# INTRODUCTION
# What is this *IDS strategic approach*

**Mostly, the phrase *strategic approach* is a license for *pinstriped* clad consultants to spout vague generalities with clauses like benchmark and envision.**

***As an alternative, This strategic approach focuses on the 3 key components Why, What & How.***

- ***Why** – Why should I initiate an IDS project*
- ***What** – What should expect in terms of benefit and cost*
- ***How** – How should seek to manage the process*

www.loud-fat-bloke.co.uk

# IDS & Security

Security is moribund with vague acronyms:-

## P.D.R.

PDR = Protection – Detection – Reaction

IDS works in the domain of *Detection*

This doesn't mean that it is somehow less important.

The faster and the more specific your *Detection* – the more efficient your *Reaction – the better your recovery*

www.loud-fat-bloke.co.uk

# Why do we need a strategic approach

Most IDS projects are perceived as failures. I would estimate at a rate of greater than 70%.

Why – three main risks for your project risk inventory:

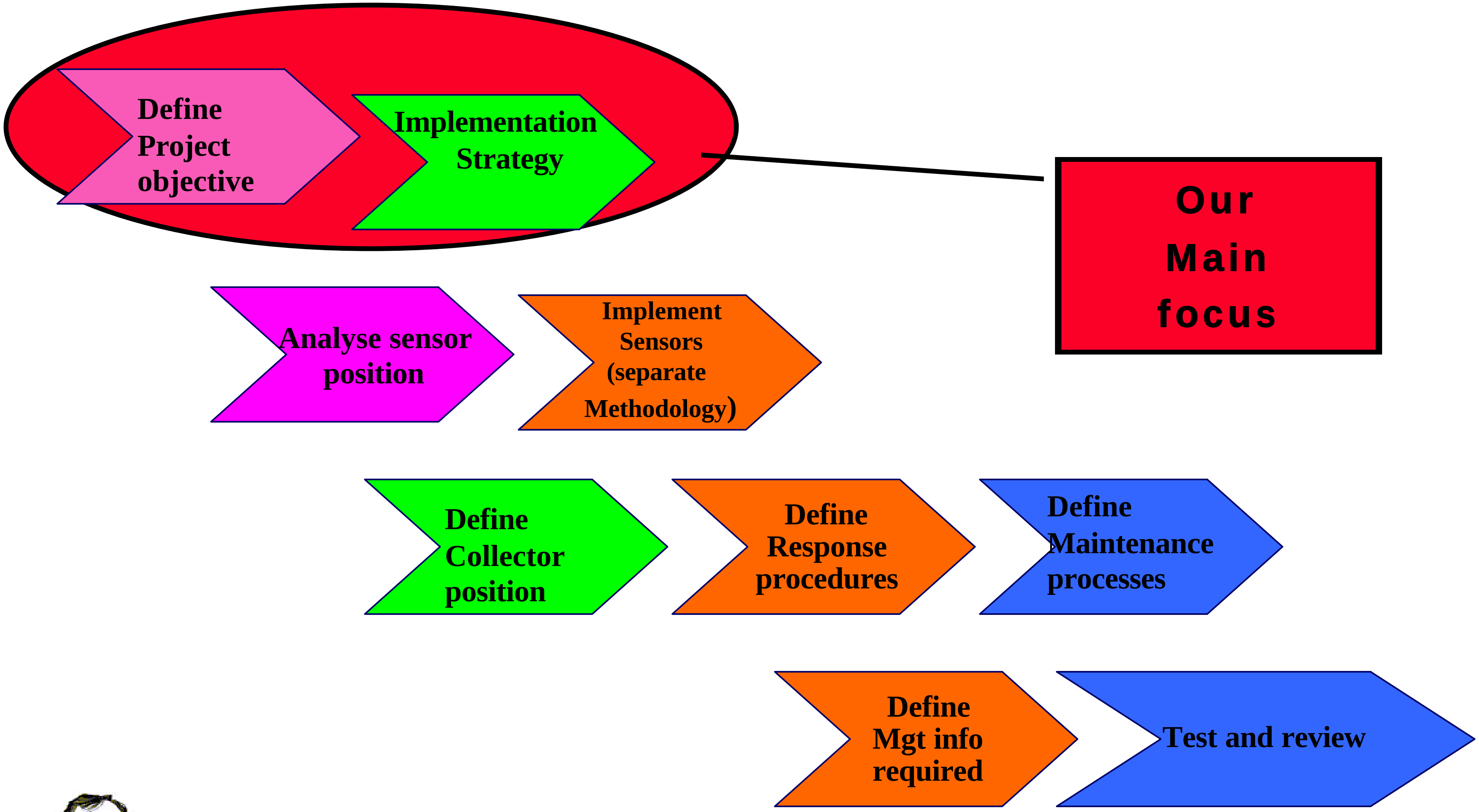
☛ The IDS technology worked but the management expections where completely off target – this type of project could never succede

