

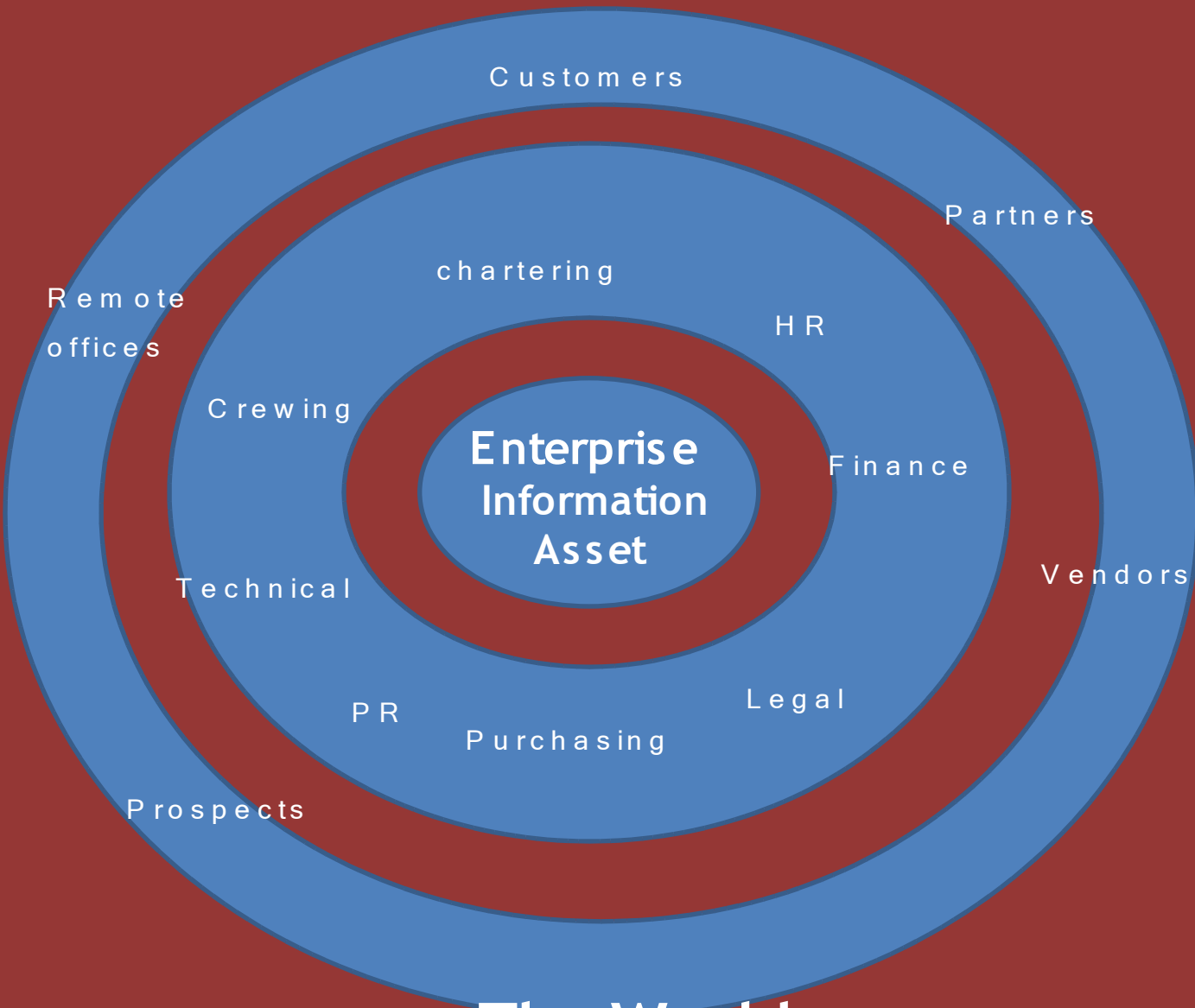
IT Security – Protecting the onboard assets



- What are we to secure
- Identifying the objectives to security
- The security process
- What are the threats
- Real life facts & Cold statistics.



