MSIS PROJECT

“THE SECURITY CASE FOR “DE-PERIMETERISATION & HARDENING THE HOST” – THE JERICHO MODEL”

BY GARY A BANNISTER

ABSTRACT

“De-perimeterisation is about moving the security emphasis from the edge of a network and onto individual devices, (hardening the host) and ultimately to individually encrypted data packets. It is about re-appraising where security controls are positioned, and about simplifying and reducing the cost of doing information security”. (Jericho White Paper Feb 2005)

This paper makes the ‘Jericho Case’, by examining the “commandments, vision, mission and detailed proposals of Jericho; it outlines how it can be done and compares this to a Fortune 100 company implementation, (a Case Study) to see where they are in the journey, how close they come to meeting the Jericho vision and its commandments, the gaps, and most importantly the strategies and value proposition as they move down this path.

This paper will also include some of the challenges and issues, as not everyone in the industry accepts all of the Jericho proposals.

There are basically two strategies to implementing Jericho:

- ❖ Removing old fashioned perimeters by partitioning networks based on critical digital assets, using encryption and secure tunneling, implementing standardized security monitoring and reporting, introducing more modern virtual technology to reduce the number of physical servers and more sophisticated vulnerability and intrusion detection.
- ❖ Externalizing desktops and applications by hardening the security within each.

This is somewhat an oversimplification as there are many new technology proposals being put forward by Jericho to further their vision, however it helps to simplify as it makes it easier to examine the fortune 100 manufacturing company selected.

CONTENTS

LIST OF DIAGRAMS

LIST OF TABLES

INTRODUCTION

Early in 2004 a group of ‘like-minded’ CISO’s (IT security VP’s) led by BP (British Petroleum), ICI, Standard Chartered Bank and the Royal Mail (British Post Office) met to discuss their strong, controversial views about the future of Digital Security and how they could promote their views and get collaboration from companies and vendors to accept their proposition. From this initial meeting, the Jericho Forum was formed in April 2004. The appendix shows the list of current members. (Please note that this list is fluid, changes often, and includes vendors who are allowed to be members but ‘observer members’ only except if they are companies in their own right like IBM).

“Jericho proposes that the current Information and Security Technology (ICT) and the way security is organized as a series of walls or layers around an organization’s private network perimeters and boundaries will need to change radically.” (Jericho Forum White Paper Feb 2005)

“Maintaining Information security at the boundaries of an organization have become unworkable, due to a mobile workforce, internet interaction between suppliers, customers, contractors, outsource partners and the various government bodies that organizations must deal with”.(Jericho Forum White Paper Feb 2005)

It has also become costly to maintain the old way of doing security and difficult to protect against some of the biggest threats companies face “internal abuse, errors, and fraud”. (CSI/FBI Surveys)

“De-perimeterisation is about moving the security emphasis from the edge of a network and onto individual devices, (hardening the host) and ultimately to individually encrypted data packets. It is about re-appraising where security controls are positioned, and about simplifying and reducing the cost of doing information security”.

This may involve moving security controls from firewalls or proxies to internal end systems or applications, or if confidentiality or data integrity is an issue, moving from data repositories and systems that store ‘data at rest’ to the data itself using cryptographic techniques.

This paper makes the ‘Jericho Case’, by examining the “commandments, vision, mission and detailed proposals of Jericho; it outlines how it can be done and compares this to a Fortune 100 company implementation, to see where they are in the journey, how close they come to meeting the Jericho vision and its commandments, the gaps, and most importantly the strategies and value proposition as they move down this path.

This paper will also include some of the challenges and issues, as not everyone in the industry accepts all of the Jericho proposals.

The Jericho Model Explained

This section sets out the model for Jericho, its vision, mission statements, its themes and proposed work groups or strands of work and research and most importantly, its commandments.

Vision & Mission

The vision statement produced by Jericho (Jericho Forum White Paper Feb 2005) states the following:

“To enable business confidence for collaboration and commerce beyond the constraint of the corporate, government, academic and home office perimeter, principally:-

- Cross-organizational security processes and services
- Information and Telecommunication products that conform to ‘open security standards’
- Assurance processes that when used in one organization can be ‘trusted’ by others. “

The Mission statement (Jericho Forum White Paper Feb 2005) says that Jericho must act as the ‘catalyst’ to accelerate the achievement of the collective vision, by:

- Defining the problem space
- Communicating the collective vision
- Challenging constraints and creating an environment for innovation
- Demonstrating market value
- Influencing future products and standards.

Themes and Work groups

Jericho has a 5 year time table. Many of the members feel that this is too optimistic and aggressive given how difficult it is to standardize, and how security technology is still geared to the old model, but most importantly, businesses, especially large businesses even with big budgets, cannot change so quickly.

There are four basic themes:-

- Enabling Adoption

To assist and enable organizations with changes especially:-

a. Governance issues

How should organizations prepare for de-perimeterisation including how they operate with other organizations?

b. Strategic Contexts

Understanding the relevant business requirements and drivers, in particular how they can turn these requirements into solution designs.

c. Business Frameworks

A common language, to be able to express de-perimeterisation goals, policies, and solutions. Included here would be governance frameworks like COBiT.

d. Security frameworks

Use of ISO 17799 or BS7799 would help to define the security requirements in a standard way but more specifically industry standards and common principles around technology.

e. Design frameworks

A standard way of addressing security architecture and design holistically for all of the ICT elements required.

f. Implementation & Operation

Assisting with the definition of roles and responsibilities, but this would fall out of the COBiT framework above.

- Developing Security Principles & Standards

Jericho will act as the catalyst for de-perimeterisation by leading the convergence, endorsement at optimum cost and effectiveness so that ICT solution suppliers can be confident of an open commercial market for Jericho Forum standards-conformant products. Jericho feels that many of the existing security standards are poorly specified, ambiguous and difficult to validate and understand by the business users.

- Building Consensus

Jericho will work from a practical basis and involve as many standard bodies, suppliers, academia and service providers to ensure that its security principles and standards are technically well founded and sponsor the appropriate research where required.

- Fostering community

Jericho will act as a peer group for sharing security knowledge and experience, continuing to develop a network of people that can find answers to questions and answers within its scope. Jericho is a volunteer organization, as such depends on its members to do the work. With this in mind, it was agreed to form five (5) work groups who would be responsible for research and development, reporting back frequently with 'position papers' and working with security technology vendors on the way forward. The following Chart shows an overview of the five groups their responsibilities and the scenarios developed for each of them:

Scenario	1) Meta Architecture	Requirements /Ontology	Technology & Solutions	Trust Models	Management & Monitoring
Wireless & Public network access			X		
Domain inter-working via open networks			X		X
Phoning from hostile environment			X		
Enable portability of identities and data	X	X	X	X	
Suppliers access to applications			X		
Outsourced help desk			X		X
XML messaging for connecting organizations	X		X	X	
Consolidate IAM	X		X	X	X
Automate policy for controlled information sharing	X	X		X	
Harmonize identities & trust relationships	X	X		X	

Table 1 – Jericho Business Scenarios to Work groups. (White Paper-Feb 2005)

In terms of scope, Jericho will NOT endeavor to develop technology, they will research and propose the "how" to do it and collaborate with organizations, academia and vendors to develop the appropriate standards, policies, technologies to achieve its goals and mission. In the table above the work groups are on the horizontal access:-

Work Group 1 – Meta-Architecture.

This work group will define the principles and technical direction that define the de-perimeterisation approach. Two choices for organizations adopting the Jericho principles, either the adoption of its enterprise ICT architecture or just software architecture for a single system or application. They will define how de-perimeterisation affects applications/systems and their constituent parts by mapping the principles and standards they develop to each part. (See chapter 4 outlining the how we do it, an example of the systems would be portals, knowledge management systems, trading support)

They will work with the other working groups to identify any business scenarios that can have a wide architectural impact.

Work Group 2 – Requirements/Ontology

This area concerns the broad spectrum of security and policy for collaboration and commerce between and within organizations. (For example many may be supported in the Semantic Web).

1. The Semantic web is a linked information support structure spanning many organizations, with multiple information sources which pose potential privacy and security concerns.

2. In particular this work group will specifically focus on data and information classification rules; web based commercial processes and trust, threat and risk models.

Work Group 3 – Technology and Solutions

1. This work group will focus on the practical security solutions and technology to meet de-perimeterisation. To do this it must keep abreast of technology and work with key vendors and in particular the other work groups.

2. The scope of the technologies will include ID management, remote access and private networking, 'Trusted platform' (digital rights management) technologies, protocols and formats, cryptographic support and key management systems and application programming and device interfaces.

3. Jericho will 'not endorse' any particular technology or product. Vendor members will be encouraged to demonstrate their product operations and solutions in terms of meeting the Jericho model.

Work Group 4 – Trust Models

De-perimeterisation requires 'trust' between the business parties both at individual levels and at system and infrastructure levels.

The main aim of this work group is to define the common frame of reference and consider a variety of 'trust models' that will be required for collaboration and commerce.

It will develop a 'standard template' that organizations can use to evaluate when designing services and formulating contracts and service agreements.

Specifically this work group will examine existing standards that support identity management and single sign on (IDM/SSO) with a view to supporting security control decisions associated with system or network access.

A critical factor in examining trust models is as Jericho says "the extent to which they can adjust when trust breaks down". With this in mind this work group will take into account notions of what is called 'dynamic trust', and what level of trust is appropriate.

Work Group 5 – Management and Monitoring

This work group will focus on how system management and monitoring tools can function securely over 'open networks'. Specifically they will look at remote management and monitoring systems, remote device and user management, Malicious software incident detection (IDS) and IDP), patch management and security status monitoring and problems and incident handling.

The "Commandments"

Ron Condon wrote in April 5th 2006 in the SC Magazine (SC April 2006 edition, "New Rules For Collaborative & mobile working) "When Moses came down from the mountain top, he carried just Ten Commandments for the guidance of mankind, but information security is a bit more complicated – we need eleven".

These comments were based on an early release of a draft proposal to introduce 11 security commandments to move towards de-perimeterisation. In December 2006, version 1.1 was published with still eleven but amended after comment from the membership. The eleven commandments are important to know and understand because it is a key driver in how organizations implement de-perimeterisation.

The author of the commandments is Nick Bleech CISO of Rolls Royce. His aim is to outline in broad terms the basics of good security in a de-perimeterised world. The 11 commandments are outlined below divided into 5 Principles:-

The Fundamentals {the security basics}.

1) The scope and level of protection should be specific & appropriate to the asset at risk.

- Individual systems must be capable of protecting themselves. It doesn't mean that firewalls are not important however, but in a de-perimeterised world the 'host must be hardened'.
- In addition solutions must be 'cost effective' and add value, it is not a question of change for change sake.

- Digital Assets must be managed and identified by their risk category; all assets and thus their protection are not created equally.
- Security mechanisms must be pervasive, simple, scalable and easy to manage.
- Too much complexity is a threat to good security.

2) **Security mechanisms must be scalable and easy to manage**.

- Security principles are required for all levels of the architecture.

3) **Assume Context at your peril.**

- Not all security designs are transferable form one environment to another. De-perimeterisation requires that whilst in is the 'ultimate goal', you cannot assume that what you are designing will work in another environment; companies must do the detail analysis.
- Problems can come from a variety of sources, you need to consider legal, geographic and cultural, and risk appetite.

Surviving in a Hostile World.

4) **Devices and applications must communicate their security policy on untrusted networks.**

- Security requirements should not be added on but be built into existing protocols. It should not be an 'after-thought'.
- Encryption does not solve everything and should be used only where appropriate.

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

- Any implementation must be capable of surviving on the raw internet.

Trust

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

- Trust is about the obligations on partners when exchanging transactions amongst themselves.
- It must be mutual and must encompass not only people and organizations, but devices and infrastructure. Levels of trust will vary by the risk of the digital asset.

7) Mutual trust assurance levels must be determinable.

- Devices must be capable of the appropriate levels of authentication for data and systems access.
- Authentication and authorization frameworks and protocols must support the trust model.

Identity Management and Federation.

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

- People must be able to manage user rights and permissions they don't control.
- Authentication must be possible without the need for creating separate identities.
- Systems must support multiple areas of control and be able to assert and pass on security credentials.

Access to Data

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

- Control attributes must be held within the data or by a separate system.
- Access and security could be implemented by encryption.
- If the appropriate data classification is used, some data may be “public and non confidential”.
- Access rights are temporary. It should not be permanent; periodically these rights must be reviewed and changed as appropriate.

10) Data Privacy (and security of ay asset of sufficiently high value) requires segregation of duties/privileges.

- Segregation of duties is recommended when controlling keys, permissions; i.e. for the trust models to work this must be handled independently.
- This must include system administration access.

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

- High Security levels should not be assigned for all data, but refer to data access above.

Why the Need for Jericho

It is important compare the business models of the past with the new realities of doing business today and in the future, which changes the requirements of today's perimeter based networks. This chapter makes the case for change and the need for De-perimeterisation. This proposition is about cost reduction and greater value derived from increased collaboration and commerce, better and improved risk management, better productivity, better integrity and reliability, and most of all business simplification.

How does it work today?

Table 2 below shows an exaggeration of an existing perimeter based system which highlights the reason it is called a 'Moat Based perimeter' system.

