgroup.org/~/media/files/europe/195_russia_vs_georgia___the_fallout.ashx.

International Telecommunications Union. (2011). *ITU National Cyber Security Strategy*. Retrieved September 19, 2013, from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

IT Governance Institute. (2005). IT Alignment: Who Is in Charge? Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/IT-Alignment-Who-Is-in-Charge_res_Eng_0105.pdf.

IT Governance Institute. (2007). *CoBIT 4.1*. ISACA.

IT News Africa. (2013). *South African cybercrime set to soar in 2013*. *IT News Africa*. Retrieved May 25, 2013, from http://www.itnewsafrica.com/2013/01/south-african-cybercrime-set-to-soar-in-2013/

Jenik, A. (2009). Cyberwar in Estonia and the Middle East. *Network Security*, *2009*(4), 4–6. doi:10.1016/S1353-4858(09)70037-6

Jiaotong, X. (2009). *Survival from Disaster : Interdependencies Management in Critical Infrastructure Networks*. Retrieved September 14, 2013, from http://www.collectionscanada.gc.ca/obj/thesescanada/vol1/BVAU/TC-BVAU-12268.pdf

Kent, K., Chavalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response*. *NIST Special Publication*. Retrieved August 08, 2013, from http://cybersd.com/sec2/800-86Summary.pdf

Keren, A., & Elazari, K. (2012). Internet as a CII-A framework to measure awareness in the cyber sphere. In Cyber Conflict (CYCON), 2012 4th International Conference on (pp. 1-13). IEEE.

Kozlowski, A. (2014). Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. European Scientific Journal, 10(7).

Kumar, M. (2011). *Anonymous takes down Sony Pictures US and UK sites*. Retrieved November 08, 2014, from http://thehackernews.com/2011/04/anonymous-takes-down-sony-pictures-us.html

Kushner, D. (2013). *The Real Story of Stuxnet - IEEE Spectrum*. Retrieved September 19, 2013, from http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Luiijf, E., Burger, H., & Klaver, M. (2003). Critical Infrastructure Protection in The Netherlands : A Quick-scan. Retrieved September 19, 2013, from

https://www.emsec.rub.de/media/crypto/attachments/files/2011/03/bpp_13_cip_luiijf_burger_klaver.pdf.

Luiijf, H., & Klaver, M. (2000). In Bits and Pieces. Retrieved September 19, 2013, from www.infodrome.nl

Marco, A., Arcuri, M., Baldoni, R., Ciccotelli, C., & Di Luna, G. (2013). *2013 Italian Cyber Security Report*. Retrieved September 12, 2013, from http://www.dis.uniroma1.it/~midlab/articoli/13CIS-Report.pdf.

Markoff, J. (2008). *Before the Gunfire, Cyberattacks - NYTimes.com*. Retrieved August 04, 2014, from http://www.nytimes.com/2008/08/13/technology/13cyber.html

Marwick, P. (1998). Vulnerability Assessment Framework 1.1, (October). Retrieved from http://cipbook.infracritical.com/book3/chapter7/ch7ref2.pdf

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., & Frye, J. (2012). *Cyber Threat Metrics*. Retrieved September 12, 2013, from http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-065.pdf

Mboneli, N., & Herbst, D. (2010). *Critical Information Infrastructures Security*. (E. Rome & R. Bloomfield, Eds.) (Vol. 6027). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-14379-3

Meinhart, R. (2006). *Analysis of U.S. Water Infrastructure from a security perspective*. Retrieved from http://www.strategicstudiesinstitute.army.mil/pdffiles/ksil353.pdf

Michael, T. (2014). *Implementing a lessons learned process that works*. Retrieved December 29, 2014, from http://www.pmi.org/learning/1999/Implementing-a-lessons-learned-process-that-works-1157

Military Operations Research Society. (2010). Batter Integrating Risk Analysis Into Critical Infrastructure Security Policies and Programs. In *Homeland Secruity Studies and Analysis Institute* (pp. 1–5).

Miller, B., & Rowe, D. (2012). A survey SCADA of and critical infrastructure incidents. *Proceedings of the 1st Annual Conference on Research in Information Technology - RIIT '12*, 51. doi:10.1145/2380790.2380805

Mohapi, T. (2013). *Cybercrime increase in South Africa forecasted for 2013*. Retrieved May 21, 2013, from http://www.humanipo.com/news/3140/Cybercrime-increase-in-South-Africa-forecasted-for-2013

Moteff, J., Copeland, C., Fischer, J., Ave, I., & Washington, S. E. (2003). Report for Congress Received through the CRS Web Critical Infrastructures : What Makes an Infrastructure Critical ? Retrieved from http://www.fas.org/irp/crs/RL31556.pdf

Moteff, J., & Parfomak, P. (2004). CRS Report for Congress Received through the CRS Web Critical Infrastructure and Key Assets : Retrieved September 14, 2013, from http://www.fas.org/sgp/crs/RL32631.pdf

Njotini, M. N. (2013). Protecting Critical Databases. *Southern African Legal Information Institute*, *16*(1), 451–536.

