Management of Risks associated with De-perimeterisation

Kwok Keong, LEE

Technical Report

RHUL-MA-2009-07

16th February 2009

Department of Mathematics

Royal Holloway, University of London

Egham, Surrey TW20 0EX, England

http://www.rhul.ac.uk/mathematics/techreports

Management of Risks associated with De-perimeterisation

Name: LEE, Kwok Keong
Student Number: 100592656

Supervisor: Peter Wild

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London

I declare that this assignment is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people. I declare that I have also read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences and in accordance with it I submit this project report as my own work.

Signature:

Date: 5 September 2008

Abstract

Our IT world today is facing *de-perimeterisation*, a term used by the Jericho Forum to represent the breaking down of the traditional network perimeters that protects an organisation's internal network from the external threats. This is due to highly connected inter-networks, proliferation of remote workers, outsourcing & partnership caused by changing business models and the weakening of the firewalls because of the numerous "holes" punched by new applications. There is without doubt that de-perimeterisation is happening and it brings many threats to organisations. One such organisation is a law enforcement agency which is the authority to fight against crime. Equipped with high-tech equipment and using latest advanced systems, the law enforcement agency has relied quite heavily on IT to assist it in its day-to-day operations. In face of budget constraints and with implementations of cost-cutting measures, the law enforcement agency is not spared the effects of de-perimeterisation and is also facing threats associated with de-perimeterisation. The understanding of these threats, analysing them and proposing countermeasures and recommendations to mitigate the risks are the focus of this study.

Acknowledgement

The author would firstly like to thank his supervisor Professor Peter Wild for his guidance on the project. His valuable advices have greatly strengthened the view points of the study. Next, deepest gratitude is expressed towards the author's organisation and superiors for giving him the opportunity to pursue this excellent Masters of Science course in Royal Holloway University. Last but not least, special thanks go to the author's family members and all his friends including numerous international friends that he has made in Royal Holloway for their support in making the author's stay here in UK the most wonderful one-year of his life. Thank you.

Table of Contents

List of Figures

List of Tables

List of Acronyms

ASP	Application Service Provider
B2B	Business-to-Business
B2C	Business-to-Customer
BERR	Department for Business Enterprise & Regulatory Reform
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DoS	Denial of Service
D-P	De-Perimeterisation
DRM	Digital Rights Management
DSL	Digital Subscriber Line
HQ	Headquarters
HVAC	Heating, Ventilation and Air-Conditioning
ICT	Information, Communications and Technology
IDS	Intrusion Detection System
IM	Instant Messaging
IP	Internet Protocol
IS	Information System
ISC	Inherently Secure Communications
IT	Information Technology
JFC	Jericho Forum Commandment
JFC#n	Jericho Forum Commandment Number *n*
LAN	Local Area Network
LEA	Law Enforcement Agency
NIST	National Institute of Standards and Technology
OS	Operating System
P2P	Peer-to-Peer
PDA	Personal Digital Assistant
QoS	Quality of Service
RHQ	Regional Headquarters
RMM	Risk Management Methodology
SAML	Security Assertion Markup Language
SCADA	Supervisory Control And Data Acquisition

SOA	Service-Oriented Architecture
SSO	Single Signed On
SU	Specialist Unit
TPM	Trusted Platform Module
VM	Vulnerability Management
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WS	Web Services
XML	Extensible Markup Language

Chapter 1

Introduction

1.1 Background

De-perimeterisation (D-P) is a term mooted by the Jericho Forum which started off from the informal meetings of a group of global corporate CISOs in 2003. De-perimeterisation is basically used to describe the gradual erosion of the network perimeter which up till now still strongly protects an organisation's internal network from the threats posed by external networks. The breaking down of the perimeter as observed by the Jericho Forum is due to a number of reasons and among them is the changing business models driven by cost-savings which encourages remote users, outsourcing and partnership. Bring along with D-P are the many threats such as loss of sensitive information and malicious insiders which will be further elaborated in the study.

A Law Enforcement Agency (LEA) is the department of the government which is responsible for maintaining law and order in a nation. The LEA exercises much of its authority to carry out its duties to ensure public safety and security. This powerful organisation however is not spared from the effects of de-perimeterised which we will see in this report. Part of the objectives of this study is also to analyse the threats that D-P brings to a LEA and propose recommendations to mitigate those risks.

1.2 Objectives

The objectives of this report are:

(i) To explain the concepts of de-perimeterisation.

(ii) To analyse the operational setup and environment of a law enforcement agency and carry out risk analysis in its facing of the issues with de-perimeterisation.

(iii) To propose practical solutions to manage the risks associated with de-perimeterisation.

1.3 Scope

The scope of the study generally covers de-perimeterisation and will not be providing an in-depth explanation on all aspects of de-perimeterisation proposed by the Jericho Forum. While the law enforcement agency would be defined, it would only be a simplified one from the author's knowledge and based on Internet resources. Details on the intelligence and operations will be excluded due to sensitivity of the information. Finally, in the risk analysis, the processes from risk treatment would not be carried in the absence of management decision.

1.4 Organisation

Following the introduction in this chapter, *Chapter 2* will try to demystify the term de-perimeterisation (D-P). It will be explained as to how D-P came about, what are the driving factors and the strategy proposed by the Jericho Forum. Some critics about the D-P concept would also be given at the end of the chapter. Next, *Chapter 3* aims to define the organisation of a Law Enforcement Agency (LEA) where the effects of D-P will be analysed. It will provide the organisational structure, the players, the assets and the network setup of the LEA. In *Chapter 4* Risk Analysis, the threats faced by a LEA in face of de-perimeterisation will be identified, the risks will be assessed and analysed. The possible countermeasures

against them would be proposed as well. Having carried out risk analysis, providing the recommendations is the objective of *Chapter 5*. Recommendations will be categorised into short-term, mid-term and long-term; short-term ones should be implemented as soon as possible while long-term recommendations are exploratory at this stage; mid-term recommendations will take a longer time to achieve but should be carried out as soon so that its full benefits could be realised in about 3 to 4 years' time. Finally, the conclusions of the study will be given in *Chapter 6*.

At the end of the report are the References. A simple Risk Management Methodology (RMM) relevant to the risk analysis carried out in *Chapter 4* is found in *Annex A*. In *Appendix A*, the project description form submitted for this report is attached.

Chapter 2
De-perimeterisation Demystified

In this chapter, we will be demystifying de-perimeterisation (D-P) by explaining the reasons behind it, the issues surrounding it and the proposed approach to the "solutions" in handling it. The purpose of the chapter is to provide the reader an overview of D-P so as to aid in the understanding of the subsequent chapters and it is not in the scope of this report to provide a complete explanation on all aspects of D-P.

2.1 Introduction to De-perimeterisation

De-perimeterisation (D-P) is a term mooted by the Jericho Forum[1]. The Jericho Forum came about in 2003 through the informal meeting discussions of a group of global corporate CISOs [1]. The forum's main objective is to create a blueprint for solutions to protect enterprise systems and data on multiple levels, using a well-defined mix of encryption, inherently secure protocols, and data-level authentication. This will allow secure and cost-effective business collaboration through the use of the Internet.

De-perimeterisation refers to the erosion of the network perimeter (formed using routers, firewalls and other network equipment) of an organization. How it came about and the strategies to deal with it will be discussed in the subsequent sections of this chapter.

[1] Jericho Forum, http://www.jerichoforum.org/

2.2 Why De-perimeterisation?

As shown in Figure 2.1, the technological advances in computer internetworking led by key drivers (such as outsourcing, off-shoring, low-cost feature-rich mobile devices, B2B & B2C integration) has slowly but effectively caused the breaking down of organisations' network perimeters.

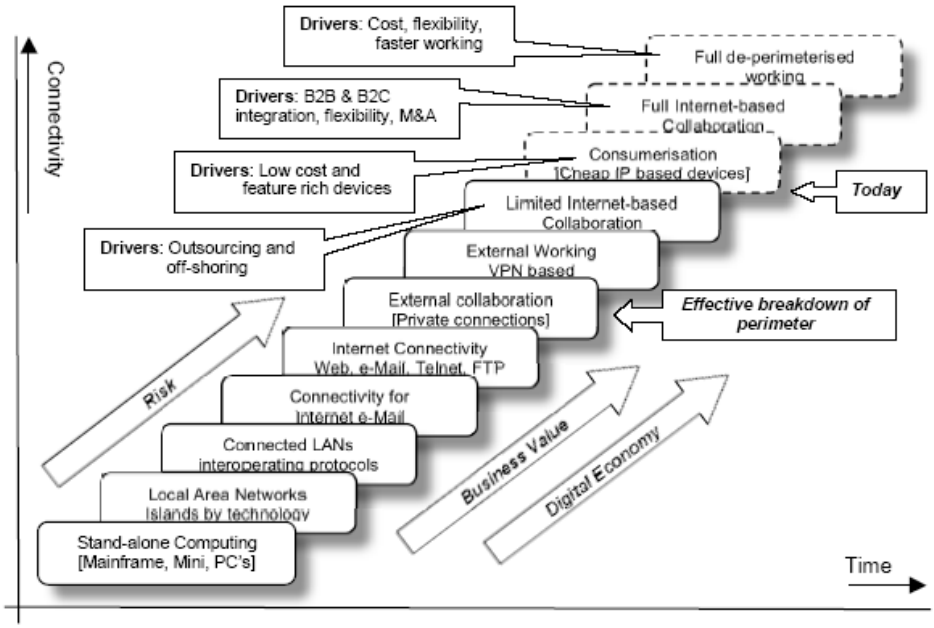


Figure 2.1 Increase in network connectivity with time (extracted from Jericho Forum [2]).

In the history of computing, computers have evolved from Mainframes to Minicomputers to Personal Computers (PCs); from standalone machines to Local Area Network (LAN) islands to Internet connectivity; from desktops to laptops to wireless devices. In addition, organisations have changed from having office-bound workers to remote workers; business models have changed from having customers visiting shops in person to purchase goods to global customers who carry out purchases from the Internet. The challenges or strains that were placed on traditional perimeter network architecture[2] can be summarized as:

[2] Extracted from Royal Holloway MSc in Information Security Autumn Seminar Series 2007 "De-Perimeterisation" delivered on 29th Nov 2007 by Andy Barlow and Darren Brooks from Accenture.

- Changing business model – this is where company employees started to move out of their offices and work as remote workers; and where business associates move into companies and work in these companies' internal network. Remote workers are equipped with laptops in order for them to have remote connections to access the company's network resources from outside their offices. The laptops, after being moved out of the company's perimeterised internal network, are now subjected to the threats in untrusted networks, in particularly malware. This creates the challenge of maintaining the laptops which is difficult but necessary to secure against threats outside the office's network. Business associates inside the company would likely be using the company's network to access external resources. This poses another threat to the company as it gives rise to potential points where viruses could spread into the company's internal network and also for sensitive information to leak out of the company. Thus, we see that the company's network perimeter has virtually become impossible to define.
- Globalisation Effect – due to the globalisation effect, applications would now require to be accessed from computer machines at varied locations crossing international boundaries through the Internet. Virtual Private Network (VPN) "tunnels" are usually established so that data could be transmitted securely across the Internet. This however punches "holes" through the firewalls making them less effective in stopping malicious content from entering the company's internal network. This has made the traditional network perimeter to be "porous" and ineffective in defending the company's network.

- Change in Technology – Technology advances caused a significant challenge on the existing architecture. Technology has created a growing use of mobile and wireless devices by an increasing "virtual" workforce; more services were allowed through the perimeter to have better accessibility to data; and many more control of non-traditional IT applications (such as telephony, HVAC controls, SCADA systems, video systems) is migrating to the Internet Protocol. All these would create more "holes" in the firewalls and opens up even more vulnerable points from which an attack can be launched into the company's internal network. Furthermore, if the attacker can successfully exploit the weakness, he could possibly control or cause denial of service to some of the critical systems used by the company.
- Remote Access – the need for remote users' access to corporate/private network over the public internet has led to the weakening of the organisation's perimeter because there is a need to have firewall rules to allow applications to work when accessed remotely. This will weaken the firewall against malicious attacks into the company's internal network. Malicious content could basically bypass the firewall's screening by going through the "holes" that are created. Hence, the network perimeter which once protects the internal network has become useless.
- Traffic Volume – the volume of data traffic through a corporate's network is ever increasing with new applications that encourage collaborations and multimedia contents. The advance in technology that increases bandwidth can never catch up with the explosion in the volume of traffic. This added much stress on the perimeter proxies that scan traffic for malicious content.

- Convergence of Identity – the growth in business and accessibility has led to an "identity proliferation" whereby a person has disparate identities in disparate locations for disparate systems and in discrete access events. It is therefore a great challenge to cater to the requirements of identification in such an environment and at the same time, maintain the perimeter. It is difficult for any applications to manage and identify such a large pool of identities across different systems and in most cases, a more than necessary number of users is allowed the access to data. As such, applications have caused bigger than necessary "holes" in the perimeter.

According to the Jericho Forum, the erosion of the perimeter is driven by three main factors [3], they are:

- Security exploits using delivery mechanisms (such as e-mail and Web) that transit the border, thus delivering the security exploits to the heart of an organisation. Due to the ineffectiveness of most firewalls in stopping data-driven attacks where malicious contents are embedded into emails and web application data, the content would basically go straight through, passing the perimeter and into the internal network of the organisation. The exploit would then find its way to the mail or application servers and compromise the machines if they are vulnerable to the exploit.
- Vendors with products that need to communicate across the border encapsulating their protocols within the Web protocols (using TCP/IP port 80 or port 443). In this way, these products have effectively bypassed the screening done by firewalls which would allow for Web protocols to pass through them. This loophole could be used by an attacker to embed an exploit that goes through the perimeter via the application.

- The demands of businesses needing to trade using the Internet and being restricted by their corporate perimeter, and either punching (further) holes in that perimeter and/or bypassing the perimeter.

De-perimeterisation is a trend that is unavoidable. As mentioned above, applications that were developed to suit business needs have been punching "holes" through the firewalls that protect an organisation's internal network from the external. The line between internal and external networks has been blurred by mobile workers working from home or from a business partner's network, and by outsourced staff working within the organization's network.