☛ The technology is/has been sold as plug and play, so even if the infrastructure could be made to work – the project losses credibility and is scrapped before essentially tailoring is performed

☛ No organisational or procedural effects are considered, so the firms ability to deal with hackers isn't changed despite the effort and technology

www.loud-fat-bloke.co.uk

# Summary of stages


Define Project objective

Implementation Strategy

Our Main focus

Analyse sensor position

Implement Sensors (separate Methodology)

Define Collector position

Define Response procedures

Define Maintenance processes

Define Mgt info required

Test and review

www.loud-fat-bloke.co.uk

Define
Project
objectives

www.loud-fat-bloke.co.uk

# What an IDS project
# WILL NOT DO FOR YOU

**Intrusion Detection Systems -**

- **Do not improve poor access controls**
- **Do not replace the need for experts analysis**
- **Do not replace incident procedures**
- **Do not solve your log management headache**
- **Do not run themselves**

# What an IDS project
# WILL DO FOR YOU

**Intrusion Detection Systems can-**

- **Speed your response to security problems**
- **Fill large holes in a security/monitoring regime**
- **Enhance hack detection, analysis and recovery**
- **Solve your security log *<u>REVIEW</u>* headache**
- **Automate many manual processes**
- **Provide good management info**

www.loud-fat-bloke.co.uk

# Why start an IDS project

## Triggers for starting an IDS – stage 1

- Attacks volume overwhelms log review
- Focus of attacks changed
- Security more high profile
- Regulatory requirement

# Why start an IDS project

**Regulatory requirement**

**DEFINITE – HK monetary authority**
**singapore monetary authority**
**European central bank**
**Vague – requirement for *formal monitoring regeme***

