

# The Porous Perimeter: Secure Collaboration

Andreas M. Antonopoulos  
Senior Vice President & Founding Partner  
Nemertes Research Inc.  
Spring 2005  
[andreas@nemertes.com](mailto:andreas@nemertes.com)



- ⊕ Introduction
- ⊕ Who is Nemertes?
- ⊕ Defining Collaboration
- ⊕ The Porous perimeter
- ⊕ Security is a top concern, so it gets top funding (NOT!)
- ⊕ Converged networks – Converged Threats (lose-lose)
- ⊕ Solutions
- ⊕ Collaboration as a security enhancer!

# Who is Nemertes?

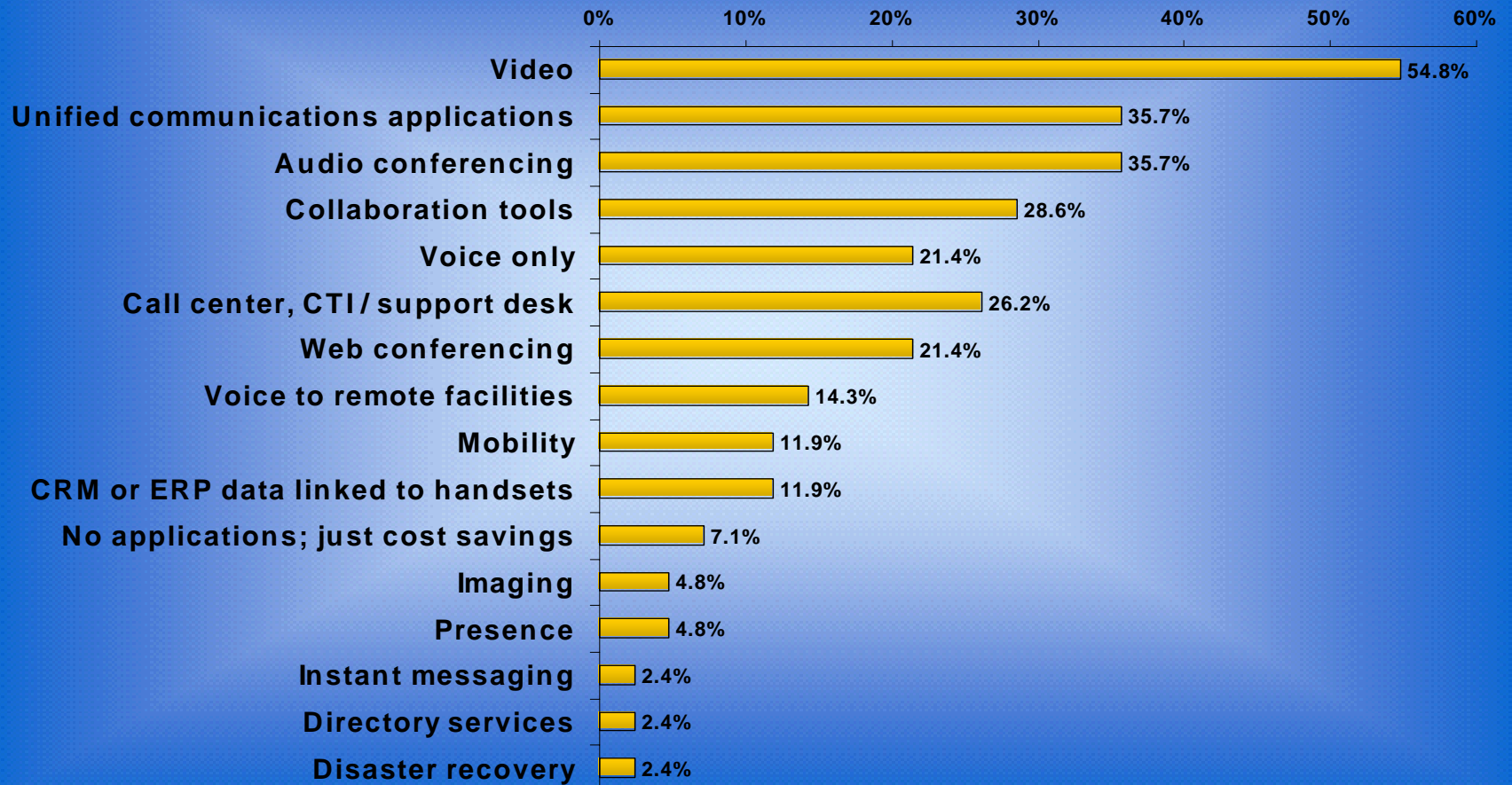
- ⊕ Business Impact of Emerging Technologies
- ⊕ In-depth interviews with IT executives from different industries
- ⊕ Quantitative data and qualitative analysis

