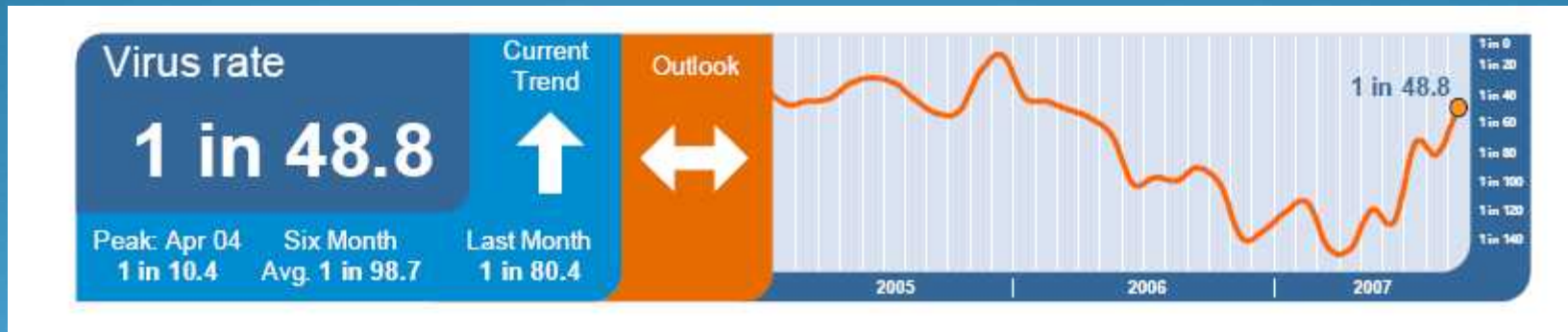
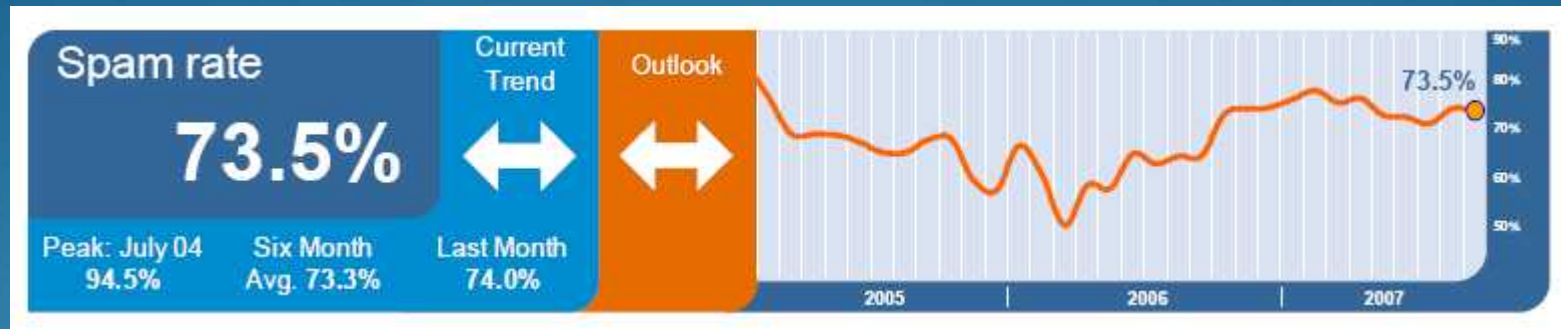




