



**Survey on Industry Measures taken to comply  
with National Measures implementing Provisions  
of the Regulatory Framework  
for Electronic Communications  
relating to the Security of Services**

ENISA/TD/SP/06/0055

**Conducted by the  
Technical Department of ENISA,  
Section Security Policies**

**February 2006**

# Survey on industry measures taken to comply with national measures implementing provision of the regulatory framework for electronic communications relating to the security of services

## 1 Executive Summary

European providers of electronic communication services use a variety of technical and organizational measures to secure their services and to fight unsolicited electronic mail (spam). This study, conducted by ENISA in January 2006, provides an overview of these measures. It is based on more than 90 responses to questionnaires that were sent to providers and National Regulatory Authorities. The outline of the study follows Directive 2002/58/EC, in particular Article 4 (Security) and Article 13 (Unsolicited Communications).

### Security Measures

The security measures that providers implement vary widely. They depend on the type of threat against which each provider focuses its defense, and the specific nature of the business the provider is in. The following list of activities would help improving technical security measures.

- To increase transparency and introduce comparability, providers could be required to report on the technical measures which they implement to secure their services.
- There should be an incentive for providers to contribute to the overall security of interconnected networks rather than protecting merely their own resources. Egress filtering could be encouraged.
- Providers need to be more proactive and monitor their networks for risks of security breaches. Providers could also be asked to report which networks they monitor.

Organizational measures are equally important, but are often neglected.

- The necessity of clear documentation and regular communications on information security as well as collection and dissemination of best practices should be emphasized.
- This includes guidance to consumers as well as guidance to the provider's staff, in particular with regard to incident response and emergency planning.
- The need for contact details for email abuse and security violations should also be stressed.

Regarding the state of the art and cost of security implementations, additional guidance is welcome, in particular around industry best practices, and should be supported at EU level. For example, the European Commission could find a way to involve National Regulatory Authorities (NRAs) for electronic communication services more actively in information security matters. NRAs or other national bodies could act as recipients of reports on the risk of security breaches.

Having providers report on the risk of security breaches is very important in order to get an overview of the risk that can be expected from a particular problem. This assumes that information on such risk of breaches has been communicated properly. Reporting of actual security breaches, publicly or anonymously, would improve the situation further.

## Unsolicited electronic mail

From a technical perspective, there is no 100% protection against spam. Technical protection against incoming spam can only be improved marginally. Unless economic models for spam change dramatically, there is probably not much more that providers can do next to applying the variety of countermeasures to the largest extent possible. Most spam originates outside of the EU. Reporting large scale email abuse, both within and – with international coordination - from outside the EU, should be encouraged. NRAs or other national bodies could take a more active role here.

A major problem is that spammers often hide their true identity. Given the variety of possible sender identification methods, consideration should be given to technical interoperability and standardization. The relationship between those national entities who control electronic communications and those who control transmission of unsolicited emails should also be clarified and simplified. Coordination is desirable at Member State or EU level. Also, the terms opt-in and opt-out and the scenarios in which they are applicable could be further clarified.

Providers in Europe are more concerned about spam emails that their customers receive than they are concerned with spam that their customers send. Here, regarding outgoing spam, they rely mostly on legal instruments such as Terms and Conditions. Enforcement could be further improved to also prevent spam originating from Europe.

## Summary

Under the regulatory framework for electronic communications, service providers have to take technical and organizational measures to safeguard the security of their services. Implementations of such security requirements are gaining in importance and have to be improved, as indicated by the conclusions above. The following report provides the data on which these conclusions are based. Based on its work program or upon request, ENISA, will - within its mandate - coordinate further analysis and continue to improve the situation of information security in Europe.