# Collaboration Technologies

- ⊕ IM
- ⊕ Voice
- ⊕ Video
- ⊕ Shared Workspaces (documents, whiteboards, apps)

# Applications Drivers

What applications are driving your convergence project?



# The Porous Perimeter

- ⊕ Organizations are becoming more interconnected
- ⊕ Partners, suppliers, customers are all connected into the data center
  
- ⊕ Organizations are becoming more “virtual”
- ⊕ 87% of workers are remote from HQ and their managers
  
- ⊕ Organizations are becoming more mobile
- ⊕ Collaboration on phones and wireless PDAs

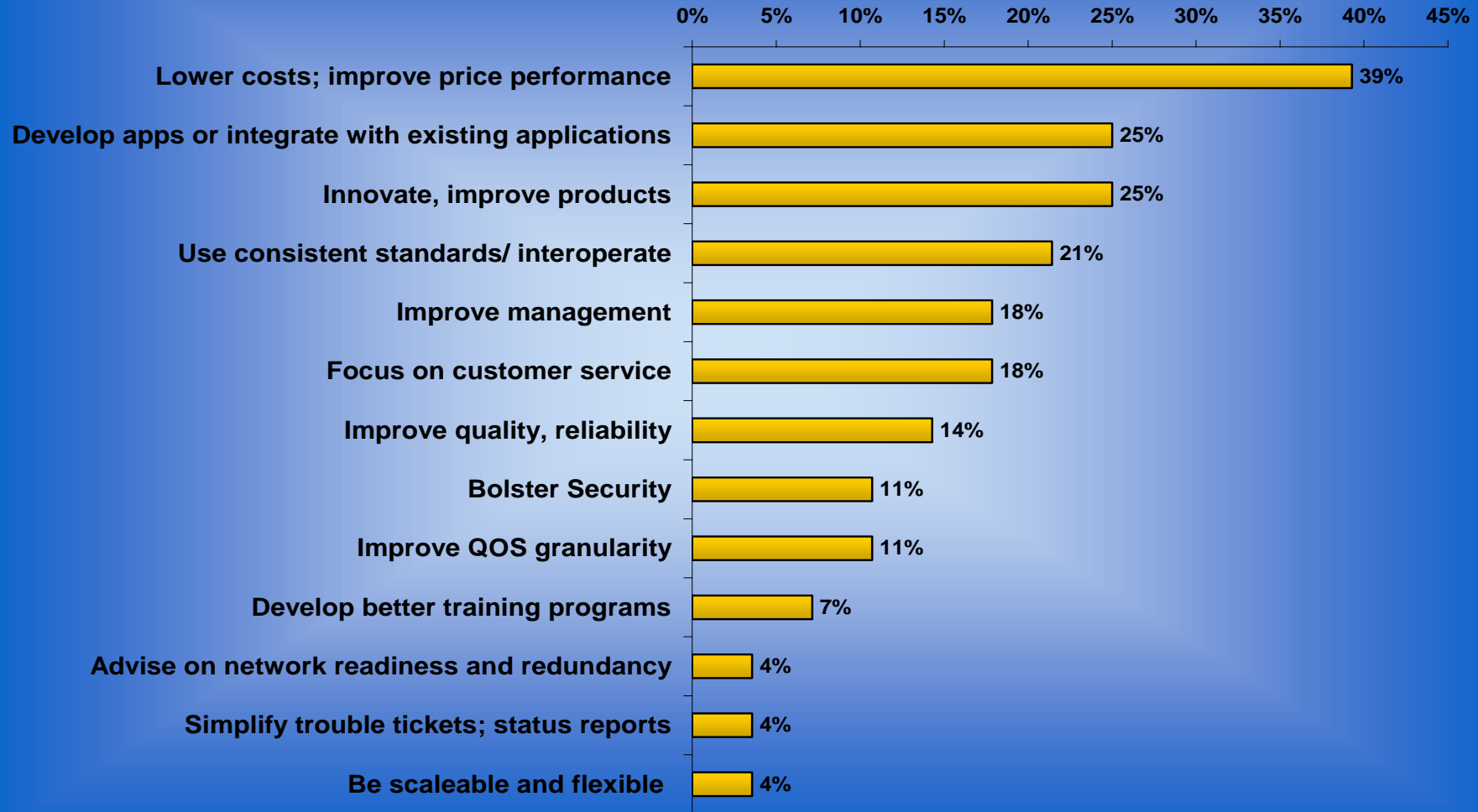
# The Porous Perimeter

- ⊕ Not much of a distinction between “us” and “them” on the network
- ⊕ Perimeter firewalls and gateways are only partially effective
- ⊕ Perimeter around each desktop/laptop?