# Managing E-mail SPAM

*The Digital Ship Conference - Athens - Oct.  
2007*

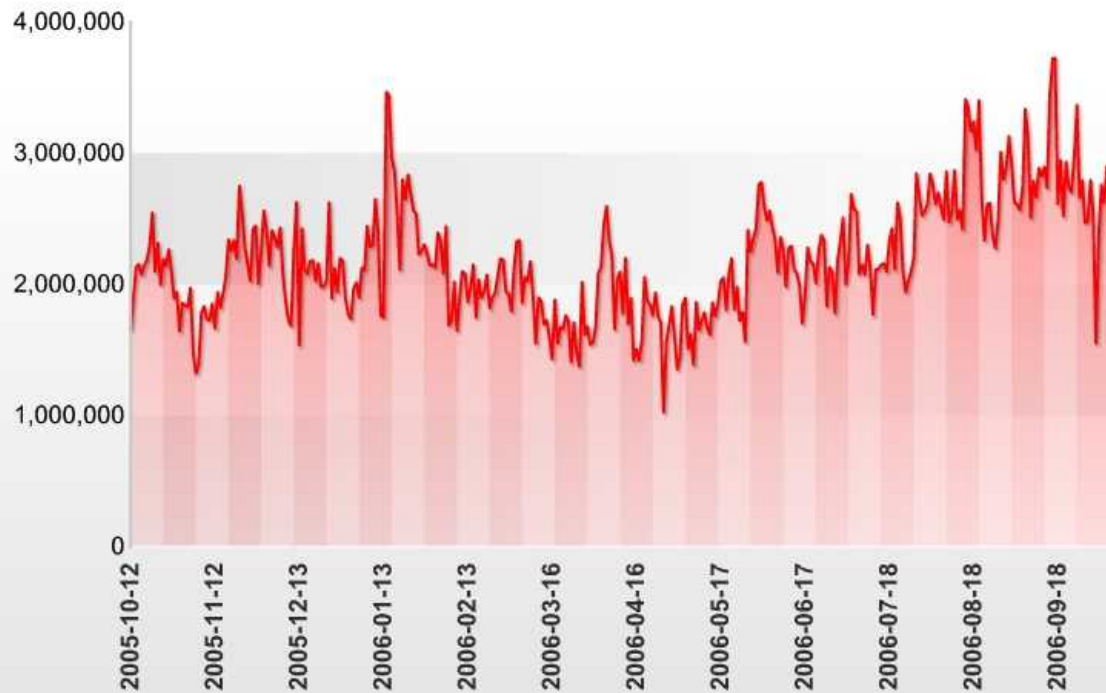
# What's in your mail



# 2006 Spam outbreaks

## Recent Spam Outbreaks - 12 Months View

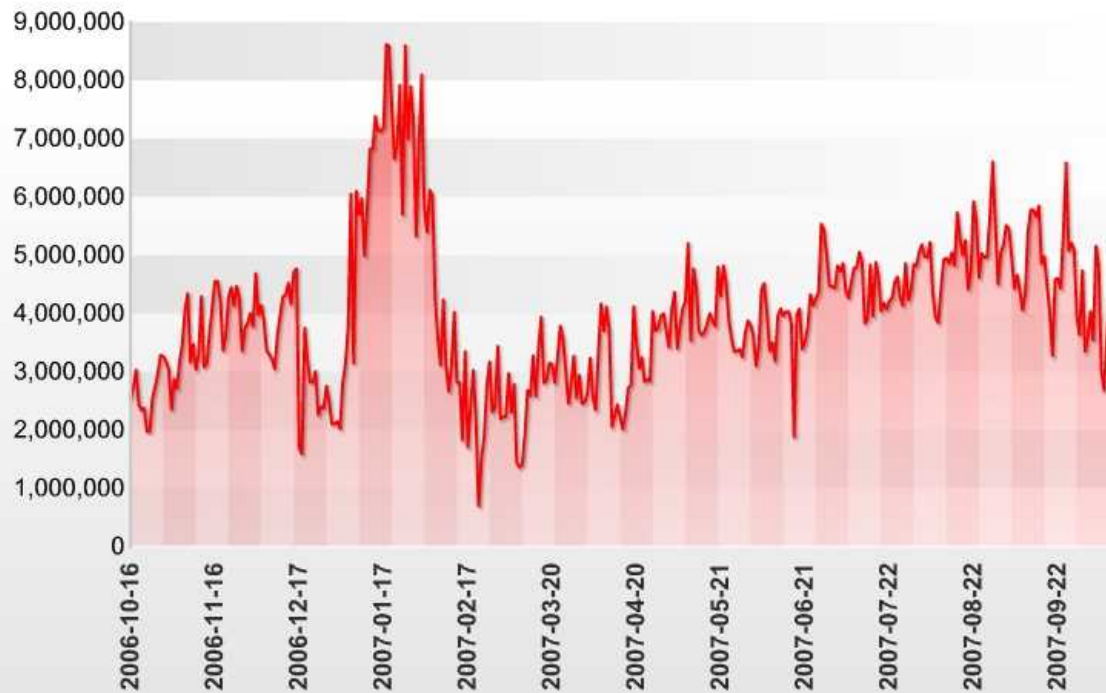
Data source: Commtouch Software Online Lab



