INS
INTERNATIONAL
NETWORK SERVICES

NetKnowledge Web Inar

Securing Your Voice Over IP Network

Presented by:

Jim Valentine, Senior Network Systems Consultant *james.valentine@ins.com*

Rick Blum, Senior Manager, Strategic Marketing *rick.blum@ins.com*

The knowledge behind the network®

International Network Services

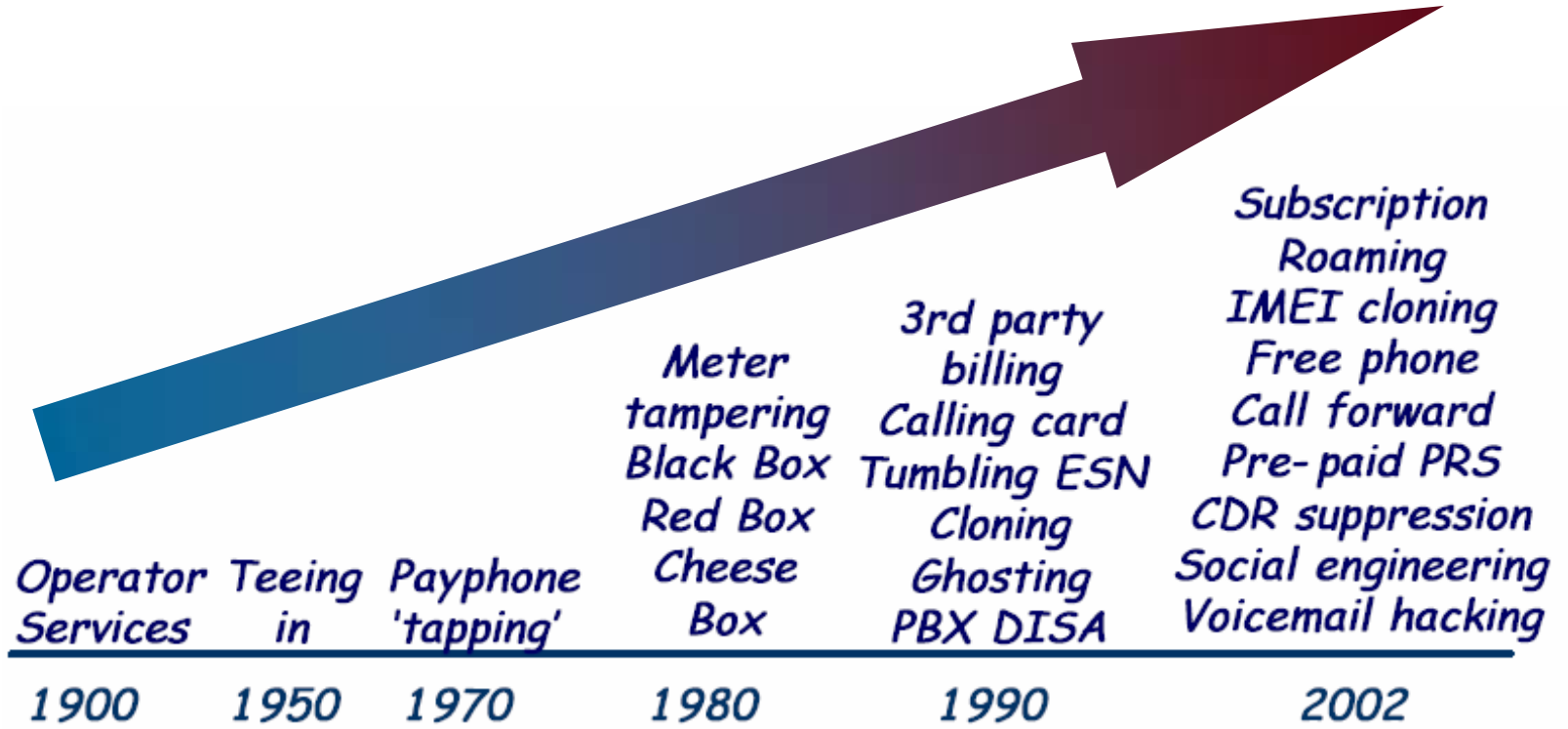
- Vendor-independent consulting services
- Build, secure and manage network infrastructure
- 30+ offices in North America and Europe
- 18,000+ engagements over 12 years
- Serve Fortune 1000 enterprises, service providers, and other network-centric organizations

