

Anti-Spam Measures Survey 2009

Pascal Manzano – ENISA

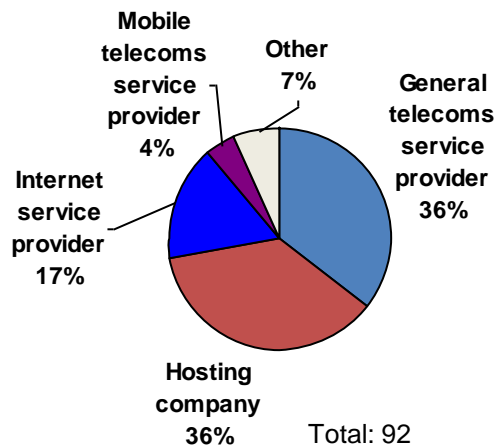
Do you remember what happen
on June 25th?

Methodology

- ★ Online questionnaire open from May until July 2009
- ★ Questionnaire used providers' best practices (MAAWG, OECD) and used European Directive 2002/58/EC to create the questions
- ★ Survey targeted anti-spam managers at email service providers throughout the EU
- ★ The objective was to include a wide range of providers of different types and sizes, and from different countries
- ★ Over 1700 email providers contacted with invitation letters
- ★ Invitation forwarded to providers associations over Europe
- ★ Contact with many providers via telephone to reach anti-spam managers and invite their participation

Respondents

Respondents by Type of Company



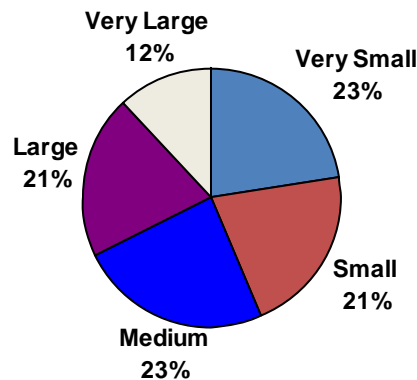
Source: ENISA Anti-Spam Survey 2009

Respondent Size Category Definitions

Very Small	Less than 1000 mailboxes managed
Small	1,000 to 9,999 mailboxes managed
Medium	10,000 to 99,999 mailboxes managed
Large	100,000 to 999,999 mailboxes managed
Very Large	1 Million or More mailboxes managed

- ★ 92 respondents; 30 different countries (26 of the 27 EU member states); 80 million mailboxes managed

Respondents by Size



Total: 92

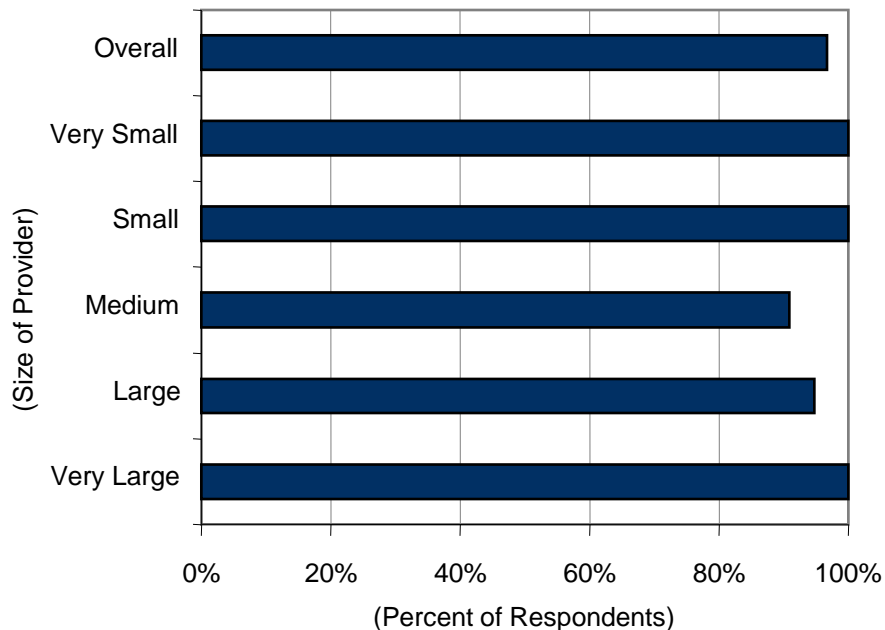
Source: ENISA Anti-Spam Survey 2009

Organizational Measures

Spam as Part of Security Operations

Addressing Spam As Part of Security Operations

Q Do you consider fighting spam as part of your security activities?



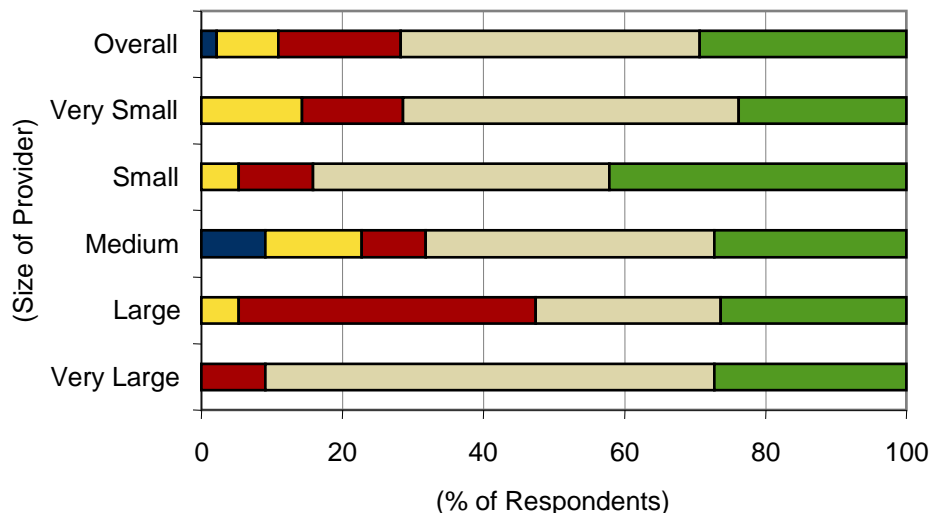
N=92

Source: ENISA Anti-Spam Survey 2009

- ★ The respondents almost unanimously said yes.
- ★ This status suggests that service providers consider it an important threat that they must address carefully

Significance of Spam in Security Operations by Size of Provider

Q How significant is spam prevention as part of your security activities?



- 1 Not significant at all
- 2 Not very significant
- 3 Neither/nor
- 4 Significant
- 5 Extremely significant

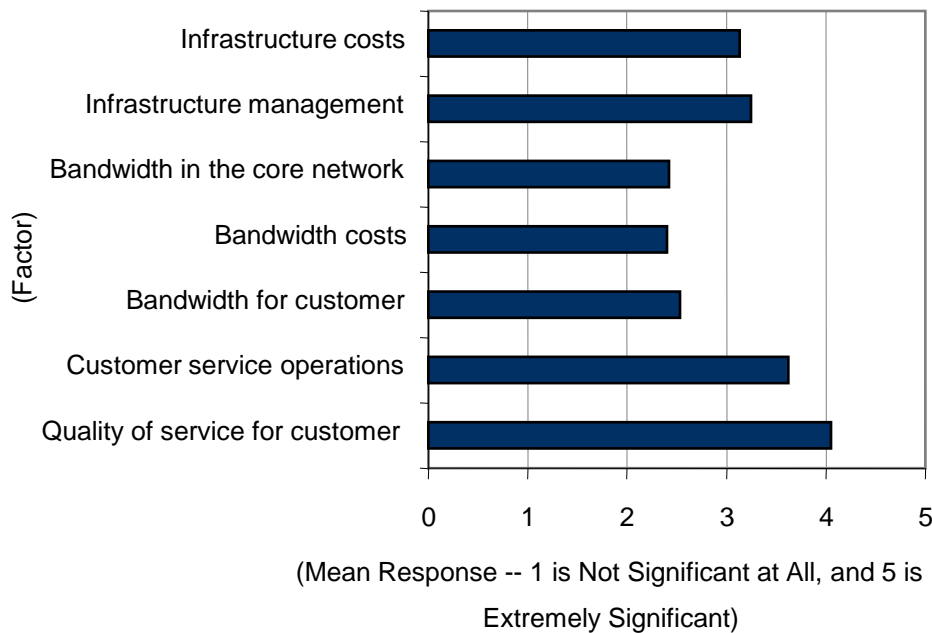
N=92

Source: ENISA Anti-Spam Survey 2009

- ★ average response: it is significant
- ★ Only 12% view spam as an insignificant part of security activities
- ★ 70% of respondents consider it extremely significant or significant.
- ★ Clearly, email providers tend to take spam seriously within security operations

Impact of Spam on Respondent's Business

Q How significant is the impact that Spam has on your business in the following areas?