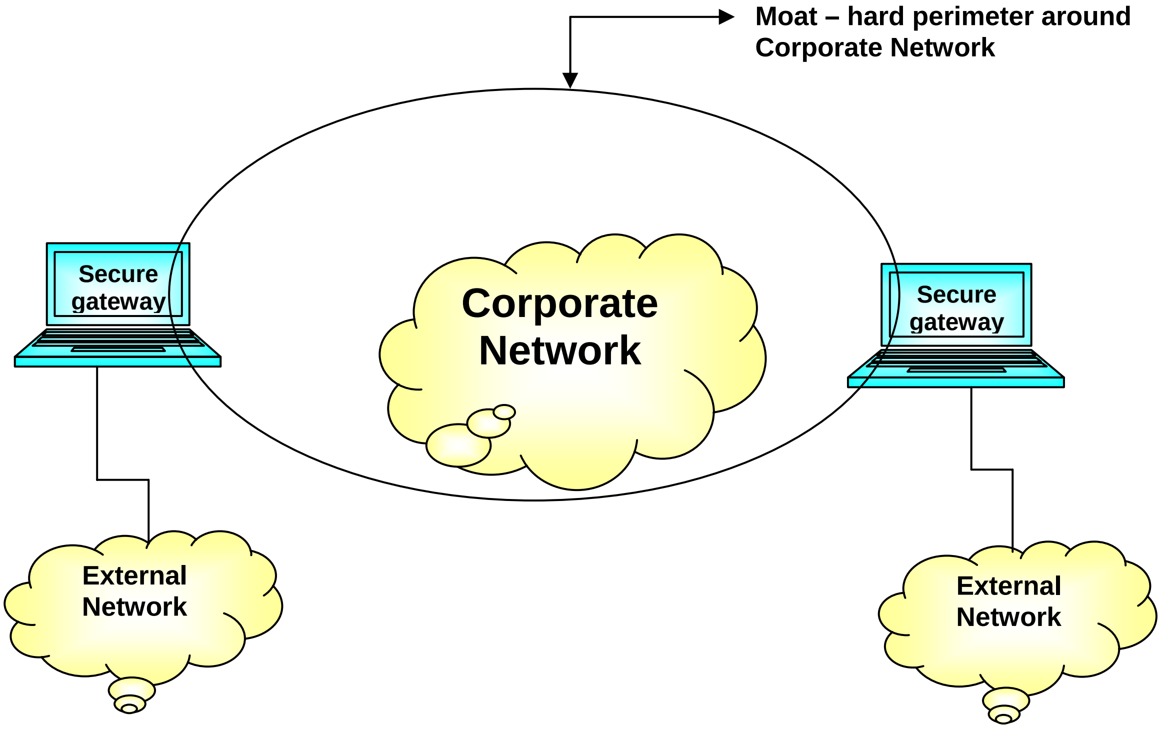


Diagram 1 – Establishing Firewalls at the Entry Points creates a moat-like effect. (Chris Hare Paper April 2005 "improving Network Level Security through real-time monitoring and Intrusion detection)

Many companies protect their networks from unauthorized access by implementing a security program using perimeter protection devices, including screening routers, firewalls and the secure gateway systems. This system cannot adapt easily to changes in business requirements like network design, traffic patterns and the connectivity requirements of business partners, customers, vendors, or governmental agencies.

Many organizations connect only to the Internet and only need to protect themselves at that point of entry. However, many organizations need to connect to business partners, who are in turn, are connected to other networks and these cannot be ignored.

This ‘moat security model’ works on the assumption that a) we can trust that which is inside and distrust everything outside. It also works on the assumption that attacks come from the external network. This model cannot therefore address the attack that comes from within, nor deal with the collaborative business model of today and the complexity that is coming.

The problem goes deeper, when one asks a company if they know what they vulnerabilities are, how many threats or attacks or breaches were received, the answers are very revealing.

The following table was taken from the FBI’s 2006 survey:-

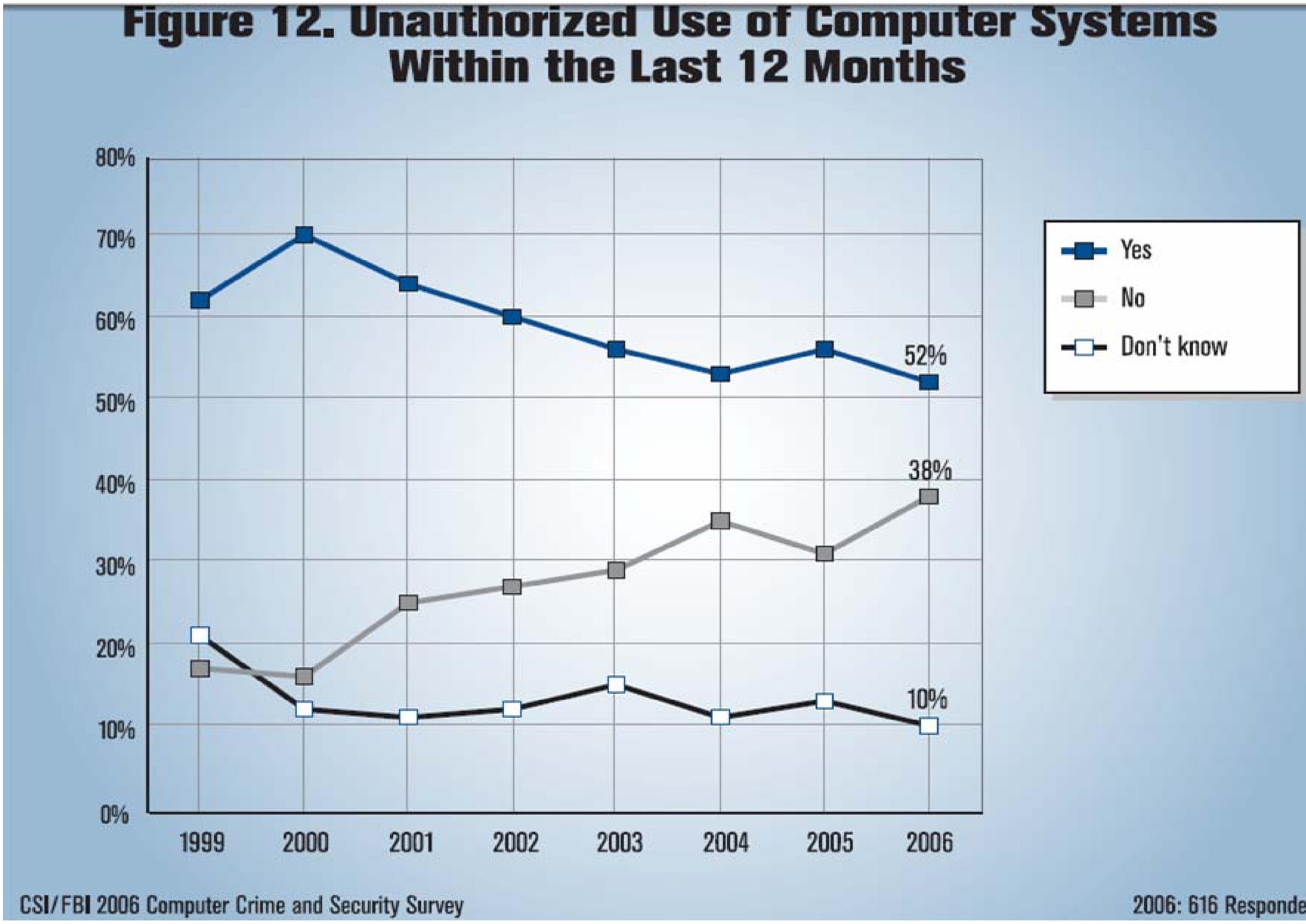
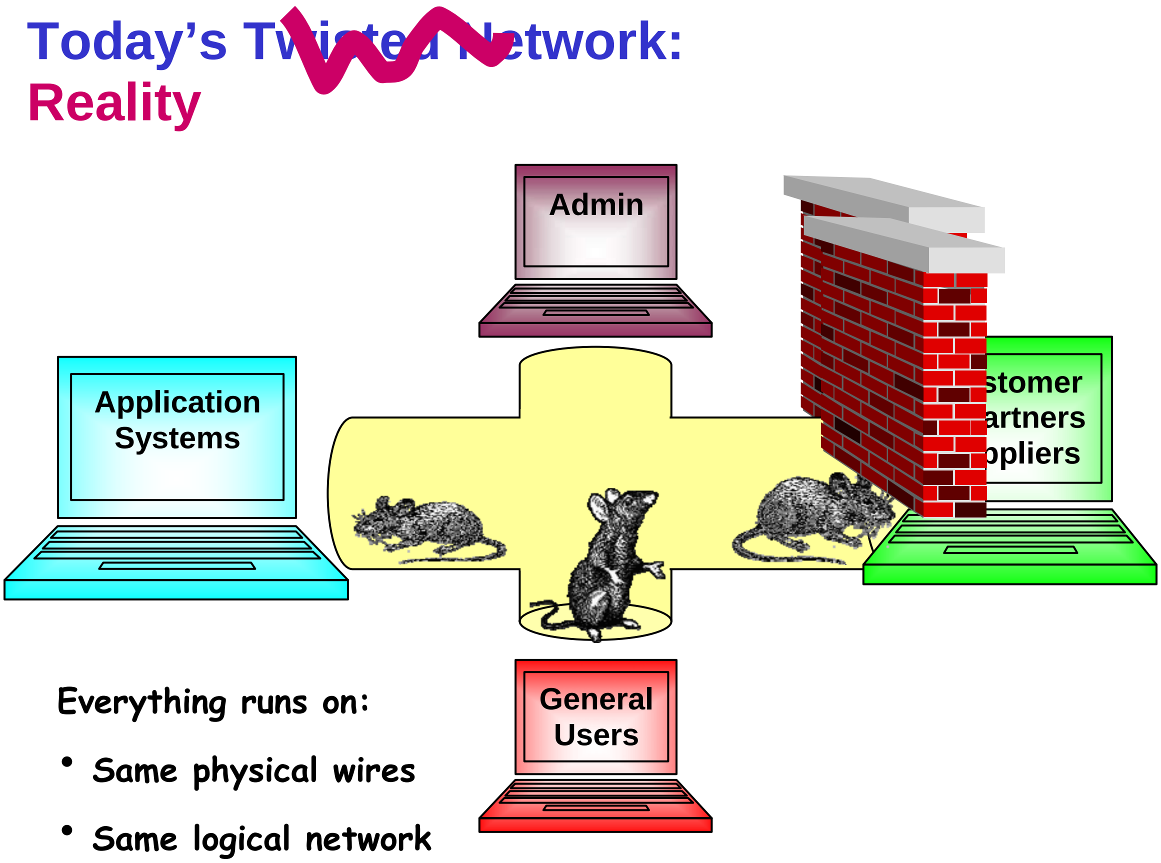


Table 2 – CSI/FBI 2006 Survey of Security Compromises in Companies.

The Table is an annual CSI/FBI report (Latest 2006 survey) conducted of the membership of the Computer Security Institute and the question asked: “Has your organization experienced an incident involving the unauthorized use of a computer system?” The interesting results are not so much about the “yes” and “no” answers but the number of “don’t knows”.

Many companies don’t genuinely know what their vulnerabilities or risks are, many don’t know if their systems are compromised. In addition many do not know where their critical information and digital assets are.

Because many of the primary threats are coming from within, it is important to either ‘fix inside of the perimeter’ or find another paradigm, namely ‘de-perimeterise”.



Today's Twisted Network:
Reality

Everything runs on:

- Same physical wires
- Same logical network

<u>Diagram 2 – Today's Twisted Network By Nick Bleech February 10th 2005 Cyber Ark Seminar</u>

Nick Bleech at his 2005 Cyber Ark seminar showed the following diagram to highlight the fallacy of our trusted network using perimeterisation which reinforces the arguments above. He has replaced the word 'Trusted" with "twisted" to emphasize the issue of internal security issues and perimeterisation.

The Case for Jericho – Why do we need it?

Organizations are changing, they are more complex; with outsourcing and use of third party companies and contractors, and it is no longer possible to distinguish between employees and contractors. Old 'trust' models of doing business are changing, protecting the castle walls with 'moats' are not viable as we need to share information, collaborate with third parties, customers, vendors, compliance regulators.

The way we work has changed, many work from home offices, teams work virtually and use not just laptops and pc's but mobile devices and PDA's like Blackberry's and IPAQ's. This in turn puts a strain on existing ways of protecting a company's information and digital assets.

This in turn changes how we do security controls, because distance, access methods imposed by existing perimeter-based networks not only makes it more complex to manage but limits the ability of organizations, for example using e commerce to meet their objectives effectively and efficiently.

The Jericho white paper states that when access requirements between networks are simple and the protocols involved are equally simple, a firewall is simple to design and operate, and if well managed provides reasonably good security. In addition proxies at the firewall provide filtered or encrypted communication to counter threats to data in transit or to exclude unwanted data and access.

However, for more complex business networks which require B2B,{business to business} or P2P {peer to peer}, more collaboration between vendors, customers, more compliance with external legislation which increasingly advocates the standardization of security, governments and individuals, this increases the cost of operations as the security controls become more complex at the firewall/proxy and the internal applications they support.

It is also the belief of Jericho that traditional assumptions that certain protocol port numbers are 'reserved' or 'privileged' so inaccessible to hostile communication applications cannot be enforced in a de-perimeterised world.

