

Implementing Effective Security

Dave Piscitello
Core Competence

Homeland Security in the United States and similar international security initiatives around the globe underscore how seriously we all must take security, in the real world as well as in cyberspace. How real are cyber threats, and whom should we be most afraid of? Learn about the mind-sets, motives, methods, tools, talents and targets of cyber-criminals and terrorists. This session also identifies 10 practices you can implement immediately to minimize your company's exposure in these challenging times.

State of Security: 2004

More

- Regulations,**
 - Media interest and coverage,**
 - Innovations,**
 - Certification programs, and**
 - F.U.D.,**
- than any other technology sector**

Regulatory terrain

More complicated each year

- **CyberRegs:** Patriot Act, California Security Breach Information Acts (CA1798),
- **Privacy acts:** HIPAA, COPPA, HCFA, GLBA, European Safe Harbor Act
- **Accountability acts:** Sarbanes Oxley
- **Random acts:** demanding compliance and preparedness considerations: Legal discovery, SEC/NASD (broker email inspection, archival)
- **Acts of Contrition:** President's Cyberstrategy, leaves private sector responsible for policing itself

4Th Estate

Another downside to Homeland Security

- **Cracking is glamorized**
 - Lamo's a homeless hero
 - Mitnick gives keynotes
- **Forensics and Pen-testing are "in"**
- **Beltway TLAs are out... no wait, in!**
 - Chastised in print
 - "Bumbling knuckle-draggers"
 - Glamorized on screen
 - **Fabulous Blonde Investigator**
 - **Cuddly Intelligence Agent**

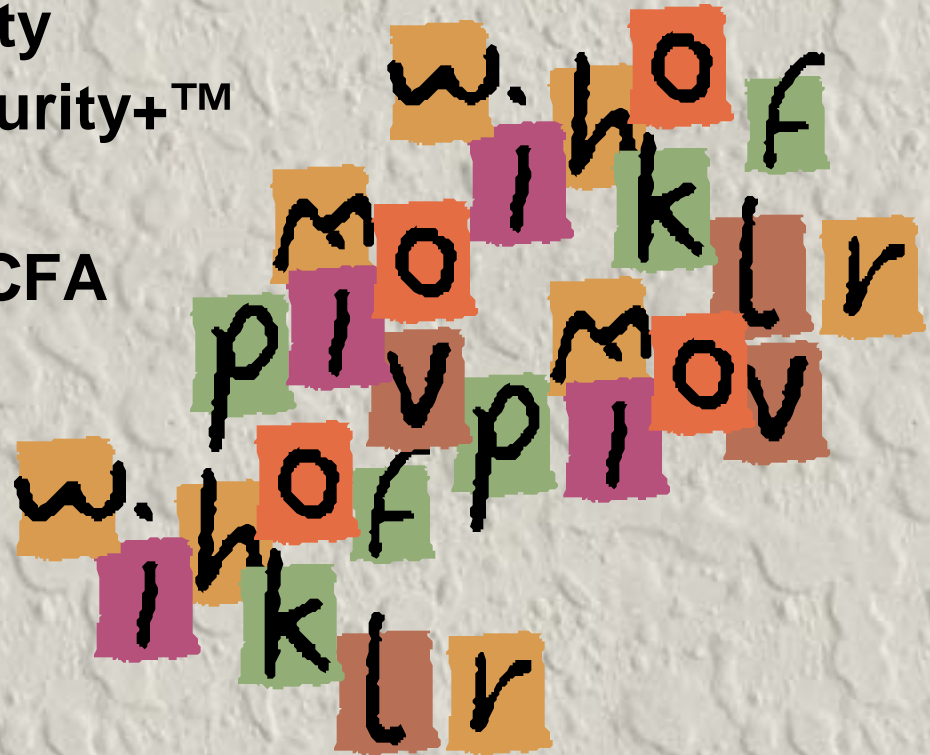


Innovations

- **Application level IDS and firewalls**
- **Application vulnerability assessment**
- **Antispam heuristics, Bayesian filters**
- **Admission control, self-protecting networks, host integrity checking (scan on connect)**
- **Authenticated email (auto keypair creation)**
- **Digital Rights Management Service**
- **Next-Generation Secure Computing Base**
- **Risk Management Systems**
- **VOIP firewalls**
- **WLAN Security (WPA, EAP/802.1x)**