N=92

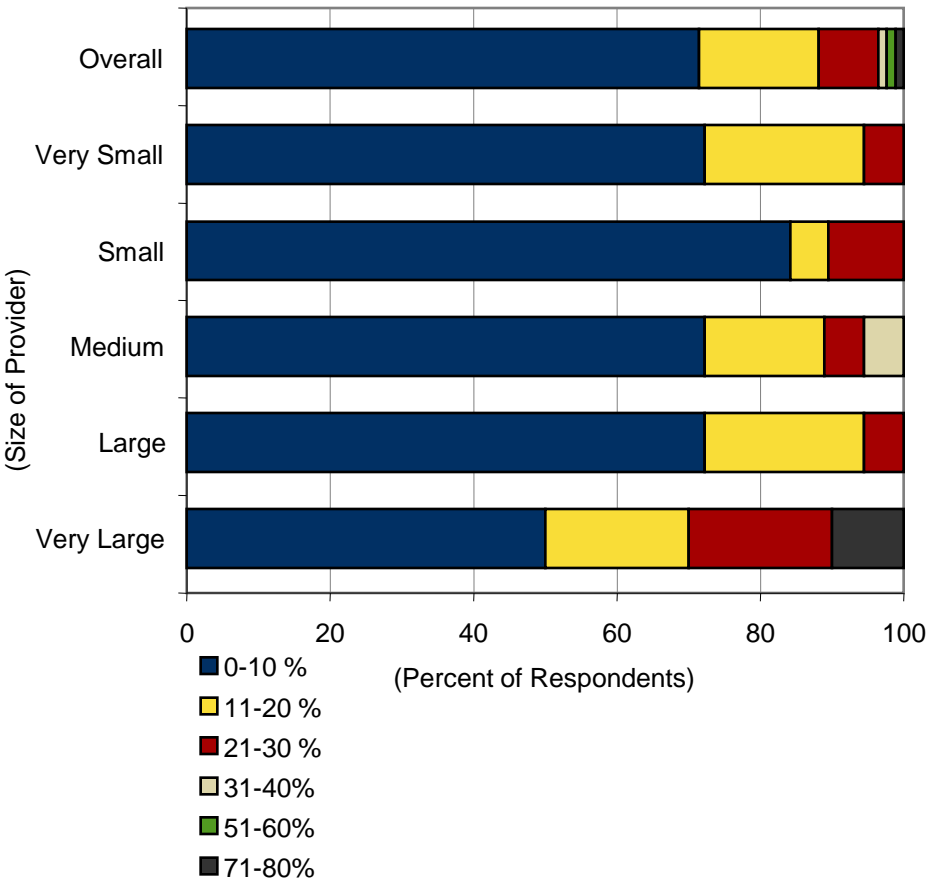
Source: ENISA Anti-Spam Survey 2009

- ★ Quality of service delivered to the customer
- ★ Impact on bandwidth is viewed generally as of low significance

Impact of Spam on Helpdesk Calls

Helpdesk Calls Concerning Spam

Q What percent of your helpdesk calls concern spam?



N=84

Source: ENISA Anti-Spam Survey 2009

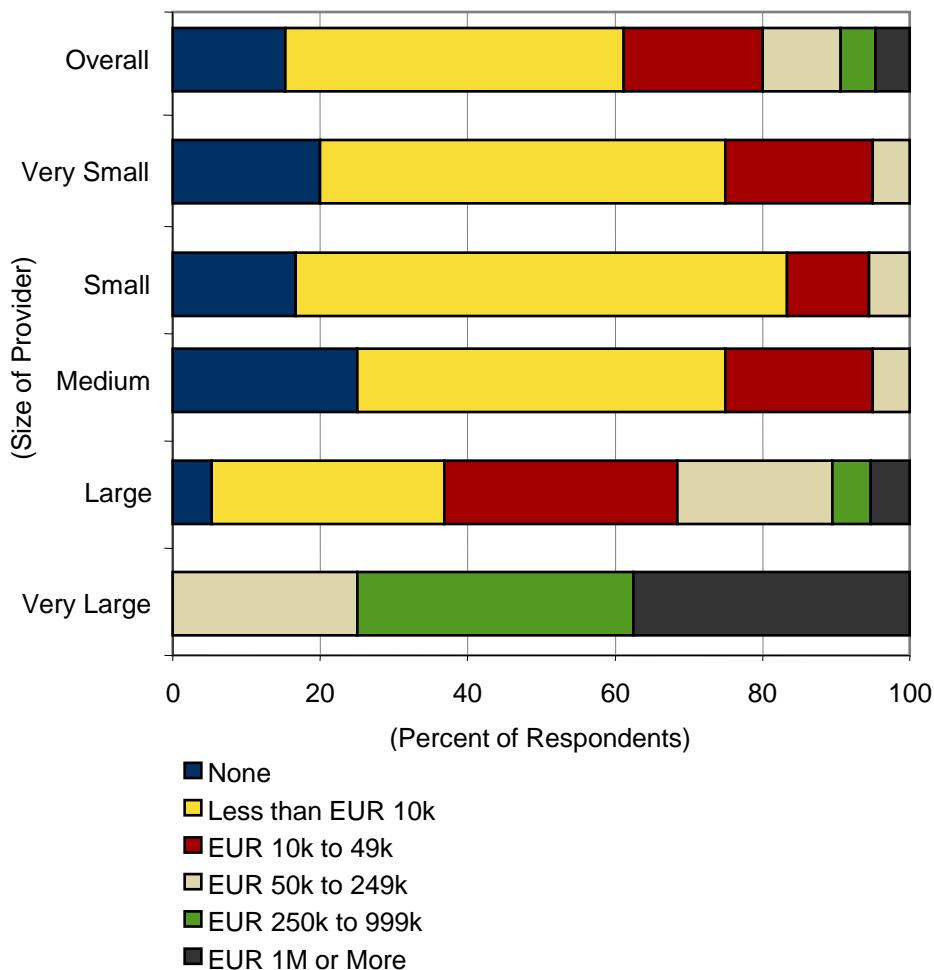
- ★ Over a quarter of respondents noted spam accounting for over 10% of helpdesk calls
- ★ However, some providers devote a large amount of helpdesk resources to the issue
- ★ Higher percentages of helpdesk calls concerning spam for the largest service providers

Organizational Measures

Anti-Spam Budget

Annual Anti-Spam Budget

Q What is your annual budget for anti-spam measures and operations?



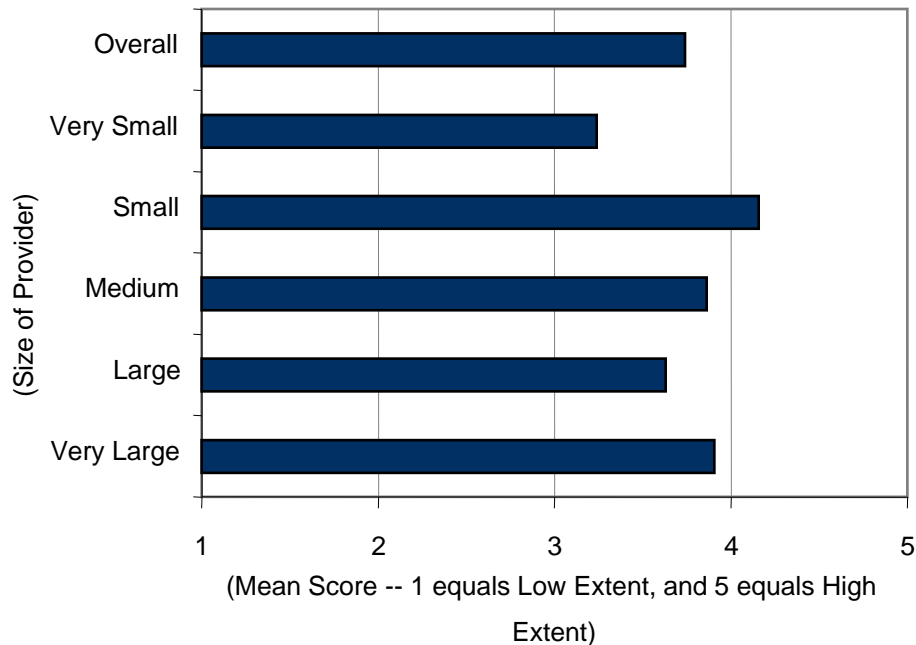
N=85

Source: ENISA Anti-Spam Survey 2009

- ★ Anti-spam budgets are considerable
- ★ Among very small providers, a quarter of respondents stated that their anti-spam budgets are over EUR 10,000 per year
- ★ Among very large providers, a third pointed to anti-spam budgets over EUR 1 million annually

Anti-Spam Measures as a Competitive Advantage for Providers

Q To what extent do you consider spam prevention as a competitive advantage?