Table 3 below summarizes the changing business trends. (Cyber Ark Seminar "Security without Frontiers" Feb 10th 2005.

Past Trends	Future Trends
Static, Long Term Business Relationships	Dynamic, global business partnerships
Assumptions that threats are external with need for perimeters to protect the inside from the outside.	Threats are everywhere, perimeters cannot defend mobile devices.
Traditional client server environment used by an office based workforce	Growing use of wireless devices by an increasing virtual, global workforce.
Operating system and network based security	Extended protection to applications and end user devices (host)
Organizations own control & are accountable for their ICT.	Shared accountability with third parties & outsourced partners. Fragmented ownership.
Individuals sit within organizations. An assumption of most identity management systems.	Individuals sit everywhere and virtually.

Table 3 – Cyber Ark Convention Feb 10th 2005 "Nick Bleech Presentation – Security Without Frontiers".

The need for change arises in several ways:

- Demand for open networks
- The connectivity requirements increase due to e commerce, public internet and the complex interfaces between them.
- The cost challenge of keeping existing security infrastructures.
- Changing existing perimeter based systems to meet the new demands is not only expensive but complex and difficult to do. We will examine a blue chip company's structure and cost issues in chapter 5.
- The need to manage complex users in terms of access control, authentication and validation puts a stress on existing systems. The need for individuals to access systems externally, internally and with different organizations is gaining recognition as a challenge in terms of how you effectively implement access controls.

The Challenges

If we accept the notion of de-perimeterisation, what are the challenges to implementing It.? Nick Bleech in his Cyber Ark seminar outlined four challenges for which he termed traffic volume, increasing service variety, application migration and encryption.

- **Traffic Volumes**

He argues that the demand for services and new technologies will generate a significant increase in network traffic volumes. CPU intensive tasks such as virus checking, IDS sensors will not be able to keep up with this demand. In addition, perimeter proxies may not be able to keep up with gigabit links. Increased traffic will also cause difficulties in decryption, and re-encryption. In addition many firewall products including packet filters, fail when they are overloaded.

- **Increasing Service Variety**

Nick Bleech feels that the existing perimeters are ‘porous’. There are an increasing number of new, complex, protocols which require proxies or what he calls ‘holes in filters’. (For example X Windows, Active X, SOAP, IOS, and IIOP).

The practice of sending traffic through the same ‘firewall friendly’ perimeter ports, i.e. the web is increasing. New protocols like SOAP use these ports by design. Older protocols are often wrapped in HTTP or HTTPS.

- **Application Migration**

Control of non traditional and some traditional applications like SAP is migrating to the web. The days when companies purchased application software, loaded it on an internal server, paid on-going maintenance fees is changing rapidly. This is a good thing as it will mean that organizations will not have to bother about upgrades and patches, but it is a challenge in terms of migrating to this model especially when many organizations still grapple with ‘legacy systems’ that cannot be moved to IP.

For example non traditional applications moving to IP are VOIP, HVAC, Process Control systems {PCN}, Video systems and automated machine tools.

- **Encryption**

Today’s firewalls have no virus checking, they are blind. TCP port and protocol information is not available for use in systems management, intrusion detection and other tools.

SSL certificates break at the perimeter when packets are decrypted at the perimeter. The devices is indistinguishable from the ‘man in the middle’ attack.

Organizations want end-to-end security with both outbound and inbound encryption and many require the notification of IP addresses and this does not proxy well. Using the existing perimeterised approach cannot address these challenges.

Chris Hare in his paper (Chris Hare 2005- Improving Network-Level Security through real-time monitoring and intrusion detection) makes the point that attempting to strengthen existing security gateways is a long term solution as users will be unwilling to accept the ‘performance and convenience penalties’ created by attempting to do this.

Business Issues To be addressed

Making the Business Case

Attempting to build a real business case with $ dollar values showing benefits and costs are truly difficult in IT and Information Security because of the disconnectedness between business and IT in organizations (them and us) it makes the analysis of true economic costs difficult. However, whilst this is a challenge for a forum group like Jericho, it is an easier task within and between collaborating organizations. This is examined later in our case study.

Privacy & Security in Collaboration.

The main issue here is that all collaborating companies want to have confidence that their privacy and security is protected and that they can trust the organizations they are dealing with, especially if we accept the Jericho scenario of “open Networks” for B2B, P2P and e commerce generally. There are no common standards and principles for addressing this; instead there are numerous vendor offers and solutions.

Offshoring & Outsourcing

To be effective and cost effective, organizations must increasingly give access to internal databases, applications, networks and information; some of these assets will be on the high criticality list.

There are no common principles or standards for addressing this, so this is an area that must be addressed if de-perimeterisation is to be successful.

External Compliance Requirements.

This is a major theme, although not specifically a work group in Jericho. Sarbanes Oxley, GLBA, HIPAA et al have focused attention on security and data privacy and protection. In moving towards de-perimeterisation, organizations will have to take this into consideration, especially when designing security assurance and internal controls into their architecture.

Technology Issues.

Existing technology was not designed with security in mind nor is it capable of dealing with the demands of e commerce. Jericho is conscious that if organizations are required to ‘start from scratch’, i.e. design on a ‘clean sheet of paper’’ so to speak, this could have serious cost implications and may not be viable to move to a de-perimeterised world. Linked to this is the issue that ‘one size may not fit all’, something that Jericho is particularly sensitive to and which will be seen more clearly in chapter 4 and 5 when we examine the “how we do it” and the real life example of a public company.

Monitoring, incident handling and management

Existing IDS (Intrusion Detection Systems) can be frustrated with many of the security controls put in place today. For example IDS needs to scan network traffic for intrusions and if it is encrypted and the IDS system cannot decrypt it, the detection will not function correctly. In addition, there is a growing need to ‘centralize’ monitoring and incident control management. Deperimeterisation will need to take this into consideration.

Trustworthiness

This is vital to effective collaboration in a de-perimeterised world. Agreeing and imposing common standards, for example certification and evaluation, will require design simplification. As the Jericho White Paper puts it “ An ability to determine the relative level or degree of trustworthiness continuously and in real time, will be more useful(either as an alternative to assurance based systems or as a complement to it), depending on the nature and value of the business relationships involved."

New and Future Technologies.

To further reinforce the case for de-perimeterisation, it is important to look at some of the key technologies that are here or coming in the future as this will show that current perimeterised systems will not be able to cope with this.

Web 3.0 {Trend Letter 2007}

One key new technology that is coming is called "Web 3.0". This was announced in 2006 and was greeted with fear, derision, skepticism and euphoria. It is not a computer application or an organization. Web 3.0 is the label given to the third generation of information sharing on the World Wide Web.

The Web's first generation (Trend calls it generation 1) ran roughly from 1996 to 1999. This allowed us to post knowledge so it could be accessed by 'flat key' searches; for example Encyclopedia Britannica. Even Google who announced the publishing of the 'world's library' uses generation 1 technology.

The development of generation 2 from 2000 to 2004 came through P2P (Peer to Peer) networking thanks to music file sharing companies like Napster. It continues to flourish today. Wikipedia for example uses this generation. In addition, blogging, or blogs, itunes, My Space and Flickr were made possible by this current generation. In addition to this, web 2.0 has the ability to connect applications such as geographic mapping with photo sharing.

Web 3.0 has been in beta test mode since 2004 and is scheduled to 'arrive' next year. It will allow what Trend Letter calls 'the fusion of human intelligence with Web Tools, and could provide the foundation for systems that can 'reason in a human fashion'.

Current networking and security 'cannot' cater for the requirements of this technology, it is too closed, and if we do what is called 'security bolt-ons' too expensive and inefficient to work.

Other key security technologies that are important for de-perimeterisation are:

- **Handheld security & the change from 'Symbol Kerberos' to standard 802.11i/WPA2 security**. (Microsoft TechNet February 2007) and (Motorola Paper "Mobility Services Platform – Feb 2007).
- **Motes or Emerson wireless measurement devices (aka Motes)** are being deployed at many of the world's refineries. These form a low-power 802.15.4 mesh network with a proprietary Hart application protocol. They get onto the plant Ethernet via a 1420 gateway device. (Emerson Global Users Exchange: Nashville, Tennessee October 2, 2006)
- **Wireless Mesh.** Firetide 802.11 wireless mesh has been field tested at a well known refinery in the UK.
- **Network Access Control Systems**. Products like CISCO Clean Access NAC appliance. Various vendor products still being reviewed by Jericho and member companies for use in their data centers. (Cisco Paper Feb 2007)
- **Personal VPN's** (Virtual private Networks) security protocols to aid wireless working in the 'wireless café' space. Products like Witopia are being evaluated. (see Witopia website).
- **Location Aware systems**. For example products like Loki from Skyhook wireless uses any WiFi application to establish your location within 50 feet in the US. Many companies are using multispectral active RFID tags (radio frequency identity) based on 6.2 GHz wide band for location aware safety systems in plants and refineries. (see Loki Beta company & Multi Spectral Solutions Inc)
- **Encryption** – new open source systems like S/MIME are add-ins for webmail. A stealth company called Koolspan is offering an SD-based encryption for mobile phones, for both voice and data. (SD means Secure Digital cards about the size

of a finger nail which is used in mobile phones to automatically encrypt all voice and data calls)

- **Firewalls** – New products will have EAL4 (US Government Evaluation Assurance Level 4 – Lab certified) and ICSA certification soon. (WatchGuard Paper Feb 2007 – Protecting Networks Against Sophisticated Threats)

This is some of the new and future technology that is important to know and understand the implications for existing perimeterised systems. As they world moves wireless and to the web, current systems will not be able to cope nor meet business expectations and future requirements.

How Do we move to De-Perimeterisation

We have looked at what de-perimeterisation is and an introduction to the Jericho model and why we need it by looking in chapter 3 at the problems and complexities of modern organizations, the case for de-perimeterisation.

This chapter outlines ‘how’ we can do it, the issues that arise and how we can overcome them. Firstly we outline the “Jericho approach” to implementing de-perimeterisation, the issues and challenges that this creates and the technological questions raised by companies who move towards this model. In Chapter 5 we will look at a practical example of how a company is attempting to actually do it.

The solution to the Jericho approach was outlined in chapter 2 in the way they have created the various scenarios and the workgroups to providing solutions. They have divided their approach around the four scenarios outlined in chapter two, namely, providing low-cost secure connectivity, supporting roaming personnel, allowing external access and improving flexibility especially for EDI or electronic data interchange.

As we outline ways of implementing de-perimeterisation, we also outline the issues and constraints that exist and which impinge on meeting fully the 11 Jericho commandments. Firstly we look at the application and architectural context involved, then we will divide up our approach into two main strategies:-

- **Strategy One -Create virtual networks to isolate critical business assets from the general network traffic.**
- **Strategy Two - Strengthening the Host. Moving access enforcement to end systems and applications.**

The Application Context

Jericho outlines the following application tools and capabilities that are necessary to support de-perimeterisation:

- Portals – Common presentation and data formats are necessary for supporting controlled sharing of information and access to applications.
- Instant messaging, email, conferencing and messaging.
- Workflow to support business applications like 'supply chain".
- Marketplaces and auctions to support what they call buyer/seller discovery and procurement.
- Knowledge management systems for supporting intellectual property development, learning and training.
- Back office pricing and settlement for trading on line
- Analysis and forecasting to combine data performance from multiple sources.

De-perimeterisation will affect these tools.

The Architectural Context

Jericho gives 4 constituent parts to this:-

- Process – the ordering and sequencing of business operations.
- Business Logic – business constraints and rules to meet specific business objectives.
- Data- both the underlying data itself and meta-data that support it (Log files etc.)
- ICT (information & Communication technology) infrastructure such as
    - Local security (firewalls, routers, IDS monitoring)
    - Platforms and devices such as Middleware and database management systems, host computer operating systems such as Linux, windows.
    - Interface standards for communications and data security.

    - Management frameworks for policy, standards, access and ID management such as COBiT 4.1, ITIL and ISO17799.

Strategy Number One – Create Virtual Networks separating critical assets.

There are several strands to this strategy:-

- Partition networks by service type which will be based on a criticality risk assessment of all Digital and information assets. The objectives are:-
    - Prevent attacks that take place in one part of the network from taking down the entire infrastructure.
- Partition networks by sub divisions (cost centers/profit centers) and by projects. The objectives here are:-
    - Protecting different user communities from each other
- Embrace Open Network and trust models. The objectives here are:
    - Cost, they are cheaper to run. (This is demonstrated in our case study). It is important to clarify what is meant by trust and open networks. Jericho is not suggesting that you combine for example general email activity with controlling an airplane in flight on the same IP network and they are not suggesting that all IP traffic is equal.
    - The existing trusted network model is broken.
    - Harmonize identities and trust relationships with individuals.(links to our host hardening strategy below)

Access over wireless & public networks

There is a need to open up access to internal systems, data and applications. Many organizations have done this by using existing authentication protocols using SSL and VPN's with the belief that it provides adequate security. Whether this is from an internet café or from home or any public space.

