

# How to help law enforcement live in a world without secure boundaries

Security perimeters have become increasingly porous with the rise of mobile technology, the Internet and increased outsourcing. **Kwok Keong Lee** and **Peter Wild** explain how a law enforcement organisation can exploit the benefits of de-perimeterisation without damaging the security of its assets.



[HOME](#)

[ERODING THE NETWORK PERIMETER](#)

[JERICHO FORUM COMMANDMENTS](#)

[ASSETS IN LAW ENFORCEMENT](#)

[THREATS AND COUNTER-MEASURES](#)

[RISK REGISTER](#)

[RECOMMENDATIONS](#)

[CONCLUSIONS](#)

[SOURCES](#)

**D**E-PERIMETERISATION (D-P) is a term introduced by the Jericho Forum<sup>1</sup> which started as informal meetings of a group of global corporate Chief Information Security Officers (CISOs) in 2003. De-perimeterisation is basically used to describe the gradual erosion of the network perimeter, which is the current means to provide strong protection to 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 are changing business models, driven by cost-savings, which encourage access for remote users, outsourcing and partnership. D-P itself brings many threats such as loss of sensitive information and malicious insiders. In this article we examine some issues associated with D-P and how the risks it brings may be managed.

A Law Enforcement Agency (LEA) is a government body which is responsible for maintaining law and order in a nation. An LEA exercises much of its authority through its duties to ensure public safety and security. Although such an organiza-

tion is given special powers, as we will see in this report, it is not spared from the effects of de-perimeterisation. In this study, the threats that D-P brings to an LEA are analysed and recommendations to mitigate the risks are proposed.

## DE-PERIMETERISATION DEMYSTIFIED

The Jericho 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. The purpose of this endeavour is to allow secure and cost-effective business collaboration through the use of the Internet. For two organisations to work together they must communicate with one another across the perimeters of their respective internal networks. This is often achieved by using Web applications and the Internet. De-perimeterisation refers to the erosion of the network perimeter (formed using routers, firewalls and other network equipment) of an organization. According to the Jericho Forum, the erosion of the perimeter is driven by three main factors<sup>2</sup>:

[HOME](#)

[ERODING  
THE NETWORK  
PERIMETER](#)

[JERICHO  
FORUM COM-  
MANDMENTS](#)

[ASSETS IN LAW  
ENFORCEMENT](#)

[THREATS AND  
COUNTER-  
MEASURES](#)

[RISK REGISTER](#)

[RECOMMEN-  
DATIONS](#)

[CONCLUSIONS](#)

[SOURCES](#)

- The existence of security exploits using delivery mechanisms (such as email and Web applications) 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 content is embedded into emails and Web application data, the content basically goes straight through the perimeter, into the internal network of the organisation.
- Vendors (with products that need to communicate across the border) encapsulating their protocols within the Web protocols. In this way, these products would effectively bypass the screening done by firewalls and this would allow 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 on businesses, needing to trade using the Internet and being restricted by their corporate perimeter, that lead them either to punch (further) holes in that perimeter and/or to bypass the perimeter completely.

The approach to take in face of de-perimeterisation as proposed by the Jericho Forum suggests that traditional security solutions, including firewalls and a maintenance of “defence in depth”, will continue to play a vital role, but there is a

*“Ultimately, in a fully de-perimeterised network, every component will be independently secure, requiring systems and data protection on multiple levels.”*

need to remain alert to how they are affected by new challenges, and, in particular, to 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, and data-level authentication.

[HOME](#)[ERODING  
THE NETWORK  
PERIMETER](#)[JERICHO  
FORUM COM-  
MANDMENTS](#)[ASSETS IN LAW  
ENFORCEMENT](#)[THREATS AND  
COUNTER-  
MEASURES](#)[RISK REGISTER](#)[RECOMMEN-  
DATIONS](#)[CONCLUSIONS](#)[SOURCES](#)

In order to encourage businesses to consider a de-perimeterised security architecture and to explain how this can be securely developed, a number of position papers have been published by the Forum. It has also published the Jericho Forum Commandments (JFCs) which are based on “good security” and 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<sup>3</sup>:

#### **FUNDAMENTALS**

1. The scope and level of protection should be specific & appropriate to the asset at risk.
2. Security mechanisms must be pervasive, simple, scalable & easy to manage.
3. Assume context at your peril.

#### **SURVIVING IN A HOSTILE WORLD**

4. Devices and applications must communicate using open, secure protocols.
5. All devices must be capable of maintaining their security policy on an untrusted network.

