

De-Perimeterisation

This Decades Security Challenge

Paul Simmonds

Global Information Security Director, ICI

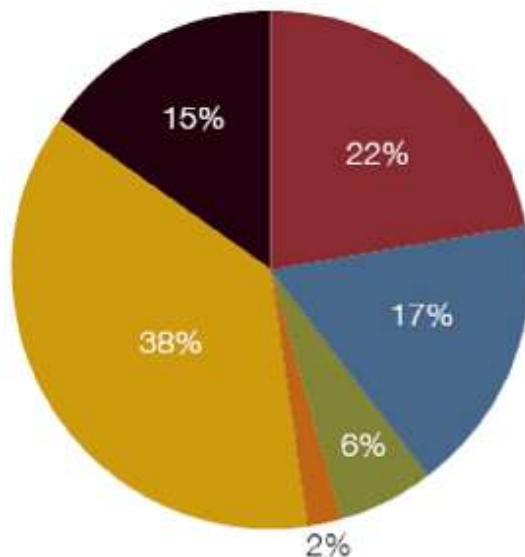
Background

- Everything is business driven
 - All projects must have a return on investment
 - Cost saving is the management mantra
 - Speed to market makes all the difference,
- Security
 - We are losing the war on good security
 - We let in both port 80 and port 25
 - The M&M Model is "old-hat" & non-sustainable,
We are too busy putting our fingers in the dyke walls to notice that the dam has already been breached.

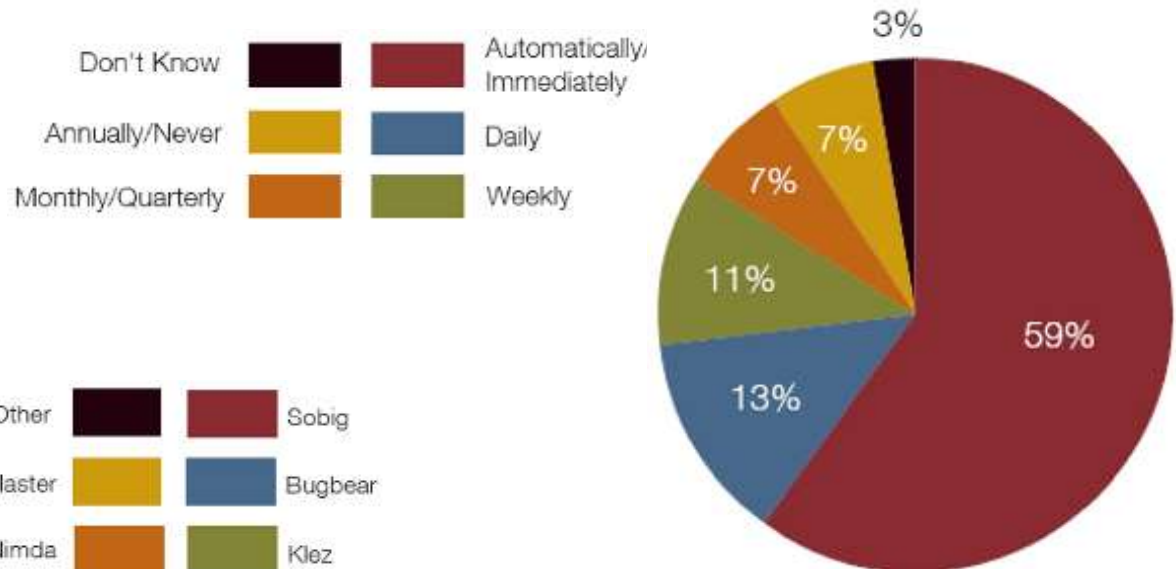
It only takes a single computer...

A majority of global corporates were affected by Blaster

Worst Virus Infection 2003



Frequency of Update of AV Software



- Around 30% of PC's at any point in time have ineffective AV
 - 2004 DTI Information Security Breaches Survey, Source: PWC (13% have no AV at all),
- It only took one Blaster (or Sasser) infected PC inside your network.

So much for the corporate perimeter

It's 11pm, do you know where your data is?

- Once upon a time, people were either staff or non-staff
 - Now there is every variant under the sun,
- Once upon a time we made no external connections
 - Now we connect to the Internet, to clients, to JV's to 3rd parties, to suppliers, to home workers
 - There is every way imaginable of connecting and of doing business
 - And there is every type of device, NAT boxes, Blackberry, Wireless Access Points and VoIP.

