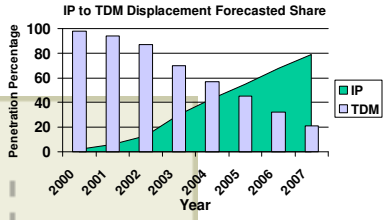
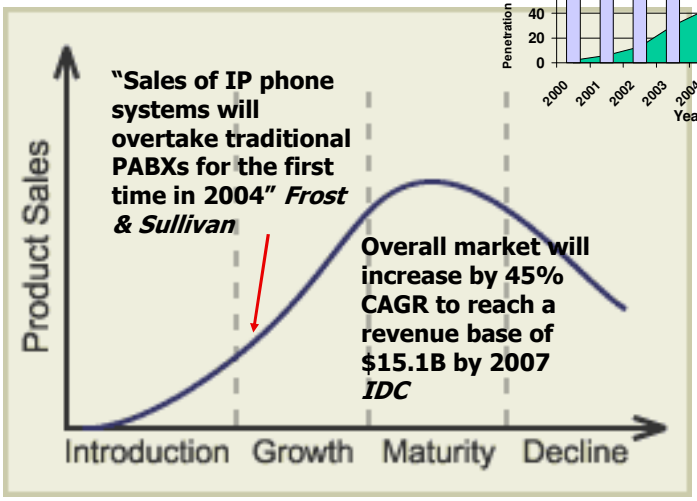
Synopsis

- **Presentation topic**: "Eggs in the basket: how voice and data convergence changes the security landscape."
- **Synopsis**: Convergence provides increased functionality and reduced support costs.
- It also changes the nature of threats and risks, increasing the need for real-time protection, detection and response.
- This presentation discusses the changing nature of threats and risks as well as looks at how to mitigate these from a combined response.

NETSTAR

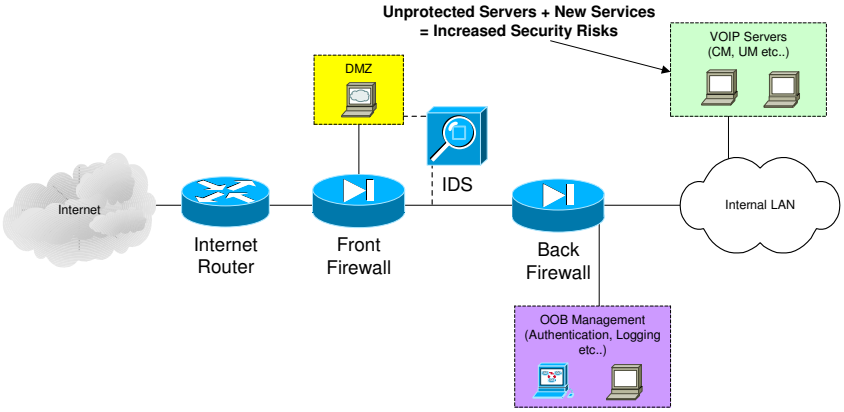
VoIP is here, now





NETSTAR

Typical converged network



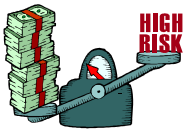
NETSTAR

Risk Assessment

Risk = Impact x Likelihood

=

x



=

x

NETSTAR

Risk Management

Risk =  x Likelihood

- Impact is context sensitive:
  - how do I use my network?
  - Does it directly support my business or customers?
  - For most organisations, impact is dominated by *availability*

NETSTAR

Risk Management

Risk = Impact x 

- Likelihood involves vulnerabilities
  - What systems do I have?
  - Are these systems vulnerable?
  - Would someone be *motivated* to hack one of them?

NETSTAR

Risk Management and IP Convergence

- How does combining my voice and data infrastructure affect my risk?
  - Impact
  - Likelihood
- Use Confidentiality, Integrity and Availability to frame analysis

NETSTAR

IP Convergence & Impact: Is there more or less money in the wallet?

Risk =  x Likelihood

Impact	< Impact	Same	> Impact
Confidentiality			✓
Integrity		✓	
Availability			✓

NETSTAR

IP Convergence & Likelihood: Is there more or less chance?