The 2008 Information Security Breaches Survey by BERR also seems to have supported the continuation of D-P [4]. As shown in *Figure 2.2* below, the overall percentage of UK companies who responded that have outsourced some IT operations remains about the same at around 52% as compared to two years ago but this is still a high figure. We can see a significant amount of 20% for large businesses to have outsourced some IT operations, including some off-shoring.

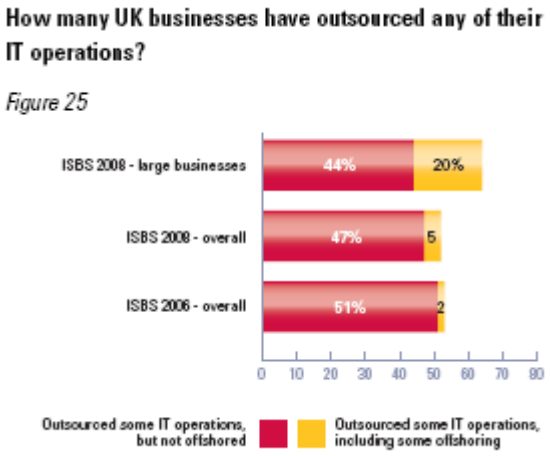


Figure 2.2 Outsourcing and offshoring of IT operations for UK businesses[3].

[3] Extracted from 2008 Information Security Breaches Survey by BERR, Figure 25 (Page 13), http://www.berr.gov.uk/files/file45714.pdf.

The survey also indicated that 54% of the UK companies now allow employees to access their systems remotely (up from 36% in 2006). In addition, the number of companies using wireless network had increased from 25% to 42% over the last two years. There is an increase in UK companies using Instant Messaging (IM) and Voice over IP (VoIP) Telephony. All these have weakened the effectiveness of the firewall which is regarded as de-facto perimeter defense in companies nowadays. With mobility and all the "holes" in the firewall, it makes companies' internal networks more vulnerable to attacks.

Mobility in the workforce, flexibility in deployment of staff, better synergy between partners and cost savings are the business benefits that have directly or indirectly lead to de-perimeterisation. However, the risks that de-perimeterisation brings include the erosion of the perimeter making it less effective against external attacks, the vulnerabilities faced by laptops and an increased threat from insiders. The D-P risks will be discussed in further details in *Chapter 4* but as we can see, the risks to information security that de-perimeterisation brings about are as much as the business benefits that can be obtained. Increasingly, information will flow between business organizations over shared and third-party networks, so that ultimately the only reliable security strategy is to protect the information itself, rather than the network and the IT infrastructure [5].

The Solution

The solution as proposed by the Jericho Forum suggested that traditional security solutions, including firewalls, and maintaining "defence in depth", will continue to play vital roles, but there is a need to remain alert to how they are affected by new challenges, and in particular continually check that their operational effectiveness is not being undermined. Ultimately, in a fully de-perimeterised

network, every component will be independently secure, requiring systems and data protection on multiple levels, using a mixture of:

- encryption
- inherently secure communications
- data-level authentication

The Roadmap – The four phases of D-P

In his interview with Network World, Paul Simmonds, CISO of ICI who is a member of the Jericho Forum Board of Management proposed a roadmap in which the transformation to a D-P world will come about [6] [7]. Graham Palmer in his interpretation of the four phases added a Phase 0 so as to show the transition from what we were, before moving into Phase 1 where what we are now.

Phase 0 – Hard shell perimeter

This is the typical traditional security model which all security professional are familiar with. As explained by Graham, the Phase 0 model is identified by the data centres, systems and applications secured by virtue of their location in the facilities of the organisation in question. These facilities are owned and operated by the organisation. Access to the resources is controlled firstly by location, depending on whether you are in the trusted part of the network or outside it. This is achieved by managing the firewalls that define the perimeter of the network. Remote access is provided using a Virtual Private Network (VPN) by establishing a secure tunnel using IPSec or other means via two-factor authentication.

Phase 1 – Move outside the perimeter

This phase is what is generally agreed as where most corporations are at in this moment. It is characterised by the increased in mobility of the workforce. Mobile workers access corporate network and resources, such as email through the Internet using "Internet Data Centres" by leveraging on the cost saving ASP model. The whole lot of things associated with D-P that are happening at this phase are what have been described earlier, like outsourcing and changing business model towards closer partnerships. This is exactly where we see the start of the erosion of the network perimeter.

Phase 2 – Remove the harden perimeter

Moving into the next phase, the perimeter does not change as a whole but the nature of it is altered. The perimeter would become a Quality of Service (QoS) border in which applications predominately proprietary ones would more than often be penetrating through the network perimeter. Secure "islands" would form through the provision of encrypted transport and authenticated access to internal data. The acceptable QoS level is a business decision as Simmonds says. One that is driven by cost justification and return on investment calculations.

Phase 3 – No perimeter

In Phase 3, the perimeter would as it seems to be gone. Access to internal data is controlled through dynamic authentication means. Work on the technologies and solutions for this phase is in its infancy where security devices need to migrate from layer 3 to layer 7 of the OSI 7 layer model. They will need application awareness in order to interpret the context of the data they are surveying on a scale not seen presently.

Phase 4 – Data level encryption

The last and final stage of the roadmap or transformation is where data level encryption is achieved. As what Graham has described, the security provided at this phase on the data would be completely integrated such that data written onto a disk for example would have all its relevant security written down as well. In other words, the data components on the disk will contain the data and the access control information, keys for encryption or read and write privileges. This has the effect of making all data 'stand alone' it is protected because the security parameters that will ensure it is used or viewed appropriately are completely central to it. When that piece of data is copied to another server the parameters are copied too, nothing changes. Therefore, the vision at this point of time as seen by Simmonds and the Jericho Forum makes the network perimeter redundant.

Phase 4 is truly a de-perimeterised environment. Terry Bebbington in his MSc dissertation drew up his vision of a Phase 4 architecture which he called the "Rosetta Model" [8]. The model consists of Trusted Brokers, Filtering Utility, Information Providers and Data Silos. The key benefits of the model are that it tries to use existing technologies and standards, and it is allows a stage approach to the transition into this phase. However, Bebbington admitted that much has to be done for it to realise, such as having a global authentication and identification standard, a legal structure as well as an efficient key management system to all the cryptographic protocols that are in use.

In order to move the whole environment into a de-perimeterised one, a number of position papers have been published by the Forum and they include one

on Inherently Secure Communications (ISC), Wireless, VoIP, Internet Filtering & Reporting, End-point Security, Enterprise Information Protection & Control (or DRM), Trust & Co-operation, Information Access Policy Management, etc. These papers serve to gear technology vendors, standards organisations and business consumers towards developing products and standards, and adopting solutions that would ultimately resolve the D-P issue.

2.3 The Eleven Commandments

In order to plan for a de-perimeterised future, the Jericho Forum also published the Jericho Forum Commandments (JFCs) that build on "good security" and to specifically address those areas of security that are necessary to deliver a de-perimeterised vision. The JFCs as depicted by the forum are categorized into 5 areas and there are a total of 11 principles as listed below [9]:

Fundamentals

1. The scope and level of protection should be specific & appropriate to the asset at risk.
    - Business demands that security enables business agility and is cost effective
    - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
    - In general, it's easier to protect an asset the closer protection is provided

2. Security mechanisms must be pervasive, simple, scalable & easy to manage.

- Unnecessary complexity is a threat to good security
- Coherent security principles are required which span all tiers of the architecture
- Security mechanisms must scale; from small objects to large objects
- To be both simple and scalable, interoperable security "building blocks" need to be capable of being combined to provide the required security mechanisms

3. Assume context at your peril.

- Security solutions designed for one environment may not be transferable to work in another. Thus it is important to understand the limitations of any security solution
- Problems, limitations and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

Surviving in a Hostile World

4. Devices and applications must communicate using open, secure protocols.

- Security through obscurity is a flawed assumption - secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use
- The security requirements of confidentiality, integrity and availability (reliability) should be assessed and built in to protocols as appropriate, not added-on
- Encrypted encapsulation should only be used when appropriate and does not solve everything

5. All devices must be capable of maintaining their security policy on an untrusted network.

- A "security policy" defines the rules with regard to the protection of the asset
- Rules must be complete with respect to an arbitrary context
- Any implementation must be capable of surviving on the raw Internet, e.g., will not break on any input

The need for trust

6. All people, processes, technology must have declared and transparent levels of trust for any transaction to take place.

    - Trust in this context is establishing understanding between contracting parties to conduct a transaction and the obligations this assigns on each party involved
    - Trust models must encompass people/organisations and devices/infrastructure
    - Trust level may vary by location, transaction type, user role and transactional risk

7. Mutual trust assurance levels must be determinable.

    - Devices and users must be capable of appropriate levels of (mutual) authentication for accessing systems and data
    - Authentication and authorisation frameworks must support the trust model

Identity, Management and Federation

8. Authentication, authorisation and accountability must interoperate / exchange outside of your locus / area of control.

    - People/systems must be able to manage permissions of resources and rights of users they don't control

- There must be capability of trusting an organisation, which can authenticate individuals or groups, thus eliminating the need to create separate identities
- . In principle, only one instance of person / system / identity may exist, but privacy necessitates the support for multiple instances, or once instance with multiple facets
- Systems must be able to pass on security credentials /assertions
- Multiple loci (areas) of control must be supported

Access to data

9. Access to data should be controlled by security attributes of the data itself.

- Attributes can be held within the data (DRM/Metadata) or could be a separate system
- Access / security could be implemented by encryption
- Some data may have "public, non-confidential" attributes
- Access and access rights have a temporal component

10. Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges.

- Permissions, keys, privileges etc. must ultimately fall under independent control, or there will always be a weakest link at the top of the chain of trust
- Administrator access must also be subject to these controls

11. By default, data must be appropriately secured when stored, in transit and in use.

- Removing the default must be a conscious act
- High security should not be enforced for everything; "appropriate" implies varying levels with potentially some data not secured at all

It can be observed that some of the commandments are basic and are good security practices, such as having appropriate protection level to assets at risk and "assume context at your peril" while some commandments are rather far-fetched goals, some of which like in data access, trust management and identity management are difficult to achieve in practice. For example, access control (JFC#9) at the data level is an enormous task due to the huge amount of existing organisation data that needs to be classified and stored together with its associated security attributes. And also, JFC#8 calls for identity to be exchanged outside the area of control and this requires a global specification standard to be written first so that a global identity management framework to be established among all players around the world before it can be realised.

2.4 Critics on De-perimeterisation

There were several critics and scepticism about de-perimeterisation. The early ones criticized the Forum as about getting rid of firewalls but this is not true. It has been clarified by the Forum that use of firewalls is still required now (which is in line with JFC#1) but they would be made more redundant with time as the IT environment adopts D-P solutions that inherently secure data [3] [10]. Eventually, the Forum predicts that firewalls may become obsolete. Other misunderstandings, such as that the de-perimeterisation is about developing a solution or strategy, has been clarified – it is not a solution and neither a strategy, it is the problem that the Forum is addressing [11].

A good discussion on the limitations of Jericho Forum's views on D-P was given by Graham Palmer [6]. After listing all the benefits that the D-P vision brings, Graham cited existing solutions still working, huge scope of work, requirement for

global solutions, reliance on prediction and restriction on encryption export as the challenges in achieving the vision.

Joel Synder is especially sceptical about the Forum. He said that "At best, Jericho will help to raise awareness of the usefulness of a defense-in-depth network security strategy. More likely, the forum will end up on the scrap heap of unrealized ideas and wasted effort." [12]. Snyder thinks that such large and architecturally elegant ideas die an ugly, lingering and expensive death, citing the public-key infrastructure (PKI) identities, X.400 e-mail and ATM to the desktop as examples.

A Computer Weekly article titled "Deperimeterised approach to security is not suitable for everyone, warn analysts" by Bill Goodwin in April 2006 warned that D-P is not for everyone [13]. The report quoted Mark Waghorne, principal adviser at KPMG, saying that for de-perimeterisation to work, most organisations would need a far more mature and consistent approach to identifying and classifying IT assets that need protection. He further mentioned that de-perimeterisation requires effective administration to secure tens of thousands of assets, rather than deploying a small number of assets to protect the entire network.

Recently, Dr Geraint Price from Royal Holloway University presented the topic "De-perimeterisation: fact or fiction?" in the Infosecurity Europe 2008 Conference held in London on 22nd April 2008 and he stated that the areas where D-P will work:

- Protection of information at all stages of the information life-cycle.
- The support of remote workers who need to access business process from home or some other premises.
- Implementation of known "good practice" and technology which has been missing previously.

Dr Price however iterated that D-P will not work or is not suitable in the following:

- Where the device is not owned by the organisation.
- In the far-reaching goals of the Jericho Forum, such as "anytime, anywhere" security.
- Extending the data security model to "arbitrary" platforms.
- Contract and trust negotiation "on the fly".
- Access Control at the content (paragraph/line) level.

He believes that further works need to be carried out in the security management; the relationship between the business process and the security; and the relationship between the security and the business drivers.

Concluding Remarks

The above discussion shows that the Jericho Forum has achieved its initial objectives in defining the problem and raising awareness through publications, press release, conferences and others. Moving on, it is hoped that more solutions would be developed taking into account the D-P issue and also more involvement could be seen in business consumers in adopting the solutions. In the subsequent chapters of this report, we will see how a typical organisation facing de-perimeterisation could implement some practical steps to help mitigate risks brought about by D-P.

Chapter 3
Defining the Organisation

In this chapter, the author would define a law enforcement agency (LEA) that would be used for analysis. Defining a complex organisation such as that of a law enforcement agency is not practical to do in this report. What would be given is a simplified view of the organisation. Much of the information here is generalised based on the author's knowledge and could be found publicly on law enforcement agencies' websites [14]. The rest of the information is formulated based on the knowledge and experience of the author. As for matters with regards to intelligence and detailed operations, they will be omitted due to their confidentiality.