So its goodbye Data Security then?

Maybe what we actually need is a new model

- We are trying to protect the money
- So we pay £100,000 for a custom truck.
- Why not just protect the money ?
- So we pay £10,000 hi-tech money container.



IDS is dead – at the perimeter

Intrusion detection's permanent placement in the Trough of Disillusionment does not mean that it is obsolete. – Gartner

- Imagine a burglar at the railway station....
 - Can you spot them in the crowd?
- Now only screen the people coming up your drive
 - Still a lot of people, but each with a legitimate function
 - Can you spot them yet?
- So look for people trying your doors and windows
 - If you can exactly define permissible behaviour, then you can easily spot anomalies.

What is the new cost model?

Anything that's free is worth what you pay for it. Anon.

- Ballpark for a fully serviced Ethernet port with Internet connectivity is around \$20 / month
 - What's the true cost of your Ethernet ports?
 - Include – WAN, Border Security, Routers, Switches, Staff, Support, Cabling etc.
- Do you still need a border?
 - Maybe what we actually want is a sieve
 - And maybe a QoS boundary,

And this becomes an ROI justification only.....

There are also business benefits

Traditional Option

New Sales Office

- Design WAN extension
- Talk to WAN provider
- Negotiate with local PTT
- Install leased line or VPN
- Install encryptors and routers
- Install switch and private wiring
- Train local support staff
- Configure & commission LAN
- Install and configure local PC's
- Negotiate with local PTT for phone lines
- Install local exchange

Time to market ~ 1 to 6 months

Deperimeterised Option

New Sales Office

- Find fully serviced office with Internet connectivity
- Plug in PC's
- Plug in VoIP phones

Time to market ~ Days

Cost savings – Enormous

Manpower saving – Enormous

Security – Increased

Flexibility – Large

“Cleverness has never been associated with long delays”

Sun-Tzu, The Art of War c 400BC.

What de-perimeterisation is not . . .

- Simply removing your border security
- Removing / replacing your firewalls
- Just distributing your security devices inside
- A crusade against deep packet inspection
- Web Services
- Document repositories
- A distributed data model
- The elimination of IDS / IPS
- A sales opportunity

. . . . but it may involve all or some of the above.

So what is de-perimeterisation?

It's fundamentally an acceptance that;

- Most exploits will easily transit perimeter security
 - We let through e-mail
 - We let through web
 - Any encrypted traffic (SSL, SMTP-TLS, VPN etc.),
- IDS has little/no benefit at the perimeter,
- That it's easier to protect data the closer we get to it,
- That a hardened perimeter strategy is at odds with current and/or future business needs,
- That a hardened perimeter strategy is un-sustainable.

So what is de-perimeterisation?

It's a concept;

- It's how we solve the business needs for our businesses without a hardened perimeter,
- Its how businesses leverage new opportunities when there is no hardened perimeter,
- It's a set of solutions within a framework that we can pick and mix from,
- It's defence in depth,

OS Agnostic: Delivery on a platform / processor / screen size independent device, usually implies a high level language, compiles "on-the-fly".

And of course;

- It must be open, interoperable and OS agnostic.

Four Phases to de-perimeterisation

■ Phase 1

- **Now:** *Move outside the perimeter*

Move non-corporate items outside the corporate perimeter and enable Internet connected working,

■ Phase 2

- **Soon:** *Remove hardened perimeter*

Pervasive authenticated access, transport encryption,

■ Phase 3

- **Near Future:** *No perimeter*

Connection level authentication, data level encryption,

■ Phase 4

- **Future:** *Data Level Authentication*

Data inherently secure and will only operate in validated secure environments by authorised people.

Phase 1 - *Move outside the perimeter*

- **Move non-corporate items outside the corporate perimeter**
- **Deliver external services outside the corporate perimeter**
- **Enable Internet connected working for staff and 3rd parties**

Solutions

- Web Services facing Internet with services delivered by;
 - Standards Browser (Thin or Lean Client)
 - Browser Technology (Lean or Thick Client)
- Staff connecting via xDSL
- Security provided by SSL/TLS
 - Extra security provided by Java / ActiveX environment inspection, Radius, SecurID
- End-point security

Lean Client: Full OS with minimal application load, possibly just a browser.

Issues

- Secure use on non-secure computers (e-mail in Internet Café)
- Integration of authentication systems (SSO when web hosted).