To overcome this Jericho proposes using stronger authentication protocols with anti-replay controls based on the "Needham-Schroeder Principles". (White Paper on using encryption for the authentication of large networks of Computers – Professor Roger M Needham Cambridge University and co-author with Michael D Schroeder Assistant Director of Microsoft Research Silicon Valley). These two authors came up with what is called the Needham-Schroeder Protocol using both private and public key encryption with systems like Kerberos). Jericho admits however, that this may not scale perfectly to meet full de-perimeterisation requirements. Jericho is proposing to examine how the 802.11x standards evolve and integrate better with other infrastructure elements in the long term.

Domain inter-working over open networks

Jericho believes that the current IP version network technology does not support managing multiple classes or qualities of service within the same configuration. The IEFT has developed draft mobile IP standards for both IP 4 and IP version 6 to enable organizations to attach fixed sub-network addresses to open networks without the need to reconfigure the address space. Jericho believe that only IP 6 versions will gain momentum, because of its added security requirements versus IP 4; however they do recognize that moving to IP 6 will not be easy, because IP 6 requires a larger IP address, from 32 bits to 128 bits. This will have huge ramifications for the world wide web and in particular domain name severs (DNS).

Roaming Personnel Connections

Jericho proposes that the availability of communication paths that can be secured using point to point security protocols is a short term issue and that the increased availability of mobile wireless data services with voice and data convergence in most industrialized countries will allow organizations to reach their mobile workforces and at low cost.

They further propose that roaming personnel may require the portability of authentication credentials, potentially including cryptographic keys, biometric data, passwords and other relevant information.

Third Party Access

Organizations must allow third parties to access major applications (e.g. like SAP) to be able to support critical business processes. If the Trust relationships with appropriate authentications is set up right, and the organization has moved to open networks then this should not be a problem. Jericho does accept however that a standard model of Trust does not yet exist, so this could be a long term implementation and solution.

Outsourced Help Desk

The same objectives for third parties, outsourced IT help desk teams need access to privileged applications and systems to be able diagnose problems. They should be treated no differently to employees. The general thesis here is that modern organizations are complex, there is no longer an inside and an outside; business process is integrated, requiring collaboration from a number of external sources and third parties.

EDI & Web Services using XML

Many organizations already have initiatives underway to implement what is becoming SOA or Service Oriented Architectures to support the Jericho model. This means redesigning interfaces and systems to use Extensible Markup Language (XML) as new software comes online that has this capability.

The World Wide Web Consortium (W3C) supported by a number of other standard bodies also support this and are beginning to include a number of security standards within XML, for better encryption, digital signatures and key management.

Also linked to this XML initiative is the introduction of SAML (Security Assertions Markup Language) which is concerned with identity and access management are under development along with the web consortium's SOAP or Simple object access protocol for various web services. These will also allow greater data integrity, confidentiality and authentication for message based communications.

Issues & Challenges with creating Virtual Networks and separating critical assets.

The purpose of this section is to honestly appraise the Jericho approach to implementing de-perimeterisation, so we have pulled together all of the issues and challenges for each of the strategies and their appropriate strands:-

- Network partitioning will add complexity as users have expectations for full access to IP based services so organizations transitioning will need to go on a stepped basis. Jericho also believes that the solution to this is customer-led standards and not vendor-led standards as is the case at present.
- In addition, the isolation of application components conflicts with server consolidation strategies. When it comes to Domain Inter-working over open networks, may organizations will approach de-perimeterisation from the 'bottom up' which will exclude looking at the whole, for example this approach tends not to look at security domains, and or performance which private networks are trying to deliver currently. They need to ensure when they change the quality of service, robustness and resiliency continues and that traffic segregation is achievable and that requirements can change on demand.
- The practical impacts of interposing domain boundaries can be severe. For example encrypted tunnels using SSL or VPN may be hard-wired to domain names and IP addresses which cannot be changed with some kind of reconfiguration.

- Security access at the VPN level also can open up risks of access rights abuse and privilege escalation. The benefits of outsourcing can be negated if the provider has to physically implement multiple segregated mini-domains to match the organizations domain structure.
- Regarding the convergence of voice and data services, in a de-perimeterised world this can be affected if organizations cannot effectively manage band width and quality of service. Companies tend to use layer 2/3 switching (Virtual Lans) for the purpose of containing rogue broadcasts but according to Jericho, this is inflexible as the tagging used to segregate traffic can easily be forged.
- Moving on to Trust models; de-perimeterisation requires that organizations re-examine and re-appraise existing relationships between individual users, their data sets, host systems and network security domains because if data is to be portable outside existing protected containers, encryption capabilities must be deployed. The problem here is that existing key management techniques are manual and difficult to scale especially for symmetric keys. The other problem is that there is no agreed standard of what a “Trust Model” should look like.
- Cryptographic key management must allow for the alternative authorized access, (for example an executive and an executive’s personal assistant) Organizations have found it difficult to apply the ‘trusted third party’ model in PKI to real business requirements. If a third party issues a logical ID, it is potentially liable for miss-issuing it, or compromising authentication credentials with which it is associated. Creating a third party contract that can deal with this has proven difficult.
- In addition, the use of the X509 standard leaves the majority of implementation concerns by organizations under-specified. KPIX and related standards attempted to add architecture and management for multiple applications to x500 and x509, but unfortunately x500 directories were largely non existent before PKI came along; the

naming conventions proved to be awkward to map to existing schemes and inflexible for multi-organizational use. Jericho believes that this is a long term issue that could and will affect how far we move towards de-perimeterisation without the full re-design of PKI. Jericho also feels that many users see ‘directory interoperability’ as the foundation for harmonizing identities and trust relationships. Unfortunately, directories concentrate the issues rather than reducing them. Also Conventional ideas about ‘role-based’ access control (access based on a role and not a person, i.e. a user is linked to a role or function which has a security access control or privilege linked to it, as opposed to direct access systems that link users individually to an application or host) assume that there is ‘open knowledge’ within the organization about who each role holder is and this is not the case. Organizations have difficulty not only understanding roles and functions, but what access privileges they should have; this is also a problem for designing segregation of duty profiles. Not only that, but this is usually considered sensitive information, so according to Jericho, this could create an unacceptable overhead to be able to maintain mappings across multiple organizations. This is a longer term issue to resolve.

- Regarding allowing more external access, there are issues regarding use of passwords and vendor offers for specific applications. Jericho believe that existing passwords will be inadequate to control access from the outside world, because they are vulnerable to all types of malicious software attack. In addition security managers are unsure of the vendor offers (e.g. SAP) which allows various options to support remote access, including linking web portals or direct support for remote sign on systems, because many of the standards to which these applications comply are not documented. However, Jericho views this as a short term issue and will examine how VPN standards can evolve to facilitate limiting onward access and terminating VPN tunnels at specific internal network addresses.

Strategy Number Two. Strengthening Host Systems by Moving ‘enforcement’ to end systems.

There are also several strands to this that need separate analysis. The main proposition here is that in conjunction with the network changes above, we must move security controls to end devices. These devices are highly mobile and therefore must be able to protect themselves. So for example we add anti virus, stronger firewalls and intrusion detection to both host devices including not just lap tops but the host applications that support them; we don’t rely mainly on network protection.

In addition, there must be improved devices like firewalls and encryption and improved software solutions with new platform designs to support them, such as NGSCB (Next generation Secure Computing Base)

Jericho is also proposing that we must have a more ‘uniform trust model’ to support user identities and establish what they are calling “citadels” for data to be able to support:

- Information needed for Regulatory disclosure such as ‘e discovery’.
- Master data and security information

Consolidating Identity & Access Management (IAM)

This refers to a class of security functionality and systems concerning the combining of user authentication, authorization and access to data to systems. Today and typically with perimeter-based systems, users have to sign on and authenticate themselves to each host application that they have access to. Not only is this costly, but inefficient as users end up with multiple user identities and multiple passwords as most users have access to multiple applications. Jericho is proposing that in their world it is important to have a single system to manage this whether an organization opts for single sign on (SSO) one solution or not. Typically, these systems will link to Human Resources (HR) but in the collaborative world will need to link to external organization systems. They recognize that these systems are not mature and are evolving.

Automated policies and standards for information sharing with others.

The security Orange Book (the US Trusted Computer Security Evaluation Criteria) and derivative standards developed in the 1980's and 1990's only offer guidance and standards for protecting data and information within the confines of the existing trusted systems. Linked to this is the current way of doing data classifications for allowing mainly internal users to access the appropriate data and information based on their authority level which is linked to a classification level, for example secret data.

This model will not work with more collaboration and de-perimeterisation as it will require an expansion of this to include external organizations and the appropriate technology to allow it to happen.

Jericho believe that to develop standards for this will require the World Wide Web Consortium (W3C) for a system called "Semantic Web" which offers the opportunity to capture and represent directly information flow control policies for collaboration and commerce.

Issues and challenges with strengthening the Host

Protecting end devices may interfere with central device management and operational support. (We will see this as one of the issues in our case study).

Many existing standards are 'broken' in practice according to Jericho. Examples quoted are:

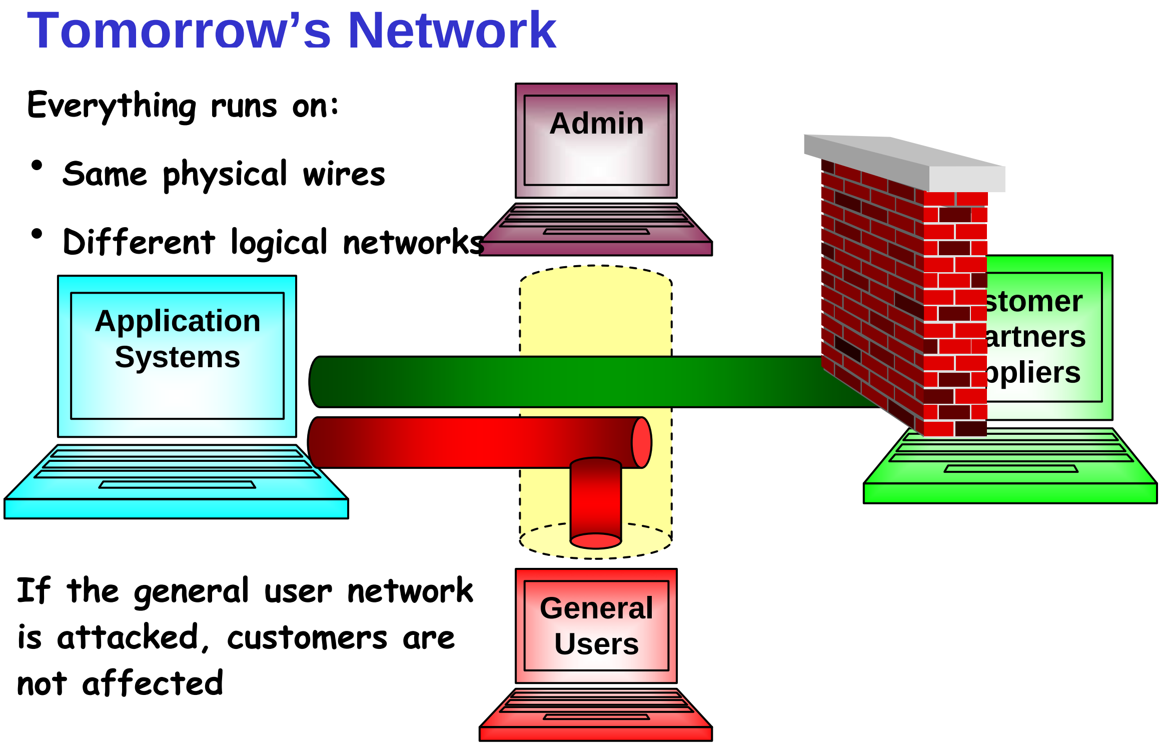
- Certificate/CRL non processing in SSL
- Bug-compatible implementations of X509 certificate policy/attribute processing in crypto library software.
- Lack of collaboration in x500/LDAP and directory interoperability.
- Reinventing the wheel for security services for XML (e.g. signatures, Encryption and Key management)
- Users don't articulate what they want so vendors make assumptions and provide products and services accordingly.

With reference to the consolidating of Identity and Access management when it applies to outsourced partners like ‘help desk’ for example, according to Jericho, many organizations lack single-sign-on capabilities of sufficient strength that can combine access to systems and applications. The problem is that a company cannot do a business case only for ‘help desk’ to justify consolidation and a move to single-sign-on. A company will have to show that from a user perspective, both internal and third party, having multiple ‘logons’ for multiple applications is not only bureaucratic and costly for perimeter-based systems but adds greater complexity for a de-perimeterised system. It is easier from a security standpoint to have a single sign on system to aid an identity management system that must administer multiple users outside of a perimeter. The second problem concerns the granting of ‘privileges’; there are long term issues with the granting of excessive privileges to systems and applications and most of these users are internal, granting these privileges externally can be a problem. However, as we have been saying, many of the problems come from inside the organization as many insiders are already non employees where the abuse can be far greater; this is becoming a real contradiction to how existing perimeter-based systems are managed.

The existing perimeterised system is based on ‘trust’, even if this is a false premise; it is difficult to effectively control access privileges, especially without a centrally managed ID management system. Moving outside the perimeter just makes this issue bigger and will demand a technological solution that centralizes and integrates all user access controls, privileges in one place.

Putting it all together we come up with an over-simplified diagram showing what it could look like:

Diagram 3 – Hypothetical Model of Tomorrow's Network from Nick Bleech February 10th 2005 Cyber Ark Seminar.