N=92

Source: ENISA Anti-Spam Survey 2009

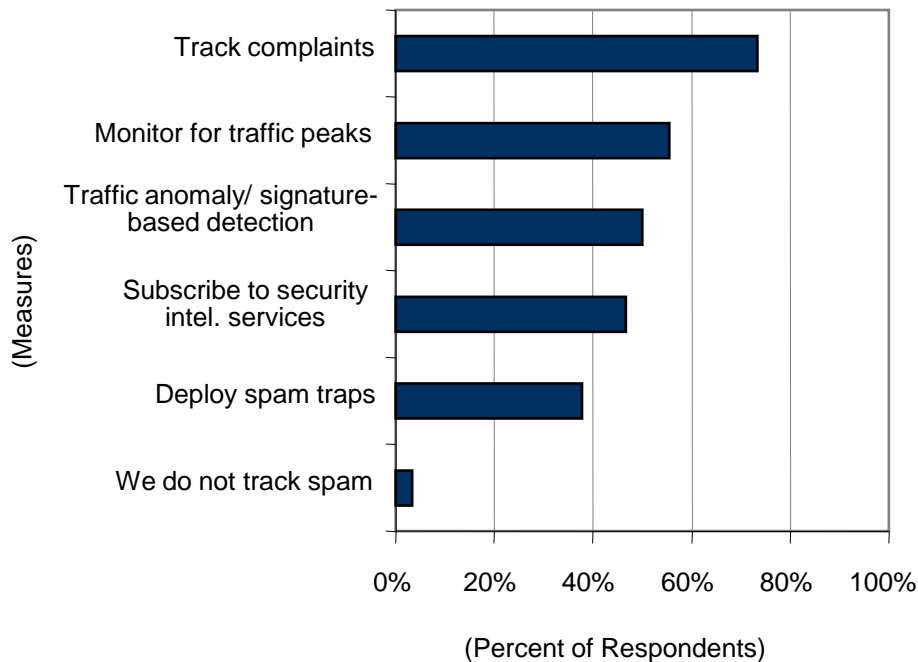
- ★ Spam prevention gives a competitive advantage
- ★ Important in attracting and retaining customers
- ★ However spam is not critical or urgent factor

Technical Measures

Measures to Detect Spam

Measures to Detect Spam Problems

Q What measures do you take to become aware of spam problems?



N=90

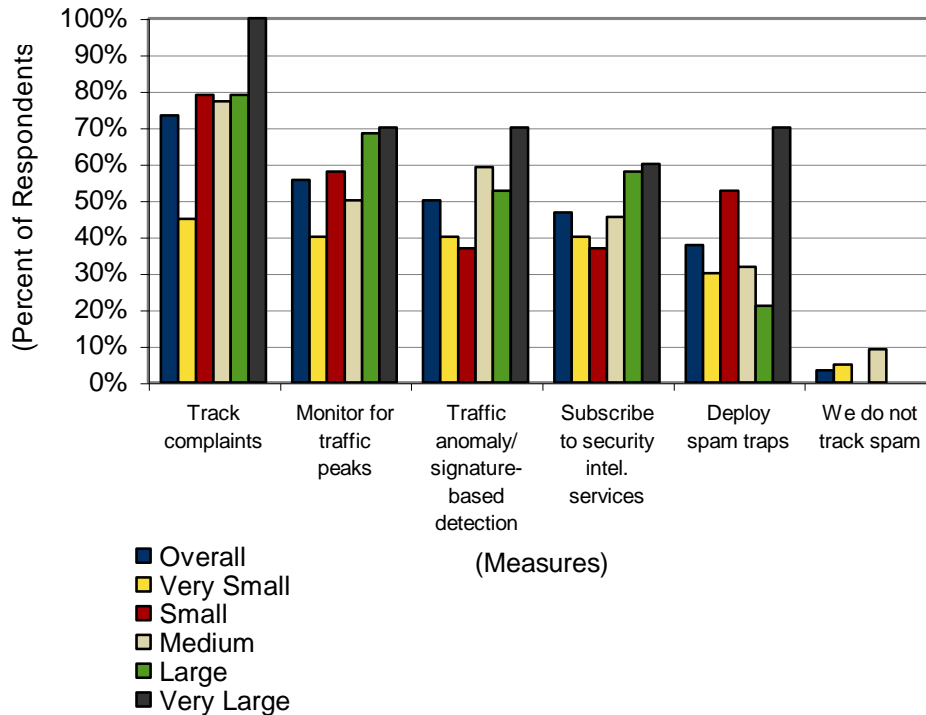
Source: ENISA Anti-Spam Survey 2009

- ★ Most common method is to track complaints
- ★ Monitor traffic peaks and conduct real-time anomaly and/or signature-based detection
- ★ Only very few respondents do not track spam

Technical Measures Measures to Detect Spam

Measures to Detect Spam Problems, by Size of Company

Q What measures do you take to become aware of spam problems?



N=90

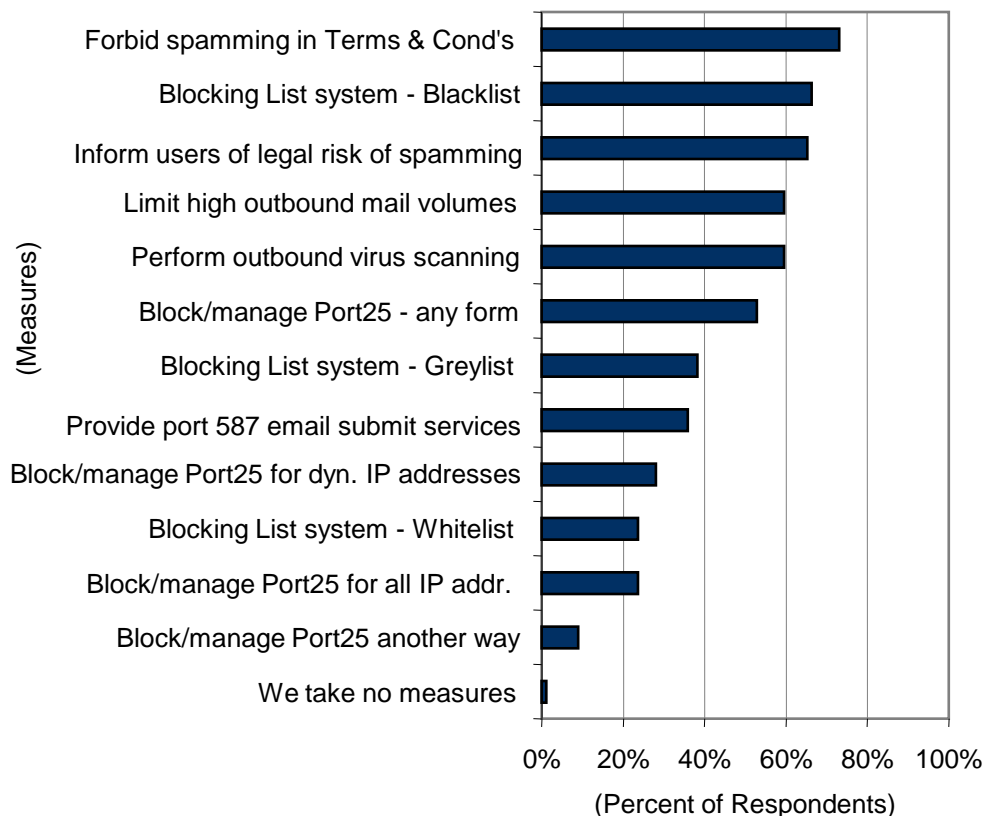
Source: ENISA Anti-Spam Survey 2009

- ★ Largest providers apply all of the measures more frequently than do the smaller providers
- ★ This variance between measures applied by large and small providers valid for other anti-spam measures

Measures to Prevent Spam Sending

Measures to Prevent Customers from Sending Spam

Q Which of the following measures do you take to prevent your subscribers from sending unsolicited communications (spam)?