Interacting with the asset



The World



Identifying the objectives

- Keep threats at bay
- Right people have access to the right assets
- Continuity of operational process
- Regulatory conformance

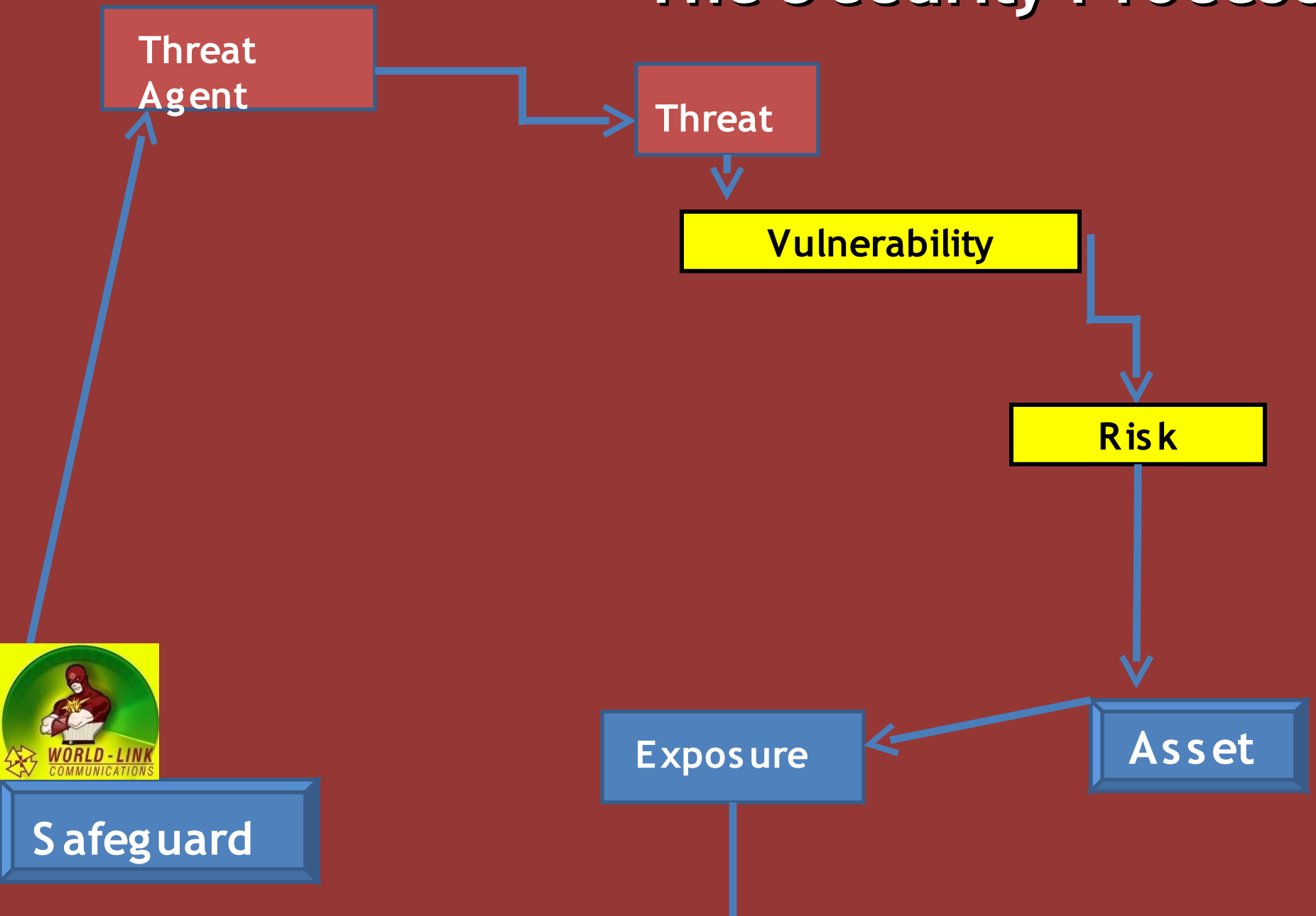
ong term security policies



Building secure systems and not Security Systems



The Security Process



Layered Approach



Layered Approach

Avoidance Level

Perimeter Defense

- Firewalls
- Anti-Virus
- Intrusion Detection
- Intrusion Prevention

Systems



Layered Approach

Control Level

User access Level

- Which users
- What resource
- User requirements
- User Privacy



Layered Approach

Assurance Level

Compliance Level

- Organization's Process
- Auditing & Reporting
- Risk Assessment
- Event response