Tomorrow's Network

Everything runs on:

- Same physical wires
- Different logical networks

If the general user network is attacked, customers are not affected

How Are Companies Implementing De-perimeterisation – A Case Study

A Fortune 100 international manufacturing company that has accepted the Jericho model started their implementation at the beginning of 2003, although the strategy and planning started before the foundation of Jericho. We will examine their strategy, their problems and issues as they move down this path; we will look at each of the strategic pieces and compare to see if they are complying with the 11 Jericho commandments and most importantly we will look at an analysis of costs and benefit information to get an idea of the business value created by de-perimeterisation.

This company created a strategy around Two Key themes:

1. Desktop & Hosts – 'Hardening' with a move towards the external internet.
    i. Linked to this is the strategy of wireless, explorer, encryption and virtual PC solutions.
2. Mega Data Center Consolidation.(MDC) Whilst this in itself does not lead to de-perimeterisation, it is a major enabler in terms of how security control and new technology is being implemented, especially how secure gateways and firewalls were set up. There are three strands to this that supports the host strengthening and is important to allow the network partioning:
    i. The New Security Environment for the MDC's
    ii. Virtual Servers using VMWARE Software.
    iii. Security Event management.(SEM)

Let us examine these strategies in more detail, focusing more on the security elements:-

Desktop and Host Strategy (Advanced Computing Environment or ACE was the name given to this strategy)

In 2003 the company formed a separate information security group reporting for the moment to the Vice President of IT. For the first time Information Security became visible and with the introduction of the Sarbanes Oxley legislation (SOX) more important in terms of security and access controls. (IS got a seat at the table so to speak). Prior to SOX, up until the end of 2002, there was no separate information security department; security was ad hoc, hap hazard, not documented and 'an after-thought'. The Global Operations Network department was responsible for security and firewall operations; there was no Alert Center, no Vulnerability analysis, no risk analysis process, nor intrusion detection systems. The network was a typical perimeterised system with a common, hard-wired standard access system called Common Operating Environment (COE) and no IT audit.

In conjunction with the IT strategic group, a strategy was formed to transform the company's computing and communications infrastructure. With 80 thousand pc's, a mixture between desktop and laptops and another 15 thousand coming online from new acquisitions, this was a huge and costly undertaking that would take several years to achieve and realize all of the benefits.

Communications infrastructure comprised of desktop computing, the network, data center, security and organizational elements. A pilot was started in June of 2003 and ran until December of 2003 and comprised of 2000 users. Not only was it well received by the users, but the 'business case' was turning out to be very attractive. (Discussed later)

Prior to this strategy the current architecture and topology was based on the old perimeterised model and this is called the COE environment or Common Operating Environment, which is 'mote like' with mainly hard wiring and intranets with access to the external internet via proxy servers at port 80. Users could visit any branch office and log into the company network.

As we will see later the main problem with this is cost, size and complexity. As the company has grown, so have the demands of new business requirements and new technology like wireless. As the castle walls expand, attempts to make the mote bigger have failed. Security is mainly network based with little or no security on individual hosts or desktops.

ACE is based on:-

- A simple ‘commodity like’ or ‘out of the box’ standard desktop with the latest Microsoft software and access to the email and other internet enabled business applications directly via the internet.
- Initial software that includes Windows XP professional operating system and office 2003 suite of products.
- Email services use Microsoft Exchange 2003 with use of MS Collaboration tools.
- Security is based on the protection of individual devices with encryption of communications traffic using SSL or Secure Socket Layer technology.
- Anti Virus was implemented using the latest McAfee software.
- Software inventory to be handled by the latest Altiris client.

In addition ACE offered a number of non core options such as enhanced support using open market assistance; access to legacy applications using IRAS4 with ‘smart card’. The ability to access the company's email outlook via the Outlook Web Access or OWA from any pc, including non company pc’s.

Also offered was an option to provide remote and automatic management of user’s PC environment and can be seen as a ‘light touch’ version of the old COE system and allows the company to cut over to the new ACE system in a phased way.

The following Table shows the estimated number of user types.

Table 4 – Estimated Number of User Types

Self-verified user	**Legacy Apps User**	**Managed User**	**Managed Legacy Apps User**	**OWA User**	**Total**
Include those using iLink and having occasional Kiosk usage. No need for iRas (legacy apps access).	**Will need access to 1 or more legacy apps using iRas. Can maintain PC themselves.**	**People who don't maintain their own Desktop environment.**	**People who need access to legacy AND who don't maintain their own PC**	**People needing occasional access to email but no permanent access to a company-PC**	
5,350	**17,250**	**35,900**	**14,800**	**22,000**	**95,300**

In addition to the company users shown here there are two types of user environment:-

- Third Party Devices

  A contractor or third party or consultant can use their own device but with a security token that allows them only to the authorized application and using an application called "I Link" which controls access via a secure gateway.

- Locked Down Devices

  Users are restricted form changing most configuration elements of their device. These devices would only reside within the old company internal network.

  In addition, Table 5 below gives a summary of ACE desktop options. It shows a comparison to the old COE systems.

Table 5 – Summary of ACE Desktop Options.

	MANAGED USER	LEGACY APPS USER	SELF-VERIFIED USER	UNTRUSTED USER (OWA)	COE3 (for comparison)
Used by	- Company staff who don’t maintain their own PC. - Company staff who reside in sites that only have legacy connectivity.	Company staff who maintain their own PC AND who use iRas4 to gain access to legacy apps	Company staff who maintain their own PC and who do not need internal apps	- BP staff working on non-BP PCs (home, Internet Cafes) or using non-PC devices (PDA’s, phones) - SOME Third Parties	Everyone
Email	ACE	ACE	ACE	Outlook Web Access	COE
Collaboration services	Messenger / SharePoint	Messenger / SharePoint	Messenger / SharePoint	Messenger / SharePoint	COE
Base PC Software	WinXP, Office 2003, ICF, Anti-virus	WinXP, Office 2003, ICF, Anti-virus	WinXP, Office 2003, ICF, Anti-virus	Browser	Win 2000, Office 2000
Additional software	Management S/W (incl. Altiris) plus possible Client Apps.	Altiris Client, Possible Client Apps.	Altiris Client (for S/W distribution and licence control).	None	As required
Wireless access in offices	Yes	Yes	Yes	Yes	Only in conjunction with internet / iRas
PC security configuration	Done for you	Done by you	Done by you	N/A	Done to you
Software procurement	Software Spectrum	Software Spectrum	Software Spectrum	N/A	Done for you
Software patching / upgrading	Done for you	Done by you	Done by you	N/A	Done to you
Assurance of configuration	Via Management software	Self-assured plus MS Quarantine on access to BP network	Self-assured plus MS Quarantine on access to company network	N/A	Automatic
What information could be compromised if PC compromised	User-specific PC content / mailbox / collaboration data	User-specific PC content / mailbox / collaboration data plus anything they can access within BP network	User-specific PC content / mailbox / collaboration data	User-specific mailbox	User-specific PC content / mailbox / collaboration data plus anything within company network
Authentication	Individual userid / passwords for intranet apps and services	Single userid / password gains access to most intranet apps and services	Individual userid / passwords for apps and services	Need to know URL for email service, userid and password	Single userid / password gains access to most intranet apps and services
Self-Support	Partial	Partial	Full	N/A	Minimal
Company Sponsored self support	Yes	Yes	No	N/A	Yes
Company Help desk	Yes (per call)	Yes (per call)	Yes (per call)	N/A	Yes

Implementation

Previously the company tended to customize or add to the normal Windows operating systems. The new strategy calls for using only an OEM or Original Manufacturing Offer as a basic principle in keeping with reducing complexity. This would prevent building desktops that were company unique.

In addition, it was decided that a desktop asset replacement policy would change so that Laptops would be replaced every 3 years and desktops every 4 years. This was important to take into consideration as a cost factor both for implementation and building the business case. Machines that were less than 3 years were upgraded to accommodate the external ACE systems. Those that were due to be changed, new pc's were procured. Previously only PC's sold by IBM were considered, this time flexibility allowing the addition of Dell and Toshiba were added as procurement policies. It was estimated that by 2004 over 30, 000 machines would be replaced.

Host Applications

In conjunction with externalizing desktops, the company also is attempting to externalize applications. However, whilst it is easier for new applications or developing applications, it is more difficult to convert large legacy applications of which this company has in abundance. In addition, ERP systems like SAP for example require major vendor assistance to move to internet versions of the software, and given the share size and number of versions and instances of these, also not a short term fix; the company recognizes and accepts that it must keep some of its legacy systems inside the perimeter, until they are replaced. This does not negate Jericho but accepts the business reality of how quickly companies like this one can change over.

To date they have externalized key applications like Travel & Entertainment, e travel bookings and other key commonly used applications. In the short term however, it means supporting both an internal and an external version of these software applications, which is the cost of change.

The Business Case for Desktop & Host Strategy.

The company used a Booz Allen cost benchmark to produce its Business Case. The following business case tells a compelling story and influenced the senior business management of the company as to the selection of the strategy. This section will be analyzed with reference to the Jericho 11 commandments.

- **Reliability**

  The box standard Microsoft XP environment is proving to be much more stable than previous windows systems, which is providing a platform for lower PC support costs and allowing more users to manage their software and security. This impacts the organization in less time maintaining and fixing older windows operating system problems and this lower support costs as is shown in Table 6.

  The office 2003 suite is generally proving to be stable and is receiving positive feedback. The help features of XP and office 2003 are much improved.

- **Connectivity**

  ACE achieves the strategy of 'living on the internet'. In addition setting up wireless network connections has proven much easier in XP. Exchange 2003 with its SSL connectivity, is living up to the company's expectations by allowing simpler and more reliable remote connectivity to email services, without the need for complex and expensive personal VPN's (Virtual Private Networks).

  In addition, the resilience of the Internet is being embedded into the company's telecommunications. As one senior manager said "The Last Mile can be vulnerable, but this can be resolved by the use of redundant circuits where required." ACE also supports the use of MPLS (Multi-Protocol Label Switching. The emerging industry standard, upon which, tag switching is based. MPLS is a widely supported method of speeding up data communication over combined IP/ATM networks. This improves the speed of packet processing and enhances performance of the network) this has provided much improved long-distance latency, introduces consistency of response to the company and allows the multiple sites that require Internal network connections to access services and applications located in the mega data centers.

- **Security**

  The user base can respond quickly to vulnerability and virus threats using Windows and Anti-Virus signature updates across the internet. Wireless access points were moved outside the firewall thereby eliminating concerns about broadcasting the company 'dial-tone'. There are built-in firewalls which are in expensive and this has worked well. In addition, the impact of virus and worm incidents at most sites using ACE has been less, in comparison to the internal sites which have seen more problems and compromised systems. The only statistical information the company would disclose to support this claim was that a 'Trojan Attack" in June of 2006 affected 43 desktops and all of these were in the old COE, perimeterised network system.

  In addition, users have taken more frequent backups using portable backup systems that images the desktop hard drive; a survey showed that internal users who had a network 'H' drive at their disposal backed up on average once a month; most of these users have a false sense of security about being safe inside the perimeter, and so feel that don't need to backup and believe that the company will do it for them), as opposed to the users that had moved to ACE, which was on average once a week. The company feels, as does Jericho that emerging technologies will further help and simplify this.

  ACE's clear segregation of clients and servers has limited damage in the event of certain security issues and breaches.

- **Flexibility & Productivity**

  Feedback from the users to date (From the initial pilot of 2000 converted users at December 2003, and as at December 2006 the company had converted 35, 000 desktops), provides strong messages that they believe they are much more productive. Examples are:-

- The convenience of wireless connectivity, (The company has converted almost all North American and European offices to wireless, including Singapore and South Africa.
- The reliability of Windows XP (Linux and Unix users may challenge this) the simplicity of SSL versus VPN, the new features of office 2003 (there is also now in some circles an expectation that VISTA, the new Microsoft Operating systems replacement for XP will be much better).
- The speed and availability of the internet, instant messaging, use of integrated collaboration tools inside and outside the firewall, such as “Live Meeting” E Symposium and Web learn plus faster start up and shut down times in comparison to the old COE environment.

