Anti-Virus Product Evaluation in the Real World

The current state of affairs

Sarah Gordon
Richard Ford

Command Software Systems
Who’s Who?

- Friends
- Employees
- Tech Support Staff
- Independent Reviewers
- Magazines
  - General
  - Virus/Security
- Commercial Evaluators
- Academic Testers
- Executive Summarizers
- Governmental Bodies
- Vendors
- ITSEC AVWG
FRIENDS AND OTHERS

• Friendly Advice
  – “It works great”
  – “I’ve never had a virus”
  – “It’s fast!”

• Employees
  – “I love to help out at work!”
TECHNICAL SUPPORT STAFF

• “I’m technical”
  – Novell, UNIX, VMS
• “I know about viruses”
  – Usenet, World Wide Web
• “I have equipment here!”
  – uhhhh...*which* equipment?
Magazines

GENERAL
• Virus collections
  – vendor, bbs, ftp, www, CD-ROM, simulator
• Testing competency
  – flawed tests
• Legal liability
• Bias

VIRUS/SECURITY
• Virus collections
  – usually good
• Testing competency
  – competent
  – documented
  – usually well interpreted
• Bias
INDEPENDENT EVALUATORS

• Who
  – qualifications
  – affiliations

• Where
  – Virus-L
  – FidoNet
Scholars and other Strangers

- Academics
- Executive Summarizers
- Vendors
COMMERCIAL EVALUATORS

VSUM
NCSA
CHECKMARK

Collection Management
- Which viruses?
  - Replicated?
  - Polymorphics?
  - Boot Sectors?

Competency of Tester
- Qualifications?
  - Affiliations?

Tests
- What was tested?
  - Results Weighted?

Review modes?
  - Interface?
  - Speed?
  - Detection?

Interpretation of Tests
ITSEC AVWG

- Common viruses
- ITW Viruses
- VATE
- Tests Against Industry Standard Collection

*using CLEFs*
Problems common to all

- Choice of test suite
- Time involved
- Bias
- Limited Functionality Testing
  - compatibility
  - scanner, tsr, disinfection
- Evaluation of tech support
Suggestions

• Realize there is not yet one complete solution
• Decide who will evaluate software
  – be aware of all influences
• Designate what will be evaluated
• Ascertain how it will be evaluated
  – gather information from specialists
  – virus/Security Specialist Publications
  – NCSA/Checkmark
Caveats

• Do not increase your organization’s vulnerabilities!
  – no in-house “tests” using simulators, CD-ROMS, FTP site, or WWW viruses!
  – weigh advice from “experts” carefully

• Do not expect more from your staff than they can reasonably be expected to provide!