- ☛ **FDIC**
- ☛ **FSA**
- ☛ **FED**
- ☛ **EBR**

www.loud-fat-bloke.co.uk

# Why start an IDS project

**Volume of attacks drastically increased**

- ☛ **size of logs too great for manual**
- ☛ **“cost” skilled staff too great**

## ***Supporting Stats***

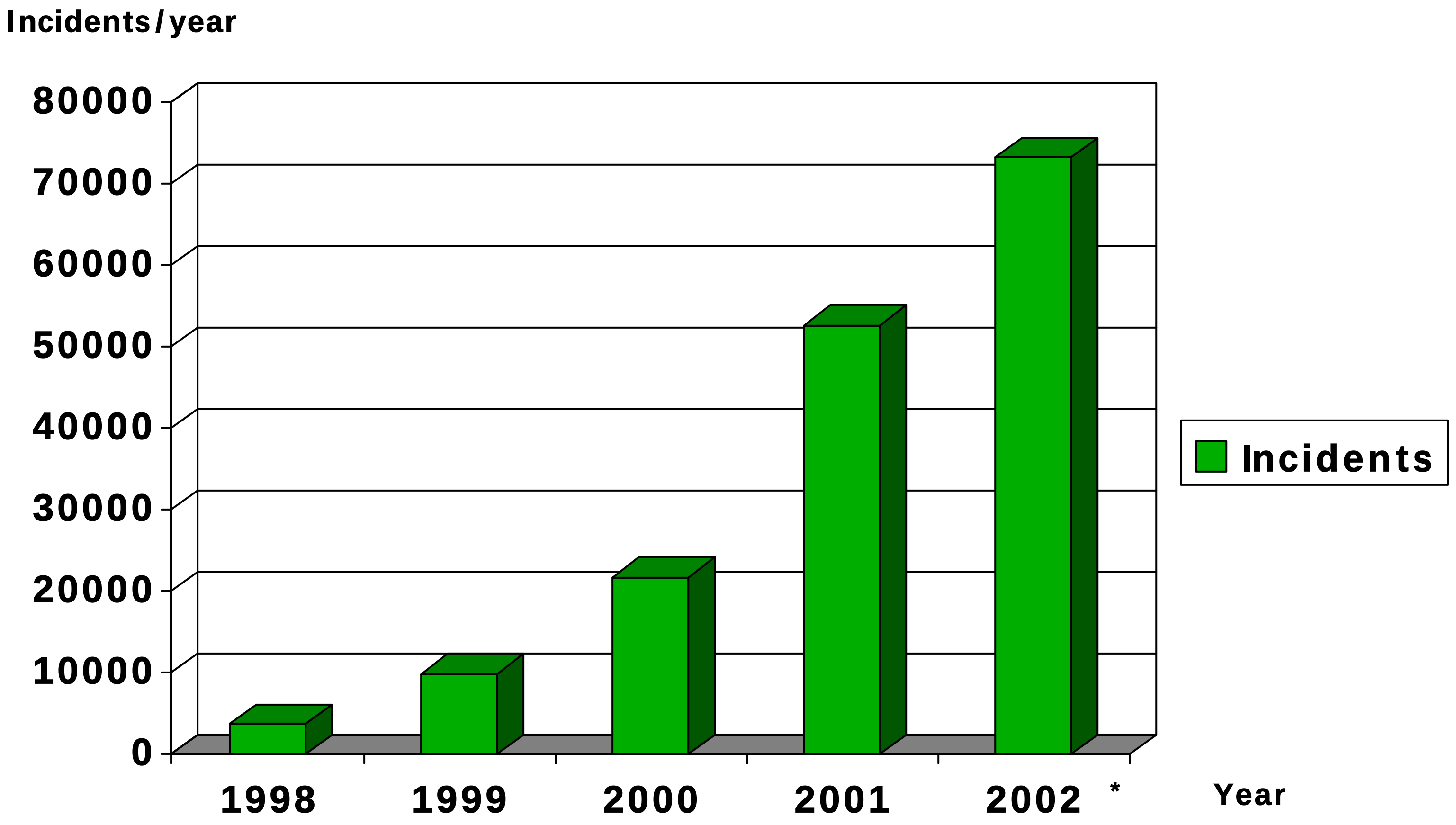
**206 Port scans/month**

**17 NBTscans/day** www.honeynet.org

**Firewall produces 100-500 mb/day**KPMG

www.loud-fat-bloke.co.uk

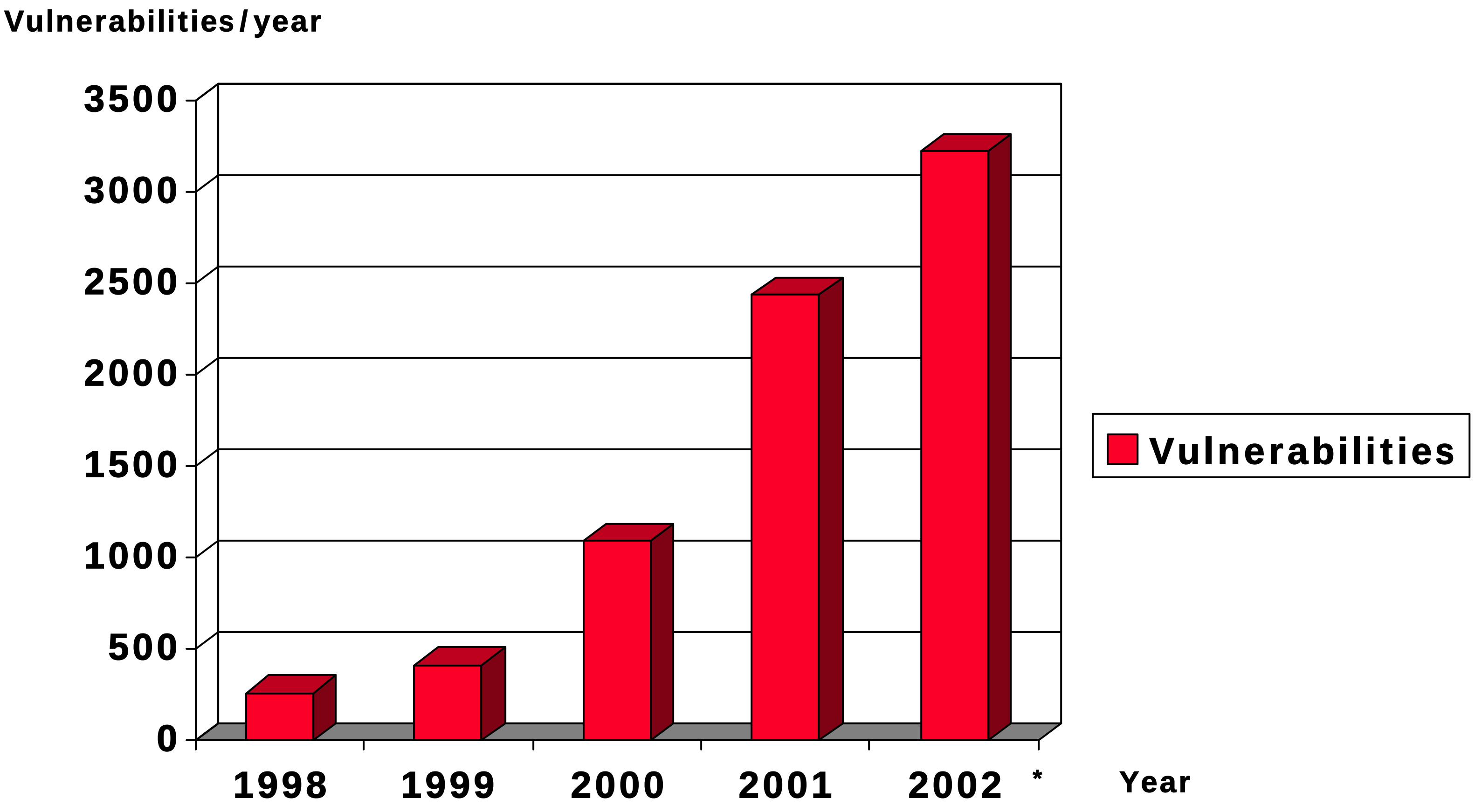
# Security vulnerabilities on the up



*** 2002 Figure for 3 of 4 quarters Source Cert/cc**

www.loud-fat-bloke.co.uk

# Security vulnerabilities on the up



www.loud-fat-bloke.co.uk

