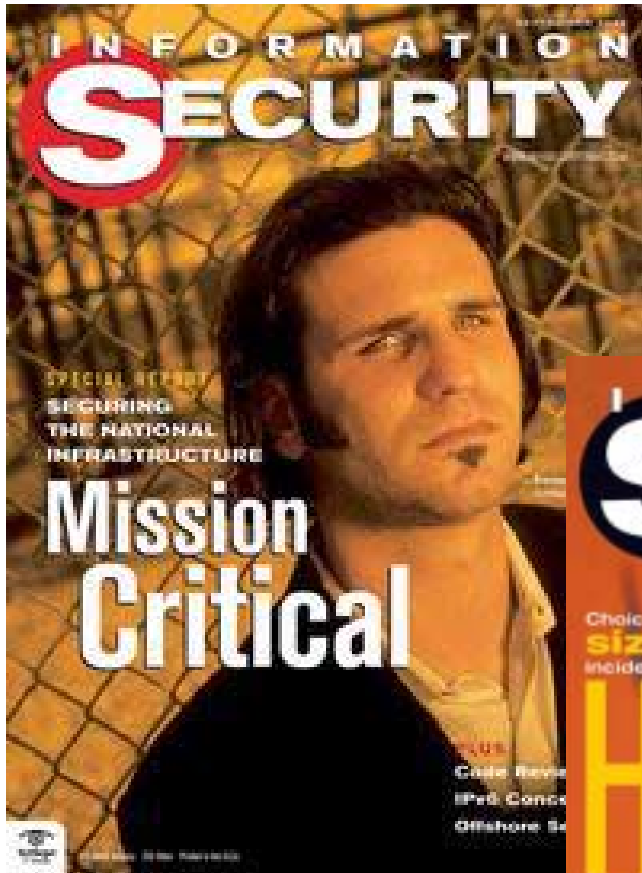




# **The State of Security: 2006**

**Andrew Briney, VP/Group Publisher,  
TechTarget Security Media Group**



# State of Security

- State of Risk
  - **Threat vectors, vulnerability trends**
- State of Risk Management
  - **How security practice and technology is responding**
- State of the Profession
  - **Evolutionary change in security management**



# **Part 1: The State of Risk**

# Threats Are Evolutionary

- # of new viruses/worms rose 30% 04-05, while the # of virus “families” decreased 30%
- Spam continues to account for about 50% of all email.
- DoS attacks rose dramatically in 2H 05, to about 1,500/day
- After dipping in 2003, # of published vulnerabilities rose in 2004 and 2005 (current rate: ~3,800/year)