#### **THE NEED FOR TRUST**

6. All people, processes, technology must have declared and transparent levels of trust for

any transaction to take place.

7. Mutual trust assurance levels must be determinable.

#### **IDENTITY, MANAGEMENT AND FEDERATION**

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

#### **ACCESS TO DATA**

9. Access to data should be controlled by security attributes of the data itself.
10. Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges.
11. By default, data must be appropriately secured when stored, in transit, and in use.

Even though there are still critics of, and scepticism about, de-perimeterisation, the Jericho Forum has achieved its initial objectives in defining the problem and raising awareness through publications, press releases, conferences and other forms of dissemination. Moving on, it is hoped that more solutions will be developed that take into account the D-P issue and also that more involvement will be seen from business consumers in adopting the solutions.

[HOME](#)

[ERODING  
THE NETWORK  
PERIMETER](#)

[JERICHO  
FORUM COM-  
MANDMENTS](#)

[ASSETS IN LAW  
ENFORCEMENT](#)

[THREATS AND  
COUNTER-  
MEASURES](#)

[RISK REGISTER](#)

[RECOMMEN-  
DATIONS](#)

[CONCLUSIONS](#)

[SOURCES](#)

**A LAW ENFORCEMENT AGENCY**

As mentioned, changes in business models have lead to outsourcing, resulting in the need to cater for outsiders to access an organisation’s internal network. This eventually leads to de-perimeter-

sation and applies even to public agencies, such as law enforcement agencies. 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 on the organisation in maintaining a team of specialists to manage such systems as IT (information technology). In a typical LEA, the obvious players are the organisation’s top-management (the Commissioner, Commanders, Directors and Deputy Directors) and the policemen. However, for a 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. Hence, as compiled in Table 1 below, there are more players in an LEA than just the uniformed officers.

The assets of a police force are plentiful, ranging from weapons, vehicles and buildings to radio communication sets, and from computer servers, data centres, desktops and laptops to sensitive data such as criminal records. They even include reputation, which is an intangible, but nevertheless very important, asset to an LEA. Some of these assets are listed in **TABLE 1**.

**TABLE 1**

**THE PLAYERS AND ASSETS IN A LAW ENFORCEMENT AGENCY**

PLAYERS	ASSETS
Top Management	Laptops
Police Officers	Sensitive Data
Middle Management	Vehicles
Associates	Buildings
Outsourced Vendors	Applications
Project Officers	Data Centres
Data Centre Staff	Servers
Security Guards	Desktops
The Public	
Users	

[HOME](#)

[ERODING THE NETWORK PERIMETER](#)

[JERICHO FORUM COMMANDMENTS](#)

[ASSETS IN LAW ENFORCEMENT](#)

[THREATS AND COUNTER-MEASURES](#)

[RISK REGISTER](#)

[RECOMMENDATIONS](#)