*  *Figure for 3 of 4 quarters  Source Cert/cc*

# Focus of attack changed

## Firewalls alone not up to the job alone

# I-spy with my little eye the 7 layer OSI

## Content attacks

Double-decode Hack

HTML print Hack

PHP Bugs

SSL / Appache

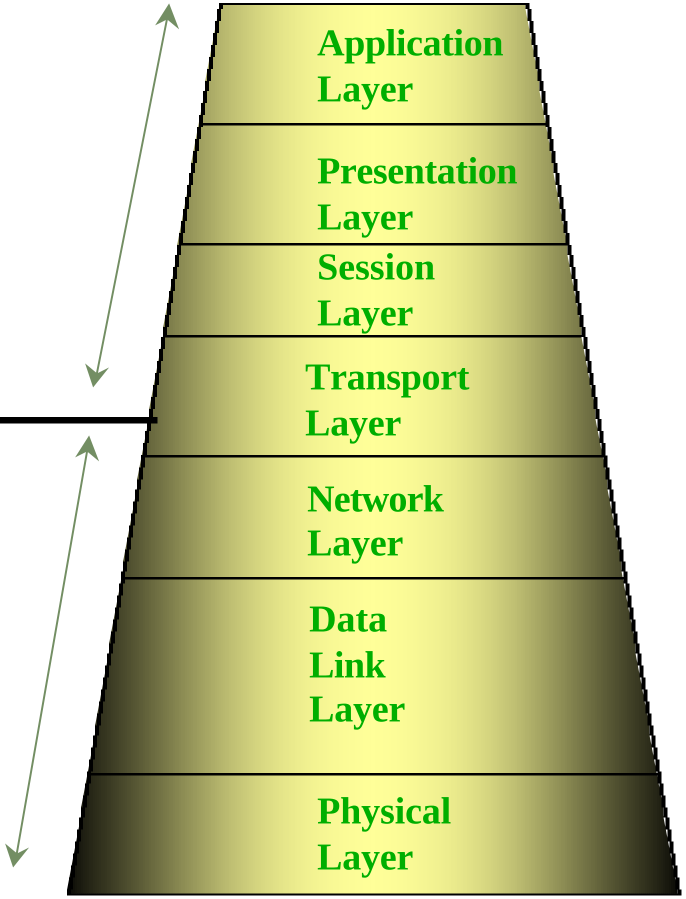
## Context attacks

Fraggle

Evil ping

Port Scan

Sadmind



Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

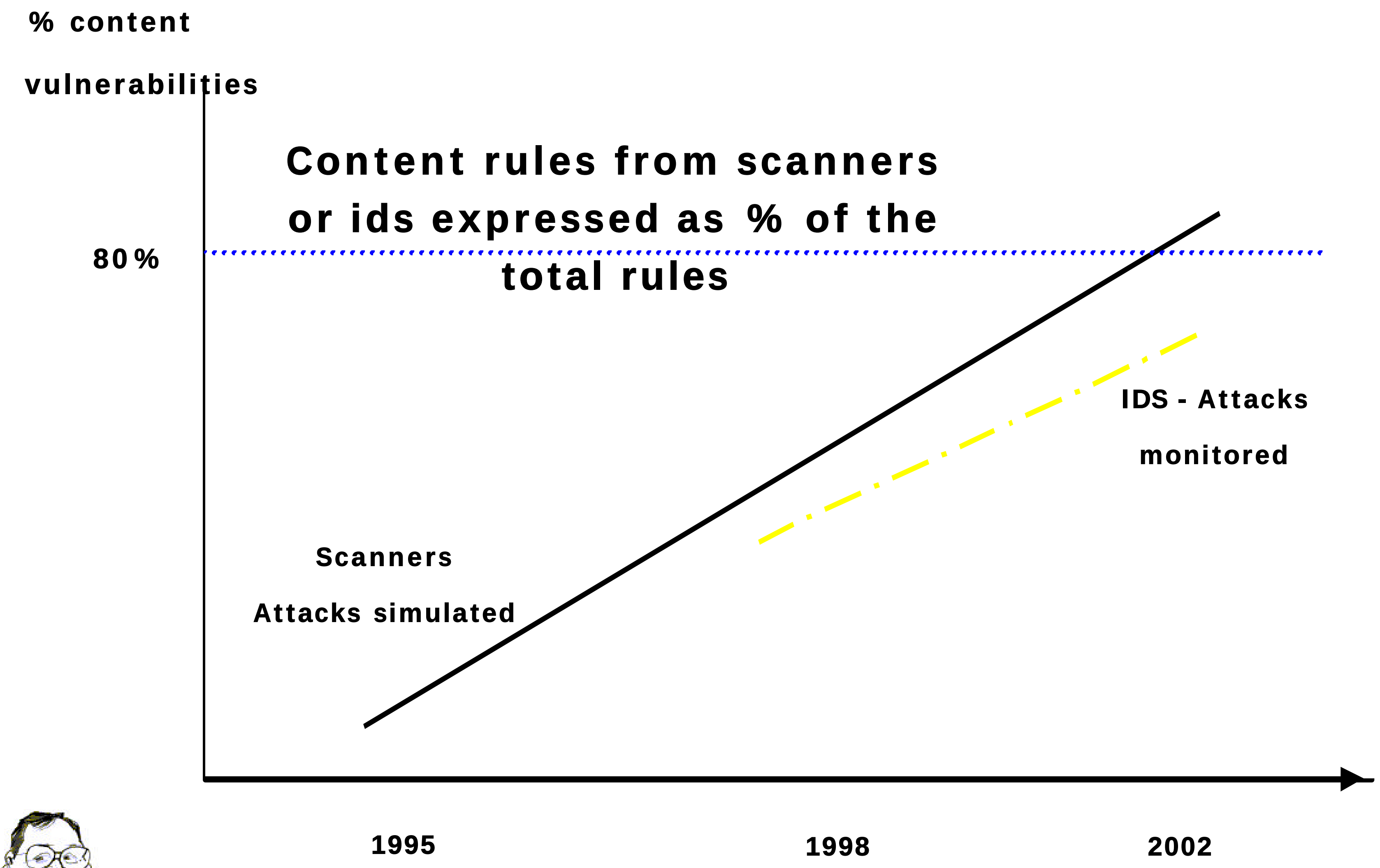
Data Link Layer

Physical Layer

7 layer osi model

www.loud-fat-bloke.co.uk

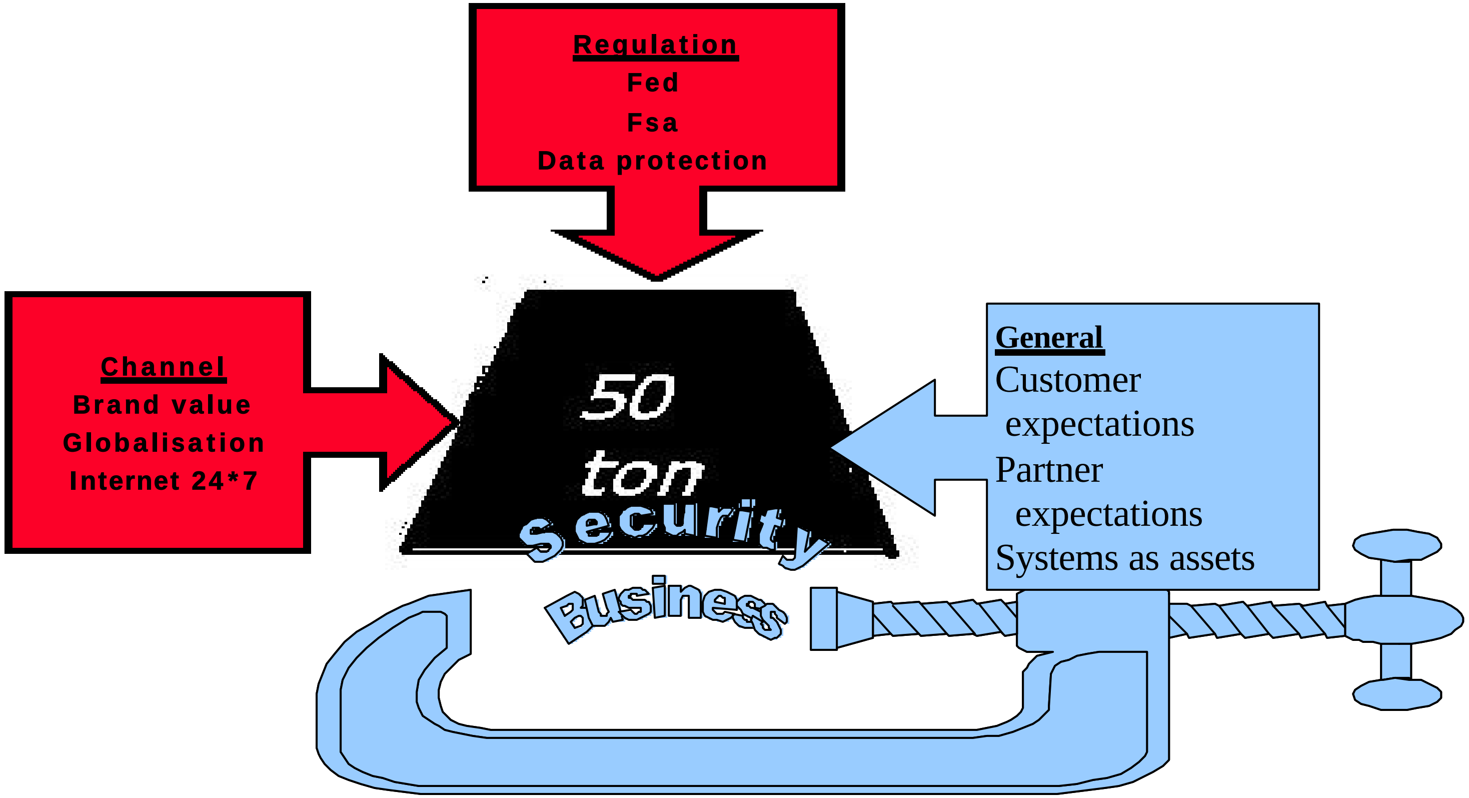
# Content attacks the Norm



Content rules from scanners or ids expressed as % of the total rules

www.loud-fat-bloke.co.uk