VoIP Security Buck Stops with Users

- **PBX vendors not responsible for switch security or toll fraud**
- **Courts place responsibility on user**
  - *Management*
  - *Telecommunications team*
  - *IT team*
  - *IT audit function*

- **U.S. legal mandates**
  - *Jurisdiction – Dept of Treasury, Secret Service*
  - *Title 18, Section 1029, US Code Credit and Debit Card Fraud Statute*
  - *Title 18, Section 1030, US Code Computer Fraud and Abuse Act*
  - *Title 18, Section 1343, US Code Wire Fraud Statute*

A Growing Problem

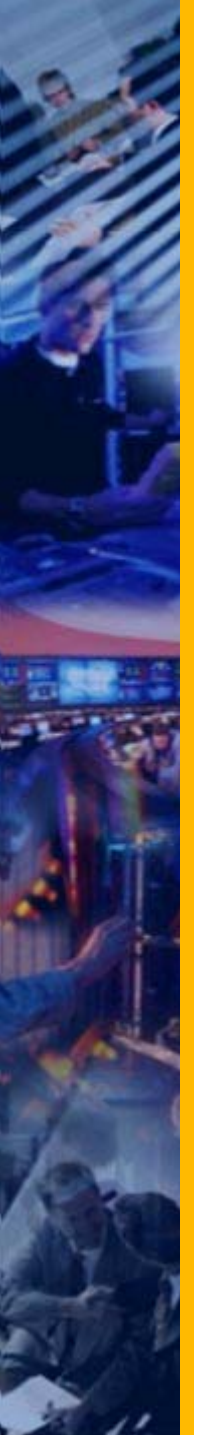


VoIP Security Vulnerabilities

- **Voice transport protocols**
  - *RTP*
  - *RTCP*
  - *SCTP*
- **Signaling protocols and architecture**
  - *SIP*
  - *H.323*
  - *MEGACO*
  - *MGCP*
- **Multivendor component environment**
- **Physical plant**

What's at Risk?

- IP phones
- Core routers
- Media gateways
- SIP proxies
- Gatekeepers
- Location servers
- Switches
- VoIP-based firewalls
- Any equipment in VoIP infrastructure



Voice Data Convergence Multiplies Threats

- **VoIP inherits IP data network threat models**
  - *Reconnaissance, DoS, host vulnerability exploit, surveillance, hijacking, identity theft, misuse, etc.*
- **VoIP QoS requirements increase exposure to DoS attacks that affect:**
  - *Delay, jitter, packet loss, bandwidth*
- **PCs = authentication; phones = any user**
- **User identity theft**
  - *VoIP inherits PBX phone vulnerability*
  - *Unauthorized access and privileges, service theft*
- **Device identity theft**
  - *Malicious devices on IP network act like IP phones*
  - *Reduced service availability, eavesdropping*
  - *Inserting/Deleting/Modifying audio streams*

Risks if Attacked

- **PBX, VM/ACD**
  - *Phone system downtime*
    - How long can you survive without your phone system?
  - *Theft of services (long distance)*
    - Estimated at over $13 billion annually
- **Modems**
  - *Computer or network penetration*
  - *Existing IP perimeter security may not detect*

Threats from Phreakers and Hackers

- **Phreakers use phone system to:**
  - *Gain free calls*
  - *Disrupt system*
  - *Fun*
- **Hackers use computer system to:**
  - *Gain free services/products*
  - *Denial of Service (DoS)*
  - *Business*
  - *Fun*