For the purpose of analysing information security threats, the organisation is defined with emphasis on the areas of information technology (IT) rather than the actual policing operation side of it. The chapter starts by giving an overview of a law enforcement agency in terms of its structure, function and operations. Then, the players in the organisation will be discussed. While it is obvious that the LEA consists of the management and its police officers in providing policing service to the public, the author would also name the other players (and the roles they play) that would allow the analysis of the impact and risks of associated threats in face of de-perimeterisation. The operating environment would be briefly mentioned. Following that, the assets owned by the organisation would be identified. And lastly, the network setup will be drawn-up to complete the whole picture of the organisation for analysis.

3.1 Overview of a Law Enforcement Agency

The Law Enforcement Agency (LEA) to be defined here consists of the Headquarters, the Regional Headquarters (RHQs) and the Specialist Units (SUs). In the Headquarters, there are various so called staff departments such as the Operations planning, Logistics, Human Resource, Finance, IT, Public Relations, etc. The command or the top-management of the organisation would also be situated in the Headquarters.

Distributed over various locations around the country are a few Regional Headquarters (RHQs). RHQs works like a "mini" Headquarters and has its own resources in managing its day-to-day functions such as operations, finance, logistics and human resource. Each Regional HQ has under its purview, a few Neighbourhood Centres and Posts located at various locations within its boundaries. In some way, the law enforcement agency resembles that of a large multinational organisation that has its operations distributed over many places around the world. A point to note here is that having a small police post located near to the community and serving to the needs of the community is the "Koban" concept developed by the Police Force in Japan and it is seen to be effective in fostering community partnership in fighting crime [15].

The Specialist Units are like the Regional HQ but they have specialized functions such as coastal patrol and public order. They themselves are also located at disparate locations and could operate on their own.

From what has been described, you can see that the LEA is a matrix type of organisation which best suit its function. The organisational structure can be represented in a chart shown in *Figure 3.1* in the following page.

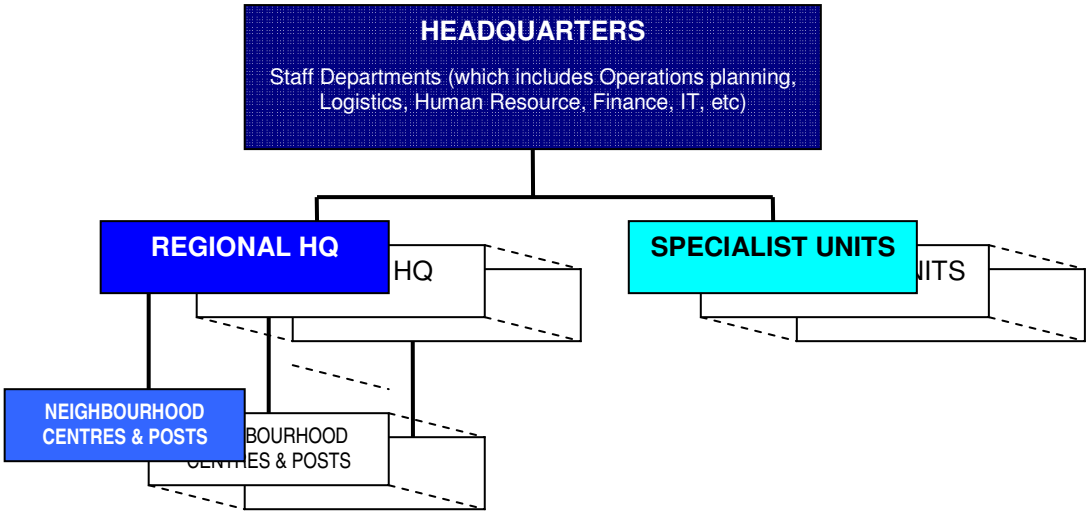


Figure 3.1 Structure of a Law Enforcement Agency.

The LEA is led by the commissioner or chief of police and assisted by several directors or deputy chief in the management of the agency. In general, the mission of agency is to maintain law and order, to protect properties and the innocents, and also to prevent and deter crime so as to keep a low crime rate.

Nowadays, most police forces[4] would deploy some form of technology to assist them in policing. They would at least need to maintain an emergency phone system to receive emergency calls from the public. Police officers on patrol would usually carry a communication device that allows them to keep in contact with their command & control centre. There would be a need for vehicles to allow officers a speedy response to incidents. A computer data network that connects up most of the police buildings or establishments should not be uncommon. In more developed police forces, many applications would be running on this network to support their

[4] The terms "law enforcement agencies" and "police forces" are used interchangeably in this report and are meant to be the same, even though law enforcement agencies encompass a broader scope than the police force and include agencies like prison services, intelligence units and those that operate internationally such as the Interpol.

day-to-day operations in terms of administration, finance, investigation, intelligence and others.

3.2 The Players

The obvious players in a police force are the organisation's top-management (The commissioner, commanders, directors and deputy directors) and the policemen. However, for the police force to function properly, there are a lot more people who need to be involved. For example, outsourced vendors are required to work within the police force - they could be contracted cleaners, security personnel or network engineers. As discussed in *Section 2.2*, changes in business model led to outsourcing resulting in the need to cater for outsiders to access an organisation's internal network. This eventually leads to de-perimeterisation. It is evident from the Metropolitan Police Service's Information, Communication and Technology Strategy paper that it has outsourced almost all of its ICT/IS supplies [16]. The author believes that outsourcing is the trend in all, if not most, of the more developed police forces around the world. It was also recently reported that Westminster Council would be outsourcing all its IT service by 2015 [17]. Outsourcing seems to be an unavoidable development in both public and private sectors. The benefits of outsourcing are basically to harness the expertise in the industry and to lessen the burden of the organisation in maintaining a team of specialists in managing the IT systems.

In this section, we will list the players that will be relevant in the analysis of the risks they bring in face of de-perimeterisation. It focuses mainly on those who play direct or indirect roles in the use of IT to allow risk analysis of the information security threats in the next chapter. The players are listed in *Table 3.1* below.

Table 3.1 Players in a Law Enforcement Agency.

Players	Description
Top Management	The top management of the organisation refers to the commissioner or chief-of-police, his deputies, commanders, directors and their deputies who together to provide directions in the operation of the organisation. They are the most important people who will decide the acceptable organisational risks. The group will also include the Chief Information Officer (CIO) or Director Technology or Director Information which are the different nomenclatures used for the person in-charge of ICT systems.
Police Officers	They are the actual officers trained to carry out policing work. These officers could be in various schemes – some could be doing specialised functions such as in investigation, coastal patrol or riot control while others might be deployed to do administrative and supporting roles in the organisation. To some extent, they will be required to use the applications and technology that are provided to carry out their duties.
Middle Management	These are the middle managers and team leaders who are in-charge of group of people in carrying out police functions as well as in administration and supporting roles. In the technology department of the organisation, the managers would be involved in the design, specification, development, testing, rollout and maintenance of ICT applications and equipment.
Associates	With better corporation between police forces around the world, it is now common to have police associates attached among police organisations. Here, associates could also refer to seconded personnel that are from another department, the higher ministry or other ministries from the government; these associates could be here for audit, for a joint project or for a job attachment.

Players	Description
	Well, seconded personnel could also refer to police officers attached to external organisations; some of these seconded officers would need to access the network resources directly from the networks in the external organisations. This is the current trend seen in many private organisations and it is certainly also a trend for law enforcement agencies. And as discussed in *Chapter 2*, this trend is certainly one of the reasons for de-perimeterisation caused by opening up of firewall rules for officers to access network resources in their respective organisations.
Outsourced Vendors	Outsourced vendors are an important player here. They could be contracted cleaners, security personnel or network engineers assisting the organisation in the specialised tasks. The group of outsourced vendors who require special attention is the IT vendors who are familiar with and usually given privileged access to the organisation's network. Controls have to be put in place to ensure that IT vendors would be able to carry out their work while security of the organisation's assets is still being properly protected.
Project Officers	Project officers are part of the technology department helping the project managers in IT projects. Like the project managers, project officers would be involved in the design, specification, development, testing, rollout and maintenance of ICT applications and equipment.
Data Centre Staff	It is assumed in this report that data centre(s) – whether in-house managed or outsourced – exists to house the servers of applications used by the organisation. Therefore, there will be staff managing the data centre and ensuring that the highest availability of the applications. The staff has physical access to servers and control the access of other personnel into the data centre

Players	Description
	as well; they will also be monitoring all the servers and response to any incidents happening in the data centre. The system administrators are part of this team too.
Security Guards	Security guards are the personnel who guard the physical premises. They provide the first line of defence against a fake visitor trying to sneak into police buildings. Security guards verify visitors' identities and do checks on belongings. These guards could be staff of the organisation or they could be outsourced to a security service provider. It is possible that they need to access an IT application of the organisation where they are working, for example, a visitor management system that determines who are the authorised visitors and vehicles into the premise. Thus, network access has to be given while controls have to be put in place to prevent abuse and possible access point for attacks on the organisation's network.
Public	The public is whom the LEA serves. There are several channels through which the public could seek services from the LEA. They can call the emergency line; they could approach the service counter of a police station or post; and more so now in a de-perimeterised world, the public goes online to access the services provided on the Internet website provided by the LEA.
Users	The users of the applications in the LEA actually include all of the above players that have been mentioned. They include of course all the employees of the LEA, the public which it serves, its associates and outsourced vendors, even the security guards could need to access the applications of the LEA. For each of the players, the access rights to be given varies and it is important that the rights are correctly given.

Putting the players together, the simplified organisation would look like the one given in *Figure 3.2*. As can be seen, the Technology Department is part of the agency led by the CIO with its Project Managers and Officers. This department has some data centre staff under its purview and has also to manage the outsourced IT vendors. Then, there are also the Associates and Security Guards which are considered outside of the organisation.

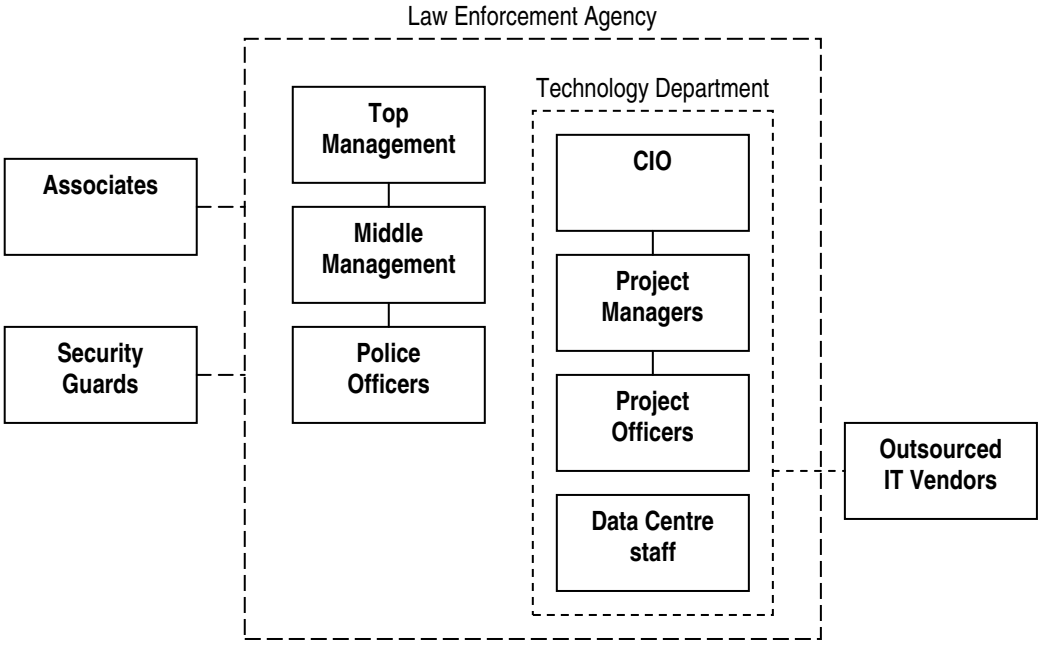


Figure 3.2 Simplified Organisational Chart of a Law Enforcement Agency.

3.3 The ICT Assets

The assets of the police force are aplenty, ranging from weapons, vehicles, buildings to radio communication sets, and from computer servers, data centres, desktops, laptops to sensitive data such as criminal records to even reputation which is an intangible but nevertheless very important to the LEA. Listed below would only be the assets that are relevant to the analysis of information security threats associated with de-perimeterisation.

Table 3.2 ICT Assets in a Law Enforcement Agency

Assets	Description
Laptops	Laptops are usually used by senior staff of the organisation to have remote access or for operational purpose due to the mobility of laptops. The remote connection to the organisation's network resources (such as emails) using laptops is common in the police forces and in many other organisations. These connections, through the use of VPN, punch "holes" into the organisation's network perimeter which is one of the factors that has caused de-perimeterisation. Laptops could also be holding sensitive information and as such, laptops are considered important assets that need to be protected.
Sensitive data	Sensitive data could include crime statistics, personal information, operational plans, criminal records, intelligence information and others. Some data could be linked to national safety and security. In police establishments and especially in governments, data is usually classified using labels such as top secret, secret, confidential, restricted or unrestricted so that access control over them can be implemented.
Vehicles	Vehicles are required for quick response to incidents. Nowadays, police vehicles are not only loaded with all sorts of equipment (for road blocks, investigation, etc), they are also fitted with radio communication sets, cameras and even mobile data terminals that links to the command & control centre. When vehicles are sent to external contractor for repair or maintenance, steps should be taken to protect the equipment.
Buildings	The building is where the police operate. It is where police vehicles are housed and where the armoury is. There could also be the command & control centre or a data centre is located within. After 9/11, buildings are

Assets	Description
	viewed to be vulnerable to attacks by terrorist using planes, trucks and bomb cars. And police buildings could quite possibly be a good target for terrorists who would like to make a point and challenge against a country's authority. Insiders are more likely able to cause damage to this asset simply due to the physical access that insiders have.
Applications	Applications are necessary for the working of the police force. The applications include the emergency call system, financial system, email system and many others. Some applications are critical for operations while others are less essential. There has been increased reliance on critical applications over the years, so much so that if these applications fail, certain police operations might not be able to function at all.
Data Centres	Data centres, whether in-house managed or outsourced, are necessary to locate servers needed to host applications needed for police operations. Sufficient security both physical and procedural for data centres is necessary to protect the servers (and the data stored within them).
Servers	Servers are where applications are hosted. They are important and should be running to ensure the required availability of applications. For added reliability, servers are sometimes configured in a high availability and high redundancy mode.
Desktops	Desktop computers provide access to the organisation's network and thus, the applications. The applications could reveal sensitive data. As such, proper controls have to be put in place so that the access terminals are not compromised, especially in a de-perimeterised environment where the presence of malicious insiders is quite possible.