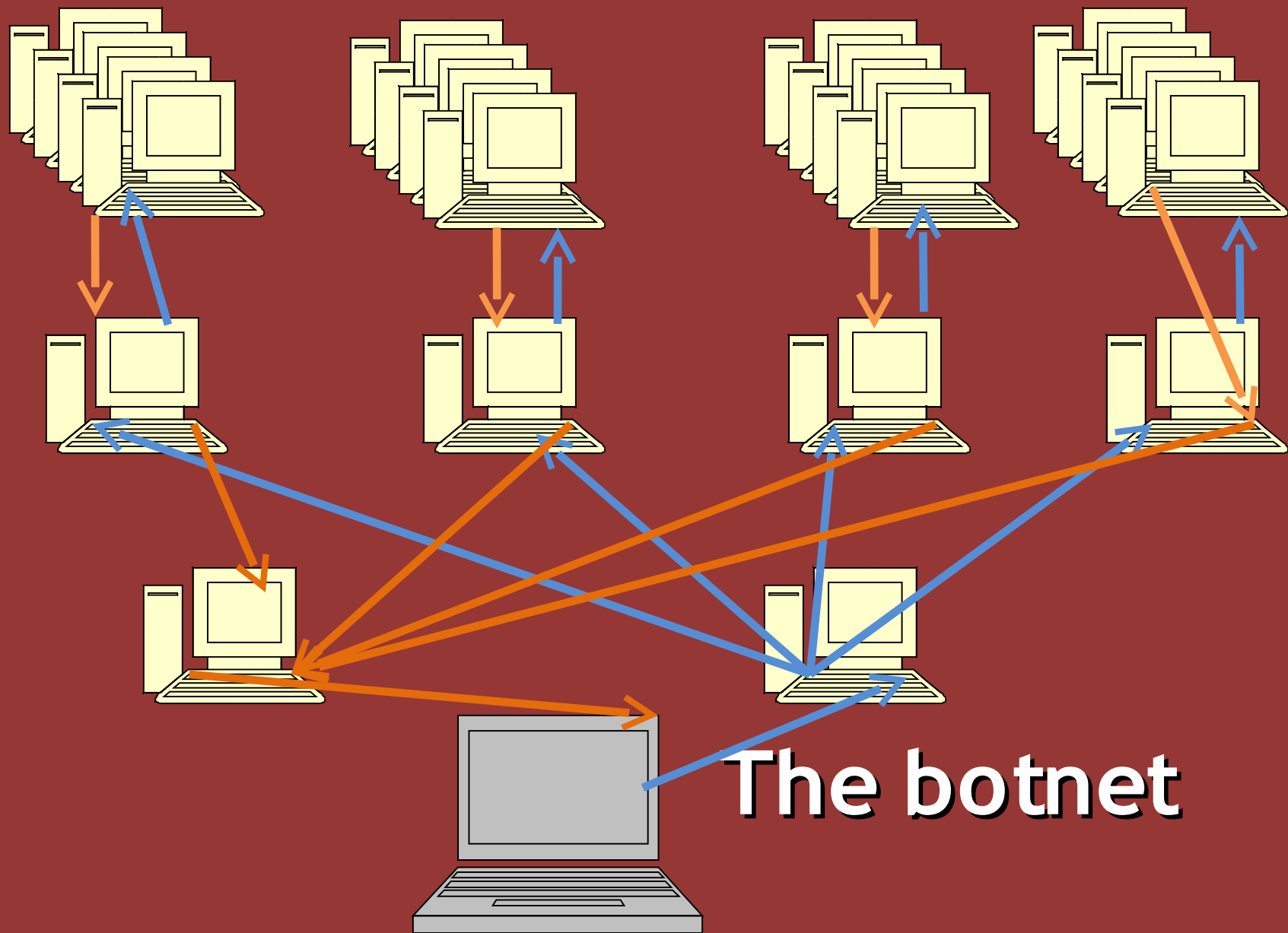


The Nature of the threat

From sneaker net to botnets



The Nature of the threat



The Nature of the threat

Number of Zombie IPs active at any one time :