Certifications

- CISSP
- ISSAP
- MCSE+Security
- CompTIA Security+™
- SCNP/SCNA
- GIAC GSE, GCFA
- EnCE
- ISCA CSA
- CCCI/CCFI
- CFCE
- CIW
- NSCP
- AIS



F.U.D. (Act 1): Cyberterrorism & Warfare

Dire warnings from the experts:

- **Our values and way of life are threatened!**
- **Cyberwarfare is imminent!**
- **Critical infrastructures are vulnerable!**
 - **What if the power is lost FOREVER?**
 - **What if our water supply is poisoned?**
 - **How will you function without fossil fuel?**



F.U.D. (Act 2): Pop Threats

Those pesky reporters warn us against:

- DOS attacks
- spam
- Spyware, contagions, malware and worms
- Phishing and Identity theft
- SQL Injection: the media doesn't actually know what this is but it's bad, right?



The 'net is **OUT OF**
CONTROL!

Live Webcam report at eleven...



**Separating F.U.D.
from Fiction**

Cyberthreats: F.U.D. or Fiction?

- **Opinions range from, “Yougoddambetcha” to “The whole notion of cyberwarfare is a scam”**
Marcus Ranum, author, *Myth of Homeland Security*
- **A practical perspective**
 - **Critical Infrastructure *networks* are NETWORKS**
 - They use COTS OSs and applications
 - They use much of the same technology you use
 - Their staff is no more skilled than yours
 - They are as reluctant as everyone else to spend money on security
 - **Ditto for non-military and DHS departments**

Real Issues to Consider

- **Should critical infrastructure and (non-military) agencies consider a higher weighting factor when assessing risk?**
 - If yes, expect rate hikes and higher taxes;
 - If no, expect security on par with your network. *Are you comfortable with this?*
- **Should they be held to higher standards?**
 - Who will develop, audit and oversee compliance to such standards?

Pop Threats: F.U.D. or Fiction?

- **Do we want to continue to deal with theft, malice, nuisance behavior and invasion of privacy?**
- OR
- **Are we willing to eliminate this “noise” over signal by implementing**
 - **Ingress address filtering (ISP)**
 - **Egress traffic filtering (your firewall)**
 - **Non-repudiable email**
 - **SSL everywhere**
 - **Strong client and consumer Identity Mgmt**
- **Both alternatives are expensive, but only one is a solution**

Analysis: Quantifying the Threats

Carnegie Mellon
Software Engineering Institute

CERT® Coordination Center

Home Site Index Search Contact FAQ

vulnerabilities, incidents & fixes | *security practices & evaluations* | *survivability research & analysis* | *training & education*

Options

[Vulnerabilities, Incidents & Fixes](#)

CERT/CC Statistics 1988-2003

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	2003
Incidents	21,756	52,656	82,094	137,529

Total incidents reported (1988-2003): **319,992**

Vulnerabilities reported

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2003

Year	2000	2001	2002	2003
Vulnerabilities	1,090	2,437	4,129	3,784

Total vulnerabilities reported (1995-2003): **12,946**

CSI/FBI 2003 Computer Crime Survey also reports drop in losses reported

Interpreting the numbers

- **Incidents and reported losses are down:**
 - We are paying more attention to security
 - Technology is improving, buy more!
 - Certification programs are assuring we all have plenty of in-house expertise
- OR
 - The expert attackers are eluding us (still)
 - Inflated loss figures of 2002 are no longer credible
 - Companies aren't reporting incidents that involve custom applications and proprietary software

Interpreting the numbers

- **Vulnerabilities reported are down**
 - We are paying more attention to security
 - Technology is improving, buy more!
 - Certification programs are assuring we all have plenty of in-house expertise

OR

- All the easy vulnerabilities have been reported
- Important vulnerabilities are not being reported
 - Who reports a vulnerability discovered in a custom (web) application? To whom?