N=89

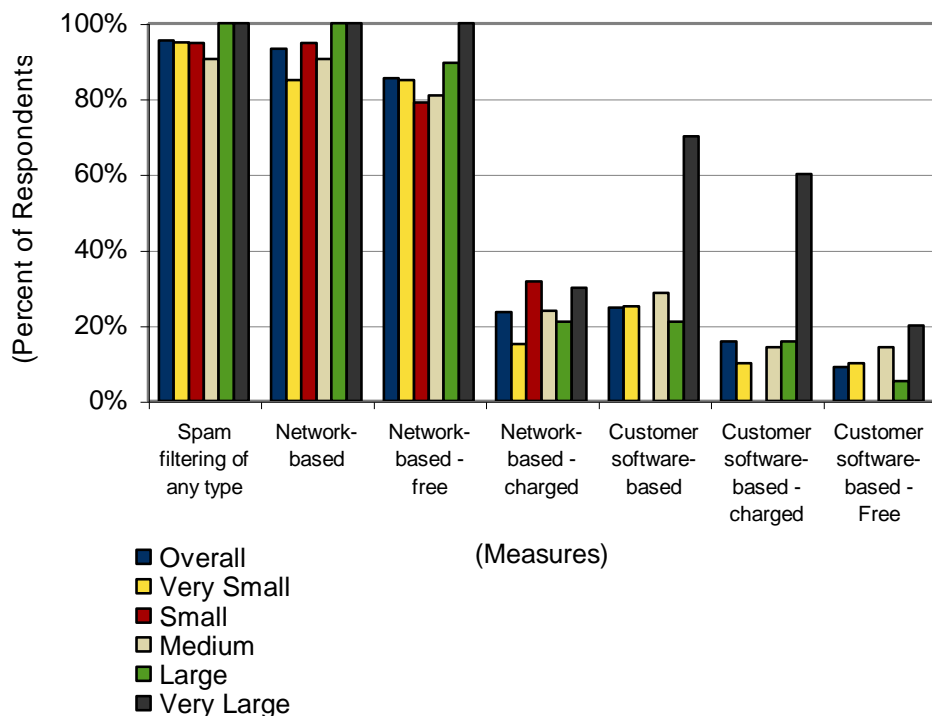
Source: ENISA Anti-Spam Survey 2009

- ★ Providers are helping to solve the systemic spam problem by shutting down spammers among their own customers
- ★ Most common measure is to forbid spamming in the terms and conditions
- ★ Almost none stated that they do not take any measures to prevent customers from sending spam

Technical Measures Spam Filtering

Measures to Prevent Customers from Receiving Spam

Q Which of the following measures do you take to protect your subscribers from receiving unsolicited communications (spam)?



N=89

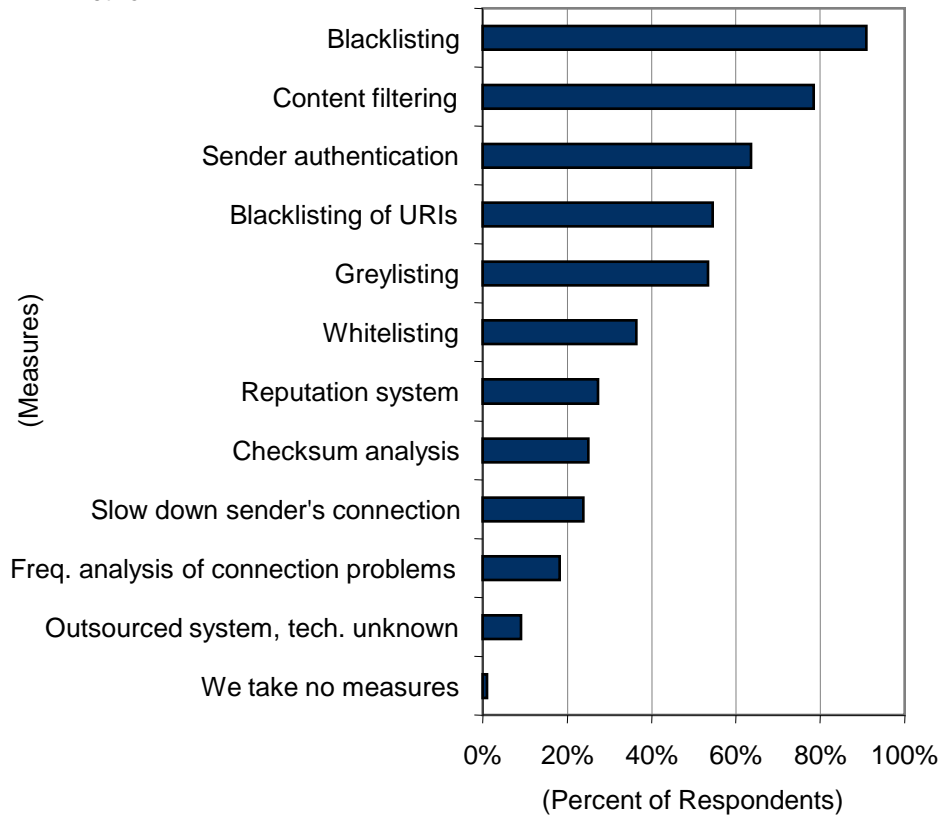
Source: ENISA Anti-Spam Survey 2009

- ★ Nearly all providers provide spam filtering to their customers
- ★ Spam filtering software for customers to install is much less common
- ★ Only a small number offer no filtering at all

Technical Measures Network Filtering

Spam-Filtering Measures on The Network

Q Which of the following spam-filtering measures do you take on your network?



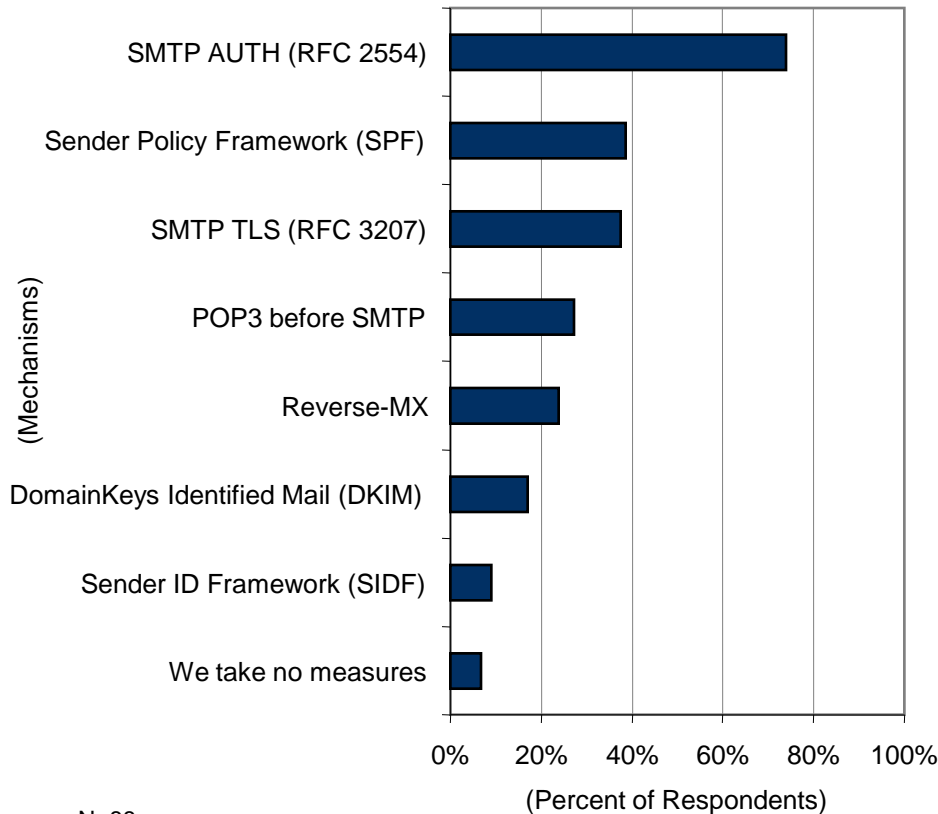
- ★ On average 4.7 measures
- ★ Most common is blacklisting
- ★ Little change with the 2007 results

N=88

Source: ENISA Anti-Spam Survey 2009

Sender Authentication Mechanisms

Q Which of the following sender authentication mechanisms do you implement?