# Reasons starting an IDS – stage 1
# Security more high profile



**Regulation**
Fed
Fsa
Data protection

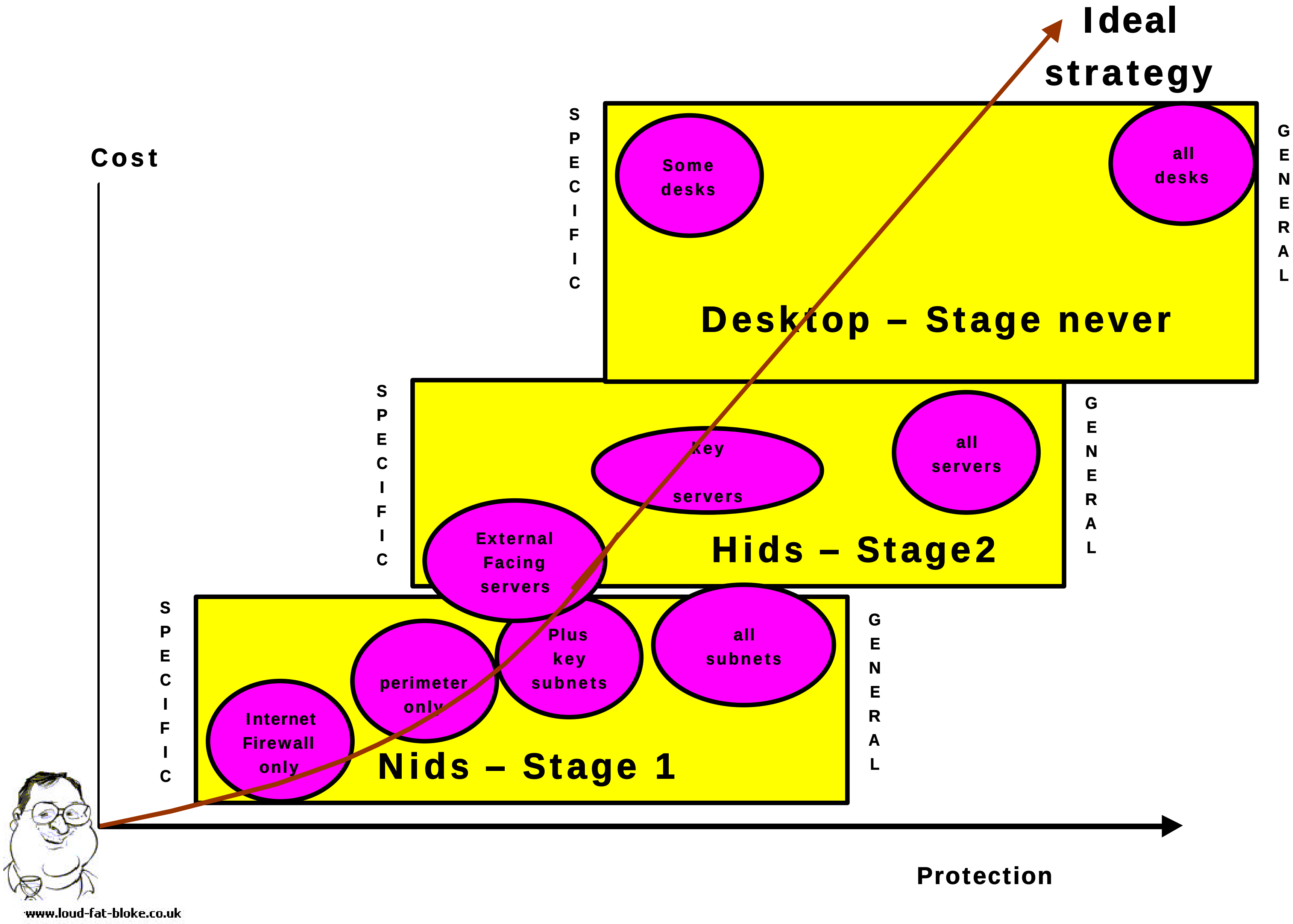
**Channel**
Brand value
Globalisation
Internet 24*7

**General**
Customer
 expectations
Partner
 expectations
Systems as assets

www.loud-fat-bloke.co.uk

# Implementation Strategy

# IDS maturity model



# Decide your final implementation level for stage 1

**Internet Firewall only**

A good starting place as traffic will be very simple

**Perimeter only**

Progress to all perimeter firewalls using the techniques learnt above

**Perimeter only + key subnets**

Beware of switched networks