Why the Skepticism?

- I've become an industry curmudgeon 😞
- Traditional targets are no longer interesting to attackers
- Application access is the all the rage, and so is application level 'cracking'
 - Everything is web
 - Web is open everywhere
 - Web applications and scripts are even more exploitable than COTS applications and OSs
 - Web authentication is (mostly) weak
 - Web access exposes back end applications and databases

Why the Skepticism (part 2)?

- We really have not improved how we
 - Develop software
 - Ship software
 - Patch software
 - Define and implement policy
 - Configure software and systems

I see Doubting Thomas in the audience...

Next Slide



Metric	ID	Date Public	Name
108.16	VU#16532	11/10/99	BIND T_NXT record processing may cause buffer overflow
104.73	VU#41870	04/03/99	Sun Solstice AdminSuite ships with insecure default configuration
99	VU#945216	02/08/2001	SSH CRC32 attack detection code contains remote integer overflow
94.5	VU#254236	09/10/2003	Microsoft Windows RPCSS Service contains heap overflow in DCOM request filename handling
94.5	VU#483492	09/10/2003	Microsoft Windows RPCSS Service contains heap overflow in DCOM activation routines
89.5	VU#150227	02/19/2002	Multiple vendors' HTTP proxy default configurations allow arbitrary TCP connections
87.72	VU#29823	06/23/2000	Format string input validation error in wu-ftpd site_exec() function
81	VU#5648	07/27/98	Buffer Overflows in various email clients
79.65	VU#970472	04/04/2001	Network Time Protocol ([x]ntpd) daemon contains buffer overflow in ntp_control:ctl_getitem() function
79.31	VU#789543	05/14/2001	IIS decodes filenames superfluously after applying security checks
78.75	VU#568148	07/16/2003	Microsoft Windows RPC vulnerable to buffer overflow
78	VU#117394	03/17/2003	Buffer Overflow in Core Microsoft Windows DLL
76.5	VU#323070	11/25/2003	Outlook Express MHTML protocol handler does not properly validate input
74.81	VU#745371	07/18/2001	Multiple vendor telnet daemons vulnerable to buffer overflow
73.5	VU#411332	07/16/2003	Cisco IOS Interface Blocked by IPv4 Packet
73.1	VU#28934	12/14/99	Sun Solaris sadmind buffer overflow in amsl_verify w
69.3	VU#952336	06/18/2001	Microsoft Index Server/Indexing Service used by IIS 4.0/5.0 contains unchecked buffer used when encoding double-byte characters
69.25	VU#107186	02/12/2002	Multiple vulnerabilities in SNMPv1 trap handling
68.4	VU#111677	10/10/2000	Microsoft IIS 4.0 / 5.0 vulnerable to directory traversal via extended unicode in url (MS00-078)

11 of top 20 "severe" vulnerabilities are **BUFFER, HEAP, or INTEGER OVERFLOWS**

5 of top 20 are **INPUT VALIDATION ERRORS**

2 of top 20 exploit **DEFAULT CONFIGURATION**

Add **1** of each if you use **SNMP**

Multiple vulnerabilities in SNMPv1 trap handling

How Serious are the Threats?