## 2 Introduction

### 2.1 Index

1	Executive Summary.....	2
2	Introduction .....	4
2.1	Index .....	4
2.2	Motivation .....	5
2.3	Request .....	5
2.4	Methodology.....	5
3	Results .....	7
3.1	Overview of the results.....	7
3.1.1	Distribution of responses relating to geography and EU membership.....	7
3.1.2	Distribution of responses with regard to types of provider .....	7
3.2	Security measures taken by providers .....	9
3.2.1	Technical measures .....	9
3.2.2	Organizational measures .....	11
3.2.3	Measures by type of provider .....	13
3.3	Anti-Spam measures taken by providers.....	14
3.3.1	Outgoing Emails.....	14
3.3.2	Incoming Emails.....	15
3.3.3	Spam coming from outside the EU .....	17
3.3.4	Unsolicited communications for the purpose of direct marketing .....	19
3.3.5	Message authentication .....	20
3.4	Appropriateness of measures taken by providers.....	21
3.5	Security breaches and anti-spam violations .....	22
3.5.1	Discovering problems.....	22
3.5.2	Reacting to problems.....	23
3.5.3	Provider's perception of legislative requirements .....	26
3.6	The Role of NRAs .....	27
3.6.1	Security and spam countermeasures.....	27
3.6.2	Nature of requirements .....	28
3.6.3	Security breaches.....	29
4	Appendix .....	31
4.1	Request from the European Commission .....	31
4.2	List of Conclusions.....	33
4.3	Legislative Requirements .....	34
4.3.1	Perception of respondents (providers).....	34
4.3.2	Transposition Status of Directive 2002/58/EC.....	36
4.4	Questionnaires .....	36
4.4.1	Questionnaire for Providers.....	36
4.4.2	Questionnaire for NRAs .....	39
4.5	Explanation of terms.....	41

## 2.2 Motivation

Providers of electronic communication services such as telecommunication companies and Internet service providers have to deal with a number of information security threats as well as an increasing amount of unsolicited emails, commonly called “spam”. The European Directive 2002/58/EC provides a framework for addressing these problems. It has been transposed into national laws in most Member States of the European Union. Providers have taken different measures to comply with these laws.

Still, the European citizen does not feel secure enough when using the Internet. This lack of trust continues to hinder the acceptance of eGovernment and eCommerce services, and delays achievement of the Lisbon goals to make the EU “the most competitive and dynamic knowledge-driven economy by 2010”. Security measures and measures to fight spam have to be improved and coordinated among the different players, in order to make the Internet a safer place.

As a first step, it is necessary to get a better understanding of the measures that providers have already taken. Making this inventory available to the providers may help them to find a more coordinated approach in the future and to raise the bar to the same level. Such a survey will also suggest certain improvements to EU or national legislation in this area. Finally, it will signal if and where the cooperation between the various players – electronic communication providers, National Regulatory Authorities (NRAs), the European Commission, governments, and the European Network and Information Security Agency (ENISA) – can be improved.

## 2.3 Request

ENISA’s Work Program 2006 includes a “*Study listing measures adopted and made available by providers of electronic communication services to comply with legal requirements regarding technical and organizational measures to safeguard the security of their services*”. ENISA will conduct this study in the second quarter of 2006. However, given that such results are considered a valuable input during the review of the provisions of the regulatory framework on electronic communications, which is taking place early in 2006, the European Commission has submitted a request for assistance to ENISA in November 2005 (see Appendix).

ENISA has accepted this request in December 2005 under the assumption that a study with such a short timeframe cannot have the same depth and breadth as had been envisioned in the Work Program 2006. ENISA promised to do everything possible to conduct such a study immediately and deliver the report by the end of February 2006. This document is the result of this study.

## 2.4 Methodology

The main goal of the study was to obtain information from electronic communication providers regarding the security and anti-spam measures they take. Two questionnaires were created.

1. One questionnaire was addressed to National Regulatory Authorities (NRAs) of electronic communication services. It was sent to all European NRAs via the secretariat of the European Regulators Group (i.e. beyond EU Member States to EEA, candidate or non EU countries).

2. One questionnaire was addressed to providers, it was sent via the same channel. All NRAs were asked to forward the second questionnaire to all providers in their country. In addition, this second questionnaire was sent via the mailing list of RIPE, the Réseaux IP Européens (i.e. beyond EU Member States to EEA, candidate or non EU countries).