# Mobility: Growing Risk

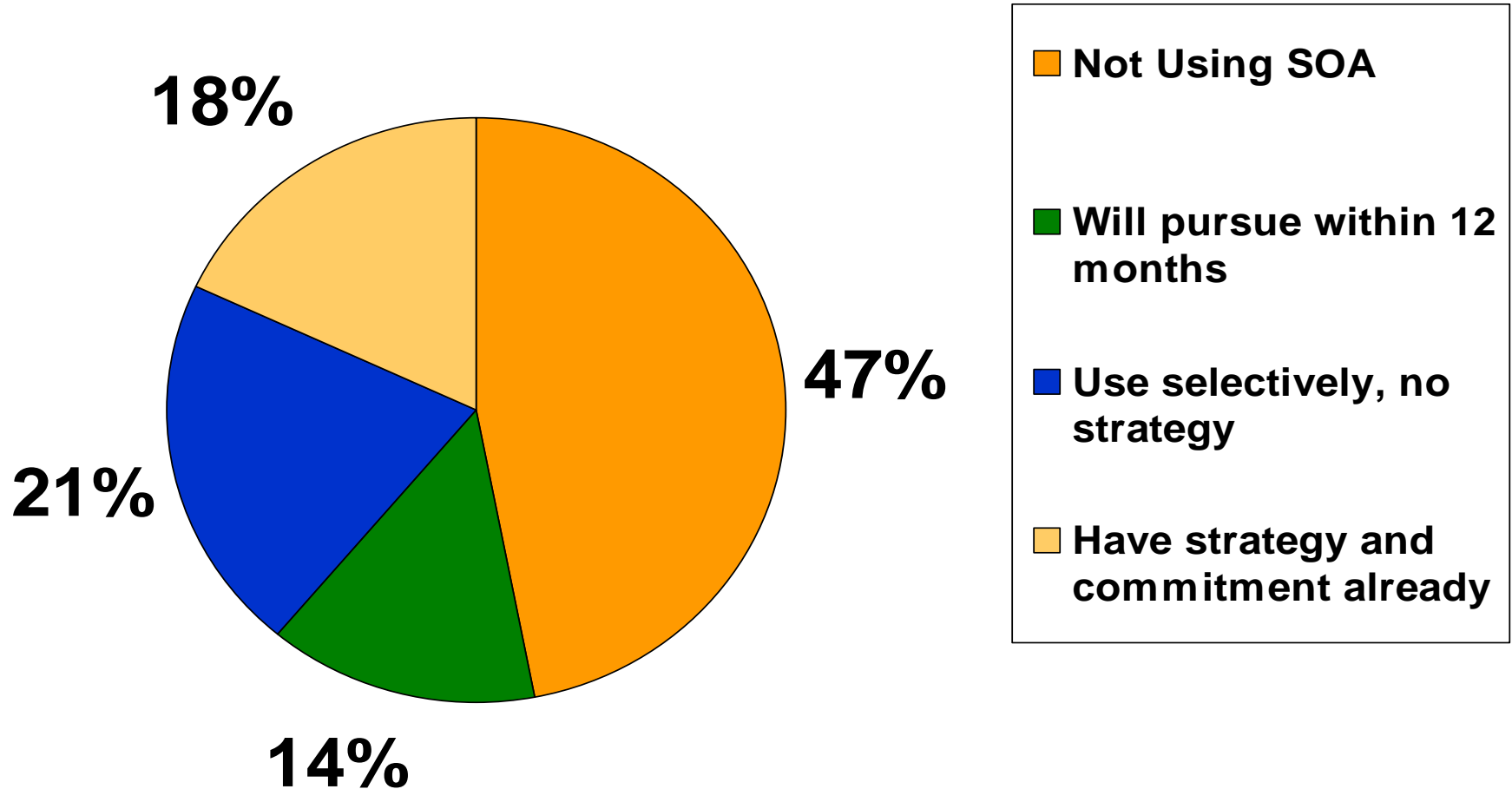
- 2 billion cell phones worldwide
- 50 million smart phones
- 72% of companies say a security policy covering mobile devices is important, but only 35% have such a policy.
- Only 42% of top security decision-makers (CSO/CIO) use passwords on their mobile devices.
- Viruses:
  - Total # of new viruses in 2005: **21,000**
  - Total # of “mobile viruses” in 2005: **225**
  - Total # of “mobile viruses” in 2006: **500 (Est)**

# Threats to Mobile Devices

- Viruses/malware/spam coming from...
  - **SMS Text messaging spam**
  - **Downloads: photos, video, email, ring tones**
  - **Bluetooth connectivity**
- Network connectivity
  - **Wi-Fi servers infected with nasties**
  - **“Greek Watergate”**: Spyware installed on central Vodafone (Ericsson) servers relayed government phone calls to eavesdroppers

# The Rise of “On-Demand”

## SOA Adoption



Source: Forrester Research  
study of 252 enterprises

# Why is SOA Dangerous?

- Reliance on distributed data controls
  - **Lack of best practices for third-party assurance or oversight**
- Non-standardized access control schemas
- Security is a checklist item
  - **Secure coding is a pipe dream**