# 2007 Spam Outbreaks

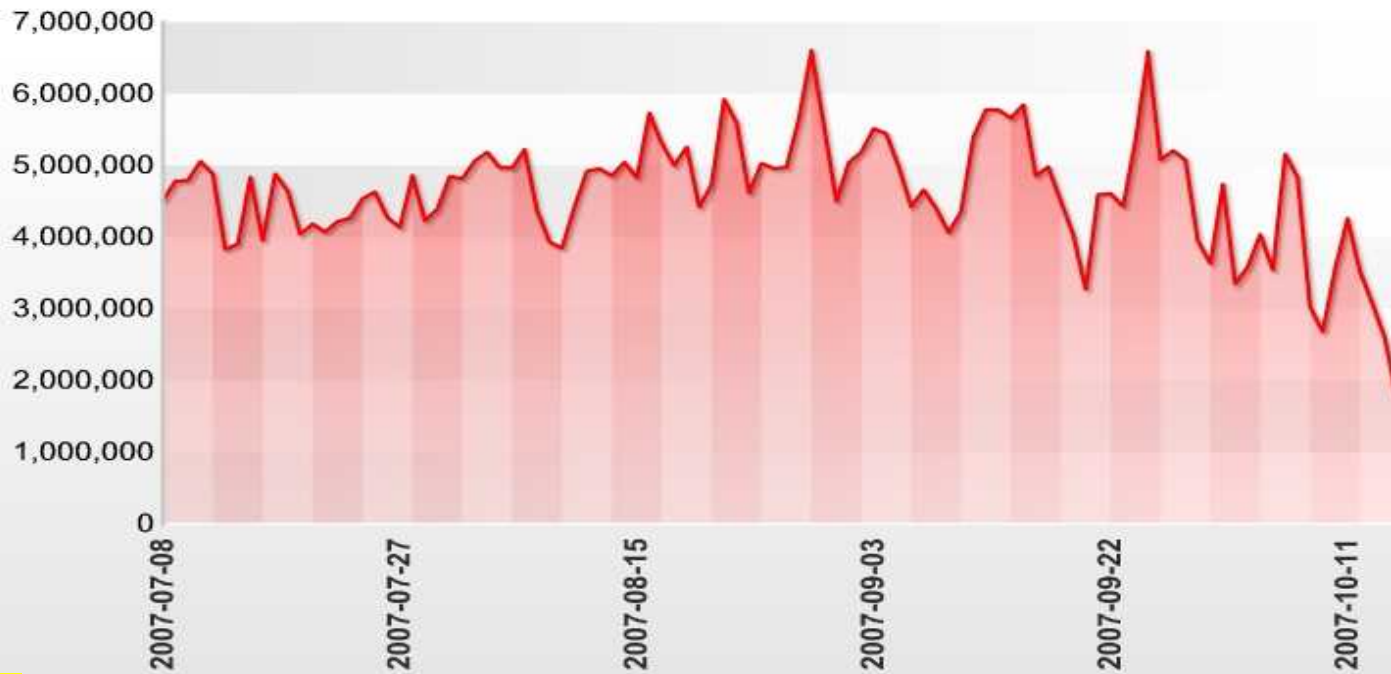
## Recent Spam Outbreaks - 12 Months View

Data source: Commtouch Software Online Lab



## Recent Spam Outbreaks - 100 Days View

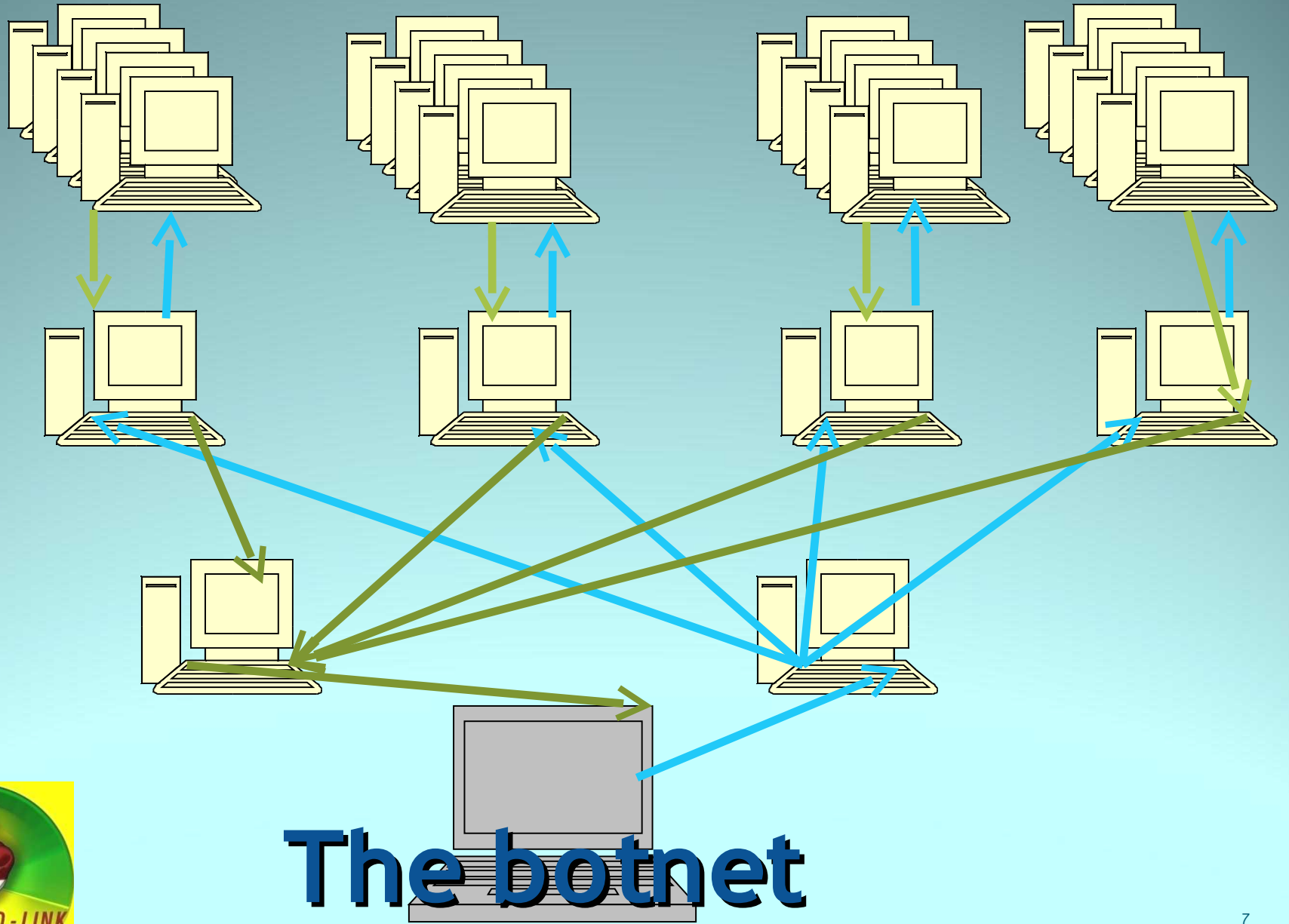
Data source: Commtouch Software Online Lab