# Stage 1 – Costs

☛ **Apart from software, stage 1 costs are low and tangible**

- Each sensor will require a decent pentium III,
- 2 nics with a 20 gig hard disk

☛ **Most IDS will only manage 10-20 sensors on 1 console/event collector**

- top of the range cpu preferably dual
- 768mb
- 300gb disk
- backup device

# Stage 1 – Benefit formula

There are many IDS cost/benefit techniques (check sans) – but here is a basic one for starters

Tangible cost reduction =

{k * "*staff cost of security log review*" }

+ *f* *("average cost of incident" )*

K = .90 = reduction in time spent reviewing your firewall logs

*F* = factor of reduced incidents

Av Cost of Incident £30k *(DTI/PWC 2002 Survey)*

www.loud-fat-bloke.co.uk

# Stage 2: Why step-up to host deployments

- Critical servers
- Exposed/shared servers
- Leaky perimeter
- Boot strap poor server security
- Protect old “green screen” type apps
- Poor internal security
- Hi internal threat

# Stage 2 – Costs

☛ **Apart from software, stage 2 costs hi and intangible**

☛ **a good HIDS will (often) require event auditing**

- Auditing often increases server cpu on unix operating systems by 10-15%
- The ids may add a further 5% on top

*how many of your servers have a spare 20% cpu & what is the cost of upgrade*

*Beware, if your IDS does not need c2-audit – it might just be doing file CRCs - NAFF*