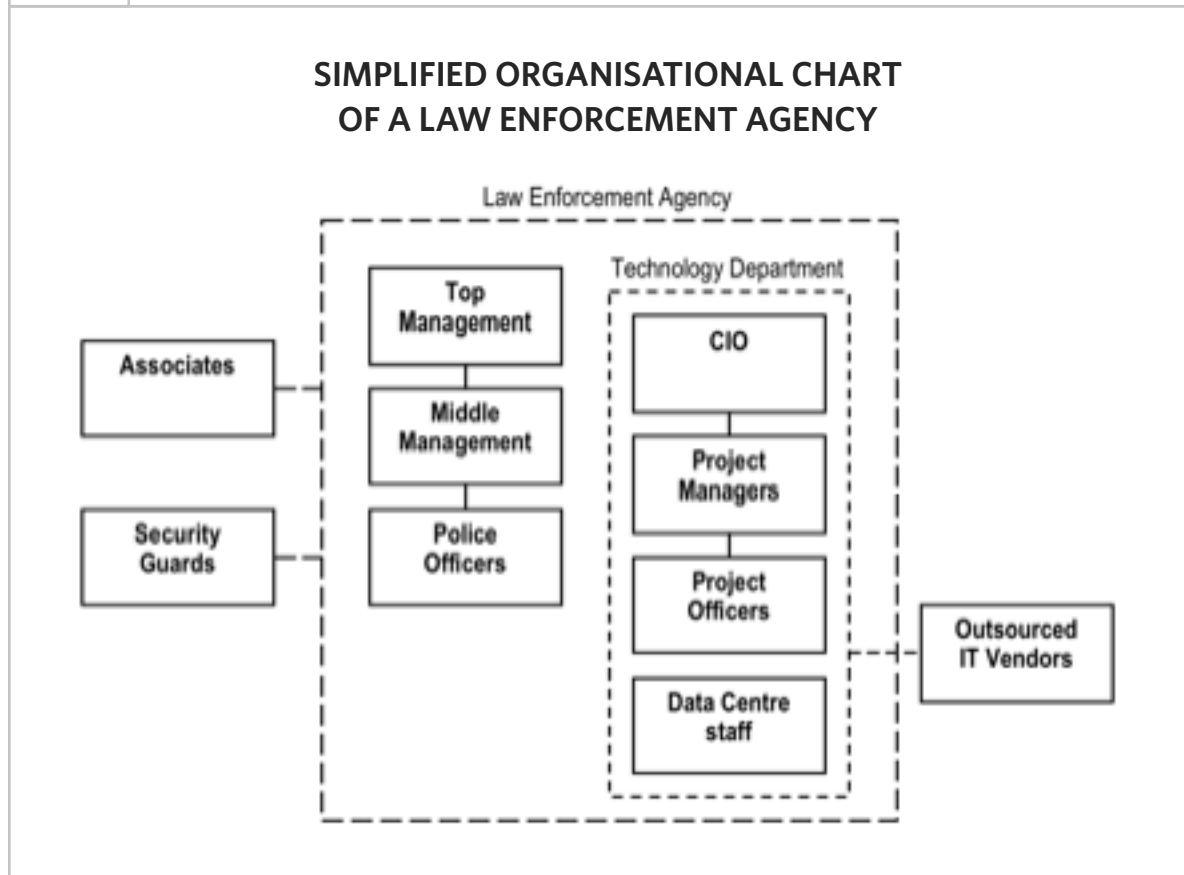
[CONCLUSIONS](#)

[SOURCES](#)

Bringing the players and their relationships together, a simplified organisational structure is given in **FIGURE 1**. As can be seen, the Technology Department is part of the agency and is lead by the CIO along with its Project Managers and Offi-

cers. This department has some data centre staff under its purview and also has to manage the outsourced IT vendors. There are also Associates and Security Guards which are considered to be outside the organisation.

FIGURE 1



**RISK ANALYSIS**

Given the threats arising from de-perimeterisation it is important for any organisation that the resultant risks are analysed and managed appropriately. Risk Management Methodology (RMM) involves carrying out *Risk Analysis, Risk Assessment, Risk Treatment, Risk Acceptance and Risk Monitoring and Communication*. Within the scope of this study, only the Risk Analysis and Risk Assessment steps have been carried out. The analysis and assessment is focused

[HOME](#)

[ERODING THE NETWORK PERIMETER](#)

[JERICHO FORUM COMMANDMENTS](#)

[ASSETS IN LAW ENFORCEMENT](#)

[THREATS AND COUNTER-MEASURES](#)

[RISK REGISTER](#)

[RECOMMENDATIONS](#)

[CONCLUSIONS](#)

[SOURCES](#)

on the risks brought about in a de-perimeterised environment for a law enforcement agency. The outcome of this exercise is the Risk Register which allows recommendations for dealing with the risks to be formulated.

*“National safety and security could be affected, possibly resulting in the loss of lives.”*

Based on an understanding of the effects of both de-perimeterisation and the organisation of an LEA, the likely attackers, the threats that the attackers bring as well as the countermeasures against the threats may be identified and these are given in **TABLE 2** (page 8). The Risk Register is compiled in **TABLE 3** (page 9).

We observe from Table 3 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. At the moment, laptops are considered the most vulnerable of all mobile devices. Not only are laptops lost in private organisations but also the loss

of laptops has occurred in government organisations. There have been recent cases of such loss in the FBI and the UK government<sup>7</sup>. It is certainly possible for it to occur in an LEA. In an LEA, where laptops often are used to store confidential information or are deployed for operations, the impact of the loss of a laptop would certainly be severe. In the worst case scenario, national safety and security could be affected, possibly resulting in the loss of lives.

Along with laptops (which are at high risk) other vulnerable assets are mobile devices such as Personal Digital Assistants (PDAs) and mobile phones. The vulnerability of the devices as physical assets liable to be stolen is itself a risk. The threat of mobile devices being exploited, resulting in the loss of sensitive information stored on them, means that special attention has to be given to these.