6 – 8 million



Number of new Zombies per day:

500,000



Average Zombie driven attack:

2 – 3 hours



The Nature of the threat

Zombies used per attack:
10,000 - 200,000

Email messages per botnet attack:
160 million in 2 – 3 hours

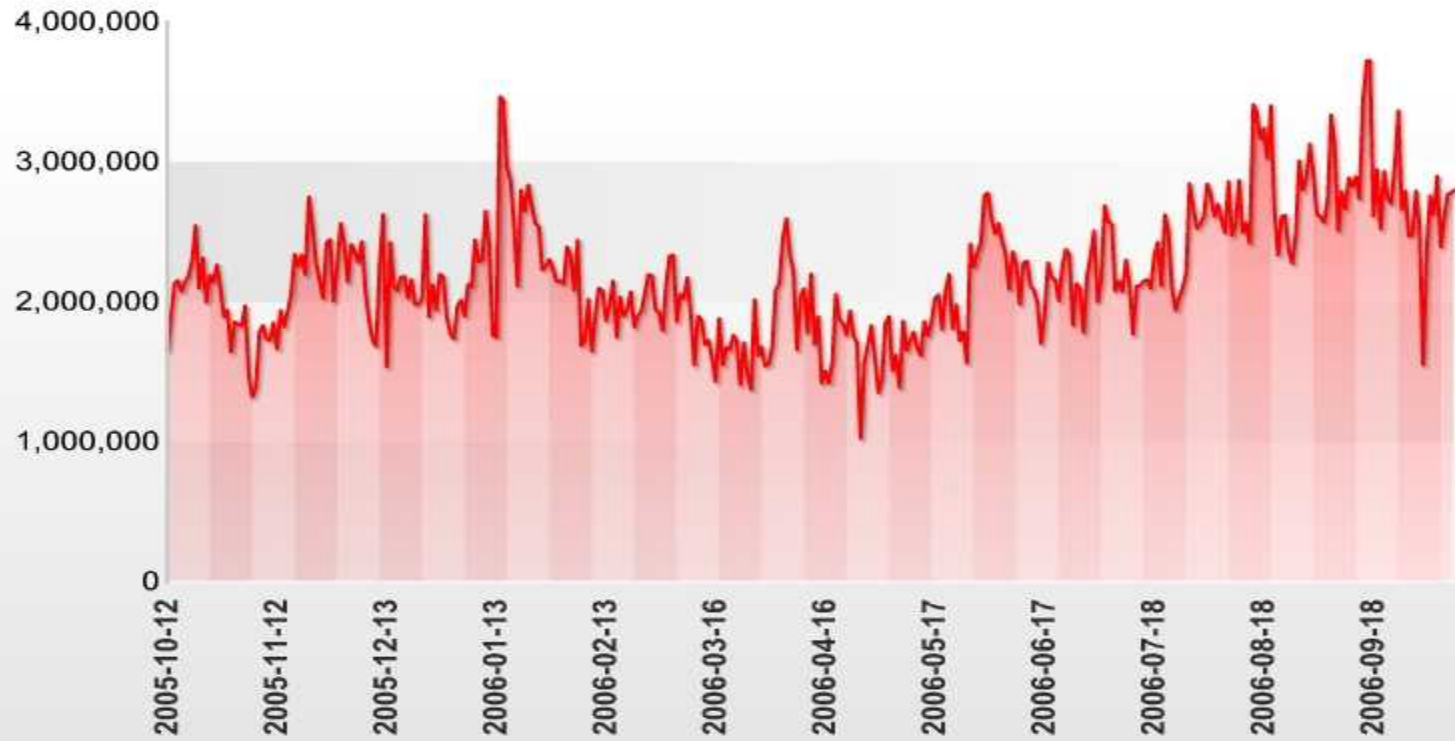


The Nature of the threat

Spam outbreaks 10-05 to 09-06

Recent Spam Outbreaks - 12 Months View

Data source: Commtouch Software Online Lab



The Nature of the threat

Spam outbreaks 10-06 to 01-07

Recent Spam Outbreaks - 100 Days View

Data source: Commtouch Software Online Lab



The Nature of the threat

- *Spam is more than 1 in 2 messages*
- *Virus by email is 1 in 65*