# W h a t K e e p s S p a m m e r s g o i n g

- F i n a n c i a l g a i n
- B o t n e t s – C o n t r o l l e d z o m b i e m a c h i n e s
- C o m p r o m i s e d w e b s i t e s
- B l e n d o f S p a m a n d m a l e w a r e





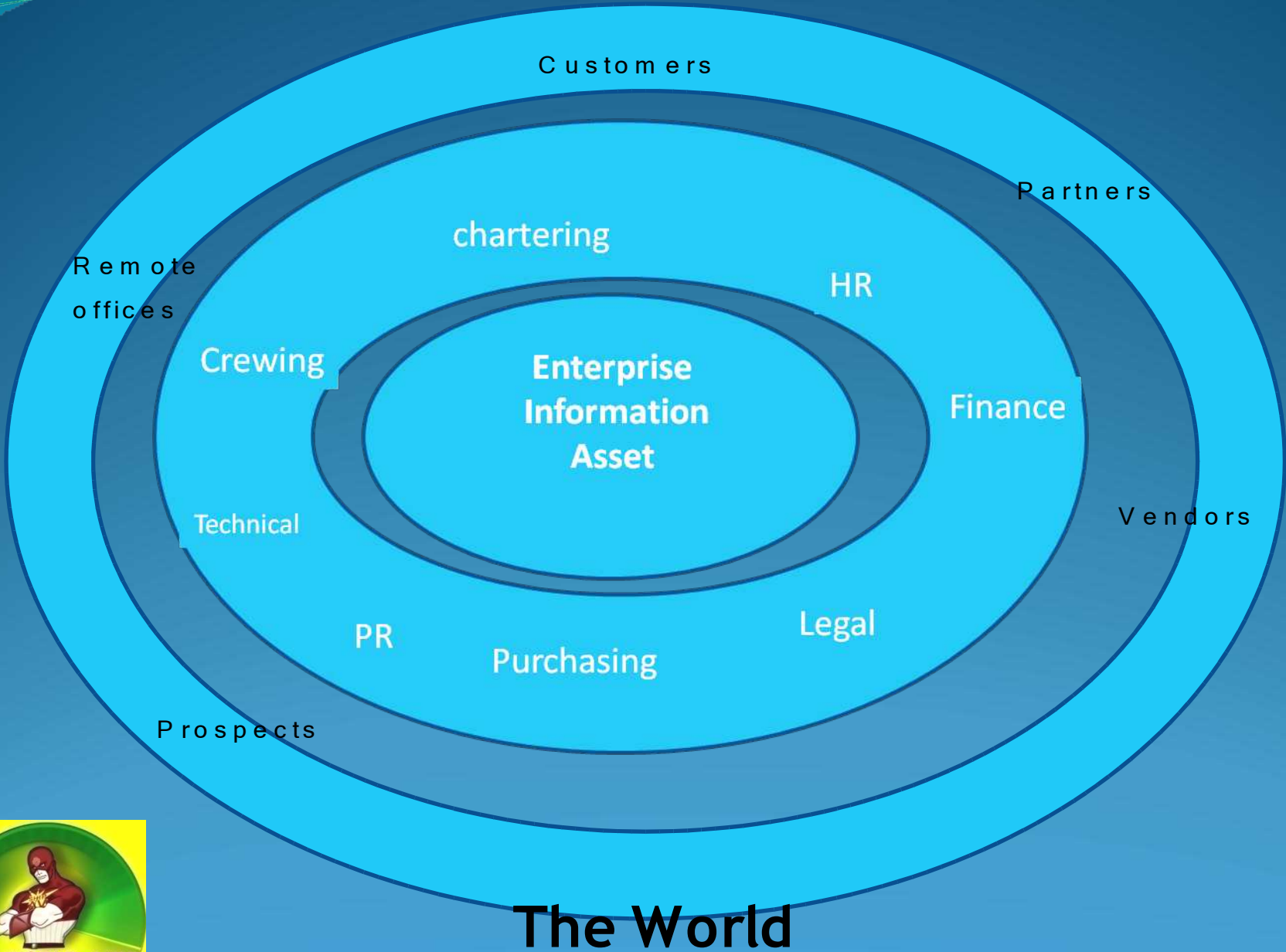