3.4 The Network Setup

To complete the definition of a LEA, the network setup of the organisation is presented in this section. In the following paragraphs, the network diagram of the LEA shown in *Figure 3.3* will be elaborated.

Firstly, as discussed in *Section 3.1*, the LEA is separated into many units, namely the Headquarters, Regional Headquarters, Police Centres/Posts and Specialist Units. All these have network connections through dedicated leased circuit lines or digital subscriber lines (DSLs) to the core network of the LEA (termed as "LEA network" here onwards). The LEA Data Centre, which houses all the servers and equipment needed for applications, is also connected to the LEA network. It is assumed that a Backup Data Centre exists for disaster recovery purpose. The Data Centres are protected from the rest of the network using firewalls. The connection to the Internet is through the data centre and is controlled with the use of firewall as well. IT vendors carrying out network administration or application maintenance would have access to the data centres.

Most police forces in the world have an Internet website to allow the public to access information with regards to security and many websites provides online applications such as to lodge a police report or to submit a job application. Public users access the LEA's Internet website through the Internet. The LEA's remote users would also be accessing to the organisational resources through the Internet using VPN which creates a secure channel into LEA network.

Associates and vendors can be situated in various locations in the LEA as indicated in *Figure 3.3*. They might or might not be given access to the LEA network, depending on their job functions. Internet access could be needed by associates to access their own organisations' network resources.

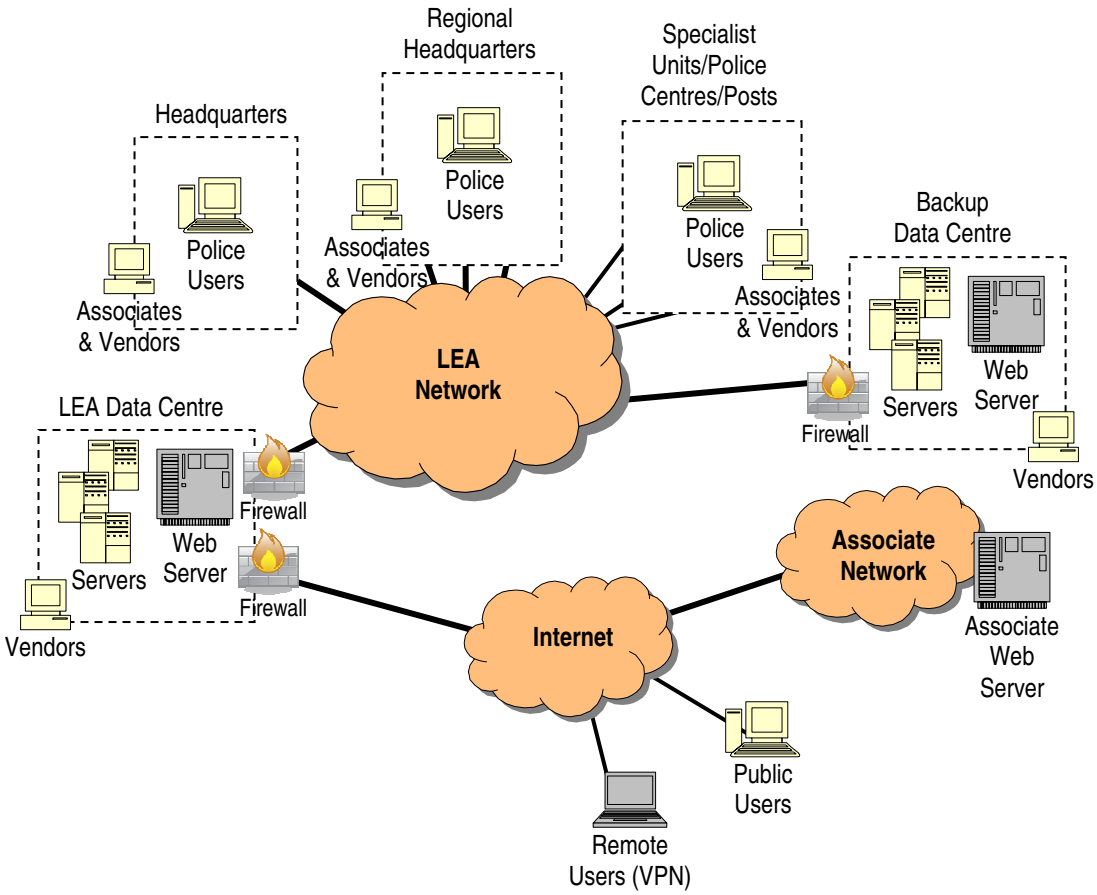


Figure 3.3 Network setup of a Law Enforcement Agency.

Chapter 4
Risk Analysis

Risk analysis will be carried out in this chapter against the threats brought about by de-perimeterisation. The outcome of the analysis is to develop some practical countermeasures against the threats. The results will be used for the recommendations in the next chapter.

4.1 Risk Management Methodology

The risk management methodology (RMM) to be used in this report is a simple qualitative one given in *Annex A*. The RMM involves carrying out *Risk Analysis*, *Risk Assessment*, *Risk Treatment*, *Risk Acceptance* and *Risk Monitoring and Communication*. However, the *Risk Analysis* and *Risk Assessment* steps would be sufficient to meet the objectives of this report. It is also not possible to go through the steps after *Risk Assessment* in the absence of the author's higher management.

The analysis and assessment will be focused on the risks brought about in a de-perimeterised environment for a law enforcement agency. The outcome of this exercise would be the Risk Register (given in *Section 4.4*) which allows for recommendations to be formulated in *Chapter 5*.

4.2 Threat Analysis

There are several threats faced by a law enforcement agency. From the assets identified in the previous chapter, the threats faced by the LEA in a de-perimeterised environment are listed down.

But firstly, let us understand the possible attackers on a LEA. The LEA faces all kinds of attackers who could do harm to the organisation's asset. They

could be terrorists, criminals, insiders and hackers but we are only concerned in this study with those that operate in a de-perimeterised environment. Terrorists for one, which has caused much fear to everyone after the 9/11 attack and 7/7 London Bombing, would still be around whether with D-P or without and as such, they will be excluded from the analysis. It is however important to identify the attackers, know who they are, what their motivations are, so that effective countermeasures could be implemented against the threats that they bring. As what Bruce Schneier puts it, "*A system that doesn't take attackers' personal goals into account is much less likely to be secure against them.*" [18]. He further warns that "*If you mischaracterize your attackers, you are likely to misallocate your defences. You're likely to worry about nonexistent risks and ignore the real ones. Doing so isn't necessarily a disaster, but it is certainly more likely to result in one.*".

Presented in *Table 4.1* are the possible attackers in a de-perimetered environment. Following that, *Table 4.2* tabulated all the threats perceived by the author.

Table 4.1 The Attackers.

Attackers	Description
Malicious insiders	The malicious insider has frequently been identified as the number one attacker or threat to an organisation, whether if he is in the private sector or in the government. This is supported in a poll conducted by Qualy in association with Jericho Forum in April 2007 revealed that 69% of European executives believe that insider threats pose more serious problem than threats from outside the organization [19]. Quite obviously, the main reason is that the insiders are the ones who have a high level of access in the organisation who can easily launch a successful attack

Attackers	Description
	on the organisation. In Bruce Schneier's book "Beyond Fear: Thinking sensibly about security in an uncertain world", he mentioned that "*Insiders are invariably more worrisome attackers than outsiders. Yet perhaps the most common security mistake of all is to expend considerable effort combating outsiders while ignoring the insider threat.*" [18]. He gave a few examples of insider attacks such as Aldrich Ames in the CIA who sold secrets to the Soviets KGB from 1985 to 1994 and Stanley Mark Rifkin who as a consultant in Security National Bank in Los Angeles transferred several million dollars into a Swiss account and converting them into diamonds. One of the countermeasures applied in LEAs and in most governments to mitigate insider threats is to carry out security clearance on all employees. This is the first step and a vital one to prevent possible malicious insiders in the future. It is also important to note who the insiders are; other than disgruntled employees, an insider could also be the associates and the outsourced vendors which includes security guards, cleaners and IT vendors.
Hackers	Hackers are a nuisance to organisations in the cyberworld. Whether it is simply for fun, for money or because of emotional hatred towards the organisation, hackers if able to successfully launch an attack could cause severe damage such as loss of availability, sensitive data, profit and reputation to the organisation concerned. A LEA could likely be a target for hackers who are police haters and hackers could steal confidential police data or cause a Denial of Service

Attackers	Description
	(DoS) to online police services through the use of Botnets[5]. Disruption to the police services could be detrimental to the reputation of the police force.
Malware	Malware generally refer to viruses, worms, Trojans and spyware. Malware are not real attackers but they too could have great impact on the availability of police services. In the BERR's 2008 Information Security Breaches Survey, it was reported that the number of UK companies that had a malware infection has decreased to 14% from 35% two years ago [4]. This as explained could be due to better anti-virus defense, reclassification of minor virus infection, improvement in law enforcement and virus writers shifting to write stealth code for organised crime. Even so, malware still remain a threat to all organisations as they still form a sizeable portion of all security breaches. Also, there is continued manpower effort spent in responding to them and contingencies are not all that effective. Furthermore, they can be used to compromise machines to increase the power and effectiveness of Botnets. Hence, the safeguards against malware should not be let down or reduced.

Table 4.2 Threats of a Law Enforcement Agency in a De-perimeterised Environment.

Threats	Description
Loss of laptop	A large increase in the number of mobile or remote workers in organisations today has indirectly led to a de-perimeterised environment. Mobility is achieved through the ubiquitous use of mobile devices, in particularly the laptops. Inevitably, the threat from the loss of laptop has increased.

[5] Botnet is a short term for "robot network" and is formed by a group of compromised computers on the network. It can be used by its controller to launch distributed DoS attacks.

Threats	Description
	Based on a study sponsored by Dell in June 2008, an astonishing 12,000 laptops were lost per week in US airports [20]. Back in June 2000, it was reported that the Defence minister of the UK government's laptop was stolen by a burglar breaking into his home [21]. Fortunately, in the statement given by the ministry, there was no sensitive data stored in the laptop. In fact, the UK Ministry of Defence (MoD) revealed that a total loss of 594 laptops from 1996 to 2002 [22]. Then in January 2007, it was revealed in an independent audit conducted that FBI had a total of 160 missing (loss or stolen) laptops from February 2002 to September 2006 and of which, many could contain sensitive and classified information [23]. This was actually an improvement from 354 missing laptops for the period October 1999 to January 2002. If public organisations like FBI and the UK government could have laptops missing, the situation could be worst for other organisations in the private sector. The reasons for the loss of laptops could be due to negligence of the user or could be because of theft by outsiders as well as insiders. But what is more critical are in the consequences in the loss of laptops. Laptops are used for remote access and if stolen, could potentially be used to attempt an unauthorised access into the organisation's network. In addition, stored in the laptops' harddisks are data and some data could be classified documents related to national safety and security in the case of a LEA. To simply sum up, we can see the threat from the loss of laptop is real and the impact is significant. Effort is needed to reduce the risk that the threat brings.

Threats	Description
Loss of sensitive information	Loss of sensitive information has always been a threat to a LEA and it has become especially so in a de-perimeterised environment. There are many incidents reported recently. Following the lost of 2 computer discs containing records of every UK child in November 2007 by the HM Revenue & Customs department in the UK [24], there are also the cases where nine NHS trusts losing patient data [25] and the lost of millions of L-driver details [26], both incidents occurring in December 2007. Yet another incident occurred recently in August 2008 where unencrypted details of 84,000 prisoners in England and Wales stored on a computer memory stick was reported to be lost by a private contractor of the UK Home Office [27] [28]. Not only could information be leaked through the loss of laptops which was discussed above, it is also equally possible for information to be lost through misplaced documents, compromising of the network by hackers, virus infection, spyware and various other means. Both insiders and outsiders are possible culprits for the loss of sensitive information. Insiders who have privileged access to information could intentionally or unintentionally leak information. Outsiders could be a hacker exploiting vulnerabilities in a web-facing server or it could a person deploying social engineering techniques to obtain classified information from the organisation. While most organisations had already have policies and procedures controlling insiders' access to information, the controls have often been overlooked for "outsiders" who are inside the organisation. These "outsiders" are the contractors, vendors and even the cleaners and security guards.