- *Phishing is 1 in 359*
- *In the Transport sector:*
 - *Virus by email is 1 in 65*
 - *Spam is at 48.9%*
- *Fleet average @ WLINK*
 - *1 in 5 is spam or @ 20%*



The Nature of the threat

Cost of Spam - From text to image

	June 2006	June 2007
Number of spam messages - per month	300	450
Text spam message	100%	65%
Image spam messages	0%	35%
Ave spam message size	9.2 KB	50KB
Monthly spam volume @ mbox	2,700 KB	22,500 KB
Mini-M @ \$1.40 /min - 2.4 kbps	\$210	\$1,750.00
Sat-B LSD @ \$1.80/min - 9.6 kbps	\$67.50	\$562.50
Sat - F & Sat B HSD @ 6.5/min - 64kbps	\$37.5	\$309.40

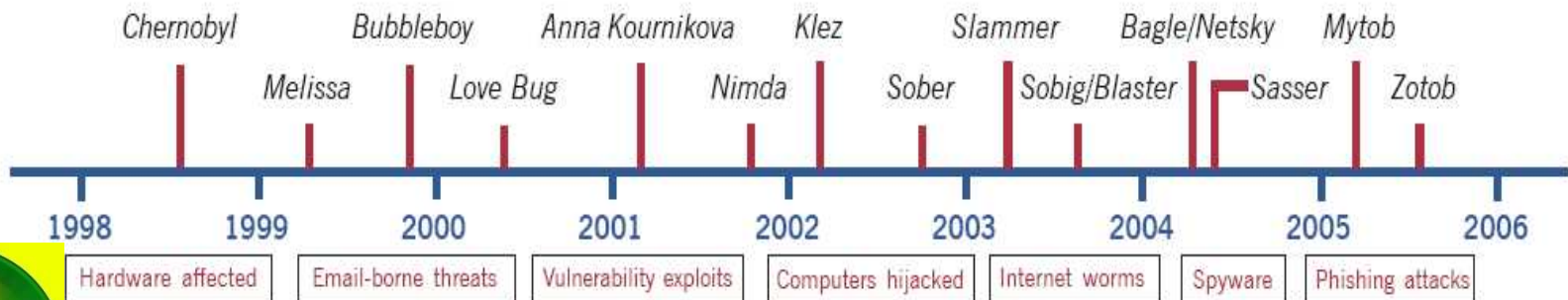
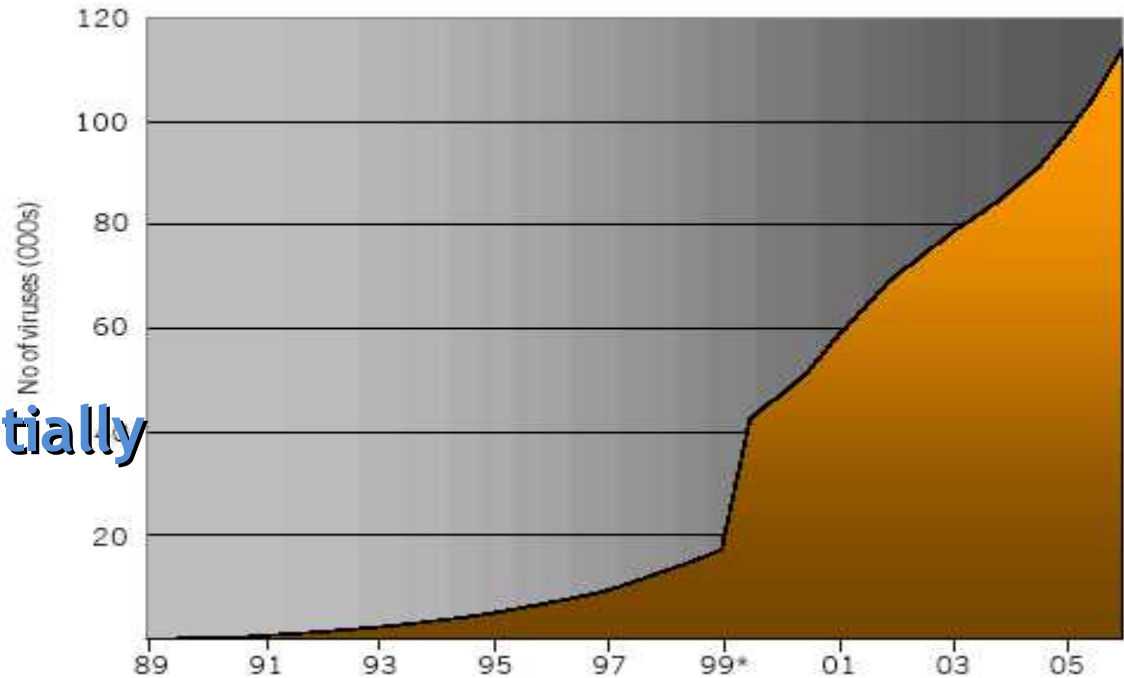