Phase 2 - *Remove hardened perimeter*

- The border becomes a QoS boundary / cost justification
- The border acts as a sieve – blocking the “lumps” only
- Parts of business connect to systems needed directly via the Internet
- Connection to 3rd parties is direct (system to system)

Possible Solutions / Technologies

- All corporate network devices allow only encrypted protocols
- Authenticated tunnels make multiple “on-the-fly” connections
- Remote extensions are ad-hoc xDSL
- Remote / Home office use encrypted VoIP phone
- Islands of secure data / services, application - application transactions

Issues

- Availability of System and OS support for above solutions
- Open standards vs. closed / de-facto standards
- Ability to monitor and correlate security information from many islands
- Internal security of systems (patch and vulnerability management).

Phase 3 - *No perimeter*

- **Move from system level authentication, to; Connection level authentication, and Data level validation**
 - can't connection to server / data store if no rights to the data
 - If you connect you can only see those files to which you have rights

Possible Solutions / Technologies

- Databases with table level and cell level access/encryption
- On-the-fly authentication for;
 - Granular System Access, Tunnel Creation, Application Execution
 - External Access, Resource Usage
- Cross business authentication of credentials (that works and is open)
- Application level firewalls & IDS

Issues

- Need to classify data / Standards for data classification
- Systems that support data level validation
- Application that allow granular security
- How do I trust/validate external users or even outside my business unit.

Phase 4 - *Data Level Authentication*

Today

- **File on disk with file level privileges inherited from the file creator and container**
- Copy that file to another server
- New file has privileges based on creator and new container.