Threats	Description
Attacks on Internet website	The police's Internet website is certainly under threat by the attacks from hackers. It could be a DoS attack to make police online services unavailable to the public or it could be a defacement of the website to cause an embarrassment to the organisation. The latter case was what happened to Scotland Yard's career website in February 2008 as reported by the Register [29]. Even though no real damage was done and the website was recovered quickly from its backup, the incident did demonstrate the vulnerability of websites.
Firewall compromised	One effect of having remote workers is that many "holes" need to be created through the perimeter firewalls in order for applications to work. Firewalls nowadays are practically loaded with hundreds if not thousands or even more rules. This makes it easy for viruses, worms or spyware to penetrate into an organisation's internal network using the ports and services that are opened. Another kind of threat faced by the firewall could possibly be the breaking down of the firewall itself. With so many rules to process, the firewall inevitably would be overloaded. Its efficiency would be severely affected and be pushed beyond its capacity eventually resulting in failure. If no redundancy and high availability are being built into the design, all the applications protected behind the firewall would just become inaccessible to all users. A hacker could also try to trigger this failure and exploit the vulnerability if the firewall does not have a failsafe mechanism to enter into the internal network.
Vulnerabilities of mobile devices	Mobile devices are in abundance these days to support mobile workers in a de-perimeterised world that we are in today. The devices that are available in the market

Threats	Description
	include the laptops that are mentioned above, personal digital assistants (PDAs), pocket PCs, mobile phones, smartphones, digital cameras, video camera, game consoles, music players and others. Many newly invented devices combine the features of a few devices, for example, the smartphone is used as a PDA and usually comes with a built-in camera. The processing power, storage capacity and functionalities of these devices are ever increasing with time. More and more devices have wireless connection capability that allows an unlimited access to information and applications on the Internet. However, came with all these convenience and functionalities are the vulnerabilities that the devices face. Vulnerabilities make it possible for an attacker to exploit the devices, deny their access to services or steal any stored information from them.
Insider attacks	As mentioned in *Table 4.2*, insiders are considered attackers and the harm that they can do is severe. It is also usually difficult to detect an insider's attack until it is too late. The malicious insiders could basically do unlimited damage to an organisation – he can steal laptops, steal sensitive data, plant a bomb, hijack a police vehicle; he can cause failure of critical equipment; he can inject a virus into the organisation's internal network; and the list of harms that an insider can do is non-exhaustive. Our discussion in *Table 4.1* has explained the threat from insiders is aggravated in a de-perimeterised world where there is more number of insiders due to the changing business models. The LEA is also not spared the effects of de-perimeterisation and its insiders could be an employee, associate, outsourced IT vendor, security guard, cleaner and anyone that has dealings with the LEA. This threat can never be better

Threats	Description
	demonstrated by the incident mentioned in "Loss of sensitive information" of this table where unencrypted details of 84,000 prisoners in England and Wales stored on a computer memory stick was reported to be lost by a private contractor of the UK Home Office [27]. The harm done could be more severe than a private organisation due to the existence of sensitive information (as explained in *Table 3.*2 on Data).

4.3 Countermeasures

The Jericho Forum has raised the awareness of the issue of de-perimeterisation (D-P) and the proposed Jericho principles as explained by the forum are not the solutions to D-P. What the Jericho Forum is trying to do is to encourage vendors to develop applications and equipment that address the issue based on the Jericho commandments or principles. While waiting for commercial solutions to appear, some practical countermeasures (or safeguards or controls) could be adopted against the threats faced in an effort to mitigate the risks. *Section 4.2* has identified the threats to a LEA due to D-P and in this section, a list of possible countermeasures will be discussed.

Table 4.3 in the next page tabulates the countermeasures against the threats identified.

Table 4.3 Countermeasures against threats.

Threat	Countermeasures	Description
Loss of laptops & laptop vulnerabilities	Encryption of laptop data	The encryption of data on laptops is not a new feature but nowadays, more products with such feature are appearing and data encryption has also been made easier. For example, Microsoft latest operating system Vista comes with a harddisk encryption feature called BitLocker [30] and Seagate has started shipping encrypted laptop hard drives [31]. By encrypting the data, we would effectively eliminate the risk of sensitive data leakage from the lost of laptops. Encryption is especially needed for the laptops of the top-management in the LEA who will have sensitive data which could be in the form of document files or emails stored on the laptops.
	Laptop hardening	Hardening of the laptop is necessary to eliminate vulnerabilities. The operating system of the laptop should be hardened. The laptop should be installed with a personal firewall, intrusion detection/prevention system and anti-virus software. A strong password login should be used and, biometrics and two-factor authentication could be used as well. Other than that, laptops could be fitted with *Trusted Platform Module* (TPM) chips and make use of the security functions provided by the TPM. There should also be policies in place to ensure regularly patching and updating of the virus definition files. All these steps make the laptop stronger for use by a remote user in the untrusted environment of the Internet.

Threat	Countermeasures	Description
	Data backup	Data backup is an essential safeguard to mitigate against loss of laptop. Even if the laptop is lost, we could at least recover the data so that the user would suffer the least disruption.
Loss of sensitive information	Data encryption	Data encryption is an effective countermeasure against loss of sensitive information. If data is properly encrypted with a good encryption algorithm, any stolen data by an attacker would almost be useless to him. Data encryption is what the ultimate goal of a de-perimeterised world as according to JFC#9. Right now, encryption is used widely where confidentiality of data is absolutely necessary such as in online transactions using SSL, in the credit cards and in the GSM mobile system. However, it is still some way to go for the industry to develop practical solution that can classify all data, encrypt the data and provide efficient access control over the data.
	Access control to data	JFC#10 stresses the importance of access control to data in a de-perimeterised world to ensure that only the authorised personnel would be able to access the data. This will prevent data leakage. For this to work, data should be properly classified and maintained as mentioned in JFC#9. However, access control at a data level is complex and difficult. It is also a massive effort to process enormous amount of data and it would require global authentication and a global standard for Identity & Trust management. Nevertheless, some form of access control of data still has to be implemented to protect sensitive information.

Threat	Countermeasures	Description
	Control of data storage devices	Data storage devices such as thumb drives (or memory sticks) and memory cards are ubiquitous these days. They have high capacity and are very small. Even smartphones, cameras and music players are capable of data storage. All these devices can be easily brought into an organisation to be used to copy out sensitive data, spread virus or do other damage. But sadly, 67% of UK companies in BERR's Information Security Breaches Survey 2008 did nothing to prevent confidential data leaving on USB sticks, etc [4]. The incident on the lost of computer memory stick containing unencrypted data of criminals in UK reported on 22nd August 2008 proved the point on the need to control of the use of thumb drives [27].
Attacks on Internet website	Hardening of servers	Attacks on Internet websites are possible if there are vulnerabilities on the web servers that a hacker can exploit. In order to avoid this, web servers should be hardened and constantly patched to remove any vulnerabilities. Penetration tests should be conducted regularly on the web servers.
	Response and contingency plan	Even if the servers are patched with the latest updates, it cannot be guaranteed that no attacks can be made on the servers. The servers will still be vulnerable to "zero-day" attacks. Therefore, it is important that a response and contingency plan to be formulated to response to an attack. In this way, we could be certain that services could be recovered in the shortest possible time.

Threat	Countermeasures	Description
	Data backup	As with the data backup for laptops, backup of the data on the web server is essential to reduce the damage of an attack on the Internet website. Should data be deleted from the server, the latest backup version of the data can be restored quickly.
Firewall compromised	Redundancy and high availability firewall	In the current de-perimeterised environment, many "holes" are punched through the firewalls. And data are now usually encrypted making it impossible for the firewall to screen for malicious content. However, as long as a truly de-perimeterisation has not been realised and practical solutions not yet been developed, the firewall still plays a rather important role as the first line of defence against attackers. Hence, the design of the firewall in an organisation should be done carefully. There has to be redundancy and high availability built into the firewalls. Firewalls should also move towards screening at the application layer so that there can be better visibility of applications in order to suit the security requirements of the applications.
	Proper maintenance	The firewall in the real world and a de-perimeterised environment has huge number of firewall rules. As part of the regular maintenance of the firewall, the rules have to be reviewed to see if the applications still need the rules so that any redundant rules can be removed. If possible, rules should be regrouped so that they work more effectively and easier to be understood by the administrator. This would ensure that there are as few "holes" as possible

Threat	Countermeasures	Description
		in the firewall and it can therefore run more efficiently.
	Backup recovery site	For a mission critical organisation such as a LEA or a bank, there would be a need to have a backup recovery site in a setup similar to that mentioned in *Section 3.4* and shown in *Figure 3.3*. Thus, if the firewall for the primary site has been compromised, the backup site could be brought up. In this way, applications could still be made available from the backup site while the connection to the primary site is cut off to prevent further damage by the attacker.
Vulnerability of mobile devices	Securing mobile devices	According to JFC#5, all devices must be capable of maintaining their security policy on an untrusted network. In a de-perimeterised environment, mobile devices are working in untrusted network, and as users of these devices, extra attention is required to secure them. The different types of mobile devices in the market are numerous. We should select those that are designed with security in mind. In his article, Shlomo Touboul talked about the vulnerabilities of mobile devices and proposed that mobile security hardware (instead of software) be used to protect mobile devices [32]. One possible candidate of mobile security hardware is the *Trusted Platform Module* (TPM) chip which is currently under much research and development [33]. The TPM could potentially provide several security functionalities such as encryption and digital rights management. For a LEA where mobile devices are to be used to store sensitive data and

Threat	Countermeasures	Description
		for operations, it might even be necessary for devices to achieve an appropriate *Evaluation Assurance Level* (EAL) of the *Common Criteria* (CC)[6].
	Policies on use of mobile devices	Policies on the use of mobile devices should be reviewed on a regular basis. The policies should be clear as to who could use the devices, how the devices should be used and maintained. The objectives are to prevent unauthorised use and possible abuse.
Insider attacks	Security clearance	Security clearance is usually deployed in a government's recruitment process where general background checks are conducted on a potential employee to ensure he or she does not have a negative record. This countermeasure could possibly remove any potential malicious insiders in the future. In the de-perimeterised environment, those who need to go through security clearance should include the contractors, vendors, associates, security guards and all others who will be "inside" the organisation and possibly have access to its assets.
	Separation of duties / Principle of least privilege	Separation of duties and principle of least privilege are what being depicted in JFC#10 with the purpose of controlling access to data. It is an absolutely essential countermeasure to prevent or to limit the damage that a malicious insider can do by ensuring that no single person has full access and that the person has access to

[6] Common Criteria (CC) is a security evaluation of computer systems to provide assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner. For more information, please see http://www.commoncriteriaportal.org/ or http://en.wikipedia.org/wiki/Common_Criteria.

Threat	Countermeasures	Description
		only the data he or she is authorised. This step is even more so important in a LEA where there exists a lot of confidential information related to public safety and security.
	Deployment and active monitoring of IDS	The *Intrusion Detection System* (IDS) complements the firewall in the protection of the internal network. It helps to detect any abnormal activities in the network such as unauthorised login, unauthorised access to data or sudden surge in network traffic. A feature of the IDS allows timely alert will be sent to the administrator to response to the anomaly.
Malware	Hardening of servers, desktops and laptops	Malware takes advantage of the vulnerabilities that exist in servers, desktops and laptops to compromise the machines. D-P has made it easier for malware to get into an organisation's internal network through the "holes" created in the firewalls. Wireless connections also make it possible for malware to bypass the firewalls and other network perimeter devices. An effective way of reducing this risk is to harden the machines commonly done by installing the latest software patches, removing unwanted services, updating the virus definition files and by having a host-based IDS.
	Secure coding practises	Malware attacks software vulnerabilities such as buffer overflow. By ensuring developers follow secure coding practises or by acquiring software that has security built into its development lifecycle, we can get some assurance that the software when in use would less likely to have bugs that will be exploited by a hacker. In the untrusted D-P world, secure software would be

Threat	Countermeasures	Description
		able to better survive against malware.
	Deployment and active monitoring of IDS	Deployment of IDS would help to quickly detect an intrusion by malware. It is usually a combination of host-based and network-based IDS that would be most effective in deterring malware. The IDS system has to be actively monitored for the protection of the network.

4.4 Risk Register

The Risk Register based on the template given in *Annex A* is presented in this section. However, the columns that are not relevant to this study have been removed. The ratings are entered based on the author's research of the threats in the current but evolving de-perimeterised environment. The author will justify the ratings given for risks that are of interest and discuss the effectiveness of the corresponding mitigating actions.

Table 4.4 The Risk Register.

S/N	Risk Statement	Possible Consequences	Likelihood	Severity	Grade	Mitigation Actions
1	Loss of laptops & laptop vulnerabilities	Loss of sensitive information; loss of reputation	Medium	1	B	Encryption of laptop data; laptop hardening; data backup
2	Loss of sensitive information	Loss of reputation; leakage of operational & business plans; law suites	Medium	1	B	Data encryption; access control to data; control of data storage devices
3	Attacks on Internet website	Unavailability of online services; website defaced	Medium	2	C	Hardening of servers; response & contingency plan; data backup

S/N	Risk Statement	Possible Consequences	Likelihood	Severity	Grade	Mitigation Actions
4	Firewall compromised	Unavailability of services	Medium	1	B	Redundancy & high availability firewall; proper maintenance; backup recovery site
5	Vulnerability of mobile devices	Loss of sensitive information	High	1	A	Securing mobile devices; policies on use
6	Insider attacks	Loss/damage of sensitive information, equipment & other assets; virus infection; unavailability of services	Medium	1	B	Security clearance; separation of duties/principle of least privilege; deployment & active monitoring of IDS
7	Malware infection	Unavailability of services	Medium	2	C	Hardening of servers, desktops & laptops; secure coding practises; deployment & active monitoring of IDS

We can observe from *Table 4.4* that the greatest risk faced with D-P is in the securing of mobile devices. This is mainly due to the liberalisation of mobile devices in a de-perimeterised world which we have touched on in the previous sections. At the moment, laptops are considered the most vulnerable of all mobile devices. Not only are laptops lost in private organisations, we could also see loss of laptops occurring in government organisations such as in the cases of FBI or UK government and let alone a LEA. The loss of laptop in a LEA where laptops are often used to store confidential information or be deployed for operations, the impact would certainly be severe. In the worst case scenario, national safely and security could be affected possibly resulting in the loss of lives. For the same reason, a compromised laptop would have severe consequences due to the leak of sensitive information. As such, based on *Table A.1* in *Annex A*, it is justifiable to

give the highest severity rating of '1' for the loss of laptops. However, the likelihood on the loss of laptops is given a rating of 'Medium' and not 'High'. It is a fair assumption made by the author because even though it is more common to see loss of laptops from the many examples cited in this report, controls are usually put in placed to manage the laptops especially in the case of a LEA who understands threats better than any other types of organisations. Extra care should have been taken to ensure accountability of laptops. The mitigating action of encrypting laptop data would reduce the impact of loss of sensitive information due to the loss of laptops to a minimum. Well, it is arguable that there could still be some chance that information could be leaked as encryption is not perfect and cryptanalysts could possibly break them given sufficient resources. However, this possibility is very low and would not be considered as part of this study. Next, the hardening of laptops as discussed in the previous section would make laptops more robust; its effectiveness nevertheless depends on the how the laptops are being managed such as whether if virus definition has been updated regularly? Whether if applications have been patched regularly? And whether usage of laptop and password policies have been strictly adhered to. Lastly, data backup reduces the loss of availability of data to the user and also limits the amount of data loss. The restoration of data would only be as updated as the last backup and this means that the user would still suffer some loss of the recent data; this is unfortunately unavoidable or would be very expensive to implement a "zero" loss of data.