- **Depends...**
 - **Who are you? What's motivating someone to attack *you*?**
 - **What are you protecting?
What's it worth?**
 - **How did you determine this?**
 - **What are you running in your shop?**
 - **How did you choose these technologies?**
 - **How good are your staff? Processes?**
 - **How are you measuring these?**

Proactive Security

**Processes, expertise, and culture
(compliance) are more important
than technology**

Proactive Security

10 ways to deal with security as a business process

- Know your company, competencies, assets
- Know what you should fear
- Know your enemy
- Make security awareness a priority
- Mind your business
- Keep tabs on how your partners are minding their businesses
- Track how your peers and competition are minding their businesses

Yeah, that's only 6.. I don't have time for 10

Know your company

- **What should you protect first?**
 - What do you do to make money?
 - What resources are critical to making money?
 - Web presence?
 - Databases?
 - Intellectual property?
 - Other (how about “people”)?
 - How can someone stop the money flow?
 - Disruption/Interference (denial of service)
 - Destruction
 - Theft
 - Me, too technology
 - Litigation (injunction, discovery, ...)

What Should You Fear?

- **Shoddy software: COTS and yours**
- **Shoddy operations**
- **Weak knowledge base and expertise**
- **Haste-to-market technology**
- **Technology purchased in haste**
- **Haste-to-production deployment**
- **Ignorance**

Whom Should You Fear?

Cyber-criminals, Terrorists, Radicals

- Funded, sophisticated

(Disgruntled) Employees

- Insider knowledge

Competitors

- Funded, possibly state-assisted

Egoists, script-kiddies, ankle-biters

- 90% of the noise and attention
- Varying degrees of talent, not funded



**T
H
R
E
A
T**

Security Awareness

- Ignorance is no excuse, but it *is* a major source of security incidents
- Educated users are
 - Less likely to fall victim to social engineering, worm attacks...
 - More likely to maintain antivirus definitions and patch levels
 - More likely to comply with AUPs, authentication methods, access controls...
- Users who understand *why* a security measure is imposed are more likely to comply

Mind Your Business

- **Improve your software evaluation and development processes**
 - Investigate QA methods of your commercial software providers
 - Insist developers (in-house and hired) employ secure coding methodologies
- **Evaluate operations areas & processes:**
 - Policy management, communication, compliance
 - Configuration control, audit, archive
 - User (Identity) management
 - Patch management
 - Software license management...

Mind Your Business (cont.)

- **Invest in expertise first, policy second, technology last**
 - You can't develop policy without folks who know the business, risks, and threats
 - You can't fully leveraged technology unless you have staff with talent to master it
 - Most security technology is underutilized
- **When hiring, consider (in this order):**
 1. Experience
 2. Character
 3. Breadth of experience
 4. Communications skills
 5. Certification

Mind your Business (cont.)

- **Haste hurts...**
 - **Haste-to-market technology is easy to identify**
 - **Are all the essentials ready-for-market?**
 - **Technology purchased in haste will break your heart**
 - **A “must-have” feature is like the elusive blonde in the Red Corvette: you forget the traffic around you**
 - **Haste-to-production = recipe for disaster**
 - **Test, develop a plan to transition to production, have a roll back plan**
 - **Underestimating or overlooking the implied security of the test environment will kill you**

Mind your partner's business

- **Partners, clients, and customers**
 - **Their client systems can**
 - **Infect your systems**
 - **Attack your systems (blended threat hosts)**
 - **Their VPN connections are potential vectors for unauthorized access**
 - **IdM processes may be interdependent**
 - **User add, drop, change, password reset**
 - **Credential protection**
 - **Education and attitude towards compliance**

If you cannot directly control or influence their processes, develop AUPs, legal framework