Merger of data and voice = merger of threats

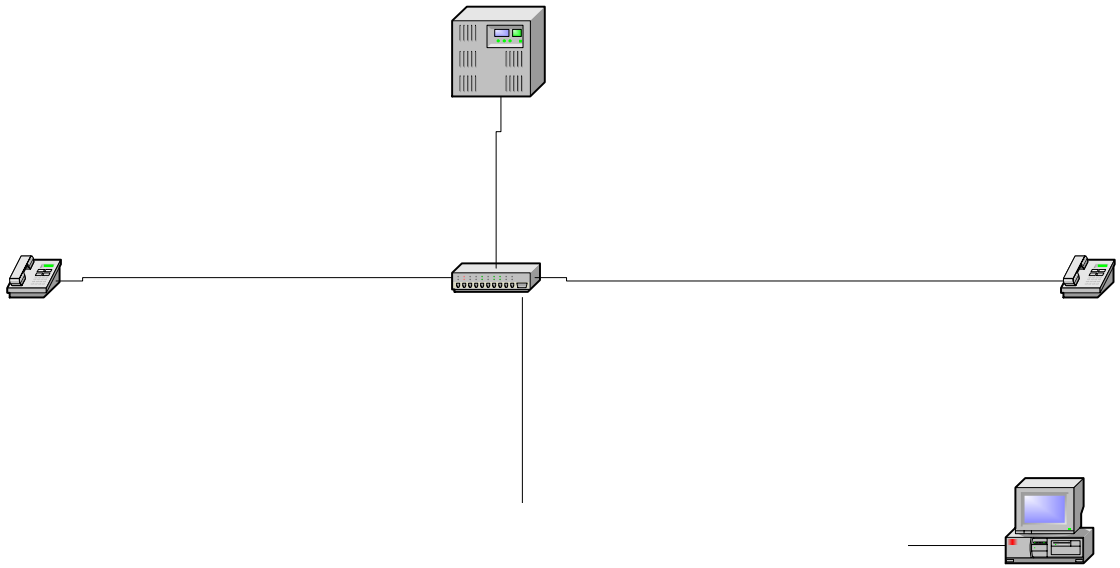
Threats

- **Session hijacking**
- **Monitoring (eavesdropping)**
  - *Internal threat*
- **Service disruption**
  - Multilayer attacks
- **Toll fraud (theft of service)**
- **Service use and abuse**
  - *Internal threat*
- **Data security**