Risk = Impact x 

Impact	< Likelihood	Same	> Likelihood
Confidentiality			✓
Integrity			✓
Availability			✓

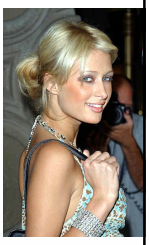
NETSTAR

Known Attacks – Traditional & VoIP

- Toll-fraud: The telecommunications industry estimates $4 billion per year is lost to phone fraud*
  - Thru-dialing and Voicemail attacks
  - Administration and Maintenance Ports
- Wiretapping / eavesdropping
- DoS – Call quality and Integrity
- Worms
- IP Tel – specific attack (C / I)

*AT&T, "AT&T Fraud Education", 2002

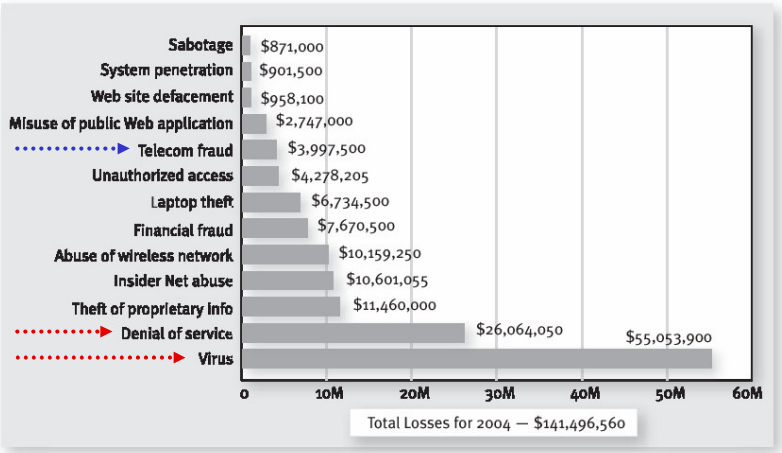
Telecom



NETSTAR

"PABX Voice" vs potential "IP Voice" losses

Figure 15. Dollar Amount of Losses by Type



CSI/FBI 2004 Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents

NETSTAR

How secure is IP Tel?

- **McAfee** chief executive George Samenuk: "the next big area for attack".
- **ISS** chief scientist Robert Graham: technology in its current guise is "completely insecure"
- **Cisco:** discounted talks about VoIP being unsafe as alarmist [but] conceded that VoIP platforms will never be immune to the determined hacker
- **AARNet:** Probably the most hostile of environments (wrt disruptive hacking rather than destructive).

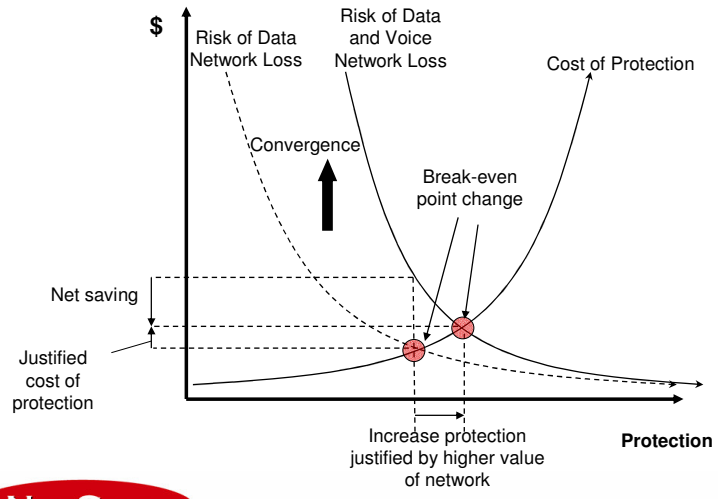
NETSTAR

Traditional weaknesses versus current and predicted threats

Impact	PABX	Converged
Confidentiality	▪ Wiretapping	▪ Eavesdropping / Sniffing
Integrity	▪ **Toll Fraud** ▪ Thru-dialing and voicemail attacks ▪ Administration and maintenance ports	▪ Attack on Call Quality and Integrity ▪ Server OS and application vulnerabilities
Availability		▪ Denial of Service ▪ Worms

NETSTAR

Summary: Cost Minimisation



NETSTAR

The last word:

- **Network World: Can you hacker-proof your IP telephony network?** The short answer is: Yes, pretty much. But it strongly depends on whose IP PBX you use and more importantly, whether you're willing to spend the dollars and the time it takes in terms of network security planning, network and personnel resources, and extra security gear.

NETSTAR

Increased Protection: Where?