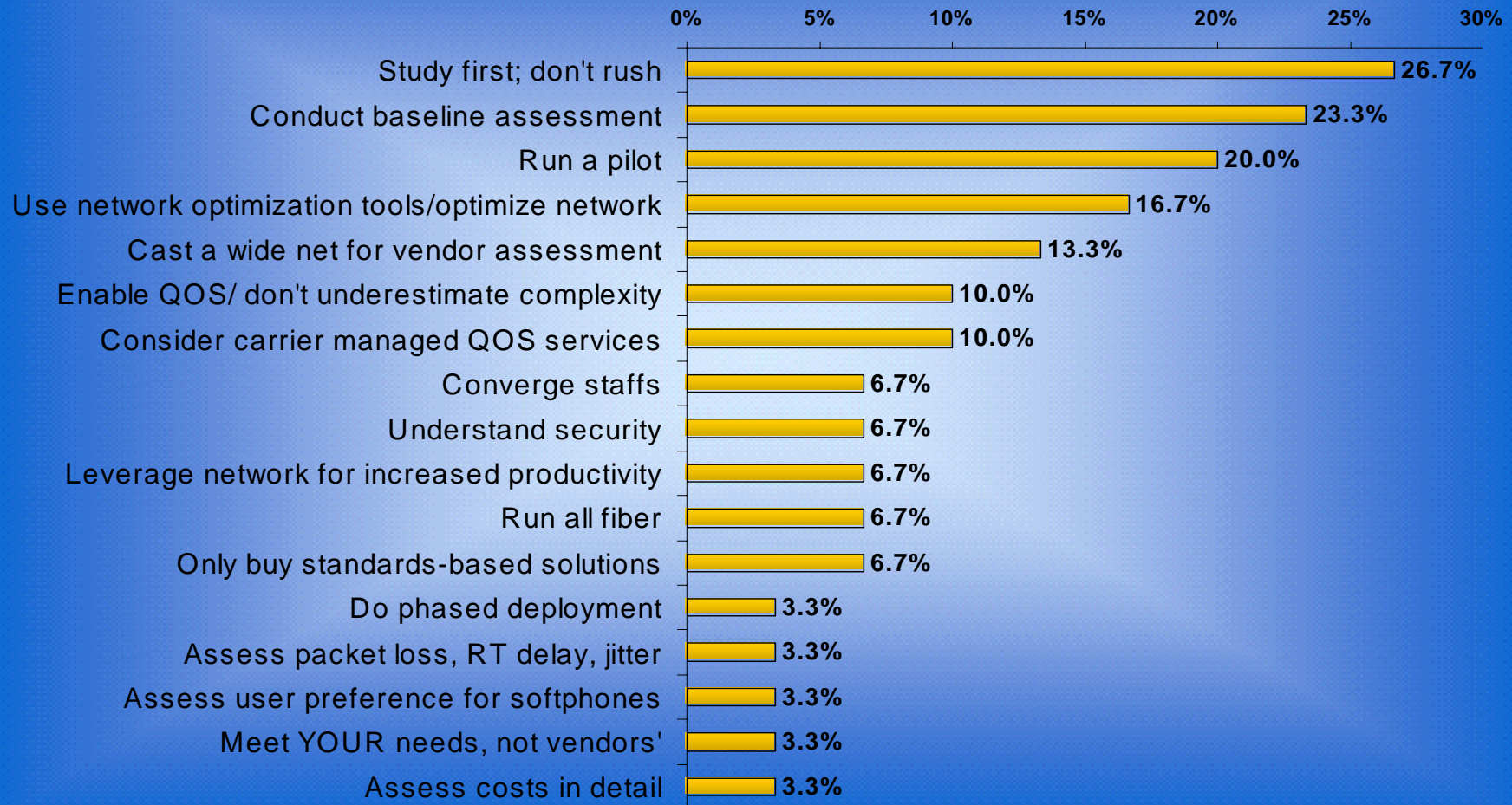
# Collaboration Security Challenges

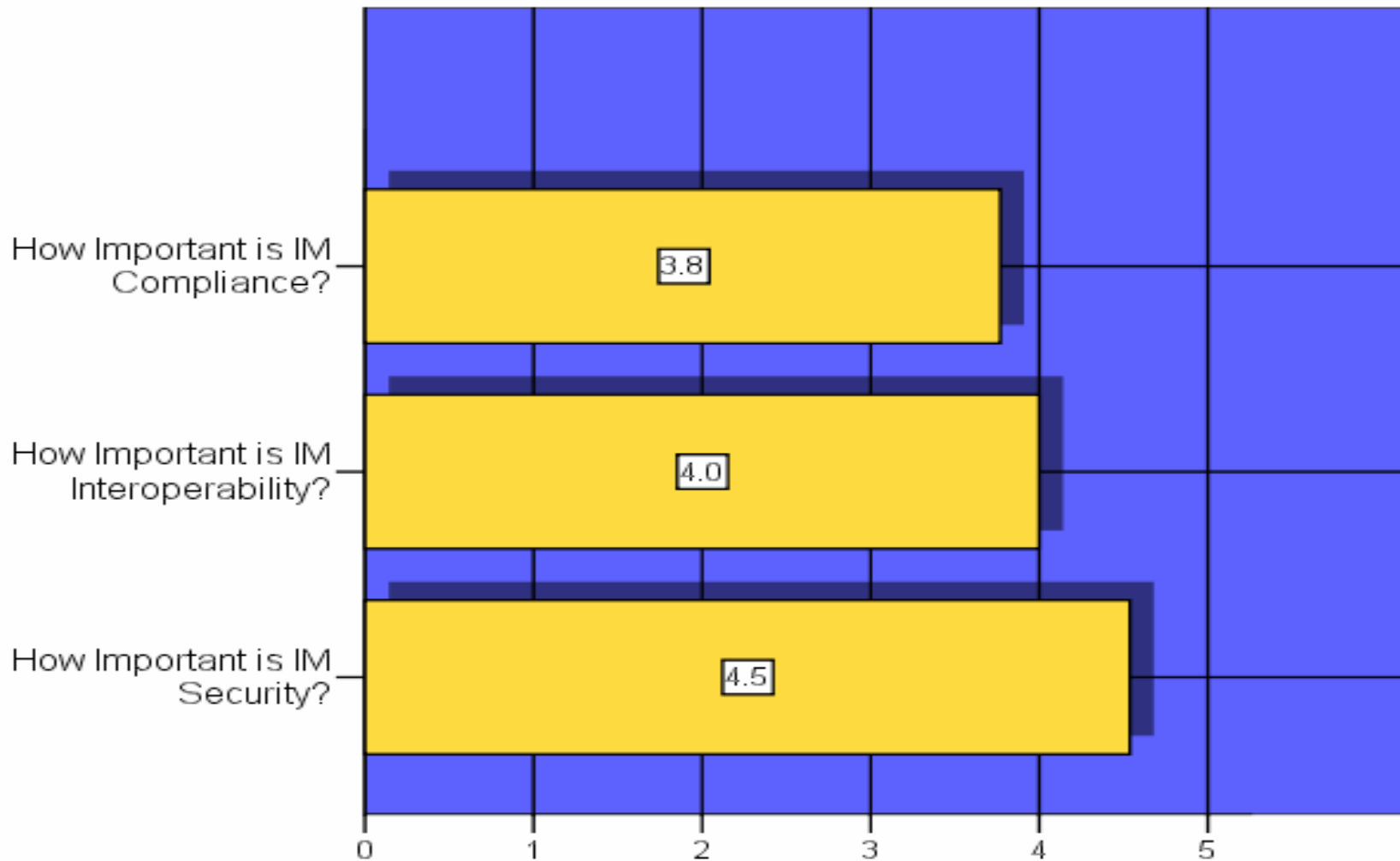
- ⊕ In practice, collaboration security is:
  - ⊕ Not a top concern for IT executives
  - ⊕ Not a top concern for vendors
  - ⊕ Not the responsibility of a single group within a company
  - ⊕ Not clearly understood