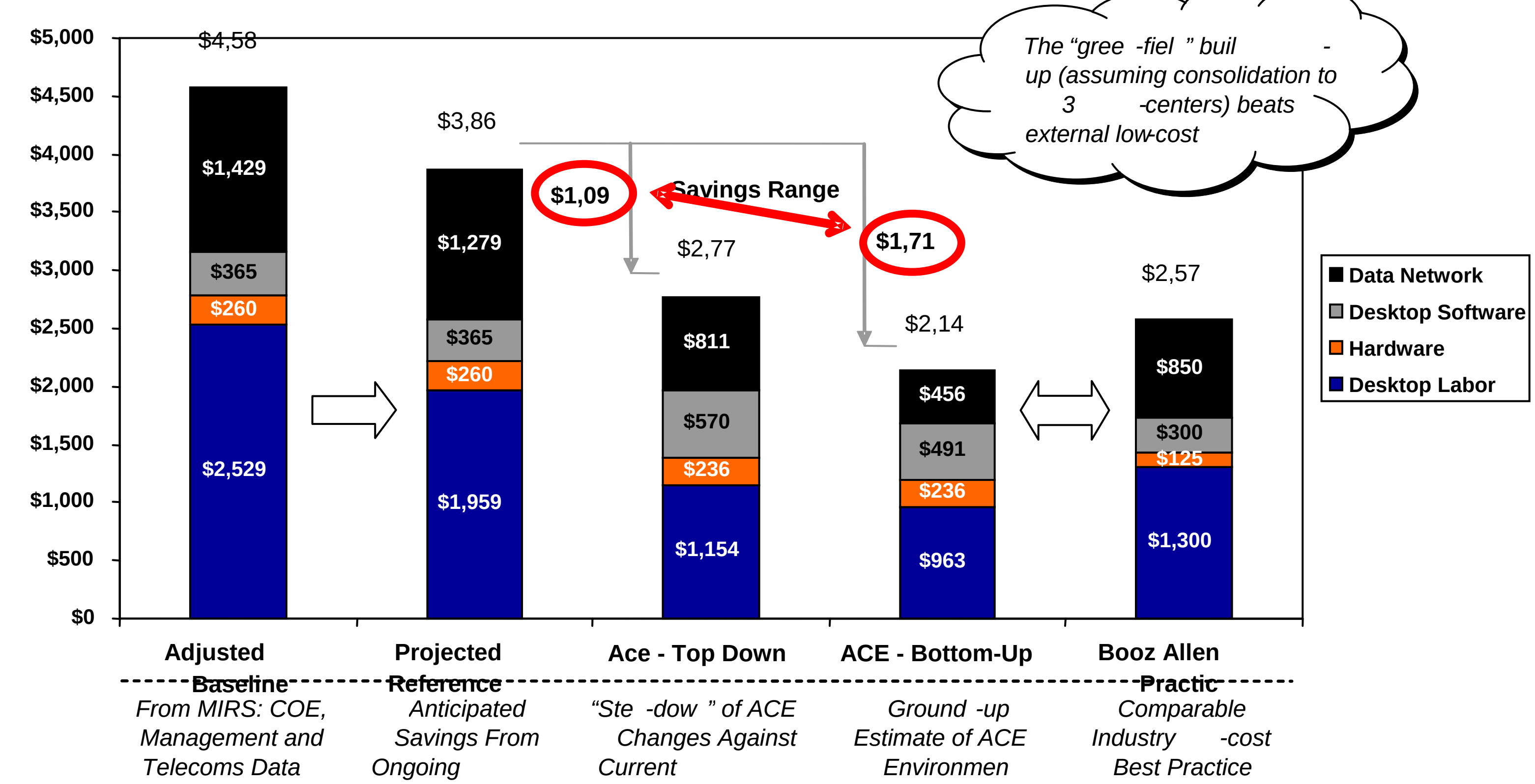
- **Cost Reduction**

The company reviewed its costs in some detail in 2003 and verified that implementation of the ACE strategy and extensive use of the internet would yield annual savings of between $70m - $117m relative to the existing COE system; assuming implementation of the data center strategy which is reviewed in paragraph 5.2 as part of strategy two below. The reference case was based on costs 15 % below those projected for 2003.

Table 6 – Business Case Cost Results

[redacted]

Summary of Enterprise Cost



The "gree -fiel " buil - up (assuming consolidation to 3 -centers) beats external low-cost

From MIRS: COE, Management and Telecoms Data	Anticipated Savings From Ongoing	"Ste -dow " of ACE Changes Against Current	Ground -up Estimate of ACE Environmen	Comparable Industry -cost Best Practice

The business case is extremely appealing, even at the lower end of the estimated savings range

Note: All scenarios exclude desktop / laptop / peripheral hardware lease and/or depreciation. Top-down and Bottom-up Vanilla estimates contain the $350 per seat that will be transferred to BU budgets for end-User support, application licences, etc. (*) Further analysis is required to identify specific WAN components that gets displaced by

- The company used a Booz Allen Hamilton 'best in class' benchmark as a comparison of its cost numbers.
- MIRS stands for Management Information & reporting system and is an IT cost data base.

- The range of cost savings generally represents differences in the extent to which the existing telecommunications network costs can be eliminated.
- The main sources of savings are support and network costs.
- This company tracks and calculates costs and benefits by establishing a cost per desktop for all IT Costs. The above analysis excludes depreciation costs, and leasing of hardware peripherals.
- Per seat cost savings range from $1,100 - $1,700 per desktop from a projected, existing COE cost base of $3,860 for desktop and data communications and $1,650 - $2,325 against 2003 COE costs.
- The higher savings estimate yields a per seat cost 20% lower than Booz Allen's most attractive benchmark shown above.

As at December 2006, these savings have not only been realized but this cost base has been maintained. Based on this the company will accelerate the changeover of all COE based systems by the middle of 2008. The actual costs per desktop have averaged $2200 per unit as at the end of 2006; this is still below the 'Booz Allen best in class' average. However, desktops still on the old COE systems pay almost double this figure; this has put pressure on the organization to advance the pace of implementation for the remaining desktops.

Mega Data Center Consolidation

Strategically this company realized that there were too many data centers, too many servers that were becoming costly and inefficient because they were based on the old perimeterised approach which was becoming no longer sustainable for this size of company.

Starting in parallel with the ACE implementation, it was decided to consolidate some 20 data centers around the world into three or four with the appropriate Disaster Recover backup site or sites.(two were planned.) In addition, the company decided to move to IBM blade server technology and virtual server architecture, (discussed in detail later) which would drastically reduce building and floor space and allow planned growth as and when needed.

In addition all Mega Data Centers would be ‘internet-facing’. To be able to create the necessary network partitions, the company made an inventory of all of its Digital Assets, including applications and did a business impact analysis with risk assessment to come up with a scheme of asset criticality based on Highly Critical Assets (HCA’s) and Low Critical Assets which would not require special encryption or other security protection. This also necessitated the introduction of a revised data classification system that would assist the new Identity management with SSO (single sign on) being developed.

As at December 2006, the company had successfully consolidated into 4 mega data centers combining host applications worldwide into three countries.

Mega Data Center (MDC) Security Architecture Explained

The above strategy creates risks and challenges for this company as technically they are ‘putting all of the eggs into one basket’ so to speak, which presents a big challenge as their could and will be with internet-facing systems, a wide audience of potentially hostile users. In addition, this change over must host both new and legacy applications.

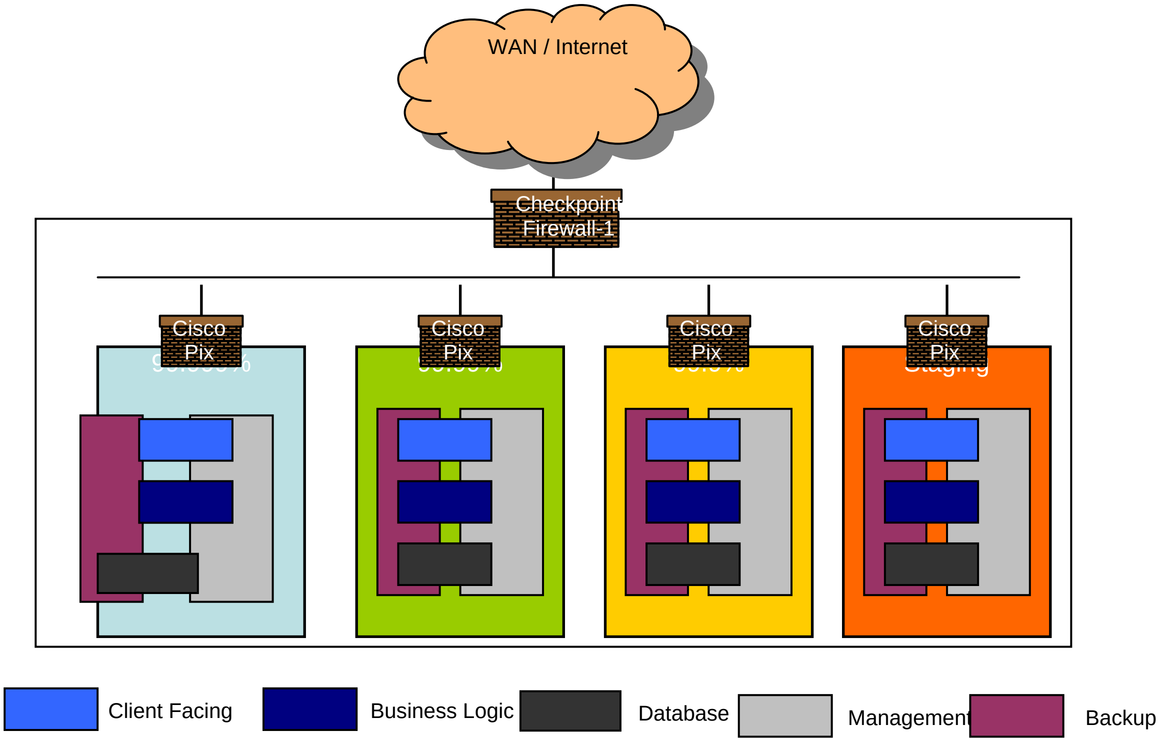
In addition, there are challenges to host the new Vanilla/ACE systems especially in terms of security access and finally the increasing reliance on single-vendor solutions such as Microsoft.

- **The Solution**

A defense-in-depth approach that will do the following:

1. Multi vendor approach, using Cisco, Symantec and other vendors
2. Extensive use of security tools such as FireMon, ArcSight and IDS
3. Monitor everything and correlate across all security events
4. Ensure security of services before they go live by doing a full assurance, penetration testing where applicable and BIA/Risk analysis.(Business Impact Analysis)

- **<u>Diagram 4 - The Security Design for the MDC (Mega Data Center)</u>**



- **The MDC Security Features**
  - A MDC perimeter with single point of control; common environment across all MDC's; which integrates with existing security tools.
  - Network "zones" within the MDC (shown in the diagram above) with a high level of segmentation by business and project (as proposed by Jericho); change control boundaries which provides a segregated environment for staging/building.
  - Security compartments within network zones that provide granular access control; facilitates IDS (Intrusion Detection Systems) deployment; and detailed audit records.

- **Additional Enhancements**
    - **Use FireMon, a tool that ensures integrity of firewall environments**. It does this by:-
        - Policy Compliance to check for and detect illegal configurations.
        - Supporting both Checkpoint and Cisco firewalls.
        - Provides off-line mechanism to query firewall policies in the event of an incident.
        - Policy revision history to track the evolution of policies.
    - **Deploy IDS** at strategic points in the infrastructure:
        - Passive Test Access Points (Taps) on all major network links that enable IDS sensors to be re-patched to cover different segments according to change requirements.
        - High Level IDS covers all traffic in/out of each network zone.
        - A more granular IDS coverage monitors traffic between security compartments within the critical server zone.
    - **Use Lightning vulnerability scanners**.
        - This is a vulnerability scanner that checks the configuration of all hosts built in the staging environment, BEFORE deployment to a live production environment.
        - It is also an Enterprise Security Manager/Configuration Manager that monitors the security configurations of all hosts also in the production environment.

- **Use ArcSight to manage and correlate data from multiple sources and provide high-value information on security events in the MDC**. It pulls all of the above together for management reporting, monitoring and especially for the Security Alert center.
  - ArcSight looks at Firewall Logs.
  - FireMon compliance checks
  - IDS sensors
  - Unix Syslogs
  - Windows Event Logs
  - Host Configuration Data (ESM/ECM)
  - Host Vulnerability Data (Lightning Scanner)

Future Technologies to be implemented

- Intrusion Prevention systems(IPS) to replace traditional Intrusion detection systems.(IDS)
- SSL prevention systems to provide more secure access to web-enabled applications for any client platform.
- Legacy applications adapted to the model through the use of Citrix/terminal servers.
- Microsoft's ISA server performs application-layer firewalling for supported protocols
- Dedicated Windows Domain infrastructure for MDC's that ensures user separation from back-end systems.
- Finally an externalized directory to complete the internet-facing model.

