



VIRCOM[™]
TRUST YOUR EMAIL, TODAY, FOREVER.

www.vircom.com

Email Protection: Assessing the Costs

Paul Vanbosterhaut - Managing Director, Vircom Europe.
January 2007.

Introduction

When considering the purchase of an email security solution (anti-Virus, anti-Spam, anti-Phishing...), it is easy to be overwhelmed by choices. The email security market is getting more and more crowded, and the offer is as varied as confusing, ranging from state-of-the-art to frivolous. How can you make sense of the market's noise and hype? How can you measure the real value of the offered products and services?

Initial estimates will compare solutions' claimed efficiency with their price. This quick comparison is often misleading: some vendors claim outrageous catch rates, and listed prices sometimes omit yearly subscriptions or hide required hardware or maintenance costs. But even with accurate information, this estimation has its limit: pricing stands only for a fraction of the total email security cost.

Assessing the costs

When assessing the cost of an email security solution, corporations should consider the following main cost areas:

1. **Product Costs**
2. **System Administration Costs**
3. **Productivity Losses** (another way to look at efficiency)
4. **Hidden Costs**

Let us review those in more details.

Purchase Cost

The purchase cost should include the cost of the solution (with the needed subscriptions and maintenance costs), the cost of required additional hardware and software if any, and the installation costs (including initial configuration).

You can disregard server and installation costs for email scanning services.

*Vircom estimates that the total purchase price usually counts for about **5 to 15%** of the total cost.*

IT Administration Costs

While required, an easy to use administration console is not sufficient to reduce administration costs. Let us point out aspects that can badly influence the cost of the four major administration tasks:

- Infrastructure Maintenance: these costs cover the fully loaded costs of IT staff time spent maintaining the solution's hardware and software (setup changes, new versions...), as well as the cost of answering help-desk calls.
- Threat protection updates: Most solutions include automated updates of their anti-Virus, anti-Spam and anti-Phishing engines. This being said, several solutions still entail administrators or users to feed a self-learning system with messages announced as spam or non-spam. This may soon represent a non-negligible cost.
- User Administration: Most companies will want differentiated settings for their users, like user-defined trusted lists for instance. Creating these users and their aliases can become very time consuming if not automated through LDAP/AD integration or other alias-aware populating processes. To reduce further administration hurdles, companies should favour solutions that ease the definition of user settings through user delegation and by configuring exceptions only.

Finally, beware that some implementations promote or require the installation of plug-ins on each client. This has a serious cost impact (installation costs but also productivity losses for all end users). *Vircom estimates that IT Operation costs usually count for about **20 to 35%** of the total cost.*

Productivity Loss

Productivity loss has been every anti-Spam vendor's principal argument. You still have many vendors' sites allowing you to calculate the cost of Spam. 70+% of this cost are due to productivity losses (basically the time taken by each user to review and delete the Spam messages in their inbox). Paradoxically, few vendors, if any, are raising that same point when highlighting the effectiveness of their solution.



VIRCOM™

TRUST YOUR EMAIL, TODAY, FOREVER.

www.vircom.com

Productivity losses are mainly influenced by the spam let through rate (spam still getting to the inbox – also called false negative rate), the false positive rate, the quarantine administration and the impact of user delegation.

- Let-through rate: The market offers lots of tools to calculate the cost of Spam. You can use the same tools to calculate the cost of left through spam. A 5% difference in catch rate may quickly represent a difference of several thousands of dollars in productivity loss.
- False positives: The cost of false-positives is highly dependent on the quality of the quarantine administration.
- Quarantine Administration: Several elements will influence these costs, like: i) does the system send scheduled quarantine digests to end users, ii) does the system allow web quarantine access and how is this access granted (password management), and iii) how easy, effective and complete are these interfaces. Ferris Research estimated in a recent report¹ that a typical medium-sized organization with good spam protection spends about \$61 per user per year for quarantine review or... about 51% of the total cost!
- User delegation: Delegating settings to users is valuable overall. It is often a must. However it will influence users' productivity. Analyse the different methods provided to users to customize their environment and assess their easiness and efficiency. These methods must distinguish between experienced and average users to avoid user mistakes and additional administration hurdles.

*While often overlooked, productivity loss still account for about **50 to 75%** of the total cost of an anti-Spam solution!*

Hidden Costs

Hidden costs are mostly infrastructure related. Administrators experience them when their system performance is hindered by hacker attacks (Dictionary Harvesting, Open Relay or Denial of Service attacks...), when their system is unavailable (due to maintenance or disaster...), or when new threats appear and new features are needed.

The better the product underlying architecture is structured the less it will suffer from those situations. While hidden costs are difficult to measure (and are not taken into account within this white paper), here are some architectural bases that can reduce them:

- Exhaustive and efficient perimeter defence
- Database support (for easier data recovery)
- Clustering support (for higher performance and redundancy)
- Inbound/Outbound filtering (for mail compliance)
- Flexibility to catch new threats (like the latest "Image Spam").

Conclusion

More than 10 years email security innovation and experience has guided Vircom in considering all cost aspects – over the years – of email security.

We know that pricing remains a key decision factor (our competitive pricing reflects that). For email security however, efficiency and effectiveness should be the key drivers in any cost assessment.

About Vircom

Vircom is a privately held, technology think-tank focused exclusively on secure messaging solutions. It was the first company to offer commercial anti-spam and email protection facilities, and today offers such capabilities as a gateway service, appliance, or complete email server.

Since 1994, well before other companies identified the email security problem, Vircom has specialized in advanced Internet infrastructure and secure messaging solutions for the ever-evolving needs of both ISP and corporate clients.

Vircom's ModusGate offers more than conventional anti-spam products. It's a comprehensive secure email gateway designed to offer the best email protection at the lowest Total Cost of Ownership. ModusGate fits seamlessly with existing Microsoft Exchange™, Lotus Notes™ and other standard email servers. In test after test, its Modus-based technology proved 98+% spam catch rate (incl. against image spam) and offered 99.9% protection against false-positives. Its flexible design provides the email assurance capabilities necessary to meet today's threats as well as the essential flexibility and scalability to meet tomorrow's.

¹ Ferris Research – Calculating Spam Cost in Your Organization - February 2005 - Report #511