CONFIDENTIALITY

- Encryption
- Authentication
- Firewall
- Audit trail

INTEGRITY

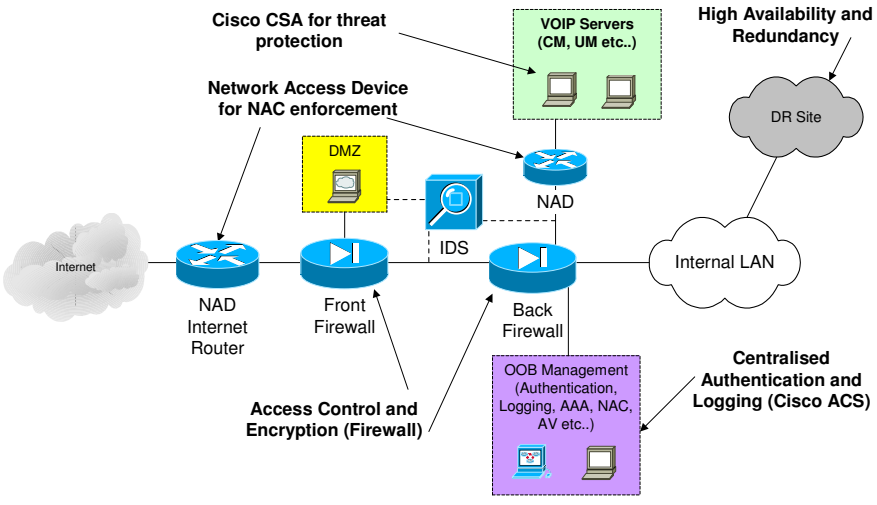
- Authentication
- Firewall
- Hash Functions
- Tripwire

AVAILABILITY

- Redundancy / High Availability
- 24x7 Monitoring
- Worm/virus protection
- Intrusion prevention
- Staff training

NETSTAR

Start with the network design…



NETSTAR

Security Features	Confidentiality	Integrity	Availability
▪ Harden routers (eg. Lock down, SNMP, ARP)	✓		✓
▪ Segment voice from data (traffic and users)	✓		✓
▪ IP Source Guard / DHCP snooper	✓	✓	✓
▪ Encryption	✓	✓	
▪ Tripwire		✓	
▪ Stateful firewalls	✓	✓	✓
▪ IDS/IPS			✓
▪ Network Admission Control (NAC) + ACS	✓		✓

NETSTAR

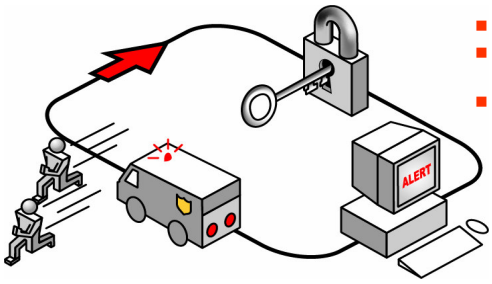
...Add 24x7 vigilance

PROTECTION

- Specialised staff
- High level of training and support
- Management systems

RESPONSE

- 24x7 capability
- Information and or skills to properly fix issues
- Incident response processes



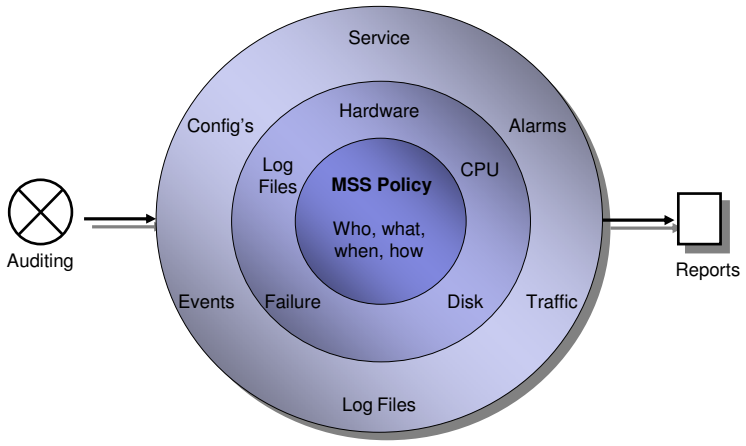
DETECTION

- Complex software
- Multiple vendors
- Real-time log collection & alerting

By 2006, information security spending will drop from an average of 6-9% of IT budgets to an average of 4-5% as enterprises improve security management and efficiency. **It is the improvement in management that holds the key to a more secure enterprise**. [Gartner]

NETSTAR

NetStar's Approach to Security Monitoring



NETSTAR

Technology is not enough!

- **24x7 management of data, security and VoIP**
- Security Focus on the Enterprise network
- Forensics Capabilities
- Incident Response Plan
- Disaster Recovery Plan
- Backup & Recovery (Including Tape Storage)

NETSTAR

What to do next…

5 Action Steps:

1. Gain Knowledge (business and technical)
2. Change Mindset
3. Identify the converged network
4. Map out the converged network
5. Take a proactive stance for a converged network security posture

Questions