# Vendor Recommendations

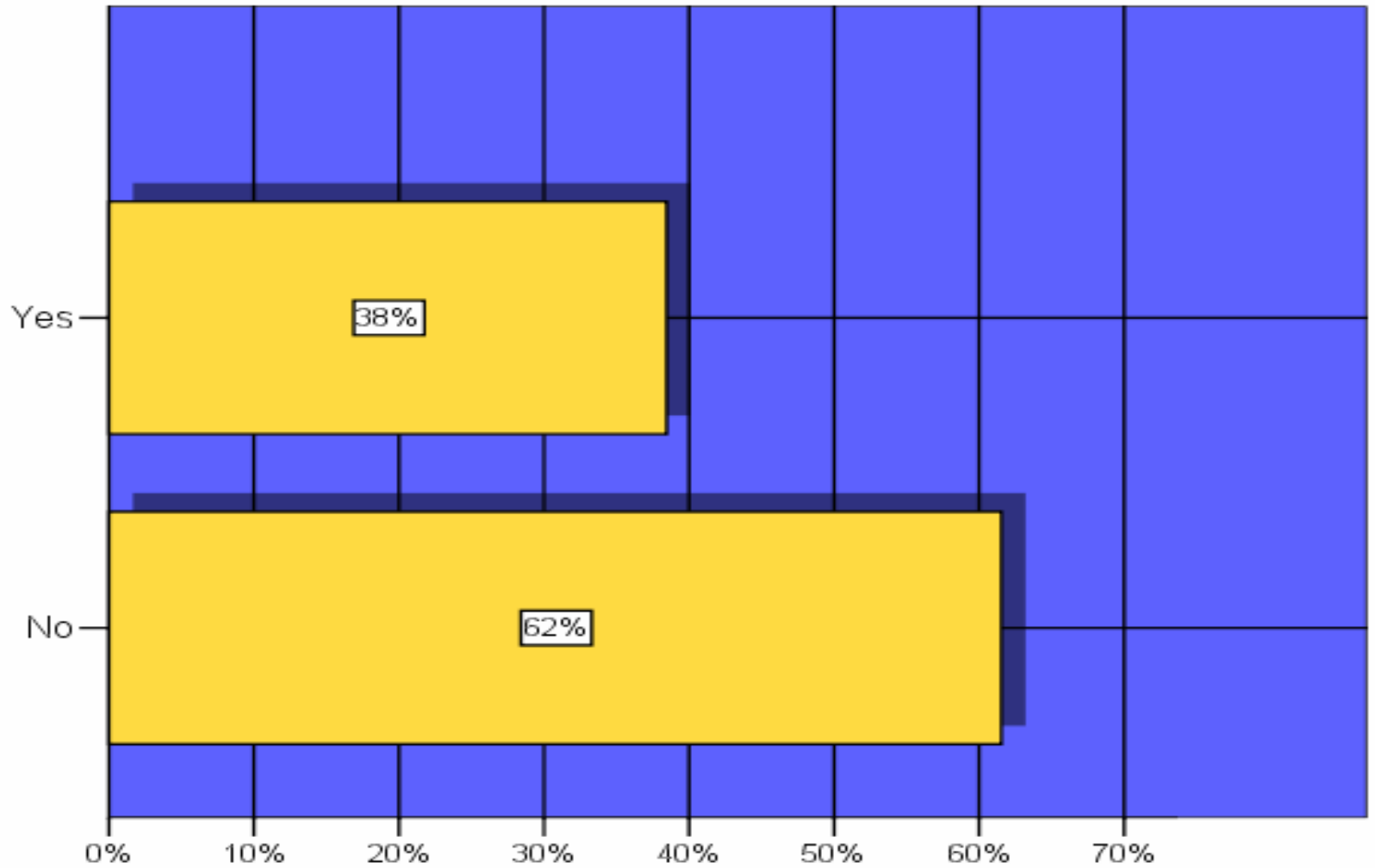


## What do you recommend to your peers?

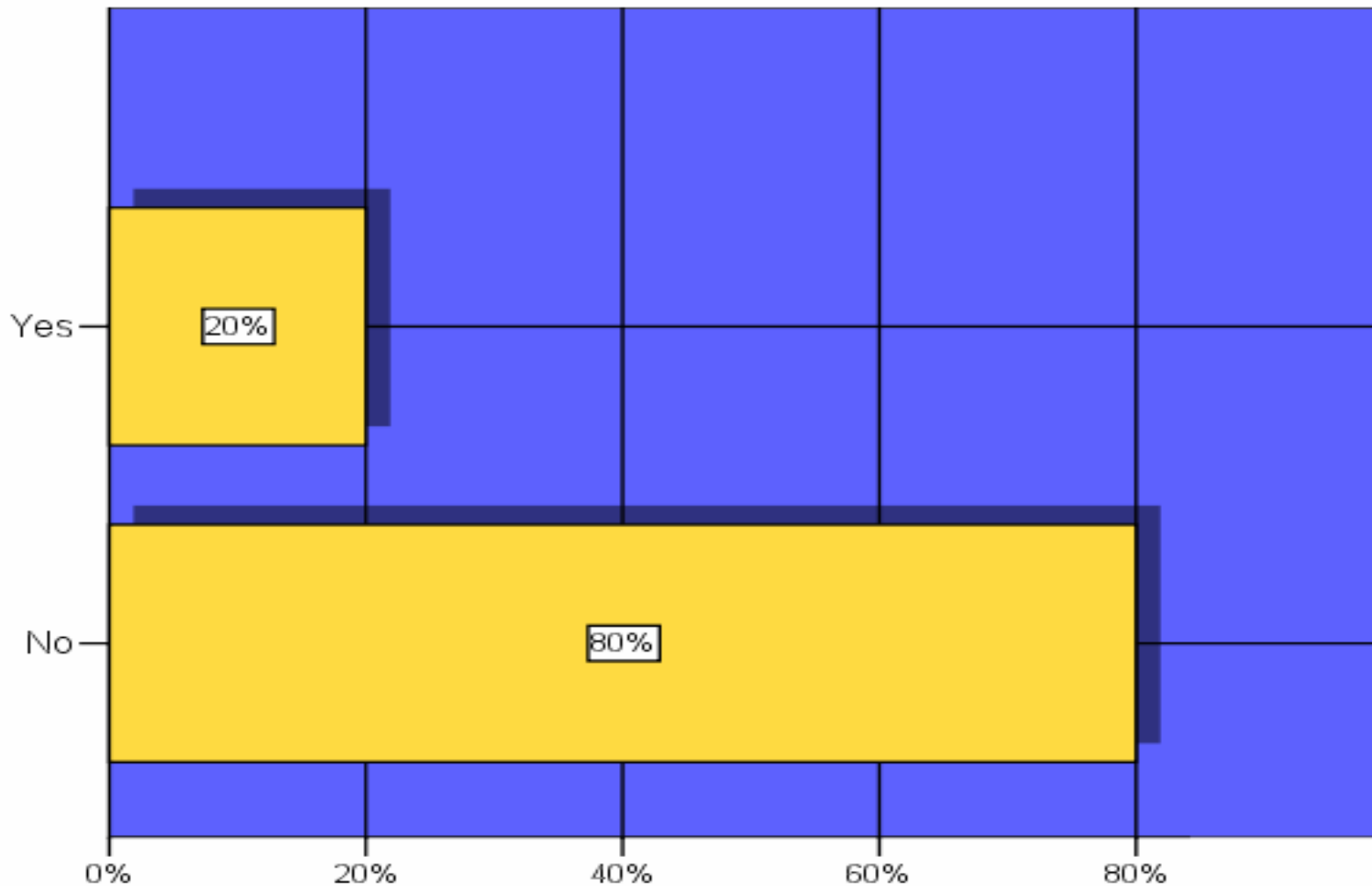




Do You Place Restrictions on the Use of IM?



# Do You Use and IM Gateway?



# Collaboration Security Challenges

- ⊕ Converged networks – Converged Threats
- ⊕ All the traditional problems:
  - ⊕ Weak operating system security
  - ⊕ Buggy applications
  - ⊕ Weak protocol implementations
  - ⊕ Weak security standards (which are not even applied)
- ⊕ Lead to all the known threats
  - ⊕ Viruses
  - ⊕ Worms
  - ⊕ Information theft/hacking
  - ⊕ Denial of Service

# Converged security threats - IM

- ⊕ But also new “converged” problems:
- ⊕ Privacy problems from leaky presence
- ⊕ Remote monitoring and surveillance
- ⊕ Spoofing and social engineering (who is on the other end?)
- ⊕ “Instant Hacking” – theft of passwords and documents via IM

# Converged security threats - Voice

- ⊕ It's not a phone, it just looks like one
- ⊕ It's not a circuit switched network, it just "feels" like one