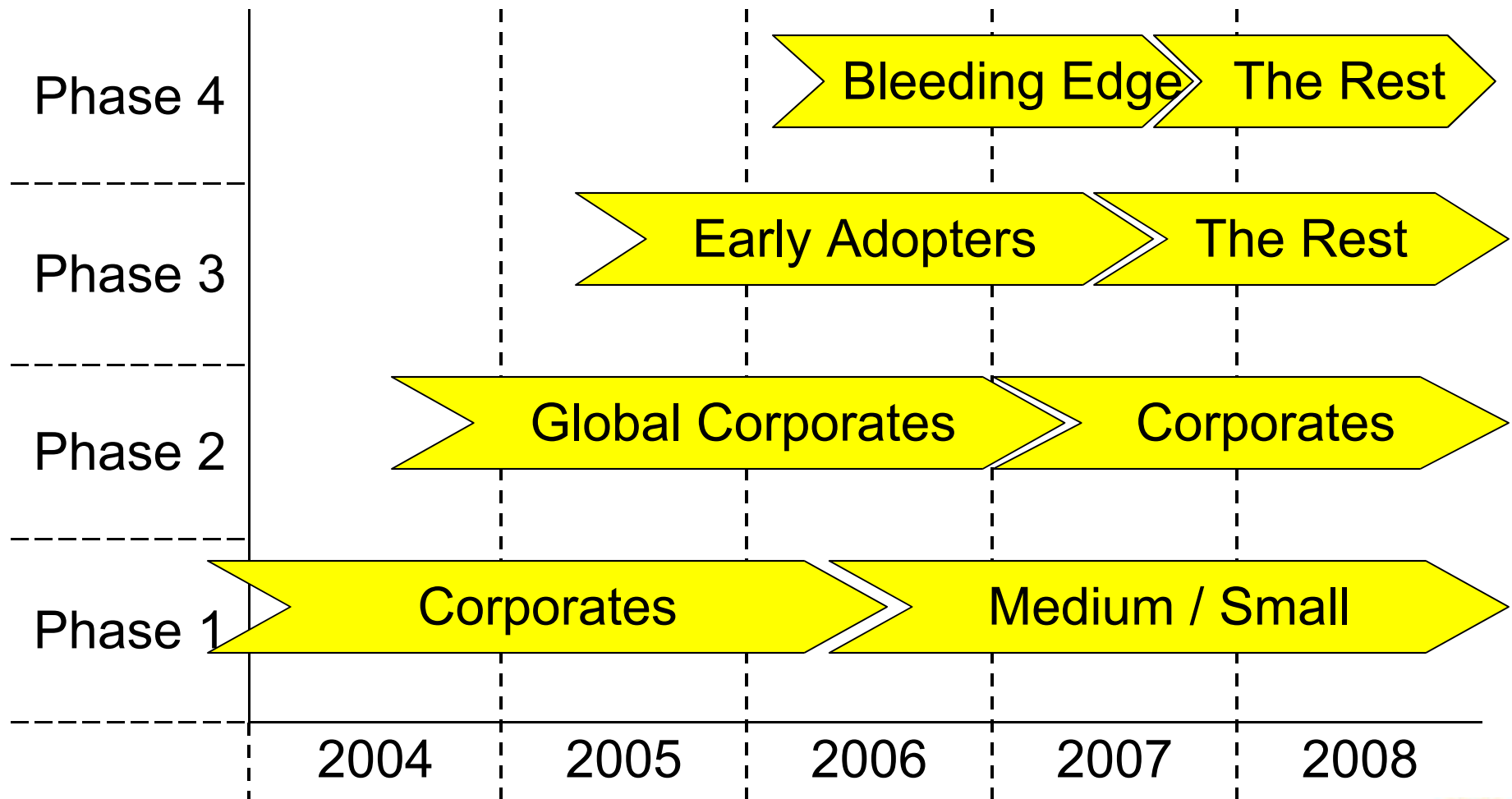
Issues

- Cross company (global) authentication
- All new application set
- Standards for data classification
- Provision of inherently secure data standards
- Provision of (open) validated secure environments.

Tomorrow

- **File on disk holds data that is encrypted with specified read and write privileges**
- Copy that file to another server
- Data has exactly the same read and write privileges as before.

So we can do this all tomorrow?



So do we just sit back and wait?

Let's review some of the issues . . .

- Patching and configuration management
- Standards for data classification
- Authentication
- Document level authentication
- Data lifetime and data expiry
- Multiple secure pipes
- Application level execution authorisation
- VoIP with VPN built-in
- Cross-enterprise trust and authentication,

How sure are we that the security / computing industry will deliver if we don't tell them what we want . . .

Jericho Forum

*So the people shouted, and the trumpets were blown. As soon as the people heard the sound of the trumpet, the people raised a great shout, and the wall [of Jericho] fell down flat, **Joshua 6, vs 20** ,*

What is the Jericho Forum?

- It's a group of like-minded corporates and organisations working on this new model
- It's hosted by the OpenGroup (<http://www.opengroup.org/jericho>),

Participants include;

- | | | |
|---------------------|------------------------------------|--------------------|
| ▪ Qantas | ▪ HSBC | ▪ Northern Rock |
| ▪ Airbus | ▪ Standard Chartered Bank | ▪ Unilever |
| ▪ ICI | ▪ British Broadcasting Corporation | ▪ Credit Agricole |
| ▪ BP | ▪ Geisinger Health System | ▪ Pfizer |
| ▪ Barclays Bank | ▪ The Open Group | ▪ ING |
| ▪ Goldman Sachs | ▪ Credit Suisse First Boston | ▪ YELL |
| ▪ Royal Dutch/Shell | ▪ Royal Bank of Scotland | ▪ Deutsche Bank |
| ▪ BAE SYSTEMS | ▪ UBS Investment Bank | ▪ Reuters |
| ▪ HBOS | ▪ UK Cabinet Office | ▪ Eli Lilly |
| ▪ Royal Mail | ▪ Rolls-Royce | ▪ Procter & Gamble |
| ▪ Clearstream | ▪ Boeing | ▪ DKW |
| ▪ GlaxoSmithKline | ▪ TRW Automotive | |

Jericho Progress

Jericho 2004 “to-do” list;

- ✓ Gather like-minded corporates and organisations
- ✓ Articulate the problem
- ✓ Put together a frame work for discussion
- ✓ Start the industry discussing the problem
- ✓ Cure European perception (engage with US companies)
- ✓ Meet to define problem scope,
 - Meet to road-map the issues (*August 26th 2004*)
 - Produce high-level, medium-level white papers (*Sept'04*)
 - Formally engage the vendors (*Fall '04*),

New;

- Resolve funding to ensure progress does not stagnate.

In closing . . .

The Jericho Challenge;

- Ultimately it's up to us . . .
- Stop designing insecure systems
 - Design systems to operate without a firewall
 - Design in security, don't paper over the cracks!
- Demand secure & authenticated protocols
 - Only open ports that support them, disable all others
 - Refuse insecure protocols,
- Understand the data flow and protocols
 - Test and validate all data
 - Authenticate all transactions.