Implementing an Enterprise Anti-Virus and Anti-Spam Strategy, Adventures in the Real World

Earl Greer

Vincil Bishop

Virus Bulletin Conference 2005

Vincil Bishop
V. Bishop Consulting
Austin, Texas USA

Anti-virus / Anti-spam

Issues and Strategies:

Delivering Value

Issues and Strategies Overview

- Issues
- The Vital Few
- Analysis
- Action
- Summary

The Issue

- *Virus infections and spam don't promote your visions or goals!*

The Vital Few

- What are the real problems surrounding the issue?

- Which ones can you solve?

- Which ones must you live with? Really it's ok!

The Vital Few

- What are the real problems surrounding the issue?

- Which ones can you solve?

- Which ones must you live with? Really it's ok!

The Vital Few

- At what point have we gotten the most bang for our buck? Find it and stick to it.

- Can the solution pay for itself? If this solution can't which solution can?

- Where is the value delivered?

Analyzing the Issue

- Anti-virus vendors and corporate decision makers sometimes miss the point.

- Buying the technology and not the solution.

- Technology has advanced, but little has changed in the level of protection.

Analyzing the Issue

- Anti-virus / Anti-spam solutions alone will not protect us.

- There is a need for effective and measurable server / workstation management.

- Choose a centralized solution over a distributed one.

Action

- Exactly what are you going to do if there is a virus outbreak?
  - How will the product support the actions of your people?

- Are you spending your money in the right places?
  - Maybe you need more workstation / patch management instead of better anti-virus and anti-spam.

And in Summary…

- The vital few / Simplify the complex.

- Never do a deal you don't understand.

- Get your workstation management under control.

- *Your talented people and not a product will make the difference in the end.*

Earl Greer

Independent Security Consultant / Author

Adventures in the Real World

Lessons Learned

- A virus detector is harder to write than a virus.

- Every anti-virus uses more than pattern matching.

- It is absolutely necessary to be able to identify a virus:
  - Removal
  - Knowledge of potential damage
  - The Boss is going to ask!

Selling Principles

- Identify and sell to the technician and the decision maker.

- Ask when the purchase will be made, strike while the iron is hot.

- Know your customers
  - Platforms
  - Software
  - Business

Short Horizon Business Model

- Don't innovate, buy an innovation.
- Spend lots on marketing.
- Give minimal support.
- Never waste money by improving your product.
- Add products to your product and sell it under a new name.

Communication Remedies

- For Customers
  - Discuss plans with the vendors.
  - Become a Beta Tester.
  - Put complaints / suggestions in writing.
- For Vendors
  - Know your customer's platforms and business.
  - Know their past bad experiences.
  - Be competitive and swift in malware removal.

Questions and Discussion

Feel free to contact us by visiting:

http://www.vbishop.com