- ⊕ It's not on a private, physically secure network
  
- ⊕ Is that a bug on your desk?
- ⊕ Is the microphone off, or is it on?
- ⊕ Caller ID means nothing
- ⊕ DTMF is not an authentication mechanism

# Converged Security threats - Video

- ⊕ Is that a camera on your desk? Is it turned off?
- ⊕ How do you know?
- ⊕ Is that confidential document on your desk?
- ⊕ Is that your acquisition plan on the whiteboard behind you?

# Addressing Collaboration Security Issues

- ⊕ Collaboration technologies are disruptive and paradigm-shifting
- ⊕ Addressing the security concerns will require more than new technology:
  - ⊕ New concepts
  - ⊕ New organizational structures
  - ⊕ New operational processes
  - ⊕ New societal “norms”
  - ⊕ New technologies

# Where is the perimeter?

- ⊕ If the perimeter is porous, does that mean you can't use gateways?
- ⊕ You still have a perimeter, it's just diffuse and therefore not sufficient
- ⊕ You still need gateways, firewalls and IDS/IPS
- ⊕ But you also need new “distributed” approaches to security

# New tools

- ⊕ Some of the new tools that will be important:
- ⊕ Identity Management
  - ⊕ Centralized management
  - ⊕ Distributed enforcement
  - ⊕ Multiple identities (user, device, application, process)
- ⊕ Endpoint Security
  - ⊕ Each entry-point (RA VPN, Ethernet port, Wireless AP) is the perimeter.
  - ⊕ Each node (laptop, desktop, PDA, phone) requires its own perimeter
    - ⊕ IDS/IPS, Firewall, Anti-malware, content inspection/blocking
- ⊕ Compliance/Archiving/Auditing
  - ⊕ Every message needs to be stored and retrievable – IM, Voice, (video?)
  - ⊕ The un-monitored channel is the one used by those hiding

## But also new opportunities

- ⊕ Disaster recovery/continuity
  - ⊕ Voice, Video and IM can be “migrated” on the fly – infrastructure independent
  - ⊕ Location of workers not as important anymore
  - ⊕ Ad-hoc groups and partnerships can be used to address a crisis
- ⊕ Collaboration enhances security
  - ⊕ New models for credentials, trust and reputation
  - ⊕ Instant communications for security alerts and notifications

Thank You!

Questions?