# The botnet



# Zombies

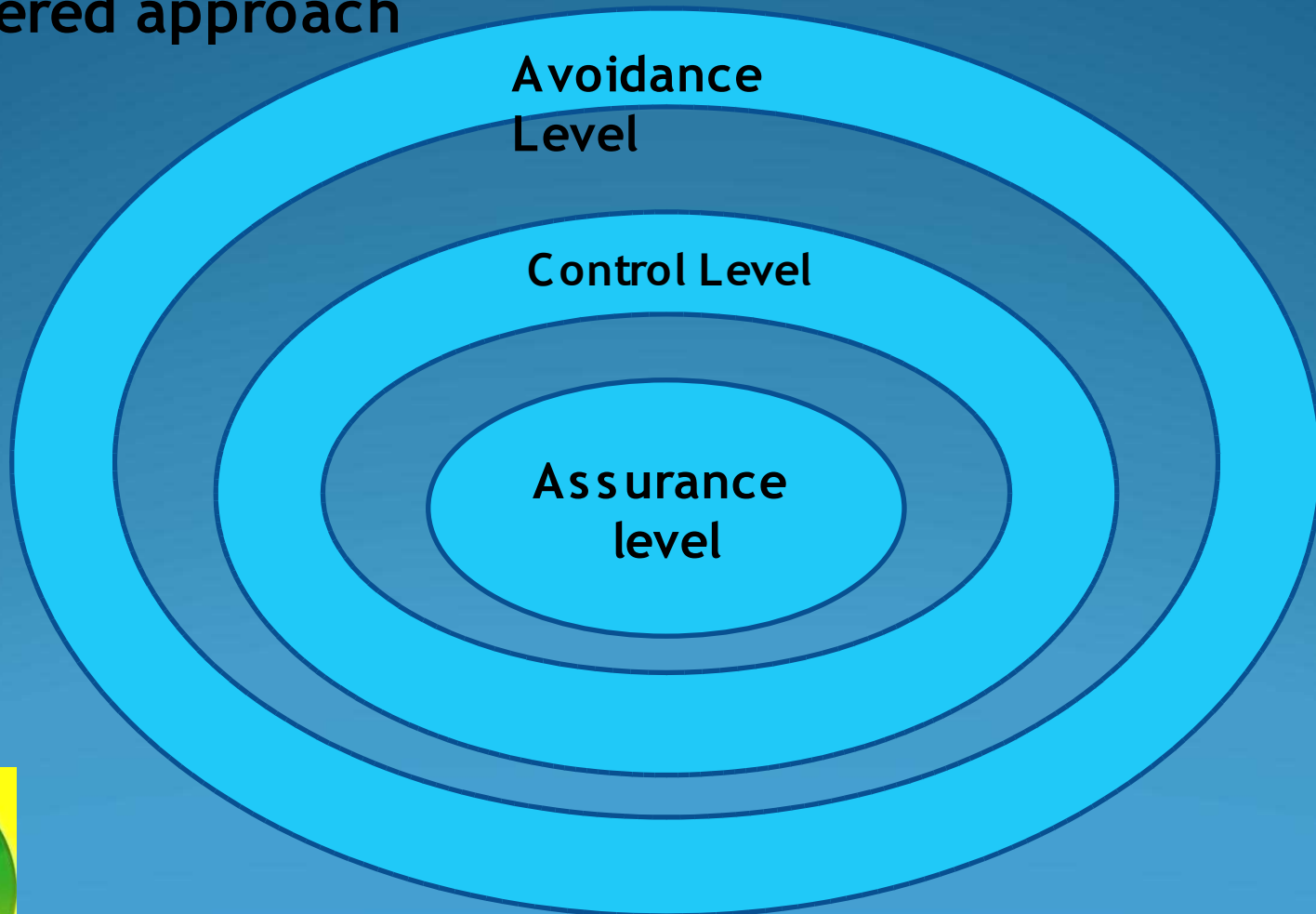
- 6 – 8 million active at any one time .
- Z o m b i e attacks last 2 – 3 hours
- Z o m b i e s per attack 10k – 200 k machines
- A botnet can deliver 160 M messages in 2 – 3 hours