# **Part 2: The State of Risk Management**

# Top 5 Priorities and Areas of Increased Spending for Information Security Pros

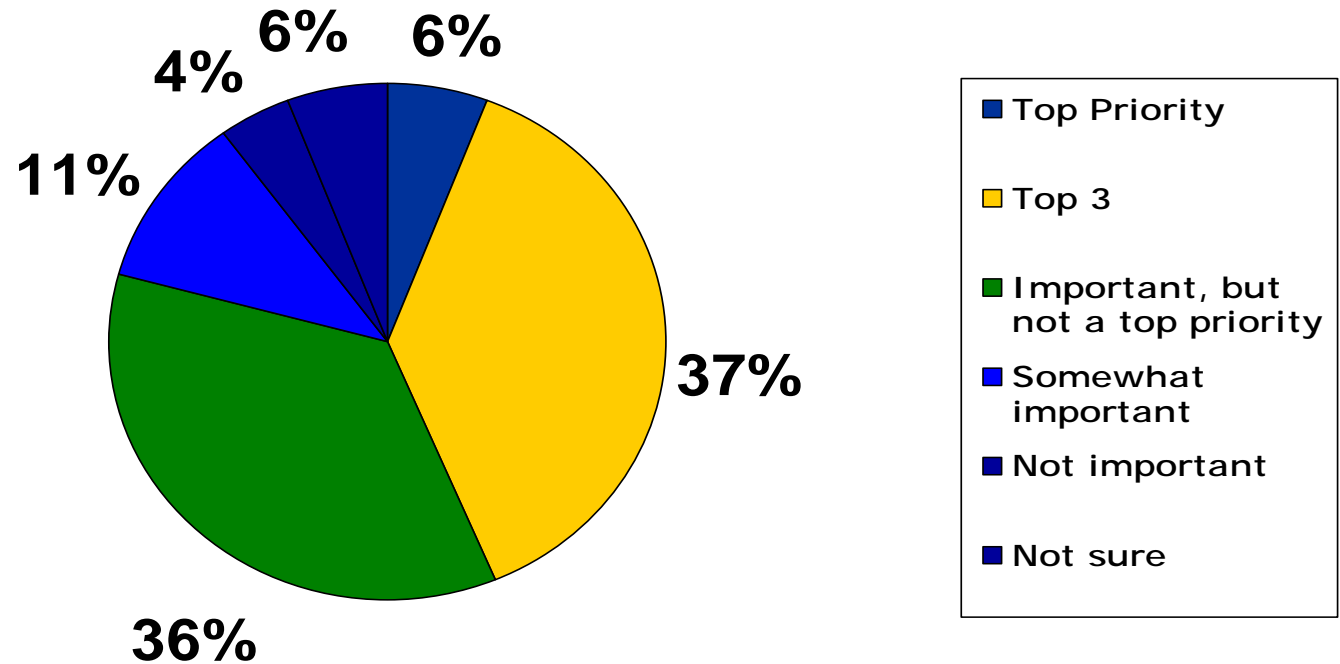
- Wireless Security
  - **#1** area of increased security spending in 2006
- Email Security
  - **#2** area of increased security spending in 2006
- Intrusion Defense
  - **89%** will make a related investment in 2006
- Compliance
  - **78%** call compliance an “important” goal; **63%** expect it to have a “high impact” on their jobs in the next 18 months
- Identity and Access Management
  - **2-Factor authentication and single sign-on are hot**

# Threat Management 2.0

- The move toward broader, more holistic threat management
  - **Consolidation of security functionality**
  - **Fewer point products for most organizations**
  - **Must be manageable by the masses**
  - **Premium on threat intelligence and response**



# How important is fighting spyware?



# More Spyware Stats

- 72% of security managers said productivity drains was spyware's biggest impact (8% said security)
- 58% said spyware will be a bigger threat in 2006 vs. 2005
- 80% have client spyware protection
- 63% have server spyware protection
- 60% have gateway spyware protection
- 52% thought the gov't should regulate spyware

# The Incredible Shrinking Perimeter

- 1996: “Tootsie Pop” Security
- 1998: “Belt and Suspenders”
- 2000: Passive sniffers behind the firewall
- 2002: Bump-in-the-wire security
- 2004: Controlling the app/OS interface
- 2006: Controlling the user/data interface

**Network**



**Host**

# Securing the Last Link

- Source-code vulnerability management
  - **Source code scanners, compile-time analyzers, application scanners**
  - **Ounce Labs, Fortify, RATS**
- IP Leakage/Host access control
  - **Oakley, Vontu, Verdasy, PortAuthority**
- Software/App DRM
  - **Adobe, Aladdin, Workshare**
- End-point security