N=88

Source: ENISA Anti-Spam Survey 2009

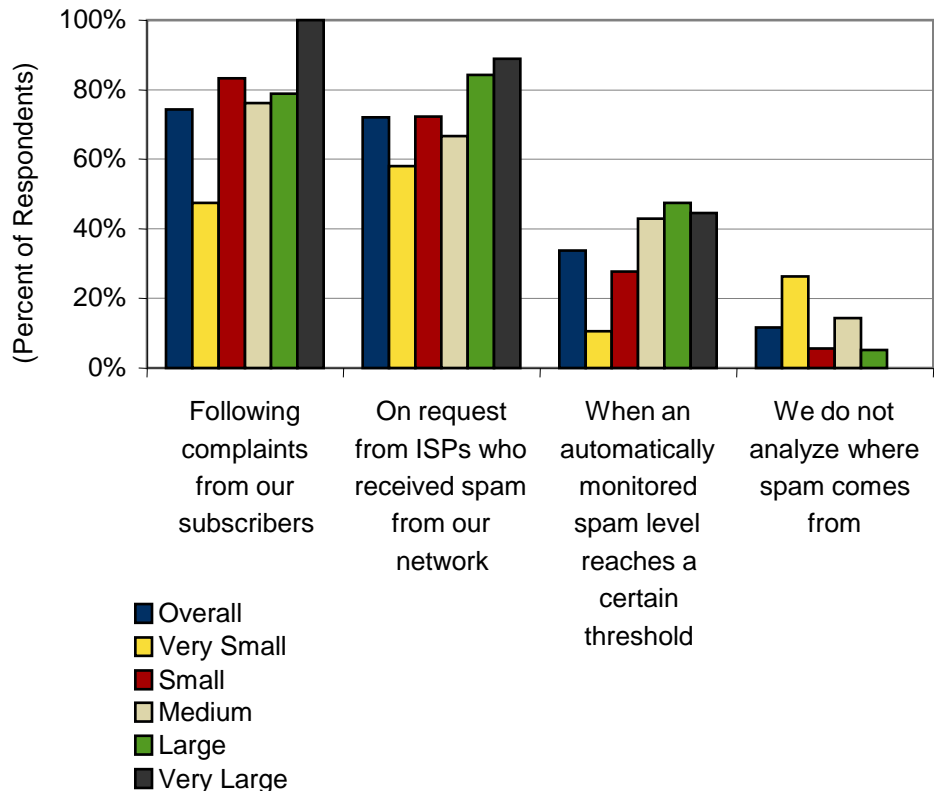
- ★ SMTP AUTH is the dominant authentication method
- ★ DKIM—up from about 5% to 17%
- ★ SIDF—up from about 5% to 9%
- ★ SPF is particularly common among large providers, while DKIM stands out among medium-sized providers

Technical Measures

Identifying Sources of Spam

Identifying The Source of Spam

Q When do you analyze where spam comes from?



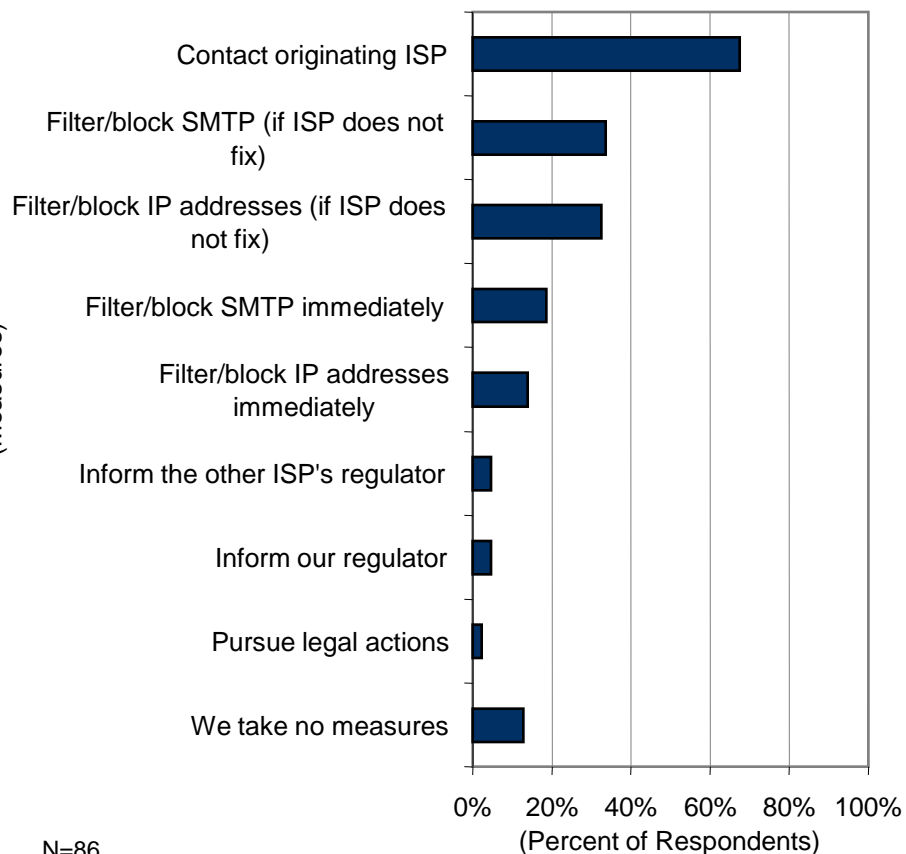
N=86

Source: ENISA Anti-Spam Survey 2009

- ★ When notified by a customer or by another ISP of a problem that they need to investigate
- ★ Very few providers said that they do not analyze the source of spam

Measures After Detecting Spam from Another ISP

Q What sort of measures do you take if you detect spam coming from another ISP?



N=86

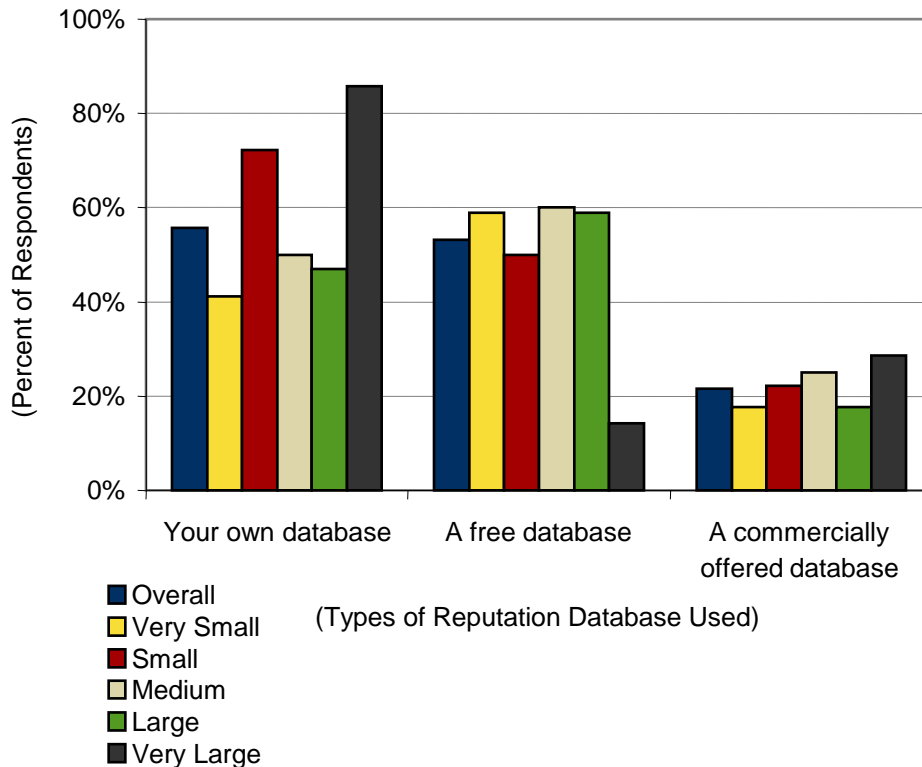
Source: ENISA Anti-Spam Survey 2009

- ★ Two thirds of providers contact the originating ISP to discuss measures that they can take
- ★ Filter or block the originating SMTP connections or IP addresses
- ★ Immediate blocking of SMTP connections or IP addresses

Reputation Databases Used

Types of Reputation Database Used

Q To maintain blacklists and other similar lists, what kind of reputation database do you use?