Track your peers, competitors

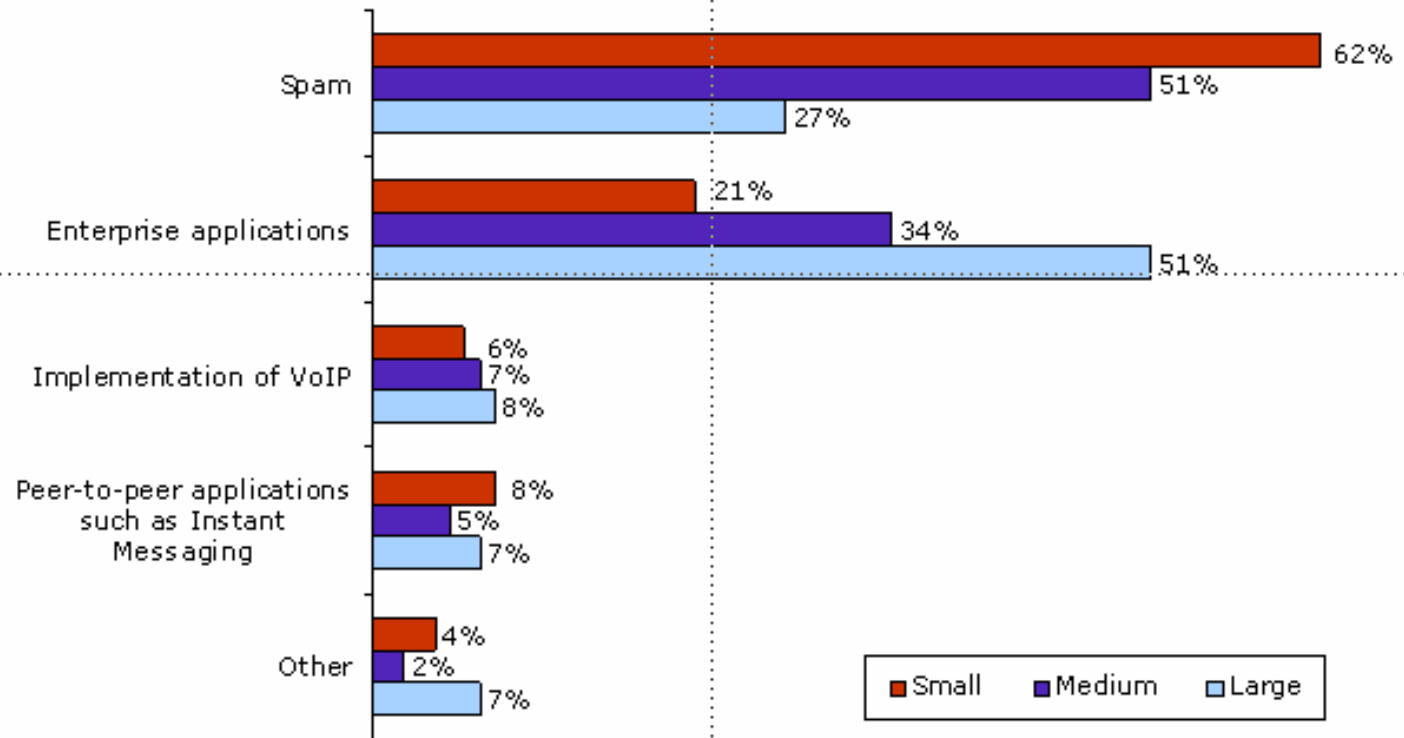
- **What are the top concerns among enterprises like yours?**
- **Get a copy of N+I's *Networking Issues Survey 2004***
 - **Fielded by independent 3rd party research firm, March 23 - 29, 2004**
 - **A random sample of NetWorld+Interop pre-registrants were invited by email to participate in an online survey**
 - **Results represent a total of 363 respondents**

2003 CSI/FBI Computer Crime and Security Survey represented 530 respondents

Teasers from survey...