# An Ounce of Prevention

## Relative Cost to Fix Software (by stage)

Design	“x”
Implementation	6.5x
Testing	15x
Maintenance	100x



# **Part 3: The State of the Profession**

# Security Pros Wear Many Hats

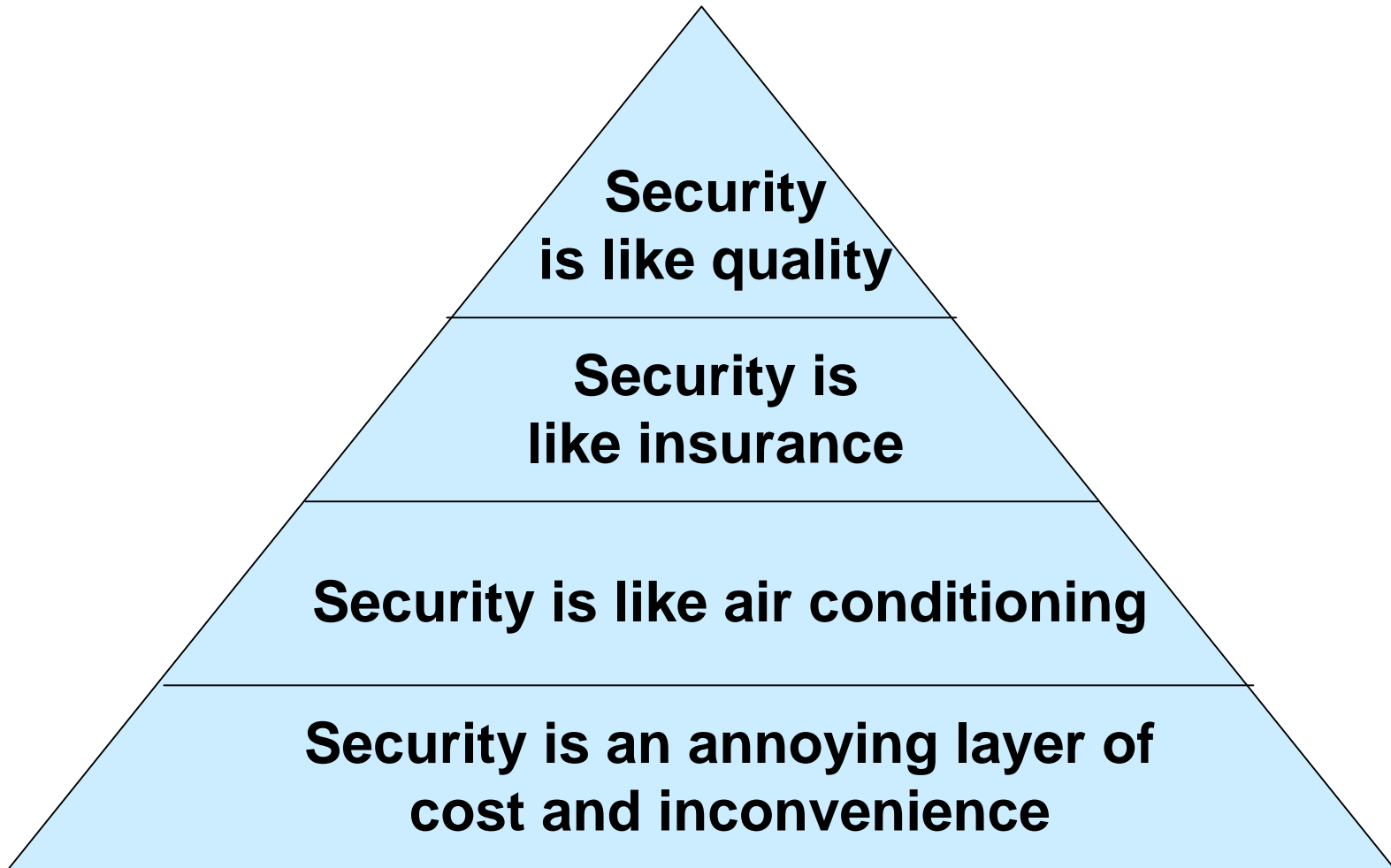
## Challenge

- Simplify security operations
- Maintain proactive defense posture
- Ensure consistent security across the enterprise
- Understand risk trending
- Formalize compliance role

## Response

- Unified Threat Management, automated provisioning, SSO
- Upgrade/replace/broaden intrusion defense systems
- Policy management tools
- Security Info Management
- Reporting, audit tools

# Stages of Security Enlightenment



# The Firefighter

- Sits around until there's an emergency.
- Puts out fires, but the damage is already done.
- Homeowners think about fire prevention only after their house burned down.



# The Dentist

- **Fixes cavities, but always urges dental hygiene.**
- **Brushing isn't enough; you have to floss, use mouthwash, massage your gums, and get routine checkups.**
- **Your password is like a toothbrush: Change it often, and don't share it with others.**



# Professionalism

- Certifications continue to rise
- The “businessification” of the security professional
  - **72% of business executives said a CISSP is more important than an MBA for ISOs**
  - **However, the skills they covet most are...**
    - Communication
    - Understanding business operations and finance
    - Strategic planning
    - Motivation with a carrot and stick

# Some Resources

- SANS/Internet Storm Center
  - [www.sans.org](http://www.sans.org)
- SecurityFocus
  - [www.securityfocus.com](http://www.securityfocus.com)
- CyberSecurity Industry Alliance
  - [www.csialliance.org](http://www.csialliance.org)
- [www.insecure.org](http://www.insecure.org)
- [www.cccure.org](http://www.cccure.org)
- SearchSecurity
  - [www.searchsecurity.com](http://www.searchsecurity.com)
  - [www.searchsecurity.com/securityschool](http://www.searchsecurity.com/securityschool)