N=79

Source: ENISA Anti-Spam Survey 2009

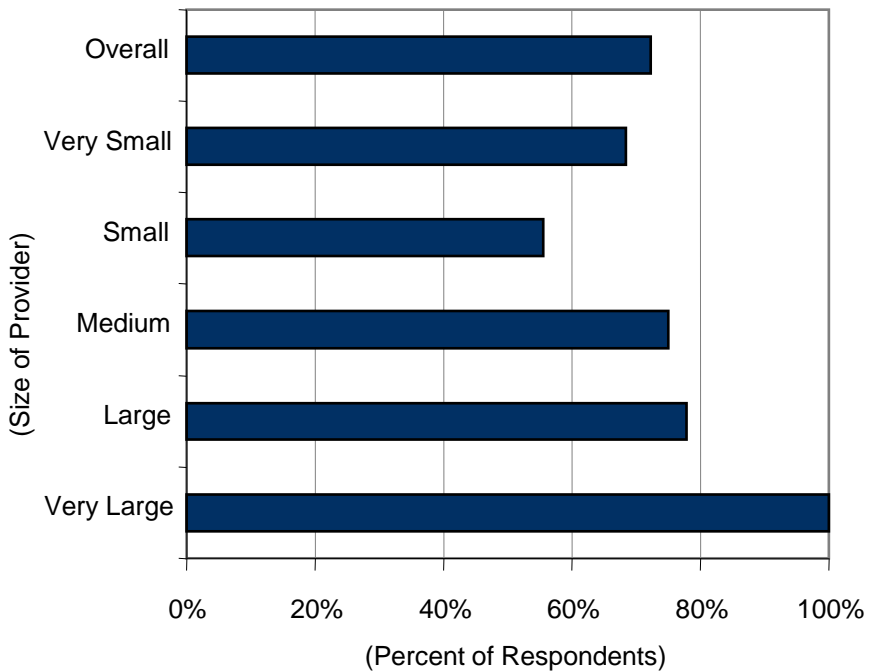
- ★ Over 50% use their own databases, while a similar number use a free database
- ★ Less than a quarter use a commercially offered database
- ★ Not mutually exclusive, and a provider may combine multiple databases from different categories

Technical Measures

Blacklist Accuracy

Experienced Accuracy of Blacklists

Q Have you ever had your servers wrongfully added to a blacklist, or wrongfully retained on a blacklist after spam problems were corrected?



N=83

Source: ENISA Anti-Spam Survey 2009

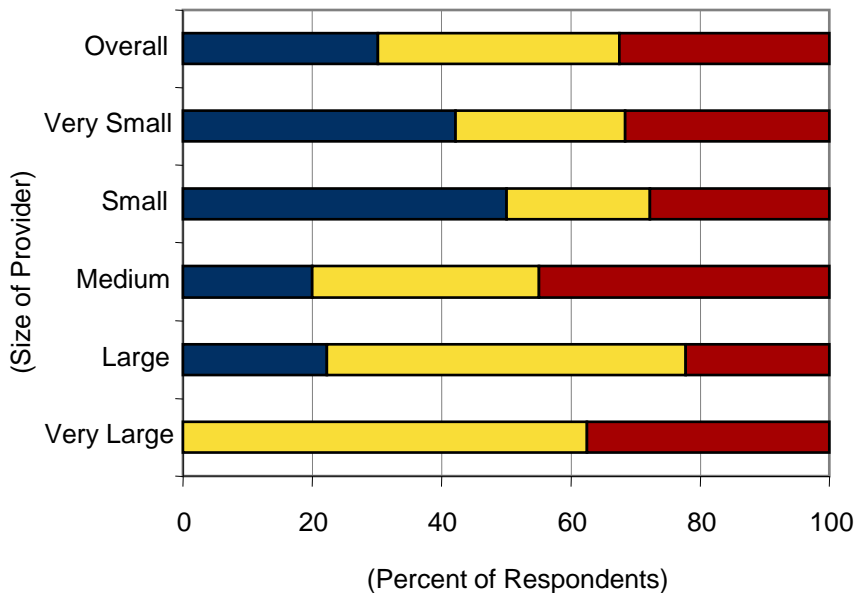
- ★ Blacklists are the most commonly used and important tools in the anti-spam arsenal, they do attract some criticism
- ★ Nearly three quarters said they had their servers incorrectly added or retained on a blacklist

Technical Measures

Blacklist Accuracy

Perceived Accuracy of Blacklists

Q Do you believe that major blacklists sometimes incorrectly include servers that are not (or are no longer) responsible for spam?



■ No, this does not often happen.

■ Yes, and it is often a big problem to get the server removed from the blacklist.

■ Yes, but it is usually easy to get the server removed from the blacklist.

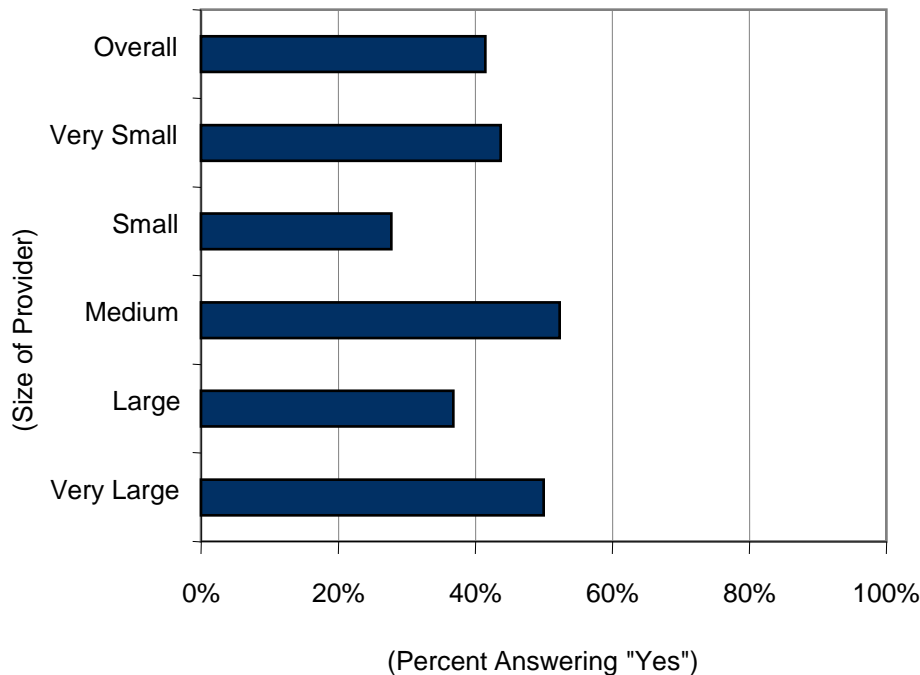
N=83

Source: ENISA Anti-Spam Survey 2009

- ★ Most providers said that major blacklists sometimes include servers that need not be blacklisted
- ★ Half said that the problem is usually easy to fix, though the other half said that it is often a problem to get the error corrected
- ★ Blacklists are the most effective anti-spam tool in use, but providers hope to see greater responsiveness from blacklist providers/developers in terms of evaluating servers that should be removed from the list

Planned Anti-Spam Measures in The Next Six Months

Q Do you plan to install or implement an anti-spam method in the next six months?



N=82

Source: ENISA Anti-Spam Survey 2009

- ★ Two fifths of providers plan to implement new anti-spam measures within the next six months
- ★ A variety of measures as being planned for the next six months