OECD. (2008). *Recommendation of the Council on the Protection of Critical Informatin Infrastructures*. Retrieved February 21, 2014, from http://www.oecd.org/sti/40825404.pdf

Onstott, C. (2014). Cyber Security Readiness : How to Improve Cyber Security Readiness, (September). Retrieved September 19, 2013, from http://ftknox.afceachapters.org/docs/AFCEA_Sept_Meetingl.pdf

OWASP. (2006). *Monitor security metrics*. Retrieved May 18, 2014, from https://www.owasp.org/index.php/Monitor_security_metrics

Paul, M. (2013). *The Ten Best Practices for Secure Software Development*. Retrieved May 13, 2014, from https://www.isc2.org/uploadedfiles/(isc)2_public_content/certification_programs/csslp/isc2_wpiv.pdf

Payne, S. C. (2006). *A Guide to Security Metrics*. Retrieved June 29, 2014, from http://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55

Pieth, M. (2004). *Cyber Security Assessment of Industrial Control Systems*. doi:10.4337/9781845421618.00007

Pollet, J. (2011). *Securing the move to IP-SCADA/PLC Networks*. Retrieved May 13, 2014, from http://www.cpni.gov.uk/documents/publications/2011/2011034-scada-securing_the_move_to_ipbased_scada_plc_networks_gpg.pdf?epslanguage=en-gb

Ponemon Institute LLC. (2013). *Risk-Based Security Management*. Retrieved May 19, 2014, from http://www.ponemon.org/blog/the-state-of-risk-based-security-management

Pothier, M. (2013). *The National Key Points Act*. *Southern African Catholic Bishops Conference*. Retrieved June 18, 2014, from http://www.eplo.org.za

Ragnarsson, J. K. (2010). *Cyber-security and Critical Infrastructure Protection: The Case of Iceland*. University of Haskoli. Retrieved September 19, 2013, from http://www.atlantic-community.org/app/webroot/files/articlepdf/cybersecurity.pdf

Rinaldi, B. S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Infrastructure Resilience in the UK: An Overview of Current Approaches. In *ICSI 2014@ Creating Infrastructure for a Sustainable World* (pp. 23-32). ASCE.

Riptech. (1999). *Understanding SCADA System Security Vulnerabilities Talking Points*. Retrieved March 13, 2014, from http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf

Rodgers, D. H. (2002). *Implementing a Project Security Review Process within the Project Management Methodology*. *Infosec Reading Room*. Retrieved March 15, 2014, from

http://www.sans.org/reading-room/whitepapers/modeling/implementing-project-security-review-process-project-management-methodology-987

Rome, E., & Bloomfield, R. (2010). *Critical Information Infrastructures Security*. (E. Rome & R. Bloomfield, Eds.) (Vol. 6027). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-14379-3.

Rosewarne, C. (2013). *The South African Cybert Threat Barometer for 2012/3*. Retrieved October 18, 2014, from http://www.wolfpackrisk.com/research/south-african-cyber-threat-barometer/

Ruus, K. (2008). *Cyber War I: Estonia Attacked from Russia | Winter/Spring 2008*. Retrieved August 01, 2014, from http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html

Saull, R. (2000). *The IT Balanced Scorecard*. *ISACA.org*. Retrieved October 11, 2014, from http://www.isaca.org/Journal/Past-Issues/2000/Volume-2/Pages/The-IT-Balanced-Scorecard-A-Roadmap-to-Effective-Governance-of-a-Shared-Services-IT-Organization.aspx

Saull, R. (2003). Linking the IT Balanced Scorecard to the Business Objectives at a Major Canadian Financial group. Retrieved October 12, 2013, from www.uams.be/itag

Scarfone, K., Grance, T., & Masone, K. (2012). Computer Security Incident Handling Guide-Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Shachtman, N. (2009). *Top Georgian Official Moscow Cyber Attacked Us – We Just Can't Prove It Danger Room*. *WIRED*. Retrieved November 14, 2014, from http://www.wired.com/category/dangerroom/

Sproles, J., & Byars, W. (1998). *Cyber-terrorism*. *ETSU*. Retrieved May 24, 2013, from http://csciwww.etsu.edu/gotterbarn/stdntppr/#Define

Stimac, S. D. (2013). *SANS TOP 20 Controls/Metrics - Information Security Standards and Guidelines - UWM Tech Wiki*. *TeckWiki*. Retrieved from https://techwiki.uwm.edu/pages/viewpage.action?pageId=7421037

Stouffer, K., & Scarfone, K. (2011). Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology.