Putting this all together we get the following diagram:

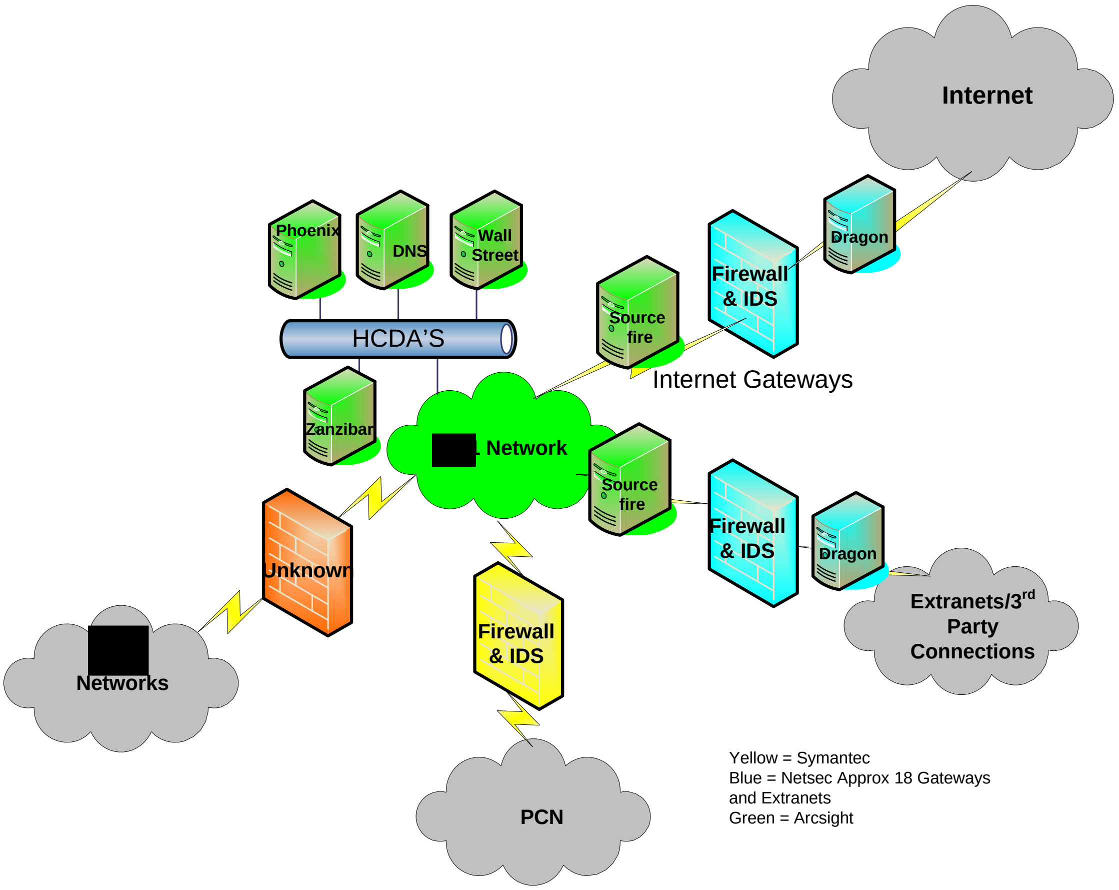


Diagram 5 – A simplified view of the company network architecture.

Some explanation is necessary. There are 5 groupings of portioned networks in keeping wit the Jericho philosophy:-

1. Internet with externalized desktop. {Dragon is an IDS system used for general IDS sensors}.

2. Extranets for third party access and collaboration. Between the internet and the extranets there are approximately 18 Gateways with Dragon ISA sensors operating in each one.

3. Highly Critical VPN like networks for critical applications like SAP, Wallstreet. Zanzibar is a Web-enabled purchase to pay software system that has been successfully implemented in the UK.

4. The PCN (process Control Network) partition uses Symantec firewalls and IDS systems. These are manufacturing and plant computerized control rooms that interconnect to the main company networks.

5. The unknown partition represents a group of unknown interconnections from some of the new acquisitions that the company has not yet analyzed in terms of requirements and company fit with the new strategy.

Virtual Server Architecture.

One of the radical new implementations started in parallel and to enhance the efficiency of the MDC's, was the idea to integrate standard Virtual Servers Architecture.

One of the radical new implementations started in parallel and to enhance the efficiency of the MDC's was the idea to integrate standard servers with networks and storage into a 'server farm" using software called VMWARE. Why is this important to meet the Jericho requirements? Attempting to externalize applications and de-perimeterise with over 1000 physical servers is not only difficult and complex, but adds additional security risk to the process of controlling and managing the network in a de-perimeterised world. So, this strategy is vital to facilitate better security controls for the MDC's and to control the externalized desktops and host applications externalized.

This allows the separation of application servers from specific physical servers, and as the number of 'virtual servers' is far greater than physical servers, it is possible to run multiple application servers, even with different operating systems, for example Linux and Windows, on each physical server. The CPU (central processing unit) of a physical server is typically just 5% utilized at any time (according to Chris Hammans Feb 2006– VMWARE Technical Director). Using "Virtualization" increases CPU utilization. Only 60 UK companies have attempted this so far including this company. They all are FTSE100 companies. (Financial Times Stock Exchange 100- similar to the Fortune 100).

The benefits have been staggering:-

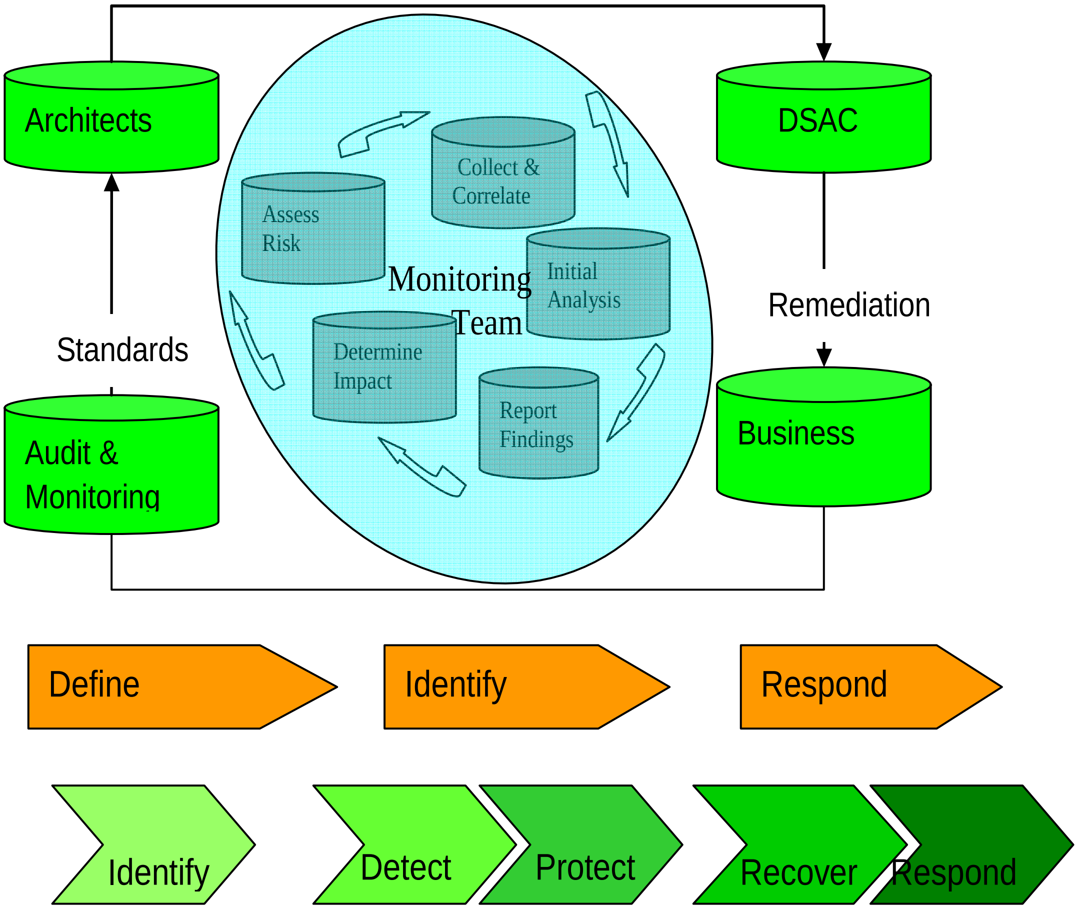
1. Reduced physical servers. Previously, within a MDC, applications would typically run on 800 physical servers, now with virtualization only 35 virtual hosts are necessary; this has greatly reduced the expensive floor space of a data center.
2. System reliability has increased and the ability of the company's systems has allowed them to respond quickly to changing business demands. Because application servers are effectively hosted on a shared infrastructure, they can now be moved form place to place with relative ease and without downtime for the business.
3. Managing Pooled Resources. This has allowed system administrators to manage pooled resources across the company, again allowing theme to respond to changing business needs.
4. Disaster recovery capability has improved. Virtualization has allowed the company the ability to restore full service from a hot site that shadows the virtual systems; there are fewer servers to cut over to.

Security Event Management (SEM)

Also being implemented was a new service called Security Event Management or SEM for short. To best describe this service the following Diagram 5 below shows the architecture for this service. There are 3 life cycle phases shown below, define, identify, respond and all require technology, processes and people.

In the blue space, there are currently 3 solutions being offered, ArcSight (already discussed) Symantec and Netsec/Verizon. There is some question about consolidating this, but this is in keeping with using multiple vendors and not locking the company into a single vendor. It may make sense later to rationalize this strategy, using just two vendors, ArcSight and Symantec. There was however, some discussion of whether to outsource this service; at the time of this case study, no decision was taken. This service is currently embedded with the Digital Security Alert Center (DSAC).

<u>Diagram 6 – SEM or Security Event Management Process</u>



Most of this process above has been automated using ArcSight to manage the Lightning scanners, FireMon integrity systems for all firewall environments, Dragon and CISCO IDS systems. The Monitoring team shown is a small staff for analyzing the information and liaises with the DSAC (Digital Security Alert Center) team. They sit at the core of this process. They are responsible for identifying the threats, vulnerabilities, detecting and alerting the businesses and operations, respond by coordinating all vulnerability patches and consulting with the incident and crisis management team for fixing incidents when they do occur.

This process plays a major role in supporting and providing information to the audit and monitoring team who are responsible for conducting assurance and IT audit both internally and for external compliance purposes.

<u>Analysis & Conclusions</u>

One of the goals of this paper was to examine a company implementing the Jericho model and compare its strategy and implementation to the 11 Commandments. The analysis will focus on these and the main question to ask is:

Did This Company satisfy the 11 Jericho Commandments?

- **Firstly the Security Basics**. **<u>Commandment one</u>** states that the scope and level of protection should be specific and appropriate to the asset at risk. This company satisfies this by:
    - Allowing individual systems to protect themselves and externalizing desktops is crucial to this. Host Hardening was prevalent and whilst this company is still on its journey, they should achieve most of this by mid 2008 by accelerating the implementation of the remaining desktops. To date, 40,000 desktops have been externalized out of 95,300. However the company accepts that because some of the legacy host systems cannot be externalized, some 17,250 desktops will require to be left in the old perimeter-based network.
    - In addition, solutions must be cost effective. This company certainly demonstrated this with their ACE strategy, savings of between $70m and $117 m per annum. (Table 6 pages 48 & 49 for the business case). Cost information was not available for the MDC consolidation and subsequent implementation of supporting security tools and systems, but anecdotal evidence suggests that with just 4 Mega Data Centers versus 20, the business case would have been extremely powerful and beneficial; otherwise approval would not have been granted to implement. In addition, the substantial reduction of physical servers

from 800 to 35 virtual hosts would have staggering cost reductions. (Not available for this paper).

  - Digital assets were identified and managed by their risk categories with security provided according to risk category. This was demonstrated in both strategies; host hardening and MDC.

- **Commandment Two** deals with the need to simplify and reduce complexity. An international, very large public company such as this company, will have difficulty to truly simplify; this is a value judgment concluded by looking at the number of vendors used and the share volume of tools, from Symantec to ArcSight; in addition the need to still keep some of the legacy systems which cannot be moved externally until their useful lives are ended, will add cost and complexity in the medium term.
- The **Third Commandment** states that "You assume context at your peril", i.e. one design in one country and one culture may not transfer for whatever reason to another country or culture. Additionally Jericho states that not all security designs are transferable from one environment to another. International companies such as this one tend to implement strategy globally; from a business perspective, an international company cannot do otherwise because of the share cost and dynamics to attempt to differentiate in the IT arena. "Bits and Bytes are Bits and Bytes"; it is not like a marketing situation where a company is attempting to do product differentiation because of different country tastes and cultures. No evidence was provided to support this particular commandment. This paper does not agree with this particular commandment; implementing computer technology in a standardized way has nothing to do with country or cultural characteristics, digital tends to transcend borders, it is how you use technology in a specific place that becomes a cultural aspect.

  This paper challenges the necessity of having this commandment, based on our case study and how companies implement security policy and standards.

- Commandments four and five concern ‘surviving in a hostile world’ and the first **commandment number four** is about communicating policy on untrusted networks.
    - This company has spent considerable time and money considering security, it was never an after-thought or add-on; a new and separate Information Security division was created in December of 2003. Also clearly demonstrated was the way the security architecture was implemented for the MDC’s including the provision of new services like SEM, the Security Event Management system and the consolidating of physical servers to virtual server farms. For host externalizing, it was also a carefully considered part of the business case. Why? Because to externalize desktops onto the world wide web makes a bold statement of “Trust” and a belief that sooner rather than later the security world will agree a common “Trust Model”, one does not exist presently. This was seen as truly radical in the business world and anecdotal evidence suggests that only 3 other companies have attempted to do this.
    - Encryption was also used extensively but based on the HCA’s or High Critical Assets, it was not implemented ‘everywhere’; cost was also a big driver here. This was evidenced in their network portioning (Diagram 5 page 55).
- **Commandment number five** is again about devices maintaining security policy on an ‘untrusted network’. Externalizing desktops and moving security to host applications has certainly demonstrated this, especially the rush to implement wireless technology, the security of which is still being developed. Why? Because wireless technology still does not have the security as with hard wired systems, it is improving. When one considers that an employee with an externalized laptop sitting in an open cyber café connecting to

his company's network using unsecured wireless, it is a testament to the trust the company has in its host and network security, i.e. attacks and threats can be dealt with.