Another high risk area is that of insider attacks. Insiders include contractors, cleaners, security guards, associates and others who have some special relationship with the organisation. Insiders may be able to do much harm to the organisation due to the privileged access that they have and, therefore, measures have to be put in place to minimise the risks that they pose.

*(Continued on page 10)*

[HOME](#)

[ERODING  
THE NETWORK  
PERIMETER](#)

[JERICHO  
FORUM COM-  
MANDMENTS](#)

[ASSETS IN LAW  
ENFORCEMENT](#)

[THREATS AND  
COUNTER-  
MEASURES](#)

[RISK REGISTER](#)

[RECOMMEN-  
DATIONS](#)

[CONCLUSIONS](#)

[SOURCES](#)

TABLE 2

**THE ATTACKERS, THREATS AND COUNTERMEASURES FOR A LAW ENFORCEMENT AGENCY**

ATTACKERS	THREATS	COUNTERMEASURES
Malicious insiders Hackers Malware	Loss of laptop	<ul style="list-style-type: none"> <li>■ Encryption of laptop data</li> <li>■ Laptop hardening</li> <li>■ Data backup</li> </ul>
	Loss of sensitive information	<ul style="list-style-type: none"> <li>■ Data encryption</li> <li>■ Access control to data</li> <li>■ Control of data storage devices</li> </ul>
	Attacks on Internet website	<ul style="list-style-type: none"> <li>■ Hardening of servers</li> <li>■ Response and contingency plan</li> <li>■ Data Backup</li> </ul>
	Firewall compromised	<ul style="list-style-type: none"> <li>■ Redundancy and high availability firewall</li> <li>■ Proper maintenance</li> <li>■ Backup recovery site</li> </ul>
	Vulnerabilities of mobile devices	<ul style="list-style-type: none"> <li>■ Securing mobile devices</li> <li>■ Policies on use of mobile devices</li> </ul>
	Insider attacks	<ul style="list-style-type: none"> <li>■ Security clearance</li> <li>■ Separation of duties / Principle of least privilege</li> <li>■ Deployment and active monitoring of IDS</li> </ul>
	Malware	<ul style="list-style-type: none"> <li>■ Hardening of servers, desktops and laptops</li> <li>■ Secure coding practises</li> <li>■ Deployment and active monitoring of IDS</li> </ul>

[HOME](#)

[ERODING THE NETWORK PERIMETER](#)

[JERICHO FORUM COM-MANDMENTS](#)

[ASSETS IN LAW ENFORCEMENT](#)

[THREATS AND COUNTER-MEASURES](#)

[RISK REGISTER](#)

[RECOMMEN-DATIONS](#)

[CONCLUSIONS](#)

[SOURCES](#)

TABLE 3

THE RISK REGISTER FOR A LAW ENFORCEMENT AGENCY

MS/N	RISK STATEMENT	POSSIBLE CONSEQUENCES	LIKELIHOOD <sup>4</sup>	SEVERITY <sup>5</sup>	GRADE <sup>6</sup>	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 and 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
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

[HOME](#)

[ERODING THE NETWORK PERIMETER](#)

[JERICHO FORUM COMMANDMENTS](#)

[ASSETS IN LAW ENFORCEMENT](#)

[THREATS AND COUNTER-MEASURES](#)

[RISK REGISTER](#)

[RECOMMENDATIONS](#)

[CONCLUSIONS](#)

[SOURCES](#)

(Continued from page 7)

## RECOMMENDATIONS

Recommendations based on the results of the risk analysis undertaken, taking into account the current environment of the IT industry, are given in [TABLE 4](#).

These recommendations are categorised as short-term, mid-term and long-term. Short-term

**TABLE 4**

### RECOMMENDATIONS FOR A LAW ENFORCEMENT AGENCY RELATED TO DE-PERIMETERISATION

#### SHORT-TERM

- Securing of mobile devices
- Vulnerability management
- Reviewing and tightening controls on insiders
- Strengthening security awareness and training

#### MID-TERM

- Adoption of Web Services
- Work towards Single Sign On (SSO)

#### LONG-TERM

- Identity and Trust Management
- Trusted Computing

recommendations are those that should be carried out immediately and could be achieved within 1 year or so. The implementation of the short-term recommendations should mitigate to a large extent 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 the mid-term recommendations in good time. 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 monitor the development of technologies in these areas within a 4 to 5 year time frame.