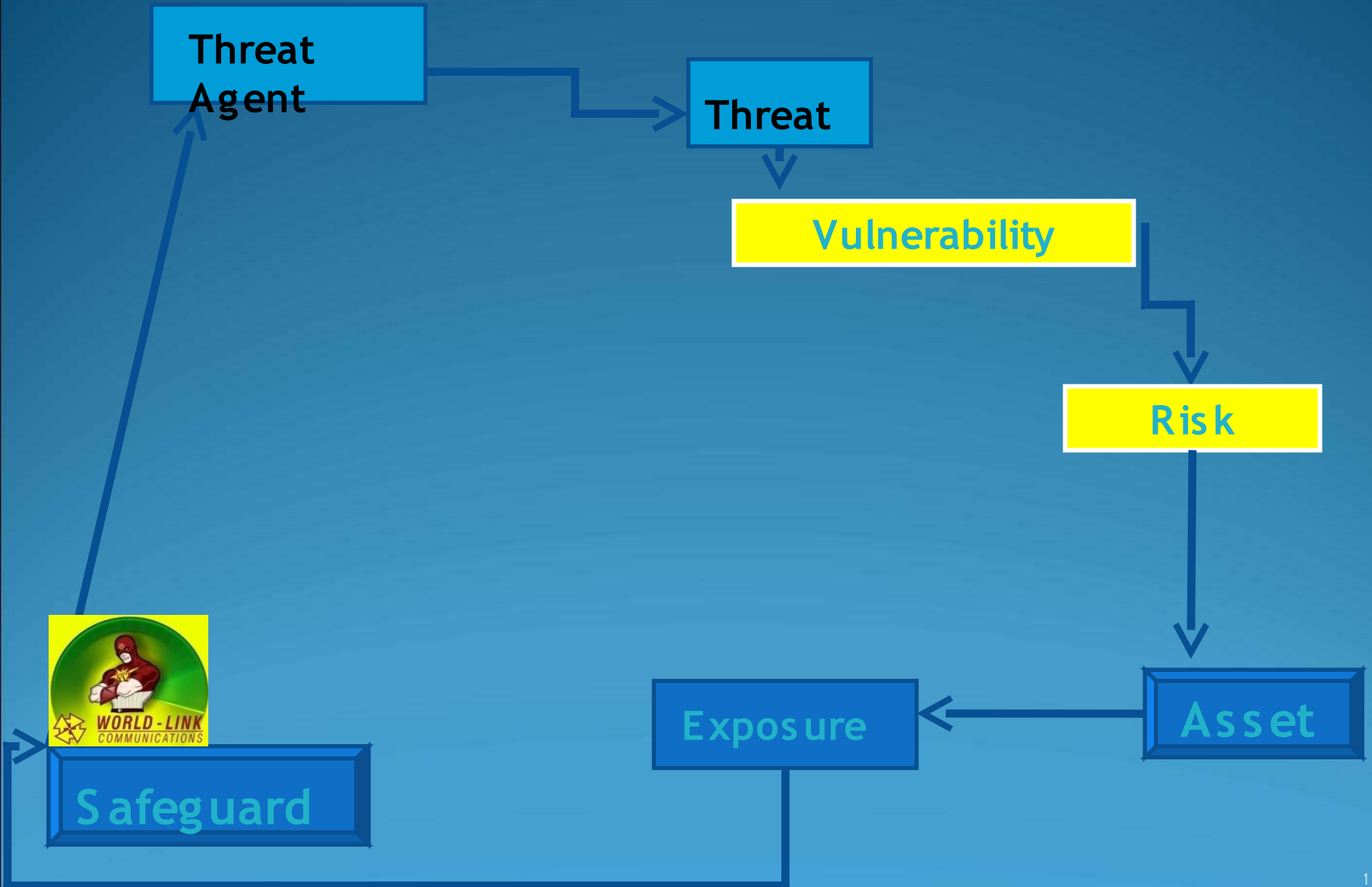


# Protecting the enterprise data

## Layered approach



# The Security Process



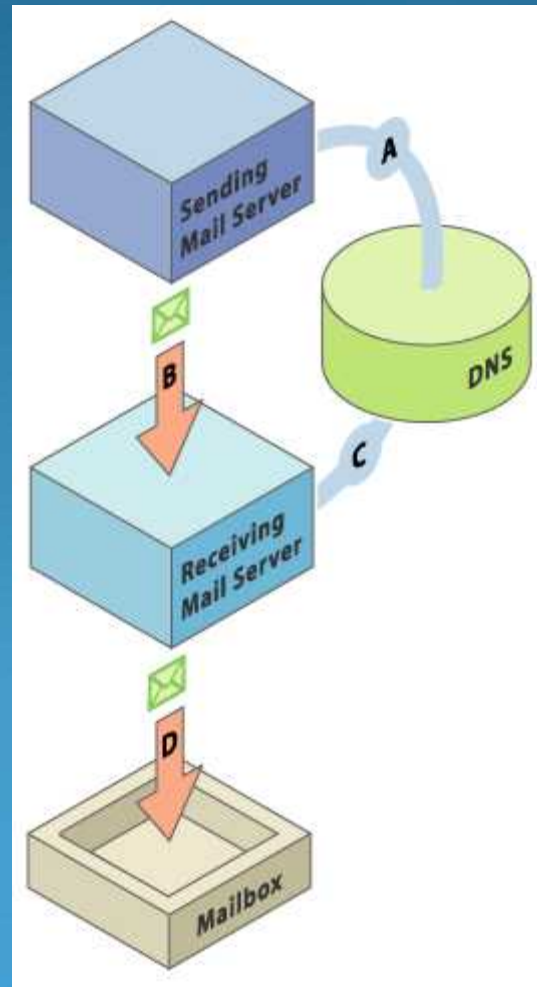
# Current Detection Methods

- Recurrent pattern detection
- Reputation databases
- Zero hour virus outbreak detection
- DKIM (Signed email)
- Sender Policy Framework