  - In addition, Security Policies and Standards were developed using their SEM (Security Event Management) system, and the company has implemented an overarching Governance Framework (COBiT) Control Objectives for IT and related technology which is the controlling framework for ISO17799 Information security (used for security standards and policies) and ITIL for IT service delivery and support and finally Six Sigma for IT Procurement processes. These are al trusted frameworks.
  - According to Jericho, any device must be capable of serving on the internet without breaking; this company has demonstrated that with its radical ACE system. Anecdotal evidence suggests that there are more desktop problems and security violations and attacks on internal perimeter based systems than the ACE systems. The company would not release an analysis of its attacks, threats or vulnerabilities, except to give an example of a bad Trojan attack in 2006 which affected only 43 desktops; all of them were on the inside, perimeterised system. Regarding the application externalizations that have taken place, it is too early to form a final conclusion; the company is still on its journey.

- **Commandment number six** states that all people, processes, technology must have declared and transparent levels of trust for any transaction to take place. Jericho has never been clear about this particular commandment, especially in the use of the word Trust as it has different meanings for different people and organizations, especially as the old model of 'trusting only people inside the perimeter' has been shown not to be true anymore as business relationships have changed.
  - This paper concludes that this company has followed this wholeheartedly with its Host hardening and desktop program but less so with its networking program.

Diagram 4 showing the new company partitioned network moves some way towards this but not entirely, as for example third party access is still somewhat segregated, suggesting that trust can be advanced only so far and more importantly that it requires standardized vendor products to assist this which is still not yet developed.

- **Commandment number seven** states that Mutual assurance levels must be determinable. This has never been clear so no firm conclusions can be made here.
    - This commandment is linked to the last one and there was no evidence that a 'trust model' exists, there is substantial evidence of security authentication and authorization processes as was seen in the SEM model, the MDC security architecture set up, the new ID management and SSO (Single Sign On system) with a new data classification system. These systems were revised and enhanced to cater for externalization and 'living on the web', but the 'trust' concept is still not clear.
- **Commandment number eight** states that Authorization, accountability must interoperate/exchange outside of your locus/area of control.
    - Again the concept of Trust is linked here and this commandment is partly adhered in the way the company allows access to its systems and data in the new partitioned network.
    - The systems also only supports one person/system/identity but with multiple instances. The introduction of a new ID management system with SSO is evidence of this but it is not complete.
    - Whilst encryption, digital certificates, security smart cards and tokens meet some of this, the ability to make access rights a temporary component was not clearly demonstrated nor the ability of the system to truly pass on security

credentials/assertions has not been demonstrated simply because the ‘trust model’ technology is not fully available. This is a longer term fulfillment.

- **Commandment number nine** states that access to data must be controlled by security attributes of the data itself. This and the next two commandments deal with Data, its access, privacy, authentication, storage and security.
  - Encryption with the new network partitioning, firewall/IDS systems was implemented, so this supports this particular commandment except for the concept of holding security at the individual data level.
  - This is new and quite a radical concept, as it is difficult to hold security attributes at the data level itself. There is evidence of holding these attributes in separate system, (refer to the ArcSight Management system) which goes somewhere to meeting this requirement. Again, the technology is not yet developed to do this. Companies still are using traditional methods of data storage, access and recovery. Control and security is put in the storage device and/or access method but not in the data itself, this is a longer term vision of Jericho.
  - The ability to handle data classification was demonstrated by their new data classification system; however this system was not integrated into the access and ID management control systems as yet, so this part of this commandment is considered not yet met.
- **Commandment number ten** states that Data privacy and high value security assets require segregation of duties and privileges.
  - This commandment was clearly complied with as the company partitioned their network based on HCA’s or high critical assets, diagram 4 clearly showed that. Segregation of duties was also implemented both at application level by use of application security profiles and SOD (segregation of duty) violation reports used

in ERP systems like SAP. And in the way developers and data base administrators have been segregated in terms of their access to systems.

- **Commandment number eleven** states that data must be appropriately stored and secured either at rest, in transit or in process.
  - There was no information on what this company's strategy was regarding its data storage, indeed a workable data retention policy, which is important to meet this commandment was absent. The company was keeping for forensic and legal e discovery requirements almost everything its storage capability would allow. For example, email was kept for everyone for at least 3 months, including instant messaging data and streaming video and other media.
  - This is expensive and unnecessary. A functioning data retention policy and system should be implemented and integrated into the technology changes the company had made. What this means is that the data classification system has not been extended to fully working data retention. It is important for the company to understand what it needs to keep, how long, who needs access to it. This in turn would dictate the technology and storage capacity required.

Final Summary conclusions about the company and where it is on its journey.

Some final and general conclusions about this company are necessary.

This paper has demonstrated that overall, this company is well underway to meeting the Jericho objectives. One conclusion is about the concept of de-perimeterisation, perhaps this is not the correct term to describe what they have implemented. They have partitioned their network based on the criticality of their assets, one of the first companies to use virtual server architecture, enhanced their security control with standardized, centralized security control systems (Re SEM), consolidated their data centers and most impressively and more radically than most companies they have externalized most of their desktop and host systems. When one compares what they have done, the only commandments that they don't meet fully are those surrounding data management and architecture, trust models and complexity. In their attempt to devolve accountability to several vendors, they in fact may have complicated the process in terms of the share volume of tools and vendors used. This paper would recommend that they attempt to simplify this.

Overall Conclusions

This paper set out to tell the Jericho story about de-perimeterisation and hardening the host; what it is, the issues and most importantly it attempted to make a case for it not only by showing how it can be implemented but more importantly by examining a large international Fortune 100 company as it attempts to implement the Jericho model. There are however some overall conclusions that must be drawn out here:

Jericho Concepts themselves.

Firstly one must conclude that some of the commandments and language used by Jericho is confusing, not only that but a lot of it has been touted as "radical new ideas".

This paper believes that de-perimeterisation is perhaps a misnomer, what we have evidenced in our research is not so much de-perimeterisation but a 're-configuration of networks' then re-perimeterisation based on partitions which were based on the criticality of the digital assets managed.

This is certainly not radical as many companies in their attempt to use the internet effectively are doing this, what Jericho seemed to be suggesting to some is that you don't need perimeters at all or in the case of some authors, no firewalls. (Abe Singer – Security Wire Daily News 5th Jun 2006) This is truly misleading and not what was meant or intended by Jericho; as Nick Bleach explained in his conference. when he explained that to reconfigure means de-perimeterisation then re-perimeterisation as was seen by the company we examined.

The second conclusion is about host hardening and externalizing desktops. This is truly radical and apart from a few companies that this paper knows of, not many other companies are attempting this; it requires the right management commitment, technology and investment. Living on the web requires tremendous host security and trust. It requires that vendors move their applications to the web, it requires a ‘paradigm’ shift in the way applications are implemented and managed, this is certainly outside the scope of this paper.

The third conclusion is about the ‘commandments’ themselves. The language used was similar to that used in the Bible, i.e. “one must do this”. This paper would like to suggest that Jericho makes proposals and suggestions, i.e. “One should do”.

Finally, it is the conclusion of this paper that some of the commandments a) should not be commandments and b) cannot be achievable until digital technology allows it to happen.(for example our issues of an agreed Trust definition and model) Jericho has been forthright already in stating this as was shown in paragraph 2 and 3. For example as was outlined in commandment number 3, “assume context at your peril” should not be a commandment, it is stating the obvious. Any company with good security and risk management in place will by default take this into consideration.

REFERENCES

- www.opengroup.org/jericho - White paper February 2005.
- SC Magazine article; April 2006 by Ron Condon; "New Rules for Collaborative and mobile working".
- Chris Hare Paper 131 –"Improving Network-Level Security through Real-Time Monitoring and Intrusion Detection". February 2005.
- Abe Singer – Security Wire Daily News 5th June 2006.
- CSI/FBI 2006 Computer Crime survey.
- Trend Letter 2007 Volume 26 on Web technology.
- www.opengroup.org/jericho - Jericho Forum Commandments
- Hand Held security – MS TechNet "Deployment of protected 802.11 Networks using MS Windows. www.microsoft.com/technet/prodtechnol/winxppro/deploy/ed80211.mspx) and (www.symbol.com/products/software/msp.html).
- Motes –Emerson Wireless Measurement devices www.emersonprocess.com/home/news/pr/610_smartpack.html)
- Network Access Control Systems - www.cisco.com/en/US/products/ps6128/index.html; www.rohati.com; www.appliedidentity.com)
- Personal VPN's - www.witopia.net; www.openvpn.net
- Location Awareness Systems - www.loki.com; www.multispectral.com
- Encryption & New Open Source Systems - www.freeigma.com
- New Firewalls - www.watchguard.com

GLOSSARY OF TERMS

ACE – Advanced Computing Environment

Active x - ActiveX is a series of high-level, Internet/Intranet technologies Microsoft introduced in late-1990. The term ActiveX itself is seldom used today, and many of the technologies were rendered defunct or renamed, but some are still in wide use.

Altiris - Altiris is a provider of IT service-oriented management software, enabling IT asset management, network security management

B2B – Business to Business Network.

Blade Server - These are self-contained computer servers, designed for high density. Whereas a standard rack-mount server can exist with (at least) a power cord and network cable, blade servers have many components removed for space, power and other considerations while still having all the functional components to be considered a computer?

CISCO – This is the leading supplier of networking equipment & network management for the Internet. Products include routers, hubs, Ethernet

CITRIX – A major supplier of remote desktop solutions, Single Sign On and VPN systems.

COE – Common Operating Environment

CPU – Central Processor Unit

EAL – Evaluation Assurance Level (Common Criteria assurance for computer products)

EDI – Electronic Data Interchange

Ethernet – This is a large, diverse family of frame-based computer networking technologies for local area networks (LANs).

FTSE – Financial Times Stock Exchange

GLBA – Gramm Leach Bliley Act for banking, insurance & financial security & privacy.

HCDA – High Critical Digital Assets

HIPAA – Health Insurance Portability & Accountability Act

IAM – Identity & Access Management.

IDS – Intrusion Detection System

IIOP - Internet Inter-ORB Protocol. Developed by the Object Management Group (OMG), to implement CORBA solutions over the World Wide Web.

IOS- Cisco IOS (originally Internet work Operating System) is the software used on the vast majority of Cisco Systems routers and all current Cisco network switches. IOS is a package of routing, switching, internetworking and telecommunications functions tightly integrated with a multitasking operating system

IP- Internet Protocol

IST- Information & security Technology.

ISA Sensors – Industry Standard Architecture sensor.

LDAP – In computer networking, the Lightweight Directory Access Protocol, or LDAP is a networking protocol for querying and modifying directory services running over TCP/IP.

MDC – Mega Data Center

Meta Data -Metadata has multiple definitions, the briefest of which is "data about data." It can generally be thought of as information that describes, or supplements, the central data.

MOTES - Emerson wireless measurement devices (aka Motes).

NAC – Network Access Control.

Needham-Schroeder – The term **Needham-Schroeder protocol** refers to one of two communication protocols intended for use over an insecure network, both proposed by Roger Needham and Michael Schroeder in a paper in 1978.

Ontology – Configuration

P2P – Peer to Peer network

PCN - Process Control Network; mainly manufacturing computer control processes.

PDA – Personal Digital Assistant

PKI – Public Key Infrastructure used in Encryption technologies.

Portal- This is a site on the World Wide Web that typically provides personalized capabilities to its visitors, providing a pathway to other content.

Proxy Server – This is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. It works like a type of firewall.

SD - Secure Digital cards about the size of a finger nail which is used in mobile phones to automatically encrypt all voice and data calls.

SAML - Security Assertion Markup Language (SAML) is an XML standard for exchanging authentication and authorization data between security domains, that is, between an *identity provider* and a *service provider*. SAML is a product of the OASIS Security Services Technical Committee.

SEM – Security Event Management

S/MIME - (Secure / Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of e-mail encapsulated in MIME.

SOAP - Simple Object Access Protocol is a protocol for exchanging XML-based messages over computer networks

SOX – Sarbanes Oxley

SSL – Secure Socket Layer, an application encryption system used on the internet.

SSO – Single Sign On.

TCP – Transmission control protocol

Virtual Network - Virtual Network Computing (VNC) is a graphical (GUI) desktop sharing system which uses the RFB (Remote Frame Buffer) protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network. It is platform-independent and works wit most operating systems.

VOIP – Voice Over Internet Protocol.

VPN – Virtual Private Network

WPA2 - Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless.

XML - XML is a markup language for documents containing structured information.

X500 - X.500 is a series of computer networking standards covering electronic directory services.

Zanzibar – Zanzibar is a Web-enabled purchase to pay software system.

802.11i - 802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology.

APPENDIX – JERICHO MEMBER ORGANIZATIONS

ABN AMRO Bank	HSBC
Airbus	**ICI**
Barclays Bank	ING
BAE systems	JPMorgan Chase
BBC	KPMG LLP (UK)
BP Plc	Lockheed Martin
Boeing	Motorola
Cabinet Office	National Australia Bank (Europe)
Cable & wireless	Pfizer
Credit Agricole	Procter & Gamble
Credit Suisse First Boston	Quantas
Deloitte	Reuters
Deutsche Bank	Rolls Royce
Dresdner Kleinwort Wasserstein	**Royal Mail**
Eli Lilly	RBS
Ernst & Young	
GlaxoSmithKline	**VENDORS**
Royal Dutch Shell	Symantec
Standard Chartered Bank	Cisco
The Open Group	Microsoft
UBS Investment bank	Cybertrust
UKCeB (Council for E-Business)	IBM
Unilever	NEC
University of Kent Computing	
YELL	
**** Red = Founders**	