We see that all the short-term recommendations (securing mobile devices, vulnerability management, reviewing and tightening controls on insiders and strengthening security awareness and training) are important for adoption by the LEA as a quick-fix solution in face of de-perimeterisation. Securing mobile devices is very important and this has to be stressed even more so for an LEA which deploys mobile devices for its remote workers and for use during operations in

[HOME](#)

[ERODING THE NETWORK PERIMETER](#)

[JERICHO FORUM COMMANDMENTS](#)

[ASSETS IN LAW ENFORCEMENT](#)

[THREATS AND COUNTER-MEASURES](#)

[RISK REGISTER](#)

[RECOMMENDATIONS](#)

[CONCLUSIONS](#)

[SOURCES](#)

the field, as these devices are likely to contain sensitive information. So, countermeasures such as data encryption, device hardening and others should be fully implemented to avoid the loss of mobile devices, the loss of sensitive information and the likely embarrassment to the LEA.

Vulnerability management would help an LEA in the same way as it does other organisations. If done properly, it would help the LEA to keep track of the threats against its assets – not only IT assets but also other assets such as weapons, vehicles and buildings. Preventing and deterring possible malicious insiders are well established practices for an LEA. With de-perimeterisation, an LEA should continue these practices, but it should also review, and possibly step-up, the controls on insiders in order to eliminate any possible oversights.

An LEA is in the business of security but it should never be over-complacent in managing security nor take security for granted. Security awareness and training should always be emphasized so that a security culture can be developed for new and existing employees in the LEA.

The core function of an LEA is to fight crime. It is not the development of IT solutions. It is a user of technology and as a user, the LEA should state what it wants, dictating its requirements to ven-

dors for solutions to be deployed in the LEA. Hence, with respect to the mid-term recommendations, the LEA should insist on Web Services and Single Sign On solutions from its vendors, supporting their application development. As both technologies are aligned to Jericho Commandments such as flexibility (JFC#1), scalability (JFC#2) and a federated identity management (JFC#8), their adoption would automatically gear the LEA towards preparing itself for, and seamlessly integrating with, de-perimeterised solutions in the near future.

As for the long-term recommendations, it is not quite as essential for the LEA to follow their progress so closely. As a user of technology, an LEA is very much dependent on its vendors to provide the solutions that will meet its requirements. Technology is developing very quickly and there is much uncertainty about how some technologies will advance in the future. Furthermore, an LEA would most likely be part of the overall IT security plan or program of the government; the IT security program being lead by the appropriate authority in the government that handles ICT developments. Nevertheless, the LEA should at least keep itself up to date on the latest news of developments concerning D-P and make its requirements known.

[HOME](#)[ERODING  
THE NETWORK  
PERIMETER](#)[JERICHO  
FORUM COM-  
MANDMENTS](#)[ASSETS IN LAW  
ENFORCEMENT](#)[THREATS AND  
COUNTER-  
MEASURES](#)[RISK REGISTER](#)[RECOMMEN-  
DATIONS](#)[CONCLUSIONS](#)[SOURCES](#)

## CONCLUSIONS

The issues that de-perimeterisation brings are real and it is happening right now in organisations all over the world.

De-perimeterisation came about basically due to the highly inter-connected networks we have today which have encouraged a rapid growth of mobile workers, driven by 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 have started to punch “holes” through the firewalls that define the traditional network perimeter. As a consequence, the firewalls are weakened and the network perimeter has now become “porous”; thus the term “de-perimeterisation” has arisen. 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 an attacker who tries to compromise the weakened firewall in a de-perimeterised organisation. Following an analysis of the threats, it can be concluded that vulnerabilities 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 can be made commercially available and be widely adopted at the enterprise level. Among the hurdles are things like data-level authentication which requires effective administration of a massive amount of data, and identity and trust management on a global scale which requires a coordinated international effort. While waiting for that to happen, organisations must do something to mitigate the risks. The recommendations given in this report are specifically aimed at this. Firstly, short-term recommendations are

[HOME](#)

[ERODING  
THE NETWORK  
PERIMETER](#)

[JERICHO  
FORUM COM-  
MANDMENTS](#)

[ASSETS IN LAW  
ENFORCEMENT](#)

[THREATS AND  
COUNTER-  
MEASURES](#)

[RISK REGISTER](#)

[RECOMMEN-  
DATIONS](#)

[CONCLUSIONS](#)

[SOURCES](#)

intended to mitigate the most serious D-P threats that currently exist in organisations. These recommendations include the securing of mobile devices and the implementation of vulnerability management. The objective of the mid-term recommendations is to mould the IT environment of the organisation into an open, scalable and interoperable architecture so 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 and Trust Management and Trusted Computing are two such areas that have been identified. We have noted that the 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 of immediate concern to the LEA at this moment. However, the LEA should keep itself informed about the latest developments.