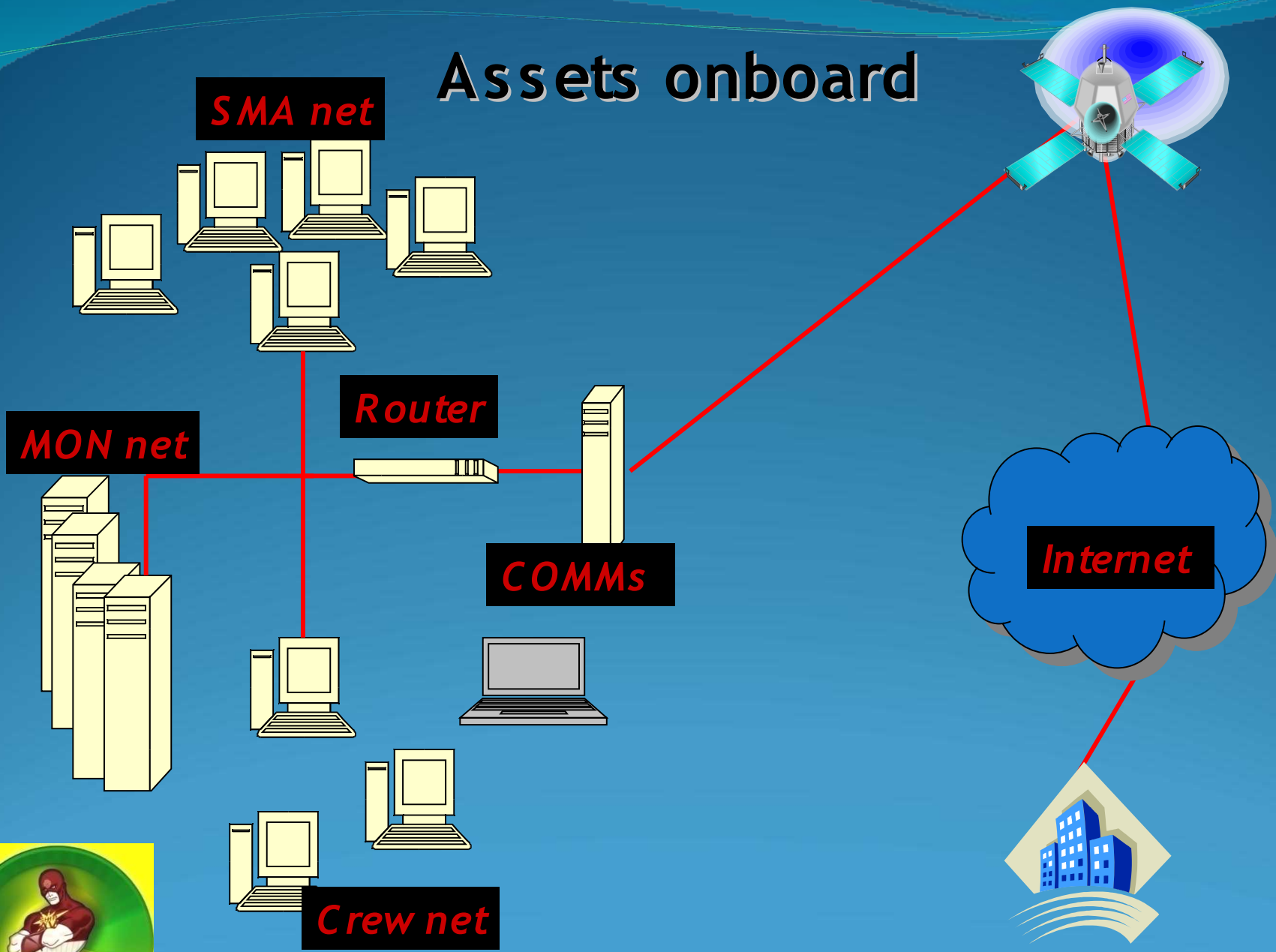


# DNS Based Email Authentication

DKIM  
SPF



# Assets onboard



# Cost of spam transmission

	June 2006	June 2007	Oct 2007
Number of spam messages - per month	300	450	550
Text spam message	100%	65%	55%
Image spam messages	0%	35%	15%
Application Spam	0%	3%	30%
Ave spam message size	9.2 K B	50K B	35K B
Monthly spam volume @ mbox	2,700 K B	22,500 K B	19,250K B
Mini-M @ \$1.40 /min - 2.4 kbps	\$210	\$1,750.00	\$1,497.00
Sat-B LSD @ \$1.80/min - 9.6 kbps	\$67.50	\$562.50	\$481.25
Sat - F & Sat B HSD @ 6.5/min - 64kbps	\$37.5	\$309.40	\$264.70



# Open Vs. Closed mailbox

## Closed System :

- Dependent on manual updates
- Vulnerable to associate spoofing
- False sense of security
- Can create more expensive problems.
- Works ??