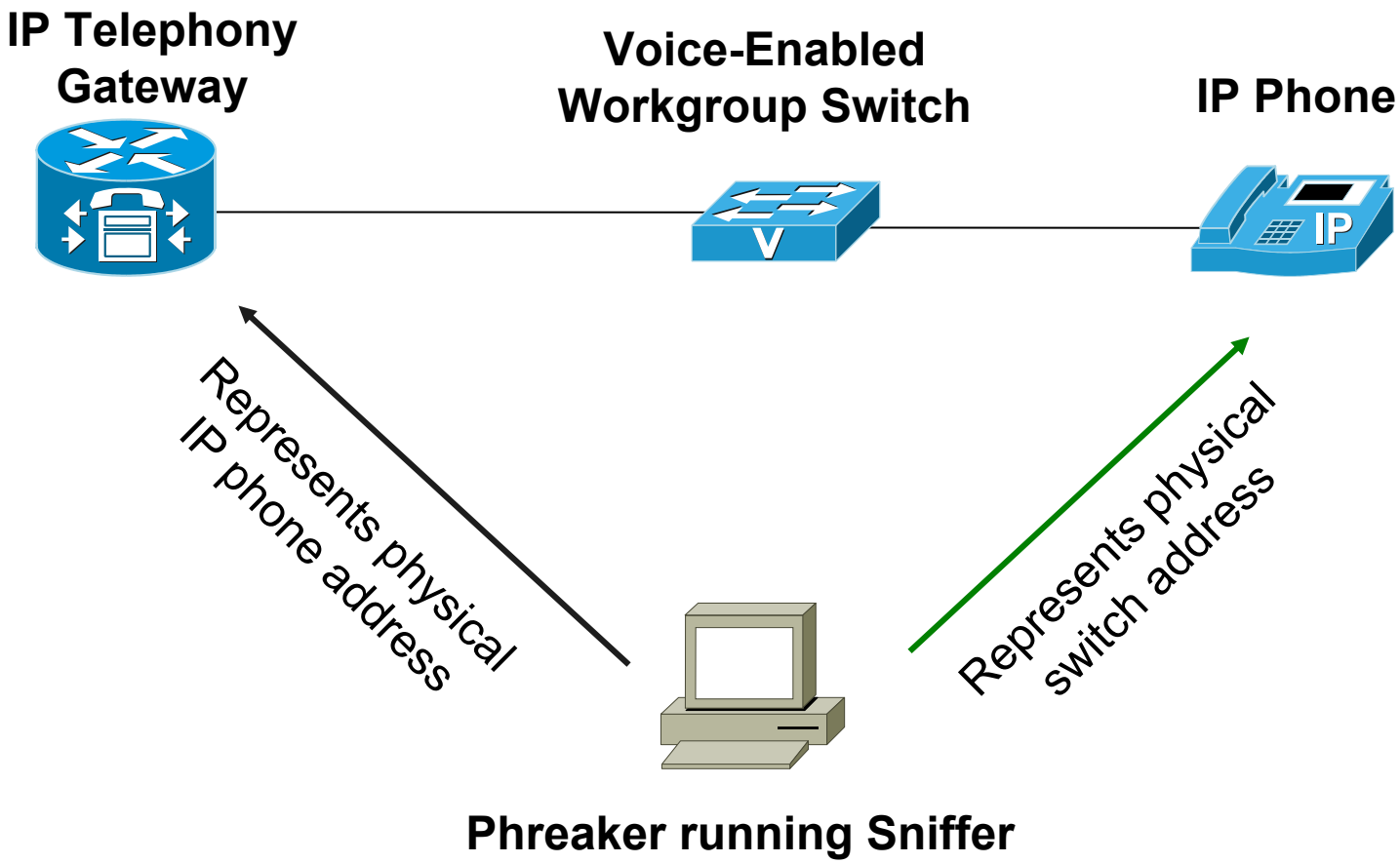
Impact: Loss of essential business resources

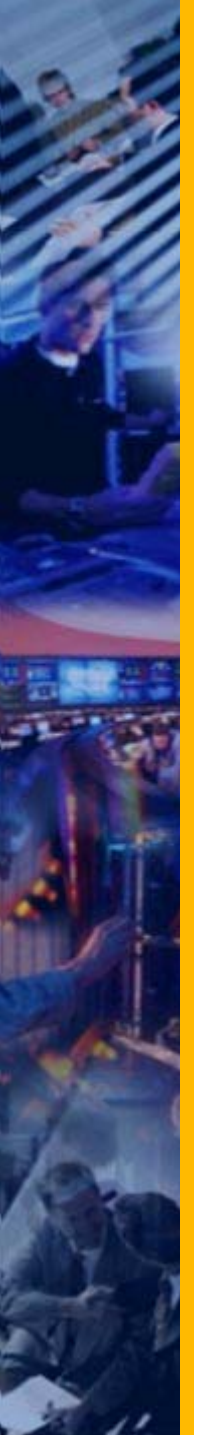
Eavesdropping Threat

- **Need access to wire**
  - Between IP phone (or customer premises gateway) and switch
  - Between two switches
- **Hub, knife, and clipper**