### DIFFERENCES BETWEEN AN LEA AND A PRIVATE

**ORGANISATION:** It is appropriate here to mention the differences between an LEA and a private organisation in the face of de-perimeterisation. In fact, there are not many differences from an IT perspective. An LEA is very much like a multinational corporation which has 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. An LEA, like a private organisation, is also constantly seeking better cooperation and partnership 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 an LEA.

However, the two entities differ in some subtle areas. Firstly, with respect to 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 is also different for the two organisations. A hacker is more likely to attack a private organisation for money while an attack on an LEA may be due to an emotional hatred. Reputation is comparatively more important for an LEA than a private organi-

[HOME](#)[ERODING  
THE NETWORK  
PERIMETER](#)[JERICHO  
FORUM COM-  
MANDMENTS](#)[ASSETS IN LAW  
ENFORCEMENT](#)[THREATS AND  
COUNTER-  
MEASURES](#)[RISK REGISTER](#)[RECOMMEN-  
DATIONS](#)[CONCLUSIONS](#)[SOURCES](#)

sation as the loss of reputation would potentially cause a total distrust in the public order system which may result in a chaotic society. In the face of de-perimeterisation, an LEA also has a greater responsibility in terms of protecting data because the consequences of leakage of sensitive information could be more serious. For a private organisation an attack would probably result in a loss of profit, whereas, for an LEA, an attack could affect public safety and security, and possibly could lead to the loss of lives.

**FINAL REMARKS:** De-perimeterisation involves a paradigm shift in the way security professionals view the network security of organisations. De-perimeterisation affects both an LEA and a private organisation. This report emphasises that organisations have to carry out risk management processes to confront the threats that de-perimeterisation brings. While existing security solutions still work, it will not be long before organisations who do not prepare for de-perimeterisation find themselves caught off-guard and need to carry out a costly and disruptive overhaul of their whole network architecture. In order to fully embrace de-perimeterisation, there is a need to make changes now to eliminate the problems of the future. ■

## ABOUT THE AUTHORS

***Kwok Keong Lee** works in technical support for the Singapore government's law enforcement agency. After completing his MSc at Royal Holloway, he will soon become leader of the organisation's information security team.*

***Prof. Peter Wild** is a professor of information security at Royal Holloway, University of London, and the director of the information security group. He coordinates the course in Security Management on the MSc in Information Security at Royal Holloway.*

[HOME](#)

[ERODING  
THE NETWORK  
PERIMETER](#)

[JERICHO  
FORUM COM-  
MANDMENTS](#)

[ASSETS IN LAW  
ENFORCEMENT](#)

[THREATS AND  
COUNTER-  
MEASURES](#)

[RISK REGISTER](#)

[RECOMMEN-  
DATIONS](#)

[CONCLUSIONS](#)

[SOURCES](#)

**SOURCES:**

<sup>1</sup> [Jericho Forum](#)

<sup>2</sup> [Jericho Forum's FAQ](#)

<sup>3</sup> [Jericho Forum Commandments](#)

<sup>4</sup> "Likelihood" is classified into 'Low', 'Medium' and 'High' where 'Low' represents a low probability of occurrence for a risk while 'High' represents a high probability of occurrence.

<sup>5</sup> "Severity" is given a rating of '1' to '3' where '1' represents that a risk has the highest impact while '3' represents a minimal impact.

<sup>6</sup> "Grade" provides the "Risk Level" of a risk and is computed from "Likelihood" and "Severity".

<sup>7</sup> BBC, "Defence minister's laptop stolen", 4 June 2000; BBC, "[Defence minister's laptop stolen](#)", 4 June 2000; "MoD loses 600 laptops", BBC News, 13 January 2002; "[The Federal Bureau Of Investigation's Control Over Weapons And Laptop Computers Follow-Up Audit](#)" report, February 2007, Pg iv.

[HOME](#)

[ERODING  
THE NETWORK  
PERIMETER](#)

[JERICHO  
FORUM COM-  
MANDMENTS](#)

[ASSETS IN LAW  
ENFORCEMENT](#)

[THREATS AND  
COUNTER-  
MEASURES](#)

[RISK REGISTER](#)

[RECOMMEN-  
DATIONS](#)

[CONCLUSIONS](#)

[SOURCES](#)