**NETWORLD
+ INTEROP**
LAS VEGAS • MAY 9-14, 2004

Biggest Resource Drain on Network By Company Size



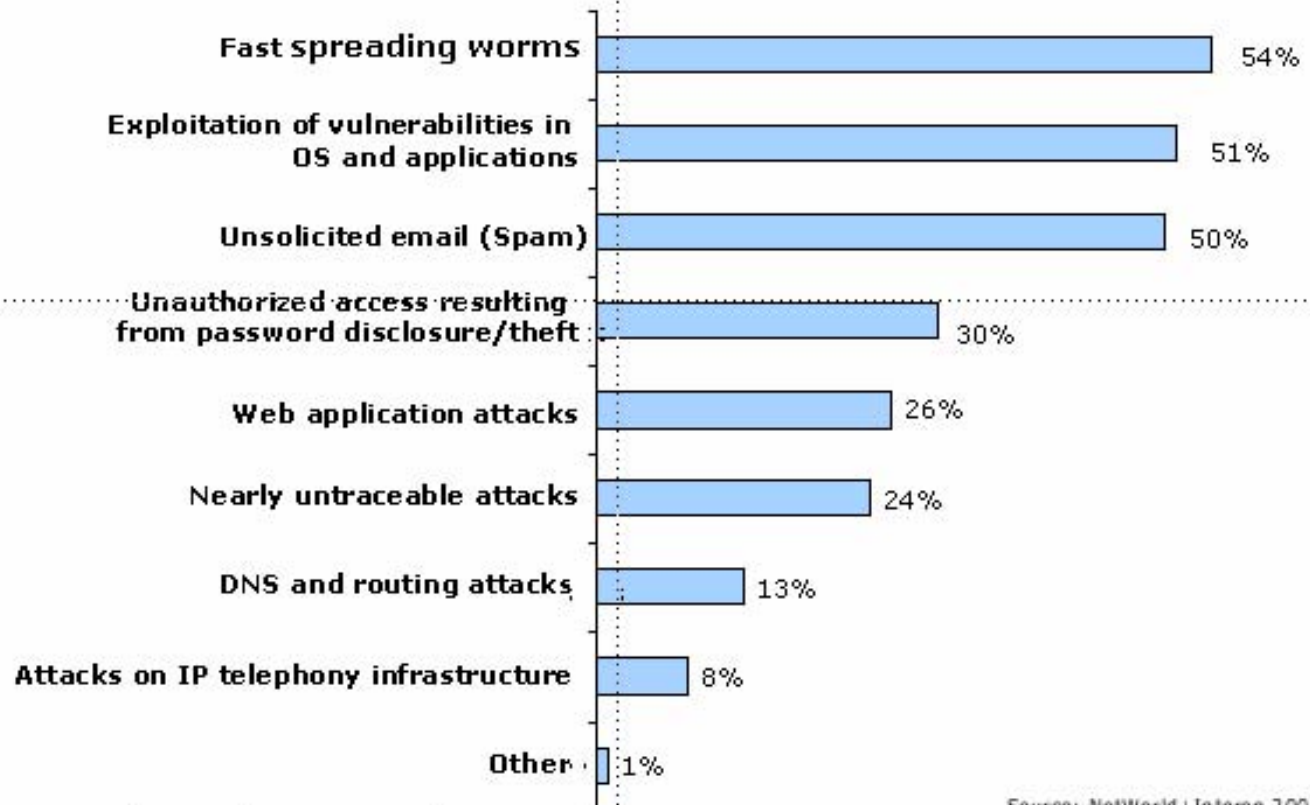
Q. Which one of the following do you suspect is the biggest resource drain to your network?
(Small=1-24 employees, Medium=15-499 employees, Large=500+ employees)

Source: NetWorld+Interop 2004
Networking Market Snapshot Survey

Teasers from Survey...