Other mobile devices (such as mobile phones and PDAs) unlike laptops however, have just only passed their infant stage of developments in terms of security. Even though there are many recent ongoing researches on mobile security, less emphasis was previously placed in the security of these devices and therefore,

the likelihood that a vulnerability be exploited is still very high. The physical vulnerability of the devices been stolen is itself a threat as we can see, for example, from the ever-increasing of mobile phones being reported missing; it was reported in November 2004 that more than 10,000 phones are lost or stolen every month in the UK [34]. Hence the rating of 'High' is given in the Risk Register for the vulnerability of mobile device being exploited resulting in loss of sensitive information stored on the device. The severity level is '1' due to the consequences of loss of sensitive information for the LEA and therefore, the outcome is a risk level of 'A'. The high risk level necessitates for special attention to be given and this we will be addressed in the next chapter on recommendations.

Another high risk area is that of the insiders and as mentioned in previous sections, insiders include contractors, cleaners, security guards, associates and others who have dealings with the organisation. Insiders could do much harm to the organisation due to the privileged access that they have and therefore, a severity level of '1' is given. The risk is tagged with a likelihood of 'Medium'; this is reasonable because most government departments in particularly the LEA would have implemented controls such as procedures for security clearance of personnel that have dealings with the LEA. It is also likely in a LEA that you will see employment of separation of duties, principle of least privilege or some other "check and balance" procedures in the handling of restricted items such as weapons, communications sets, etc. As such, it is more difficult and there is less chance for a malicious insider to do harm. Nevertheless, it is still a 'Medium' likelihood and not an absolutely 'Low' as D-P has increased the number of associates and so called "insiders" brought about by outsourcing, partnership and collaboration. Other than, security clearance, separation of duties and principle of least privilege, the

mitigating action of deploying an Intrusion Detection System (IDS) or prevention system could be used to give alerts of any anomaly. This to some extend restricts the amount of damage that an attacker can do. The limitations of such a technological solution however are that such systems could be fooled by a clever malicious insider and also, if not properly managed and monitored, the systems are of no use.

Looking at *Table 4.4* again, you will notice that 2 out of the 7 identified threats are given the severity rating of '2' while the rest have '1'. The two threats are Attacks on Internet websites and Malware infection. These two threats are still of concern to organisations but over the years, better written software and more effective antivirus applications had been able to put the threats under control. The harm or impact that the threats can do has been narrowed. As such, the severity posed by these risks warrants a '2' and not '1'. In fact, both risks also have been given 'Medium' likelihood and the risk level of both risks are 'C'.

The mitigating actions proposed against firewall being compromised are redundancy & high availability firewall, proper maintenance and having a backup recovery site. All these, if properly implemented, would be effective in preventing the firewall from being compromised in a de-perimeterised environment. As mentioned previously, before better solutions tailored to a D-P world appear, the firewall is still an important device that provides the first line of defence against external threats.

Chapter 5
Recommendations

The recommendations given in this chapter are partly based on the results of risk analysis done in *Chapter 4*. They are also based on the author's knowledge and experience in the IT industry, his understanding, interpretation and idea of de-perimeterisation through the research that he has done on the topic.

These recommendations are categorised into short-term, mid-term and long-term. Short-term recommendations are those that should be carried out immediately and could be achieved within 1 year or so. It is hoped that the implementation of short-term recommendations would mitigate to a large extend the immediate threats brought about by de-perimeterisation. Mid-term recommendations are the ones which require a longer time, say from 2 to 3 years to achieve. Nevertheless, work has to be carried out early so that it will be possible to realise the goals of mid-term recommendations. On the other hand, long-term recommendations are exploratory. Solutions for long-term recommendations might not yet exist or are experimental or are not mature enough to be deployed at an enterprise level. It is however a wise idea to keep a lookout on the technologies developed in these areas within a 4 to 5 years' time frame.

The chapter ends with a discussion on the essential recommendations specifically for a LEA and how secure would the LEA be if some or all the recommendations are followed.

5.1 Short-term Recommendations

The short-term recommendations are:

- Securing of mobile devices

- Vulnerability management
- Review and tighten controls on insiders
- Strengthen security awareness and training

Securing of mobile devices

It was evident from the risk analysis in *Chapter 4* that one of the biggest priorities and the immediate task to mitigate risks in face of D-P is in the securing of mobile devices. In order to secure mobile devices, we need the devices to have anti-virus & intrusion detection applications, personal firewalls, hardened OS, data encryption functions, strong password access control, biometrics access, two-factor authentication, CC certified and many more. For laptops and other devices with storage capacity, physical access control is important to prevent lost by simple theft and also to minimise the loss after losing them. Currently, Hewlett-Packard, IBM, Toshiba, Dell or Samsung have already started shipping some of their laptop models fitted with TPM chips that could provide some security feature to make laptops more secure [33]. But unfortunately, the functionality offered by the chip is limited at this moment. However in the future, all mobile devices could possibly be fitted with *Trusted Platform Module* (TPM) chips that could give assurance that the running application software is genuine and the machines themselves cannot be easily compromised. All these countermeasures together with proper policies and adherence to best practises in managing the pool of mobile devices in the organisation would definitely reduce the risk to the minimum.

Vulnerability Management

Vulnerability Management (VM) is another short-term measure that will help to mitigate the risks brought about by de-perimeterisation. With effective VM, we can have an automated means to get rid of the vulnerabilities that exist in all the machines of the organisation.

However, care has to be taken in the implementation of VM. It is important to note that VM is not all about patching and is not only a technical solution; VM is a whole management process. According to Gartner analysts, "*the vulnerability management process includes policy definition, environment baselining, prioritization, shielding, mitigation as well as maintenance and monitoring.*" [35]. As how Anton Chuvakin explains, the vulnerability management process starts from a policy definition document that covers an organization's assets (such as systems and applications) and their users [36]. Such a document and the accompanying security procedures should define the scope of the vulnerability management effort as well as postulate a "known good" state of those IT resources. Chuvakin further added that even if you patch all the known software vulnerabilities, you can still be attacked and compromised by intruders who exploit undisclosed flaws. He stressed that "*… apart from a sensible vulnerability management program and careful network and host security monitoring that might make you aware that you've been hit, you need to make sure that the incident response plans are in order. … to be addressed by using the principle of "defense in depth" during the security infrastructure design. Get your incident management program organized ….".*

Hence, we can see that with a properly implemented vulnerability management programme, we can gain assurance that all devices (especially the mobile ones) will

be free from vulnerabilities and also ensure a working framework that allows the continuous monitoring of vulnerabilities against the ever evolving threats.

Review and tighten controls on insiders

With de-perimeterisation, it is timely to review and tighten the controls on insiders. As insiders pose a big threat with potential serious damage that they can do in an organisation, considerations have to be carefully made when determining the access rights that each insider has. Some proven principles such as separation of duties and principle of least privilege should be applied where necessary. The use of technology such as the IDS could be applied here to alert the administrator of possible unauthorised access, policy violation and other anomalies. Lastly, policies, procedures and controls should be reviewed to ensure they are keep updated to the changes and needs in the de-perimeterised environment.

Strengthen security awareness and training

People are often viewed as the weakest link in security. But Bruce Schneier has pointed out that people could also be the most effective defence mechanism against threats [18]. In areas where technology has not reached the level to allow machines to work effectively without human intervention such as in identification, people would be more superior and more resilient against attackers who try to deceive the machine or a computer security system. Therefore, in order to remove people from becoming the weakest link in security and at the same time harness the capabilities of people, security awareness and training is of utmost importance. New employees should be instilled with a sense of security. And existing

employees are to be reminded of the security policies, procedures and the D-P threats that loom within the organisation, especially those associated with insiders.

5.2 Mid-term Recommendations

There are two mid-term recommendations to confront the threats of D-P, namely adoption of Web Services and working towards SSO. They should be carried out now and be incorporated into the new applications developed for the organisation.

Adoption of Web Services

XML or *Extensible Markup Language* is a meta-language which defines a set of rules or syntax to describe the elements in a XML document. *Web Services* (WS) use XML and it is an open standard. Applications using web services would be highly scalable and would allow for interoperability. Interoperability is a desirable property in a de-perimeterised environment where network perimeter is blurred between internal and external networks. Within the web services, there is a list of WS security components being defined. These components include *XML Signature*, *XML Encryption* and SAML (*Security Assertion Markup Language*) which provides integrity, confidentiality and authentication services respectively. Web Services is a likely candidate as the universal standard to be used in a de-perimeterised world as it is an open, secure standard (meeting requirements of JFC#4), allows data encryption (JFC#9), is flexible (JFC#1), scalable (JFC#2) and it allows interoperability between different systems. *Identity Management and Federation* is also possible as accordance to the requirements of JFC#8 by using

web services; this is in the case of *Liberty Alliance*[7] which is used as a *Single Signed On* (SSO) identity management scheme. SSO will be discussed shortly. Do however bear in mind that web services also has some shortcomings such as the overheads and inefficiencies, and it requires careful specification of all the elements and attributes in XML documents for interoperability. Hence, it will take a little longer before it can be more widely accepted.

Work towards Single Signed On (SSO)

Single Signed On (SSO) allows a user to login once into a system and be able to use various services provided by different applications without having to login again. It allows identity management which is necessary in a de-perimeterised environment. With SSO, it is hoped that we would be better able to manage users having multiple identities at varied locations, and from there, controlling the data access of the users would be possible.

While there has not been a SSO standard been defined, the Liberty Alliance project mentioned earlier has much potential to be one. Liberty Alliance is an industry consortium formed in 2001 by global companies which includes British Telecoms, Intel, Sun Microsystems, Oracle, Novell, Computer Associates and many more. The main goal of Liberty Alliance is to establish open specifications that support a range of network identity based interactions, and give business a basis for new revenue opportunities building upon existing relationships with consumers and

[7] Liberty Alliance project is an industry consortium. It has produced a series of specifications designed to support the notion of federated network identity (http://www.projectliberty.org).

partners, and a framework that gives consumers choice, convenience and control when using any Internet-connected device[8].

Even though there is currently no standard specification for SSO, the availability of SSO solutions in the market is not lacking. It is important for an organisation to implement an SSO solution so that new applications being developed can be incorporated onto it. This would be a more effective way of managing identities in a de-perimeterised environment and allow possibility for an easier future integration or migration into a truly global identity & trust management system.

5.3 Long-term Recommendations

As part of the long-term goal in solving de-perimeterisation, organisations should keep a constant lookout for the latest development of commercial products that meet the Jericho principles. The areas to lookout for are in Identity and Trust Management and in Trusted Computing.

Lookout for Identity and Trust Management

Global Identity and Trust Management is difficult to achieve. It requires new standards to be written and solution has to be implemented on a global scale for it to work. For a truly de-perimeterised environment, a global identity and trust management framework is needed as depicted in JFC#8. The *Infocomm Development Authority of Singapore* (IDA) has in 2005 announced an *Infocomm Security Masterplan* which includes a *National Trust Framework* (NTF) conceptualised in 2006. NTF's objective is to develop a national framework that

[8] Extracted from "Applications & Business Security Development: Identity Management" lecture notes (Pg 29) by Allan Tomlinson, Information Security Group, Royal Holloway, University of London, 2008.

provides greater assurance and trust, so that Singapore can continue to leverage on its infocomm successes [37]. This is an example of an identity & trust management framework implemented on a national scale. Certainly, it would be interesting to follow-up to see the solutions that would evolve in the near future and hopefully, the solutions turns out as what was perceived in the Jericho principles.

Trusted Computing

The other area to pay close attention to is in Trusted Computing. With Trusted Computing, the computer will consistently behave in specific ways, and those behaviors will be enforced by hardware and software [38]. Trusted Computing which is led by the Trusted Computing Group[9] is currently under much development. The group aims to develop standard specifications for a *Trusted Platform Module* (TPM) to be fitted onto every mobile device. The TPM, which has several security functionalities such as encryption, can be used in the areas of digital rights management, identity theft protection, and protection from viruses & spyware. Trusted Computing can potentially help to make millions of mobile devices secure by protecting the devices from malware and from hackers' attacks. It thus meets Jericho principles JFC#4 & #5 where devices would be robust enough to operate in an untrusted network using open source, secure protocols. As mentioned previously in this report, various brands of laptop models were already been shipped with the TPM chips even though the full functionalities of the chip have not yet been utilised. Soon, we could see the chip being fitted onto mobile phones and many other mobile devices.

[9] https://www.trustedcomputinggroup.org/home

5.4 LEA and the Recommendations

In this section, we will discuss the proposed recommendations in relation with the environment of a LEA. What are the recommendations that are essential to the LEA? And if some or all the recommendations are followed, how secure would the LEA be?

We could see that all the short-term recommendations (securing mobile devices, vulnerability management, review and tighten controls on insiders, and strengthen security awareness and training) are important for adoption by the LEA as a quick-fix solution in face of de-perimeterisation. We have emphasized many times in this report the importance of securing mobile devices and this has to be stressed even more so for a LEA which has been deploying mobile devices, which are likely to contain sensitive information, for its remote workers and for use during operations in the field. The threats to mobile devices in the de-perimeterised world are real and we have cited incidents of laptops that were lost in even the perceived secure environment of government departments. So, the recommendations such as data encryption, hardening and others should be fully implemented to avoid loss of mobile devices, loss of sensitive information and likely the embarrassment to the LEA.