The Nature of the threat

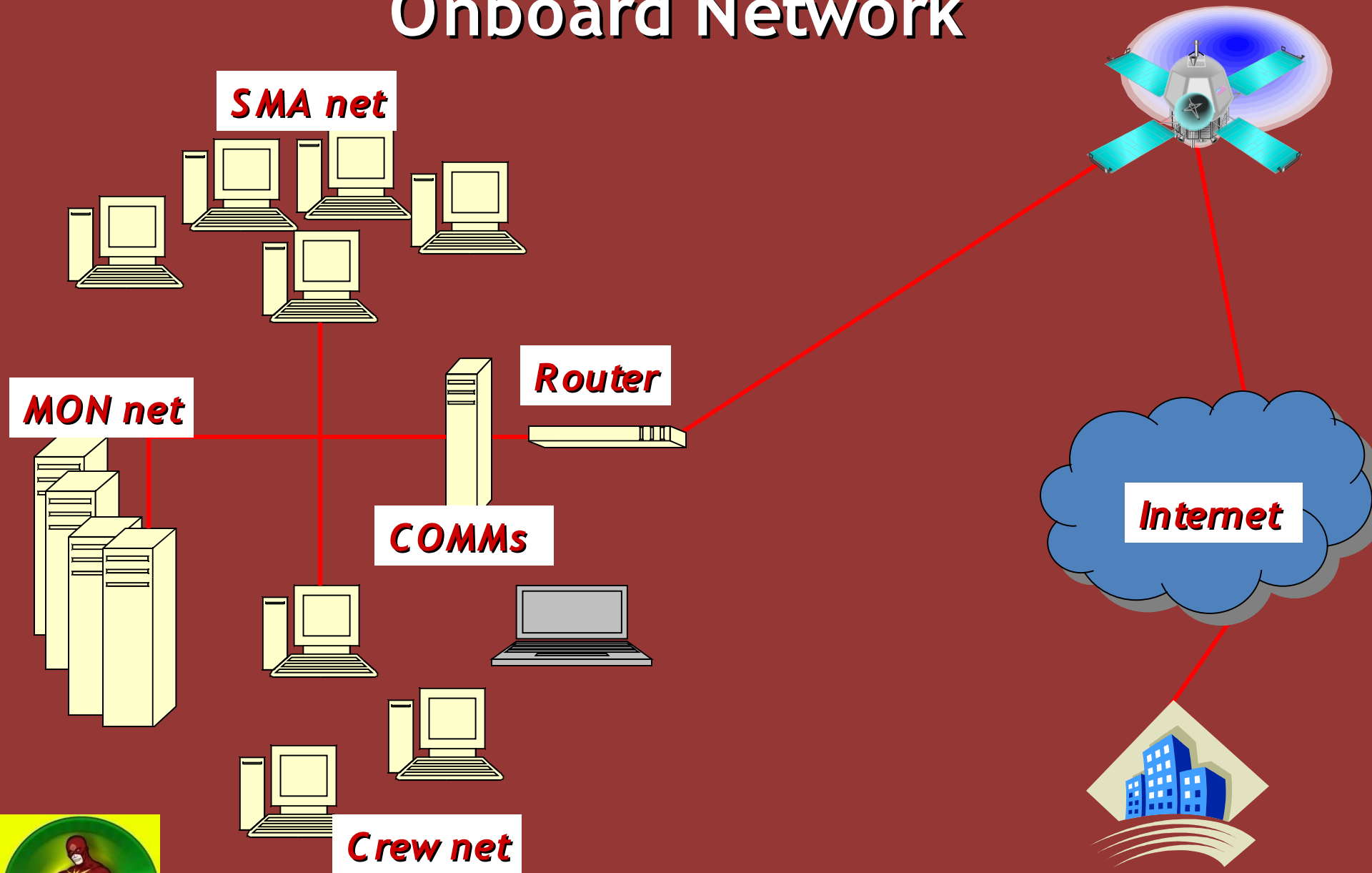
Viruses in the wild:

15,000

and growing exponentially

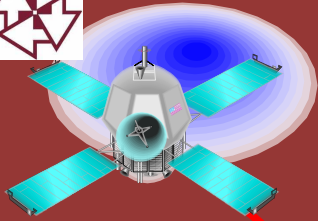


Onboard Network

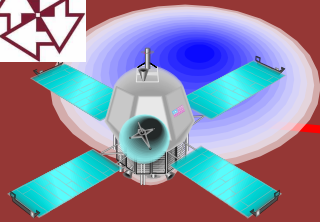


The protected Assets

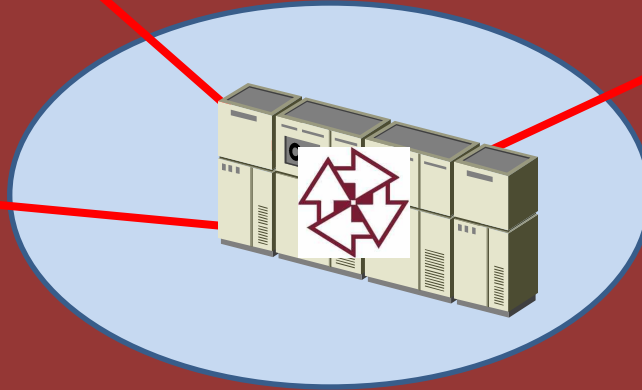
Authenticating
WLINK SAC @
LE



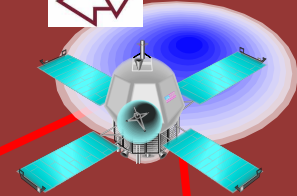
Authenticating
WLINK SAC @
LES



WLINK Hub
Boston



Authenticating
WLINK SAC @
LE



Secure VPN Connection



Protecting against onboard threats

At the e-mail gateway:

E-mail Spam & Virus protection.

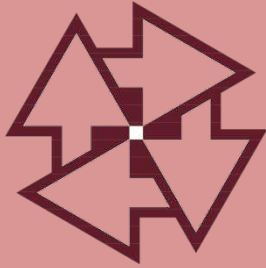
- Reputation - DNS black lists .
- Fingerprinting & Signatures (Hourly updates)
- Heuristic Analysis .
- Bayesian Probability.
- Domain Keys .
- Customer defined rules .
- White lists .



IT Security – Protecting the onboard assets

- The threat is real.
- Requirement for multi-layered defense strategy.
- Frequent review of policies & Systems.
- Proactive role in provider services.





WORLD - LINK

COMMUNICATIONS



Thank You

Partners in Global Communication

References: White papers from IBM, Sophos, & Commtouch.