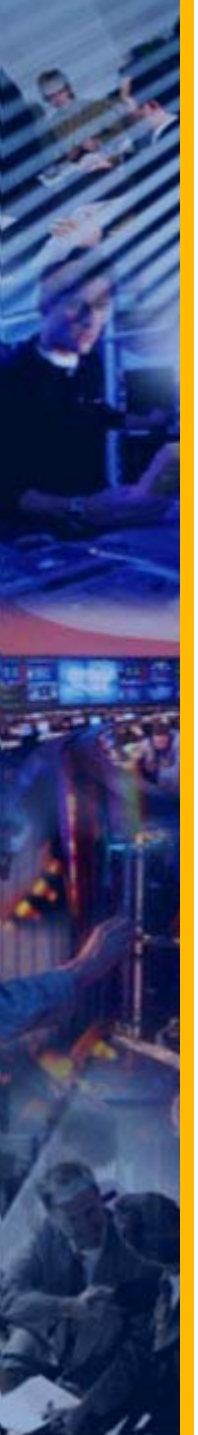
Free Phone Call Threat





Denial of Service Threat

- **DoS venues**
  - *Flood*
  - *Abuse protocols*
- **Target devices**
  - *IP phones (easy)*
  - *Routers, switches (depends on equipment)*
  - *Signaling gateways, media gateways, SIP proxies*
  - *Any device in the path a call takes from a caller to a called party*

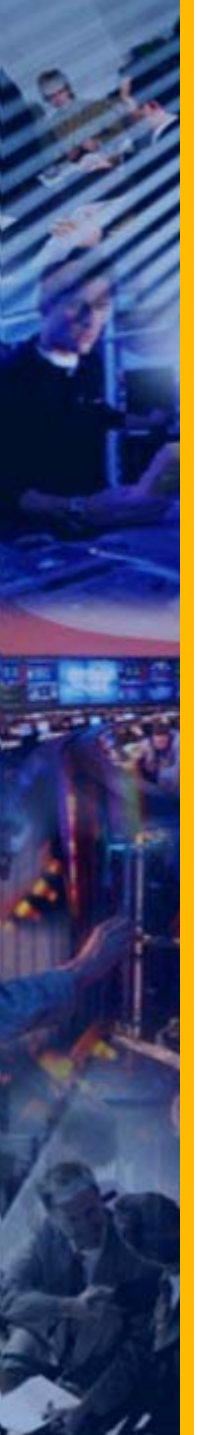


Media Transport: RTP Security Issues

- **Denial of service**
  - *Handling SSRC collisions*
    - Sending command using SSRC of another participant
    - Claiming SSRC of a user
  - *Packet injection*
    - Same SSRC, higher sequence number, higher timestamp
    - The fake content played before the real one
- **Quality of service: bandwidth attack**
  - *Changing audio encoding during session*
- **Encryption fix**
  - *DES – breakable (like other technologies and products)*
  - *If SIP used, DES key sent in clear with SDPs "k" parameter*
  - *Actually introducing more delay and jitter*

No Holy Grail Security Infrastructure

- **Each company unique**
  - *What works for them may not work for you*
- **No vendor offers perfect solution**
  - *Prove it*
- **No solution is complete**
  - *Layered systems*
- **Layered defense starts with you**
  - *People are best defense*
  - *Policy and procedure critical*

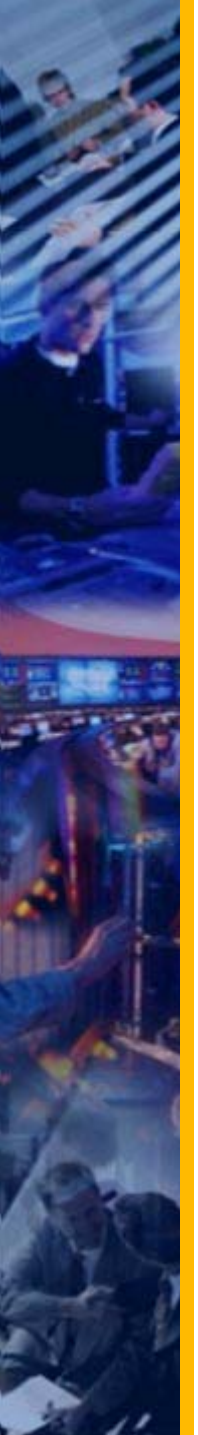


Combating PBX & VM Vulnerabilities

- **First review available documentation**
  - *Voice systems manuals*
  - *NIST Special Publication 800-24 on PBX vulnerability*
- **Internal control and audit**
  - *Centralize telecom services requests*
  - *Develop policy and perform assessments*
  - *Recheck periodically*
- **PBX vendor or 3rd-party reporting**
  - *Look for unusual patterns*
  - *Consider log consolidation*
- **Toll fraud insurance**
  - *May be available from long-distance provider*
- **PBX disaster recovery and continuity plan**