# Stage 2 – Before buying a hids

- Would a state monitoring program serve you better
- Would an intelligent syslog program serve you better

# Analyse sensor position

www.loud-fat-bloke.co.uk

# Sensor position

Not rocket science but it is amazing how many people don’t define where. Consider:

- What you are protecting
- What OS or Network type is available
- What is the value of it

Implement

Sensors

# See separate methodology

## $$ Tipp $$

Run small packages of functional IDS units through a  cycle of  implement, test & tune policy -  then iterate the process for other locations and departments

This get results early-on in the project and provides evidence of the Projects success & success  before the inevitable performance or maintenance problems emerge

## See separate methodology

**www.loud-fat-bloke.co.uk**

Define Collector position

# See separate methodology

## $$ Tipp $$

All large IDS suffer from data problems.  Consider

•Who gets the data

•Who needs an IDS console and who need just alerts from TNG or OpenView

•How much data are storing – what are your top-10 events and do they represents over 60 percent of your data?  Is stored just to be on the safe-side or for forensic purposes?  If Yes get a management reporting product

See separate methodology

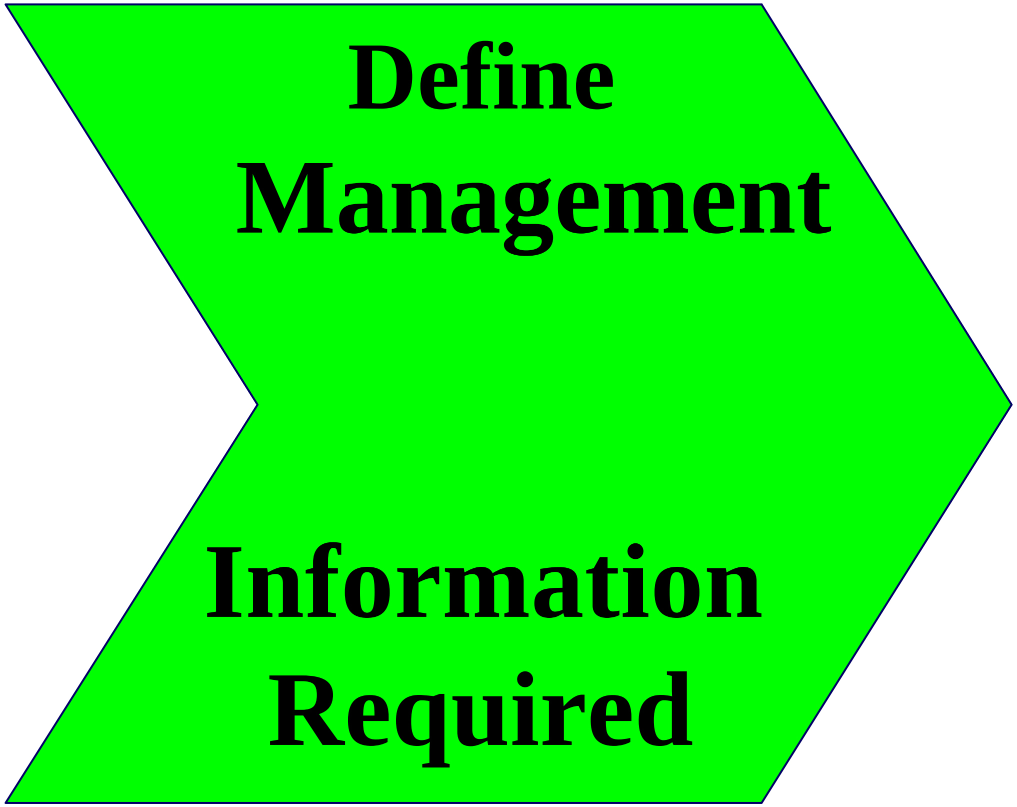
www.loud-fat-bloke.co.uk

**Define Response Procedures**

www.loud-fat-bloke.co.uk

See separate methodology

www.loud-fat-bloke.co.uk



Define Management

Information Required

# $$ Tipp $$

Getting a  large IDS project off the ground is difficult – But the there is no other subject that can provide such good press for hard pressed security analysts -

•Produce a few coloured graphs at the end of each project stage – to show all the hack attacks and unauthorised activity.  This demonstrates that the product is working.

•Produce an attacks against MailServer, Webserver and Firewall report – include it in your monthly or quarterly report to the audit committee.  Let them know that risks are really out there.

# Define

# Maintenance

# Processes

www.loud-fat-bloke.co.uk

www.loud-fat-bloke.co.uk