Technical Measures

Anti-Spam Software Solutions

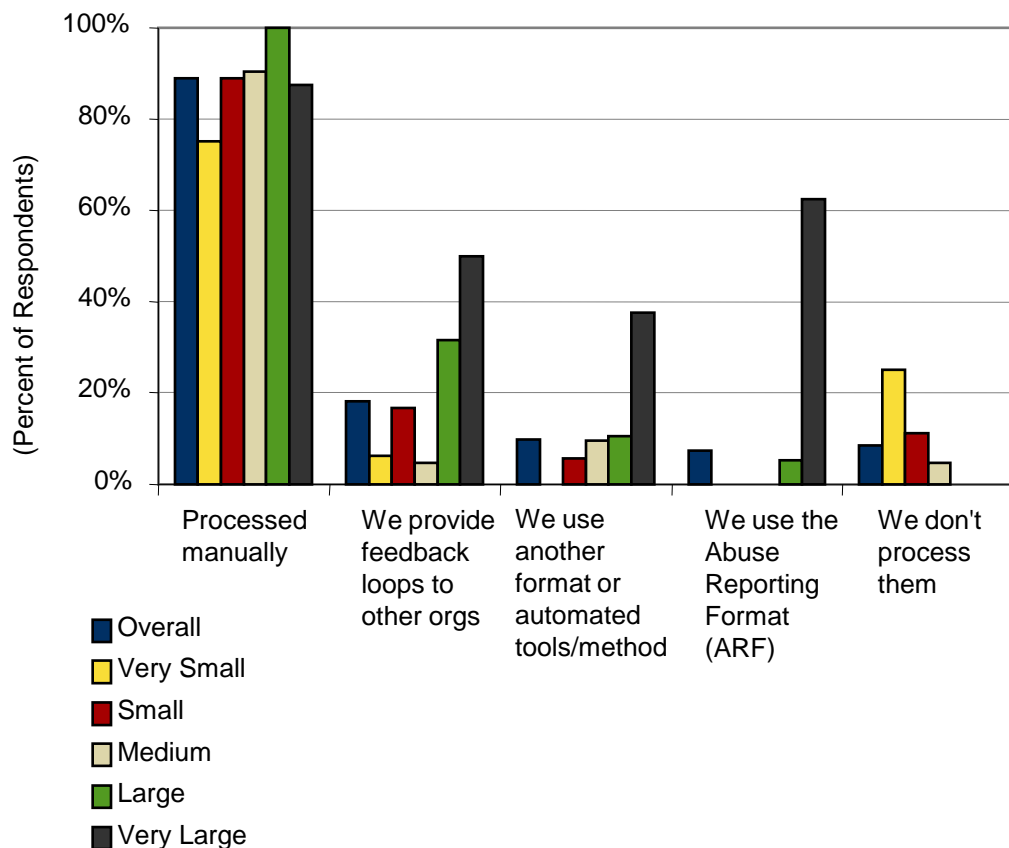
- ★ Many respondents emphasized that open-source software plays a prominent role in fighting spam.
- ★ Most commonly mentioned software was SpamAssassin, a free open-source application that uses a combination of anti-spam measures, including DNS-based and checksum-based spam detection, Bayesian filtering, blacklists and online databases.
- ★ Dozens of other commercial and open-source applications were also mentioned, though usually once or twice each.
- ★ The variety of choices, and the frequency of selection of both commercial and open-source applications, reflect the important role that both the open-source and commercial anti-spam activities play in the fight against spam.

Technical Measures

Processing Abuse Reports

Processing Abuse Reports

Q How do you process abuse reports?



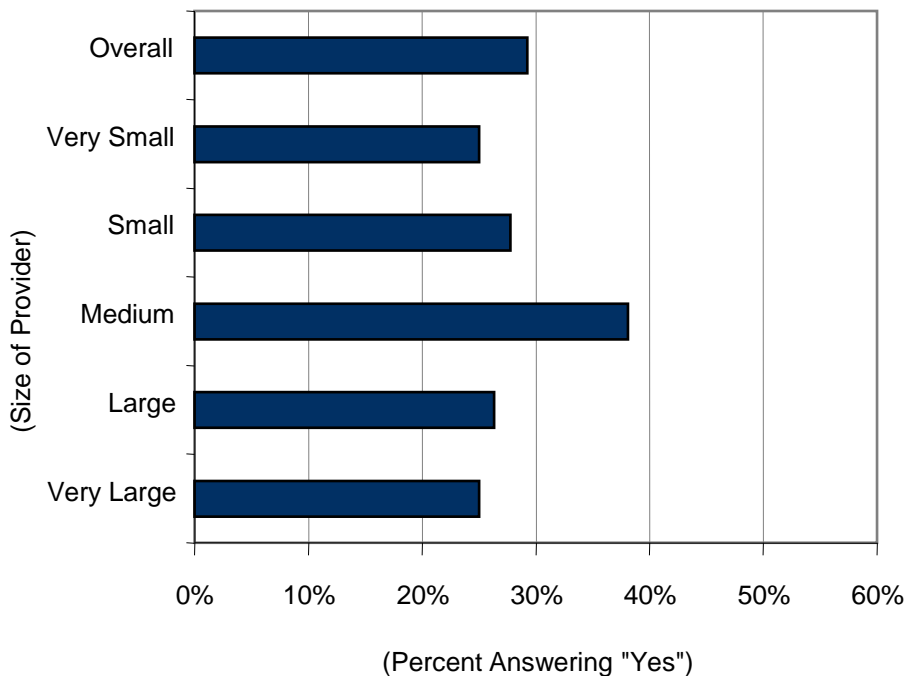
- ★ In most cases, abuse reports are processed manually
- ★ Only a small percentage of respondents (16%) provide feedback loops to other organizations
- ★ Only 8% of respondents reported using the Abuse Reporting Format (ARF)

N=82

Source: ENISA Anti-Spam Survey 2009

Potential Conflict Between Spam Filtering And ISP's Obligations to Protect Privacy and Deliver Mail

Q Do you think that there is a conflict between the use of spam filters that block some messages and the ISP's obligations to deliver messages and protect privacy?

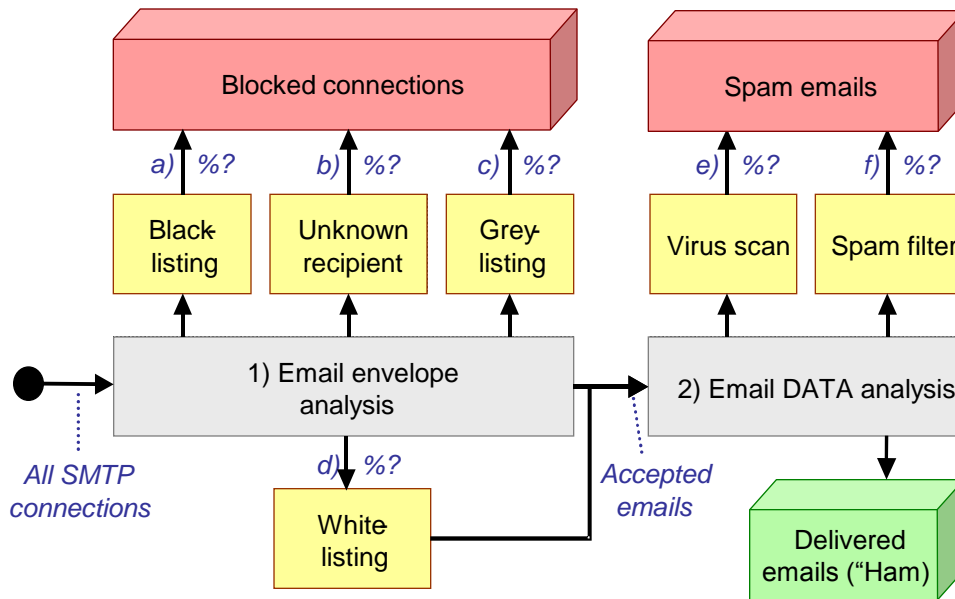


Source: ENISA Anti-Spam Survey 2009

- ★ Nearly a third of providers reported that they think there are conflicts between the use of spam filtering and the ISP's obligation to deliver messages and to protect privacy
- ★ European Commission's Article 29 Data Protection Working Party opinion explain that spam-filtering can be justified under the EU's legal framework for privacy and communications, though providers should take steps to ensure that their spam filtering is compliant, including informing the users

Effectiveness of Measures Messages Filtered and Delivered

Effectiveness of Anti-Spam Measures: Diagram of Connections and Messages Blocked, Filtered, or Delivered



- ★ Effectiveness of measures and scale of the spam problem
- ★ We asked providers to estimate the percent of SMTP connections that are blocked or aborted due to, blacklisting, greylisting, or unknown recipient, as well as the percent accepted due to whitelisting, and those accepted after passing through these filters