Vulnerability management would help LEA in the same way as other organisations. If done properly, it would help the LEA in keeping track of the threats against its assets – not only IT assets but also other assets such as weapons, vehicles and buildings. Putting checks on insiders, preventing and deterring possible malicious insiders are what LEA have been doing well all these while. With de-perimeterisation, the LEA should continue its practices, and review and maybe step-up the controls on insiders so as to eliminate any possible over-sights.

The LEA is in the business of security but it should never be over-complacent in managing security and take security for granted. Security awareness and training should always be emphasized so that a culture sense of security can be developed for new and existing employees in the LEA.

As the core function of a LEA is to fight crime and not in the development of IT solutions, it is a user of technology and as a user, the LEA could state what it wants or dictate its requirements for solutions to be deployed. Hence, following the mid-term recommendations, the LEA should insist on *Web Services* and *Single Signed On* solutions from its vendors supporting its application development. This would automatically gear the LEA towards preparing itself and seamlessly integrate itself with the de-perimeterised solutions in the near future.

As for the long-term recommendations, they are not quite essential for the LEA to follow closely. As a user of technology, the LEA is very much dependent on its vendors to provide the solutions that meet its requirements. Technology is developing very quickly and there is much uncertainty on how some technologies will advance in the future. Furthermore, the LEA would most likely be part of the overall IT security plan or program of the government; the IT security program being led by the authority in the government that handles ICT developments. Nevertheless, the LEA should at least keep itself updated on the latest development news of D-P.

In summary, the author thinks that the short-term recommendations are all essential for the LEA to mitigate D-P threats. The LEA would definitely be more secure in terms of preventing loss of mobile devices, loss of sensitive information, insider attacks and any other forms of security breaches, and be significantly strengthened in managing of its IT assets in face of D-P if all short-term

recommendations are followed. The LEA can state what it wants for the mid-term recommendations to better prepare and adapt itself for the increasing effects of D-P in the near future. The long-term recommendations, however, are of less importance to the LEA at this moment. The LEA could however keep itself updated on the latest development in D-P to gear itself towards the truly de-perimeterised world of the future.

Chapter 6
Conclusions

The issues that de-perimeterisation (D-P) brings are real and it is happening right now in organisations all over the world. In this report, we have demystified the term "de-perimeterisation" by explaining how it came about, what are the driving factors, the issues it brings and the strategy to developing and adopting solutions that could confront it.

De-perimeterisation came about basically due to the highly inter-connect networks we have today which encouraged a burst of mobile workers driven by the cost-saving considerations. Changing business models have also led to more outsourcing, off-shoring and partnerships between companies and organisations. In order for mobile workers to work efficiently and effectively at home or at remote locations, applications started to punch "holes" through the firewalls defining the traditional network perimeter. With this, the firewalls are weakened and the network perimeter now becomes "porous". This perimeter is seen to have "eroded", and thus the term "de-perimeterisation". The Jericho Forum who invented the term de-perimeterisation has published among its vision and position papers, a set of eleven Jericho commandments or principles which set the strategy in developing solutions that could confront the threats in a de-perimeterised world. Part of the strategy is to develop solutions that use encryption, inherently secure communication and data-level authentication.

From our understanding of de-perimeterisation, we have identified the threats that it carries. The threats, for example, could come from a hacker who tries to compromise the weakened firewall in a de-perimeterised organisation. Following analysis of the threats, the author concludes that security of mobile devices and

malicious insiders are the two biggest risks faced. Mobile devices provide access to an organisation's network and with the proliferation of mobile devices due to a large increase in mobile workers, these devices now face increased threats such as theft and malware attacks. Malicious insiders who have privileged access within the organisation are also a threat to the organisation.

Unfortunately, we are still not yet ready for a truly de-perimeterised environment. There are still many hurdles to overcome before practical solutions could be made commercially available and be widely adopted at the enterprise level. Among the hurdles are things like data-level authentication and global identity & trust management. While waiting for that to happen, organisations must do something to mitigate the risks. The recommendations given in this report is specifically aimed at this. Firstly, short-term recommendations are intended to mitigate the most serious D-P threats that currently exist in organisations. These recommendations include the securing of mobile devices and implementing vulnerability management. Then, the mid-term recommendations' objective is to mould the IT environment of the organisation into an open, scalable and interoperable architecture such that it is able to easily adopt D-P solutions in the future. Using *Web Services* and having SSO solutions are the proposed mid-term recommendations. Lastly, the long-term recommendations keep the focus of the organisation in areas where new developments could possibly help organisations move towards a truly de-perimeterised world and be completely protected from D-P threats. *Identity & Trust Management* and *Trusted Computing* are two such areas that have been identified. We have also discussed that all short-term recommendations are essential to the LEA while the LEA as a user of technology can state its requirements for mid-term recommendations. Long-term

recommendations however are not really important for the LEA at this moment. But, the LEA should keep itself updated on the latest development of D-P.

Differences between a LEA and a Private Organisation

It is appropriate here to mention the differences between a LEA and a private organisation in face of de-perimeterisation. In fact, there are not many differences that we can see from an IT perspective. The LEA is very much like a multinational corporation with its offices distributed around the world – the LEA has its regional headquarters distributed across the country. Both organisations rely to a large extent on IT systems and technologies for their day-to-day operations; they are faced with pressures to remain cost effective to be competitive and efficient. The LEA, like a private organisation, is also constantly seeking better co-operations and partnerships with its counterparts to enhance its operational efficiency. Hence, the effects and threats that D-P brings to a private organisation would also be felt by a LEA.

However, the two entities defer in some subtle areas. Firstly, in their business objectives, the LEA unlike a private organisation is not profit-oriented but aims to provide law and order in a country. The motivation of attackers for the two organisations is also different. A hacker is more likely to attack a private organisation for money while an attack on a LEA is more due to an emotional hatred. The reputation for a LEA is comparatively more important than the private organisation as the loss of reputation would potentially cause a total distrust in public order system which may result in a chaotic society. In face of de-perimeterisation, a LEA also has a greater responsibility in terms of protecting data because the consequences of leakage of sensitive information, unlike a private

organisation which probably result in the loss of profit, that in a LEA could affect public safety and security, and possibly could lead to the loss of lives.

Areas for further studies

De-perimeterisation is currently a widely talked about topic where development of its solutions are still evolving. There are areas related to de-perimeterisation that do not fall within the scope of this study and are therefore not covered in this report. Here is what the author believes would be of interest for further studies:

- Identity & Trust Management for De-perimeterisation
- The Legal Aspects in a De-perimeterised World
- Architecture for a De-perimeterised Environment

Identity & Trust Management has been mentioned a few times in this report and this essential thing for de-perimeterisation is a good area to research into to see the effects, and how identity and trust can be managed with de-perimeterisation. Next, the legal aspects in a de-perimeterised world is least talked about. A study into it could potentially provide an insight into the various legal issues brought about by de-perimeterisation. And lastly, the architecture for a de-perimeterised environment is listed as an area of further studies. While the Jericho Forum has published a position paper for the architecture of a de-perimeterised architecture which favours a Service-Oriented Architecture (SOA), a de-centralised trust framework and P2P applications based, it still leaves much room to define a more concrete architecture and to explore on how the architecture could work with real world application scenarios [39].

Final remarks

De-perimeterisation involves a paradigm shift on the way security professional view the network security of organisations. De-perimeterisation affects both a LEA and a private organisation in the same way. Much has been talked about in this report that organisations have to carry out the risk management processes to confront the threats that de-perimeterisation brings. While existing security solutions still work, it will not be long for organisations who do not prepare for de-perimeterisation to find themselves caught off-guard and be thrown into the need to carry out costly and disruptive overhaul of their whole network architecture. In order to fully embrace de-perimeterisation into our network, there is a need to make changes now to eliminate the problems of the future. What will be the future of network security be like? And how powerful will be the network security components in a de-perimeterised network architecture? The answer, as what David Lacey, the founder of Jericho Forum puts it, "*Only one thing seems certain: It will be different from today.*" [40].

References

[1] Jericho Forum, http://www.opengroup.org/jericho/about.htm

[2] Jericho Forum's Business Case for Deperimeterisation, http://www.opengroup.org/jericho/Business_Case_for_DP_v1.0.pdf

[3] Jericho Forum's FAQ, http://www.opengroup.org/jericho/faq-at.htm

[4] 2008 Information Security Breaches Survey by BERR, http://www.berr.gov.uk/files/file45714.pdf

[5] Jericho Forum, The What & Why of De-perimeterisation, http://www.opengroup.org/jericho/deperim.htm

[6] ScienceDirect, De-perimeterisation: Benefits and Limitations, Graham Palmer, 26 November 2005. http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VJC-4HNF68X-3&_user=122871&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_version=1&_urlVersion=0&_userid=122871&md5=b3806f02e2aa18da4d3d396c556220ee

[7] Network World, "Security is a world without borders", Cummings Joanne, 27 September 2004. http://www.nwfusion.com/buzz/2004/092704perimeter.html

[8] MSc Information Security Dissertation, "De-perimeterisation v Defense in Depth", Terry Bebbington, Royal Holloway, University of London, 2006/7.

[9] Jericho Forum Commandments, http://www.opengroup.org/jericho/commandments_v1.2.pdf

[10] Network World, Tim Greene, 10 Sep 2007, http://www.networkworld.com/news/2007/091007-jericho-forum-firewalls.html

[11] Jericho Forum Newsletter, July 2007, http://www.opengroup.org/jericho/newsletters/news_0707.pdf

[12] Network World, "De-perimeterization: Jericho Forum misses the mark", Joel Synder, 15 August 2005. http://www.networkworld.com/columnists/2005/081505faceoffno.html

[13] Computer Weekly, "Deperimeterised approach to security is not suitable for everyone, warn analysts", Bill Goodwin, April 2006. http://www.computerweekly.com/Articles/2006/04/28/215495/deperimeterised-approach-to-security-is-not-suitable-for-everyone-warn.htm

[14] Law Enforcement Agency related websites

Metropolitan Police Service (UK)
http://www.met.police.uk/index.shtml

New York Police Department (US)
http://www.nyc.gov/html/nypd/html/home/home.shtml

Los Angeles Police Department (US)
http://www.lapdonline.org/

Tokyo Metropolitan Police Department (Japan)
http://www.keishicho.metro.tokyo.jp/foreign/submenu.htm

Singapore Police Force
http://www.spf.gov.sg

Royal Malaysia Police Force
http://polismalaysia.brinkster.net/Royal%20Malaysian%20Police%20Force%20-%20About.asp

Australia Federal Police
http://www.afp.gov.au/home.html

[15] Wikipedia, Koban, http://en.wikipedia.org/wiki/Koban_(police_box)

[16] Metropolitan Police Service, Directorate of Information, "Information, Communication and Technology Strategy", 7 September 2006.
http://www.met.police.uk/foi/pdfs/aims_objectives_plans/corporate/information_communications_technology_strategy.pdf

[17] Computer Weekly, "Outsourcing: Westminster Council IT infrastructure free by 2015", Rebecca Thomson, 21 July 2008.
http://www.computerweekly.com/Articles/2008/07/21/231565/outsourcing-westminster-council-it-infrastructure-free-by.htm

[18] Bruce Schneier, "Beyond Fear: Thinking sensibly about security in an uncertain world", Copernicus Books, 2006, Chap 5, Pg 60-71.

[19] Real-time survey conducted at Jericho Forum Conference of InfoSecurity Europe, Qualy, 26 April 2007.
http://www.opengroup.org/jericho/live_poll_pr.pdf

[20] "Airport Insecurity: The case of missing or lost laptops", Ponemon Institute, 30 June 2008.
http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf

[21] BBC, "Defence minister's laptop stolen", 4 June 2000.
http://news.bbc.co.uk/1/hi/uk/776364.stm

[22] "MoD loses 600 laptops", BBC News, 13 January 2002.
http://news.bbc.co.uk/1/hi/uk/1757792.stm

[23] "The Federal Bureau Of Investigation's Control Over Weapons And Laptop Computers Follow-Up Audit" report, February 2007, Pg iv.
http://www.usdoj.gov/oig/reports/FBI/a0718/final.pdf

[24] The Guardian, "Personal details of every child in UK lost by Revenue & Customs", Deborah Summers, 20 November 2007.
http://www.guardian.co.uk/politics/2007/nov/20/economy.personalfinancenews

[25] BBC, "Nine NHS trusts lose patient data", 23 December 2007.
http://news.bbc.co.uk/1/hi/uk/7158019.stm

[26] BBC, "Millions of L-driver details lost", 17 December 2007.
http://news.bbc.co.uk/1/hi/uk_politics/7147715.stm

[27] BBC, "Company loses data on criminals", 21 August 2008.
http://news.bbc.co.uk/1/hi/uk/7575766.stm

[28] BBC, "Firm 'broke rules' over data loss", 22 August 2008.
http://news.bbc.co.uk/1/hi/uk_politics/7575989.stm

[29] The Register, "Scotland Yard careers website defaced", John Leyden, 25 February 2008.
http://www.theregister.co.uk/2008/02/25/met_police_defacement/

[30] Microsoft Technet, "BitLocker Drive Encryption".
http://technet.microsoft.com/en-us/windows/aa905065.aspx

[31] Computer Weekly, "Encrypted laptop hard drives arrive from Seagate", Antony Savvas, 13 March 2007.
http://www.computerweekly.com/Articles/2007/03/13/222387/encrypted-laptop-hard-drives-arrive-from-seagate.htm

[32] Shlomo Touboul, "Deperimeterisation Developments - Securing the Mobile Workforce of the Future", Yoggie Security Systems, April 2008.
http://www.globalsecuritymag.com/Shlomo-Touboul-Yoggie-Security,20080402,2452

[33] BBC, "What price for 'trusted PC security'?", 18 March 2005.
http://news.bbc.co.uk/1/hi/technology/4360793.stm

[34] BBC, "Help for lost or stolen phones", 23 November 2004.
http://news.bbc.co.uk/1/hi/technology/4033461.stm

[35] Amrit T Williams & Mark Nicolett, "Improve IT Security With Vulnerability Management", Gartner, 2 May 2005.
http://www.gartner.com/DisplayDocument?doc_cd=127481

[36] Computer World, "Five mistakes of vulnerabilities management", Anton Chuvakin, 11 January 2006.
http://www.computerworld.com/printthis/2006/0,4814,107647,00.html

[37] "Infocomm Security Masterplan and National Trust Framework", Infocomm Development Authority of Singapore, 2007.
http://www.ida.gov.sg/Programmes/20060925100740.aspx?getPagetype=36

[38] Wikipedia, Trusted Computing.
http://en.wikipedia.org/wiki/Trusted_Computing

[39] Jericho Forum, “Position Paper: Architecture for Deperimeterisation”, ver 1.0, April 2006.
http://www.opengroup.org/jericho/Architecture_v1.0.pdf

[40] Network World, “The future of network security”, David Lacey, 31 January 2008.
http://www.networkworld.com/columnists/2008/013008-jericho-network-security.html

Annex A

Risk Management Methodology (RMM)

The number of different risk management standards is aplenty. Examples include the NIST's Special Publication 800-30 (2002) "Risk Management Guide for Technology Systems" and the ISO 27005:2008 standard on Information Security Risk Management. In this Annex, a simple qualitative Risk Management Methodology (RMM) would be given and be used in this report. The flowchart depicting the processes in risk management is as shown in Figure A.1 below.