# Open Vs. Closed mailbox

- Managing closed mailbox
  - Address book synchronization
  - Web interface to vessel mailbox
  - Shore staff access to vessel mailbox
  - Service provider cooperation:
    - Re-send rejected messages
    - Automate white list buildup
    - Assist in white listing hosts.



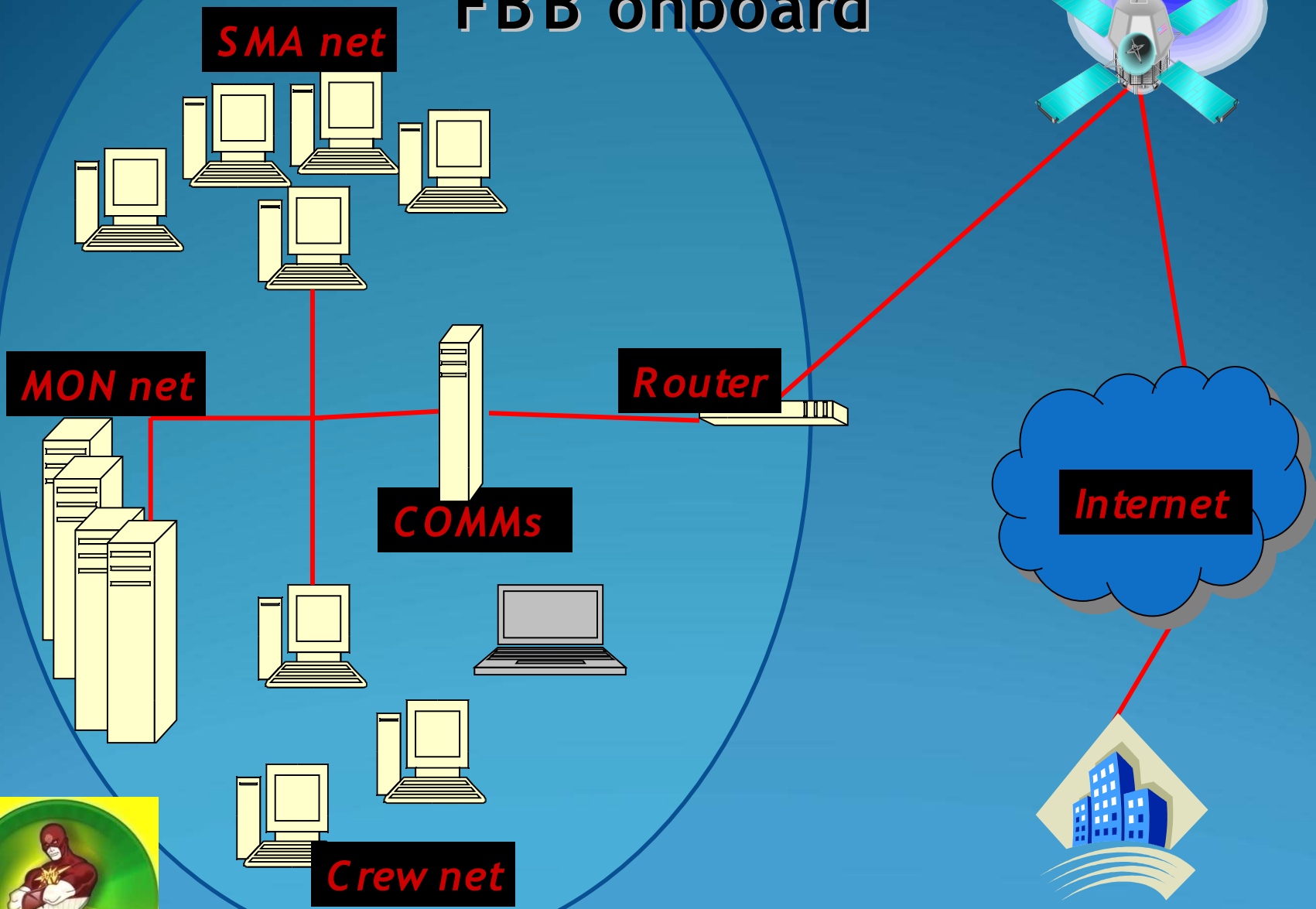
# Data security with FBB

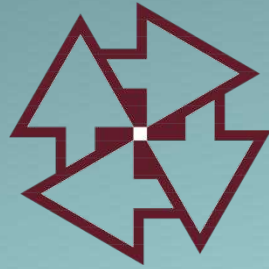
Legacy Systems	FBB
Dialup connection - minutes	Always available - hours
Dialup PC connected	Onboard LAN exposed
MPDS 40 - 80 Kbps	Background IP - 200 - 400 Kbps
Dialup connection to collect mail	Mail over internet
MPDS brows to trusted Intranet	Brows the internet

**It takes only 60 minutes for a none protected PC to become infected on the internet.**



# FBB onboard





# ***WORLD - LINK*** ***COMMUNICATIONS***

**Thank You**



## **Partners in Global Communication**

References: White papers from IBM, Sophos, & Comm touch.