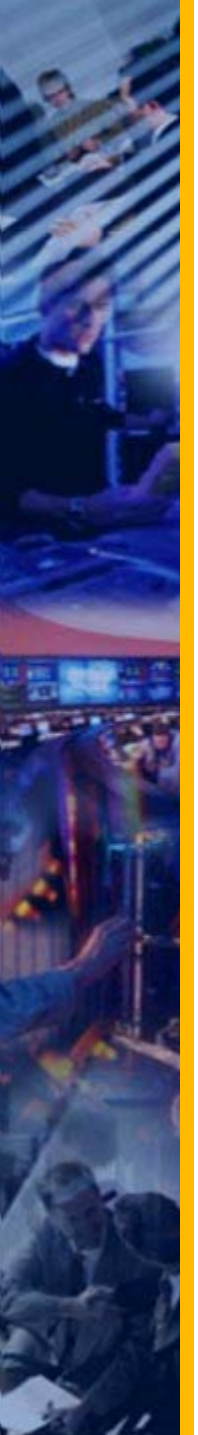
Typical PBX Assessment

- Security policy
- Physical access
- System configuration
- Log
- Disaster recovery plan



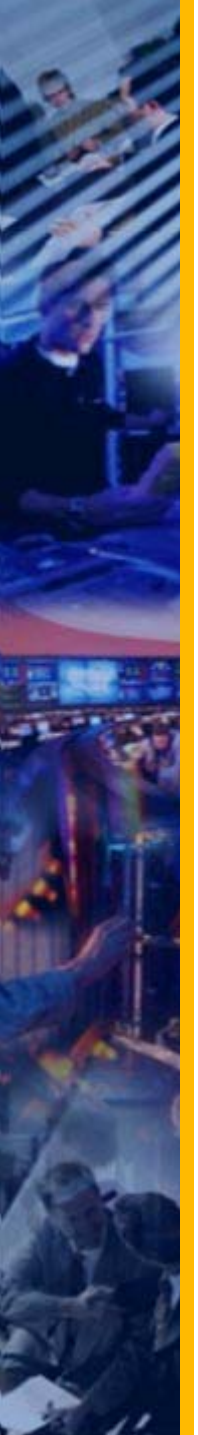
PBX Best Practices

- **Internal control and audit**
  - *Develop policy and perform assessments*
  - *Eliminate unnecessary modems*
  - *Centralize architecture*
- **When vendors use modems for support**
  - *Turn off when not needed*
  - *Use centralized remote access*
  - *Audit usage*
- **Authentication**
  - *Make passwords strong and unique*
  - *Use two-factor authentication: tokens (SecurPBX Agent)*
- **Filter traffic between PSTN/gateways and PBX/IP network**
  - *Telephony firewall*



VoIP Best Practices

- **Build separate DHCP servers**
  - *One for voice (IP phones)*
  - *One for data (PCs)*
- **Disable automated phone registration**
  - *Prevents rogue IP phones from grabbing a directory number from the IP PBX*
- **Monitor MAC addresses within voice segment**
- **Filtering in all segments should limit devices in unknown segments from connecting to IP PBX**