Tashi, I., & Ghernaouti-Hélie, S. (2007). Security metrics to improve information security management. Las Vegas. Retrieved from http://www.isy.vcu.edu/~gdhillon/Old2/secconf/secconf07/PDFs/47.pdf

The Centre for the Protection of National Infrastructure. (2005). An Introduction to Forensic Readiness Planning Technical Note, (May). Retrieved October 12, 2013, from http://www.cpni.gov.uk/Documents/Publications/2005/2005008-TN1005_Forensic_readiness_planning.pdf

The Centre for the Protection of National Infrastructure. (2011). Securing the move to IP-based SCADA/PLC networks Types, (November). Retrieved from http://www.cpni.gov.uk/documents/publications/2011/2011034-scada-securing_the_move_to_ipbased_scada_plc_networks_gpg.pdf

South African Government. Electronic Communications Security (PTY) LTD Act No 68 of 2002 http://www.saflii.org/za/legis/num_act/ecsla2002473.pdf

The Presidency. Electronic Communications Security Act 2002 (2003). South Africa. Retrieved from http://www.saflii.org/za/legis/num_act/ecsla2002473.pdf

The United States Government. (1997). *Protecitng America's Infrastructure*. Retrieved October 11, 2013, from https://www.fas.org/sgp/library/pccip.pdf

The United States Government. (2000). National Plan for Information Systems Protection. Retrieved from https://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf

The United States Government. (2009). Overview of the Cyber Campaign Against Georgia, (August). Retrieved October 12, 2013, from http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

Theron, P., & Bologna, S. (2013). *Critical Information Infrastructure Protection and Resilience in the ICT Sector* (p. 318). IGI Global. Retrieved from http://www.igi-global.com/book/critical-information-infrastructure-protection-resilience/70773

Traynor, I. (2007). *Russia accused of unleashing cyberwar to disable Estonia*. Retrieved July 31, 2014, from http://www.theguardian.com/world/2007/may/17/topstories3.russia

Trimintzios, P., & Gavrila, R. (2013). *National-level Risk Assessments*. Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report

United States Government. (2015). *Lessons Learned*. Retrieved December 29, 2014, from http://ocio.os.doc.gov/CommerceITGroups/Commerce_IT_Review_Board/PROD01_007947

US Office of Personal Management. (2014). *Using a Balanced Scorecard Approach to Measure Performance*. Retrieved October 11, 2014, from http://www.opm.gov/policy-data-oversight/performance-management/reference-materials/historical/using-a-balanced-scorecard-approach-to-measure-performance/

Viveros, S. (2012). *Pacific Northwest National Laboratory Report Reveals Dramatic Increase in Cyber Threats and Sabotage on Critical Infrastructure and Key Resources*. Retrieved November 09, 2014, from http://www.mcafee.com/cf/about/news/2012/q2/20120618-01.aspx

Von Solms, S. (2013). ITU National CyberSecuirty Strategy Guide. Retrieved October 01, 2014, from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

Wall, K. (2006). The state of municipal infrastructure in South Africa and its operation and maintenance. Retrieved October 12, 2013, from http://www.cidb.org.za/Documents/KC/cidb_Publications/Ind_Reps_Other/ind_reps_state_of_municipal_infrastructure.pdf

Wang, A. J. A. (2005). Information security models and metrics. *Proceedings of the 43rd Annual Southeast Regional Conference*, *2*, 178. doi:10.1145/1167253.1167295

Waters, K. (2007). *Why Most IT Projects Fail. And How Agile Principles Help | All About Agile*. *allaboutagile.com*. Retrieved October 17, 2014, from http://www.allaboutagile.com/why-most-it-projects-fail-and-how-agile-principles-help/

Watts, D. (2003). Security & Vulnerability in Electric Power Systems. *In 35th North American Power Symposium*, vol.2, pp. 559–566.

Wenger, A., Metzger, J., & Dunn, M. (2004). Critical Infrastructure Protection : Survey of World-Wide Activities . 1, (September 2002), 1–10. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/paper_studie_en_pdf.pdf?__blob=publicationFile

Willke, B. J. (2007). *A Critical Information Infrastructure Protection Approach to Multinational Cyber Security Events*. Retrieved October 11, 2013, from http://www.enisa.europa.eu/activities/cert/events/files/ENISA_best_practices_for_ciip_Willke.pdf

Zorz, Z. (2012). *Info about 0-day SCADA flaws offered for sale*. *Help Net Security*. Retrieved November 15, 2014, from http://www.net-security.org/secworld.php?id=13994