**NETWORLD
+ INTEROP**
LAS VEGAS • MAY 9-14, 2004

Most Worrisome Security Issues



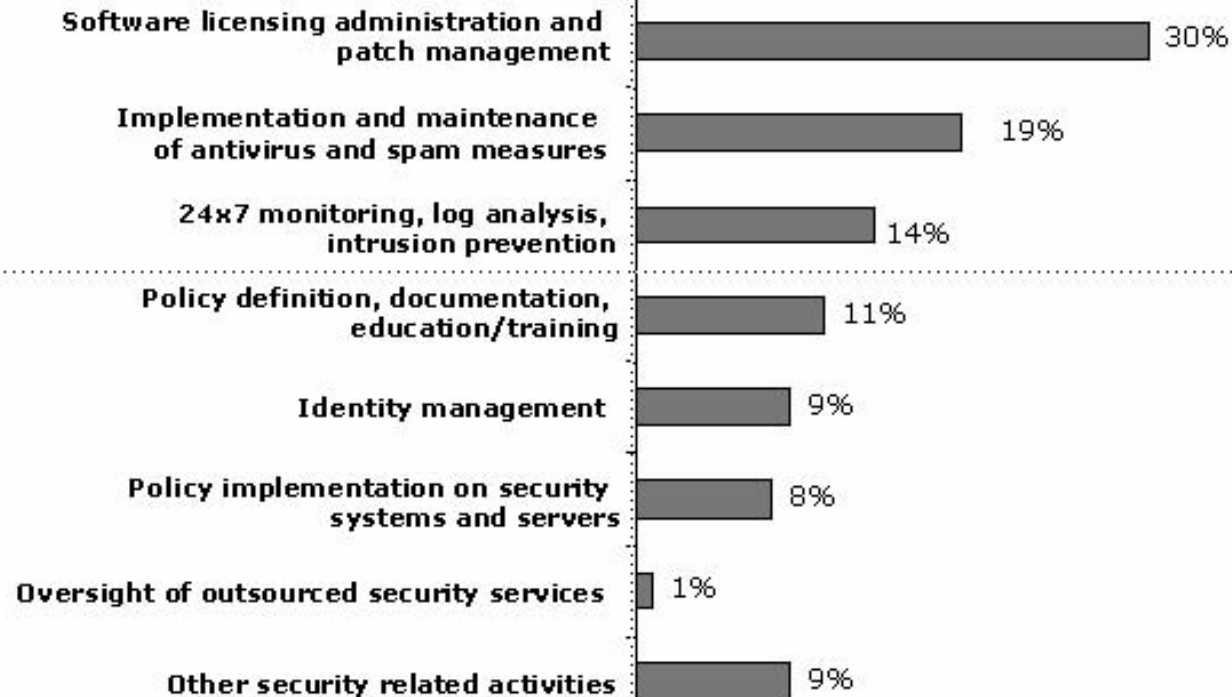
Q. What security issues have you the most worried?

Source: NetWorld+Interop 2004
Networking Market Snapshot Survey

Your 3rd and *Final* Teaser...

**NETWORLD
+ INTEROP**
LAS VEGAS • MAY 9-14, 2004

Security Process that is the Biggest Resource Drain



Q. Which of the following security processes is the biggest drain on your organization's resources?

Source: NetWorld+Interop 2004
Networking Market Snapshot Survey

**Some of you came to
hear about security
technology...**

**We're still applying Band-Aids to
severed femoral arteries, but
they are better Band-Aids...**

Intriguing technology

- **Admission control**
 - Variety of methods that determine whether a system is “clean” before it’s admitted to a network
- **Authenticated email**
 - Mail systems weed out spam and unauthorized users by enforcing an authentication policy
 - IMO, best long term solution to spam
- **Application Protection**
 - Variety of intrusion detection methods applied to applications (e.g., web, DB, ...)

Intriguing Technology

- **Identity Management**
 - Holy Grail of user account provisioning and maintenance, also encompasses central access/authorization policy administration
- **Risk Management systems**
 - Vulnerability assessment is enhanced by applying assessing the risk associated with discovered vulnerabilities. Determines if a vulnerability is exploitable and assigns priority to vulnerability mitigation
- **WLAN Security enhancements**
 - Collectively, these allow organizations to create integrated (media-agnostic) LANs

Questions?

Thank you!