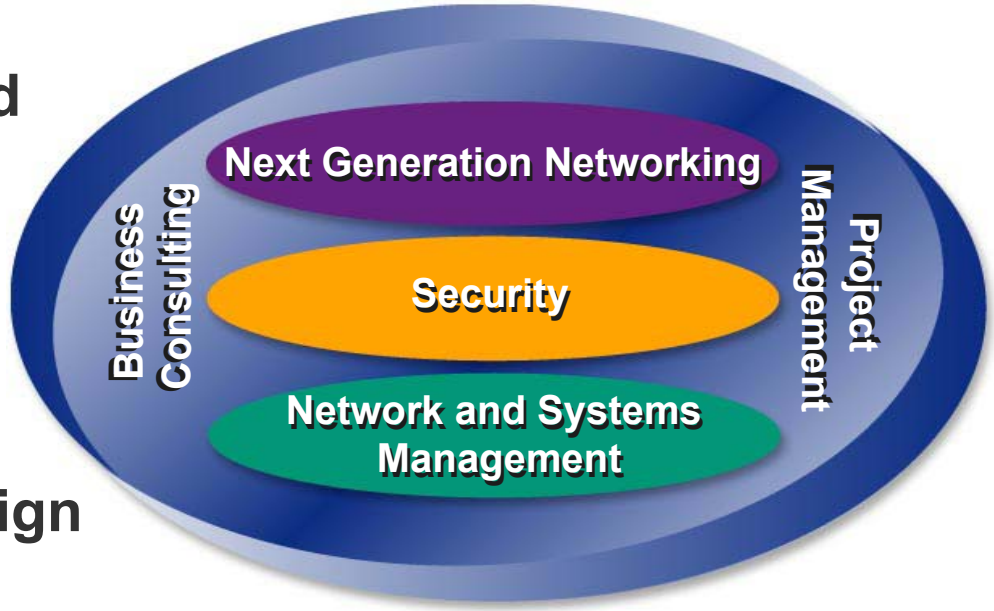


The Bottom Line

- *VoIP security is users' responsibility*
- *Vulnerabilities of voice and data systems carry over to VoIP*
- *Risks too big to ignore*
- *No turnkey solutions*
- *Implement security best practices with unique VoIP security measures*

INS Convergence Consulting Services

- Business strategy and network planning
- Network assessment
- VoIP architecture design
- VoIP implementation
- VoIP operations and optimization



Question and Answer

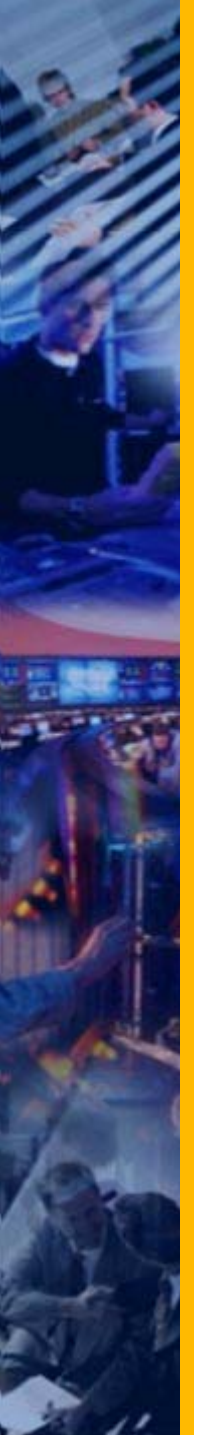
- **Tell us what you think about this webinar**

  http://www.ins.com/knowledge/surveys/feedback.asp

- **Upcoming webinar**
  - *Analyzing Business and Operations Processes for Improved Service Management, August 27th*
- **For more information**
  - *Call 1-888-767-2988 in the U.S., 44 (0) 1628 503000 in Europe, or 1-408-330-2700 worldwide*

INS Resources

- **White Paper**
  http://www.ins.com/knowledge/whitepapers.asp
  - *Voice Over IP: An Overview for Enterprise Organizations and Carriers*
- **NetKnowledge Webinars**
  http://www.ins.com/knowledge/webseminar_archives.asp
  - *Getting Started on Voice Over IP*
  - *VoIP Design Challenges and Solutions*
- **Survey Reports**
  http://www.ins.com/knowledge/surveys.asp
  - *Network Convergence*
  - *Network Quality of Service*



Glossary

- DES – Data Encryption Standard
- DoS – Denial of Service
- MEGACO – Media Gateway Controller
- MGCP – Media Gateway Control Protocol
- PBX – Private Branch Exchange
- RTCP – Realtime Control Protocol
- RTP – Realtime Transport Protocol
- SCTP – Stream Control Transmission Protocol
- SDP – Session Description Protocol
- SIP – Session Initiation Protocol
- SSRC – Synchronization source identifier (RTP header)
- TCP/IP – Transmission Control Protocol/Internet Protocol
- VoIP – Voice over Internet Protocol