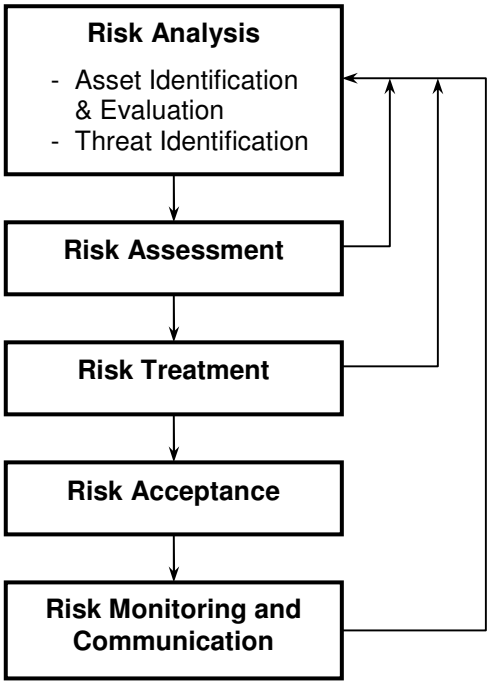


Figure A.1 Risk Management Process Flow

In *Risk Analysis*, Asset Identification & Valuation, Threat Identification and Vulnerability Identification would be carried out. Threats and Vulnerabilities would also be defined.

Risk Assessment involves using a methodology in evaluating risks. It encompasses Likelihood Analysis and Impact Analysis used to determine the Risk Levels of all the risks associated with the assets. Controls which are currently in

place and further controls if needed to reduce the Risk Levels would be recommended in the assessment report. Table A.1 below defines the severity of the risks identified based on their impact. Subsequently, the risk level will be determined from Table A.2 which is computed from the impact (or severity) and probability (or likelihood) of the threats to the assets.

Table A.1 Definition of Risk Severity[10]

Description of Risk Severity	**Severity**
The risk, once realized, will result in ■ Highly costly loss of major tangible assets or resources; ■ significantly violate, harm, or impede an organisation's mission, reputation, or interest; or ■ result in human death or serious injury.	*1*
The risk, once realized, will result in ■ Costly loss of major tangible assets or resources; ■ violate, harm, or impede an organisation's mission, reputation, or interest; or ■ result in human injury.	*2*
The risk, once realized, will result in ■ Loss of major tangible assets or resources; or ■ noticeably effect an organisation's mission, reputation, or interest.	*3*

Table A.2 Determination of Risk Level

	Risk Level		
Probability / **Severity**	*Low*	*Medium*	*High*
1	**C**	**B**	**A**
2	**D**	**C**	**B**
3	**E**	**D**	**C**

All the risks would be collated into a risk register which form part of the risk assessment report. The risk register and an example are shown in Table A.3 and Table A.4 respectively.

[10] Adopted from NIST SP 800-30 (2002).

Table A.3 Risk Register

S/N	Risk Statement	Consequences	Likelihood	Severity	Grade	Change Since Last Assessment	Mitigation Actions	Action Party	Status of Risk Mitigation Actions

Table A.4 Example of Risk Register

S/N	Risk Statement	Consequences	Likelihood	Severity	Grade	Change Since Last Assessment	Mitigation Actions	Action Party	Status of Risk Mitigation Actions
1	User introduces new requirements after Tender award	Financial, Project-specific (scope, schedule)	High	1	A	New	The project team will have to assess if the new requirements are critical to user operation. If yes, inform Vendor of the new changes via contact variation else put on hold as enhancement after the System is roll-out. Most importantly, change control pro	John Tan (Project Manager)	Open - Planned change control process to be formalized in the next steering committee meeting in Jan 07.
2	Delay by vendors to deliver the require solution to meet National Initiative timeline	Project specific (schedule)	Medium	1	B	Down	In the tender requirements, the timeline was explicitly mentioned with buffer of 1 month included. Also project manager is updating IDA on the initiative progress status. Will escalate when there is any possibility of critical path task delay.	John Tan (Project Manager)	Open - Continued closed monitoring.
3	No funding available to start initiative.	Project specific (financial)	Low	1	C	Unchanged	As this is a government wide initiative, hence it is likely to be approved. In addition, the various staff units will be informed early.	John Tan (Project Manager)	Close - Funding acquired for initiative.
4	No user champion / sponsor to take ownership of the project.	Project specific (user ownership)	Low	2	D	Unchanged	Get senior management to nominate user champion / sponsor. Also likely candidate to be Unit A. Hence will approach them to get them involved at onset of the project.	John Tan (Project Manager)	Close - User Sponsor and Champion is Unit A.
5	Insufficient PMT resource to support this initiative / project as there are other projects involved.	Project specific (resource)	High	2	B	Up	Inform PTD management on the resource and projects status that PMT is supporting. Compute FTE to justify resource consumption. Prioritize work / project assignments with management.	Mary Wong (Head PMT)	Open - Currently resources is holding up. Will continue to monitor closely.
6	Delay in tender award which will affect payment milestones especially FY closing.	Project specific (financial)	High	2	B	Up	Prepare in advance the necessary work tasks for tender evaluation and processing with the various staff units. Assign dedicated team member to work on tender evaluation and review tender evaluation task closely to aid team member when required.	John Tan (Project Manager)	Open - Tender to close on 9 Feb 07.
7	PMT staff retention especially when IT industry is doing well in general	Project specific (resource)	Medium	2	C	Unchanged	Develop teamwork within the team. Encourage project ownership and create an environment for all to learn. Constantly talk to team members.	John Tan (Project Manager)	Open - On-going.

The risk assessment report would be presented to the management for *Risk Treatment* where management decisions to accept, avoid, transfer or mitigate risks are made. Control actions to be taken to mitigate risks would be prioritized and thereafter implemented. Any residual risks would then be made known.

Risk Monitoring & Communication is about monitoring the risks that have been identified as well as measuring the effectiveness of the controls that are put in place. These steps are important not only in ensuring continuous improvement but also ensuring the integrity of the whole framework.

Appendix A

Project Description Form

Project Description Form

MSc Information Security

One copy of this form (or a typed or computer-generated version) is to be completed by each project student and sent (by email) to the project supervisor **by the end of the second semester at the latest**. If the project supervisor is satisfied with the contents then they should sign the form for their own records and inform the student. The student should keep a copy of the final project description form. If the project starts to deviate significantly from the originally approved proposal then the student should discuss this with the project supervisor and, if necessary, complete a revised form.

TO BE COMPLETED BY THE PROJECT CANDIDATE

Name: *Kwok Keong, LEE*

Contact email address(es): *kwokkeong.lee@gmail.com*

Provisional Title of Project: *Management of Risks associated with Deprimeterisation*

1. Statement of Objectives

a. What do you intend to achieve?

(1) To explain the concepts of deperimeterisation.

(2) To analyse the operational setup and environment of a law enforcement agency and carry out risk analysis in its facing of the issues with deperimeterisation.

(3) To propose practical solutions to manage the risks associated with deperimeterisation.

b. Why have you chosen the proposed project?

After attending a seminar on Deperimeterisation, it has become clear to the author that deperimeterisation is the current problem faced by all organisations. The problem is especially acute in the author's organisation (which is a law enforcement agency) where there exists sensitive data is to be kept confidential. The author's interest in the topic has greatly increased and it is hoped that some practical solutions (such as segregation of duties, clear policies, access rights to folders, workaround solutions using existing software, etc) could be proposed to help the organisation to manage the risks faced with Deperimeterisation.

2. Methods to be used

a. How do you intend to achieve the objectives listed above?

Here are basically the various sections of the project:

(1) Introduction

- this would be the introduction to the project

(2) Deperimeterisation

- this section will cover the literature review and detail concepts of deprimeterisation which include the background, the 15 commandments and the discussion/arguments on the topic

(3) Operational setup and working environment of the Law Enforcement Agency

- in this section, the general operational setup and working environment of a Law Enforcement Agency would be defined

(4) Risk Analysis

- a detailed risk analysis (by adopting an existing risk management methology) with respect to the problems faced with deprimeterisation will be carried out in this section
- if necessary, the author would seek assistance from his organisation to better understand the existing safeguards/controls that are put in place

(5) Recommended Solutions

- the recommend solutions to manage risks associated to deperimeterisation will be given
- if necessary, the author would seek assistance from his organisation to see how improvement could be made and further safeguards/controls could be put in place

(6) Conclusions

- this would be the conclusions of the project

b. What is your strategy for getting started?

To carry out a Literature Review and gain as much knowledge as possible on the concepts of Deprimeterisation. The available resources include mainly the Internet, Journals and past MSc project reports.

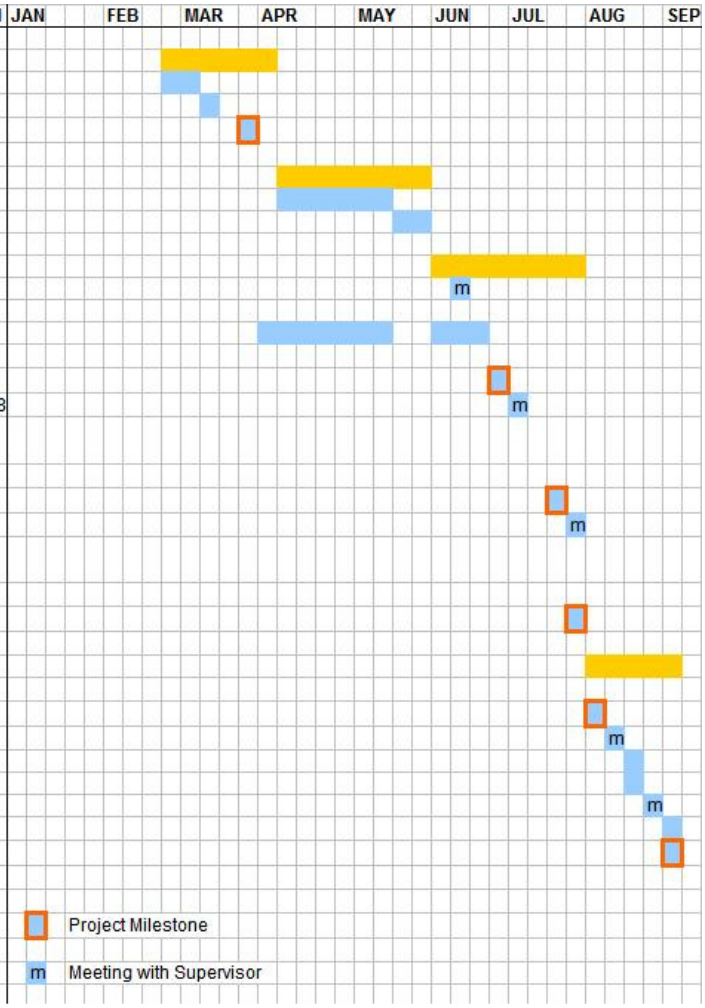
Then on, start to analyse the author's organisation and define its structure, operations, etc. Help would be solicited from the author's organisation, if necessary.

Following that, the author would proceed to carry out risk analysis and finally recommend solutions to manage the risks.

3. The work plan

Provide a rough schedule, showing any key milestones in the project.

S/N	TASK	DURATION
1	Project Plan	
	Prepare Project Description Form	
	Submit Project Description Form	06 Mar 08
	Finalise Project Description Form	20 Mar 08
2	Examination	
	Exam Study	
	Exam Period	
3	Project	
	Meeting with Supervisor (project kickoff)	Jun 08
	Literature review	
	Submission of Progress Report 1	27 Jun 08
	Meeting with Supervisor (Progress Report 1)	early Jul 08
	- update on Literature Review on Deprimeterisation and Defining of organisation	
	Submission of Progress Report 2	25 Jul 08
	Meeting with Supervisor (Progress Report 2)	end Jul 08
	- update on Risk Analysis and Recommended solutions	
	Completion of Project	
4	Project Report	
	Project Report writing	
	Submission of 1st Draft Report	08 Aug 08
	Meeting with Supervisor	
	Report amendment	1 week
	Submission of 2nd Draft Report	22 Aug 08
	Meeting with Supervisor	
	Report amendment	1 week
	Submission of Final Report	05 Sep 08



4. Additional comments

Use this section to make extra comments on the proposal on matters not covered above (use extra space if necessary). Include details of any involvement of external organisations.

The scope of the project would only involve the administrative systems of the law enforcement agency and would not include the operational and intelligence systems. Hence, the results of this project could possibly be also applicable to other organisations that uses IT in their day-to-day operations.

Where necessary, the author would solicit advices and help from the author's organisation which is a law enforcement agency.

TO BE COMPLETED BY THE PROJECT SUPERVISOR

I approve the attached project plan.

Signed :

Name : *Peter Wild*

Date : *6 Mar 2008*