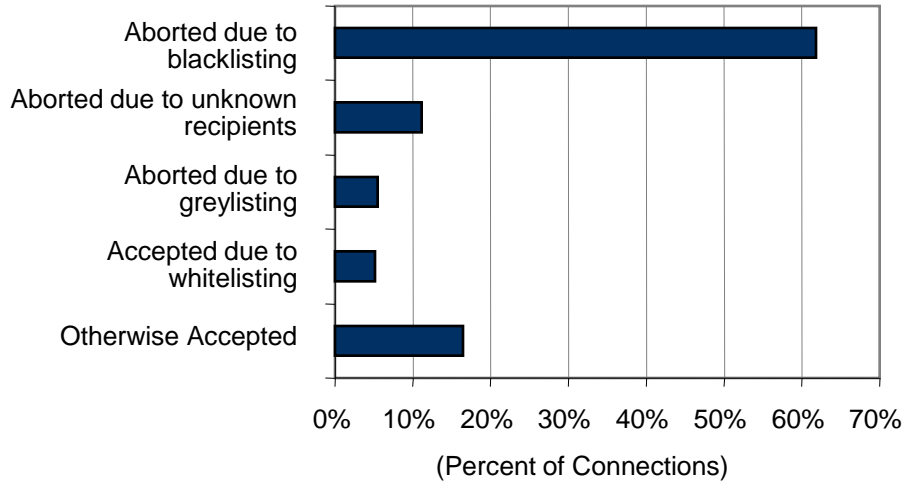
Source: ENISA Anti-Spam Survey 2009

Effectiveness of Measures

Messages Aborted or Filtered

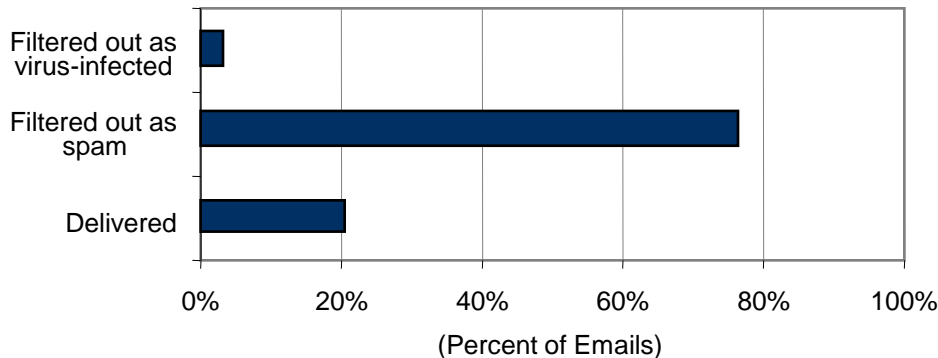
SMTP Connections Aborted or Accepted

Q Could you provide us the following information about your anti-spam system?
Percentage of SMTP connections ...?



Accepted SMTP Connections Resulting in Blocked or Delivered Email

Q Of those connections that are accepted, what is the percentage of emails...?



- ★ Majority of answers with a total of over 70 million mailboxes under management
- ★ In the SMTP analysis, blacklisting accounts for the vast majority of aborted spam.
- ★ Once the messages are accepted, they are then analyzed by virus scanners and spam filters. Virus scans eliminate 3%, while three quarters are filtered out as spam. The remaining 21% of messages are actually delivered.

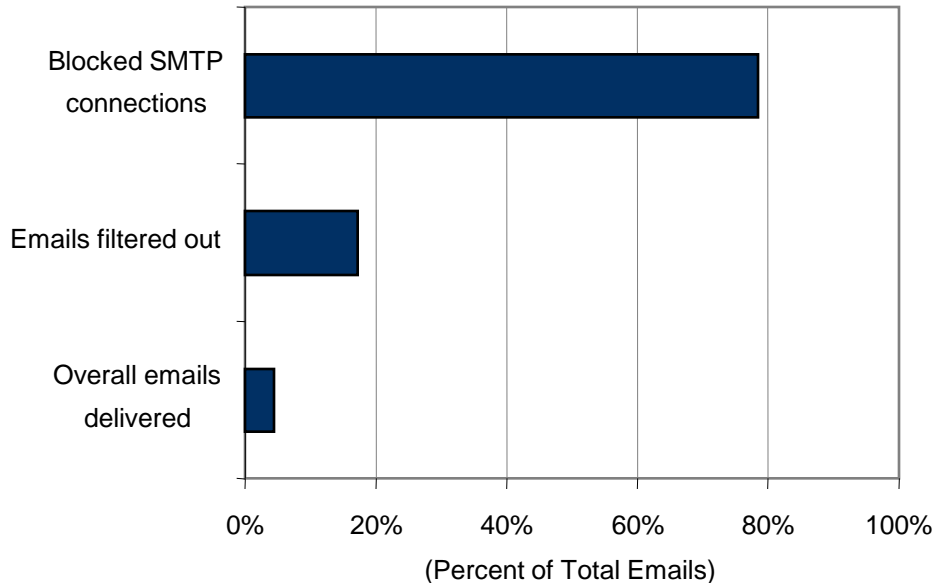
N=58

Source: ENISA Anti-Spam Survey 2009

Effectiveness of Measures

Messages Blocked, Filtered, or Delivered

Overall Email Traffic Blocked or Delivered



N=58

Source: ENISA Anti-Spam Survey 2009

- ★ Only 4.4% of the total email traffic is delivered, with 95.6% blocked by the various anti-spam measures
- ★ With only a small portion of email traffic being delivered, the anti-spam measures in use appear to be cumulatively effective.

Conclusions

- ★ Providers take spam seriously as a security challenge, but it is not a critical threat.
- ★ The various anti-spam measures currently filter out over 95% of email traffic, greatly reducing the volume of spam that customers receive, without causing significant problems with false positives. Anti-spam measures are doing their job, reducing the threat of spam to a manageable security process. This process still requires focus, expertise and resources, but it is arguably predictable.
- ★ Little has changed over the last two years. Most measures are applied by similar proportions of providers to what was observed in 2007.
- ★ However, many providers indicated plans to implement new measures in the coming six months. Thus, although usage levels of various measures have remained constant, providers are frequently adjusting or upgrading their measures to ensure that they remain effective.
- ★ These results, combined with the moderate significance assigned to spam by providers, suggest that spam prevention has reached a sort of equilibrium, in which substantial efforts are required to manage spam, but the challenges and countermeasures are generally well-understood. The countermeasures are proving effective, when managed and updated properly, so little major changes seem to be required.

Recommendations

- ★ Though anti-spam measures are proving generally effective, these efforts could still be improved. For example:
 - ★ Email providers should take a more proactive approach to monitoring spam and identifying the source, so that appropriate actions can be taken by originating ISPs.
 - ★ Blacklist managers need to ensure that it is easy to remove a server or domain from a blacklist when spam problems have been rectified. And with so many different blacklists in use, collaborative efforts to share data on servers that should be removed from blacklists would help to address the problem. Wider use of whitelists could help in this effort.
 - ★ Providers should look to increase the abuse report feedback loops with other providers and aim to automate abuse reporting processes, possibly adopting the Abuse Reporting Format (ARF).
 - ★ Providers should seek collaborative solutions to fight spam, as many, but not all, already do. For example, notifying ISPs that originate spam that they are doing so and discussing countermeasures with them will help to cut off spam at the source.
 - ★ Policy-makers and regulatory authorities could help spam prevention efforts by further clarifying the apparent conflicts between spam-filtering, privacy, and obligation to deliver, particularly by distributing and promoting awareness of the findings of the Article 29 Data Protection Working Group, which outlines the legal basis for spam-filtering based on the EU legal framework.
 - ★ Institutions that aim to aid public and private efforts against spam should promote open collaborative solutions to spam, such as reporting of spam sources to other ISPs and authorities; the Abuse Reporting Format; contribution to collaborative solutions; and sharing of best practices across the industry to aid providers that need to improve their anti-spam measures.

Additional Resources

- ★ There are many additional resources that can be useful in further investigating, tracking, and participating in the anti-spam dialogue. Selected examples are highlighted below.
 - ★ **The Article 29 Data Protection Working Party**, "Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services", 21 February 2006 (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp118_en.pdf). In this document, the Working Party explains its view on the legal basis for spam filtering.
 - ★ **ETIS**, a global association of telecommunications service providers, has an Information Security Working Group that contributes to anti-spam efforts, along with other security initiatives. More information is available at http://www.etis.org/activities/Information_Security_Group.asp
 - ★ **EuroISPA**, the European ISP Association (<http://www.euroispa.org/>). EuroISPA represents European ISPs, participating in industry discussions and publishing position papers on issues relevant to its members.
 - ★ **The Verband der Deutschen Internetwirtschaft e. V. (eco)** is very active in the anti-spam dialogue, including hosting regular anti-spam summits. The most recent summit information can be found at <http://www.eco.de/antispamsummit2009>.
 - ★ **The Messaging Anti-Abuse Working Group (MAAWG)** regularly publishes findings on the abusive emails blocked or filtered by its members. A recent study can be found at http://www.maawg.org/about/MAAWG_2008-Q3Q4_Metrics_Report.pdf. Much more information about global anti-spam efforts can be found at the MAAWG website at <http://www.maawg.org>.
 - ★ The disconnection of the McColo server farm in California in November 2008 temporarily reduced the amount of spam being sent worldwide and yielded useful insight into both spam's origination and the effectiveness of anti-spam measures. **Richard Clayton** of the University of Cambridge, UK, published one study of the anti-spam measures during that period, called "**How much did shutting down McColo help?**" that can be found at <http://www.ceas.cc/papers-2009/ceas2009-paper-16.pdf>.
 - ★ Additional insight into the impact of the McColo server farm on spam can be found in **Symantec's** monthly reports called "**The State of Spam**", which can be found at http://www.symantec.com/business/theme.jsp?themeid=state_of_spam.