The complexity of the task and the challenging timeframe made it necessary to focus the study in a certain way. In particular, the following should be noted:

- Given the short timeframe, ENISA decided to keep each questionnaire at only 2 pages, as short and as simple as possible. Only this allowed ENISA to set a tight deadline for the responses and still receive a reasonable number of answers. ENISA allowed a deadline of three weeks, and extended this deadline once for another 10 days.
- The questionnaires were phrased slightly differently for NRAs and for providers, but both questionnaires covered the same topics and followed the outline of Directive 2002/58/EC in the same way. Hence the results of the questionnaires are comparable. Both questionnaires are listed in the appendix.
- This is not a legal research project. ENISA decided to have its Technical Department reply to the European Commission's request and conduct the study. Consequently, the study looks at technical and organizational matters that providers have taken and does not analyze national laws.
- For the providers, ENISA offered three different ways to respond: via email using an MS Word version of the questionnaire, via fax using a PDF version, and via a web form that was set up particularly for this study. Surprisingly, only one respondent used the fax. About a third chose to use the web form, while two thirds send back the MS Word document.
- The provider questionnaire offered the possibility to remain anonymous. Even though about a third of the providers chose that option, virtually all of them gave their contact details (so these replies can be considered authentic and valid). However, ENISA does not provide details of the responses, neither in this document nor via other channels.

Overall, ENISA received more than 90 responses (some came in too late), of which 17 responses from NRAs and 74 responses from providers were taken into account. This number is significant, but not necessarily sufficient. Further research will be necessary to represent the situation in Europe comprehensively and in detail.

Also, please note that not all responses were complete. 2 NRAs responded only with a short email and some responses from providers were sent anonymously, i.e. without indication of the country. So for some questions the total number of responses is less than 74 or 17 respectively, depending on the type of question. The evaluation of these responses is provided in the following chapters.

## 3 Results

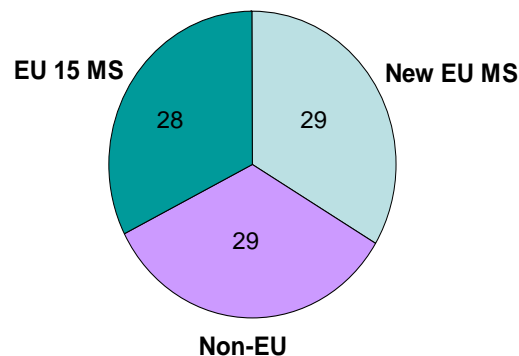
### 3.1 Overview of the results

#### 3.1.1 Distribution of responses relating to geography and EU membership

Responses were received equally from all regions of Europe, though not from all countries. The distribution of responses is also balanced with regard to another criterion: Member States of the so-called EU 15, Member States of the countries that joined the EU on the 1<sup>st</sup> of May 2004, and non-EU states answered approximately equally. Obviously organizations in new Member States – although less numerous - are more motivated to invest time in a reply. Another reason is probably the size of the country: in smaller countries, forwarding a questionnaire to the right person to answer the questions may be much easier.



All responses – EU versus non-EU



Number of responses: 86

Regarding the non-EU countries, Norway (which is part of the EEA) provided a large number of responses, followed by Bulgaria. These countries do not necessarily have to comply (yet) with transpositions of EU Directive 2002/58/EC, but given the integration of European networks and the fact that problems – and solutions - in those countries have an effect on EU countries, these responses provide valuable insights.

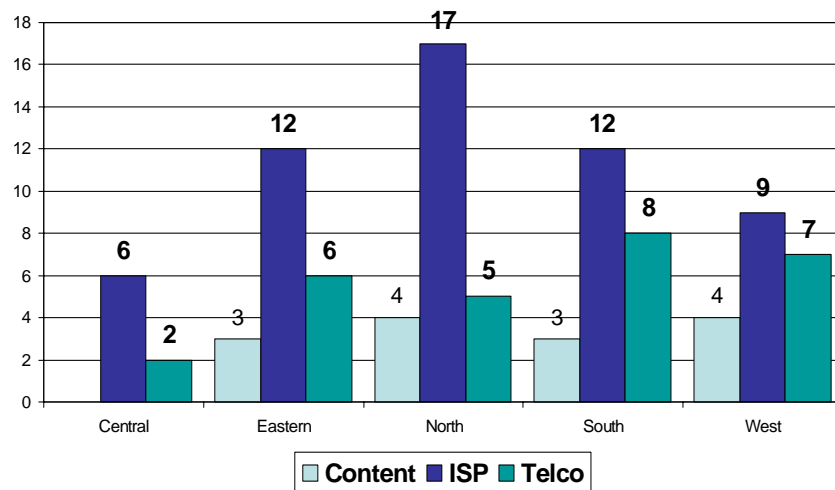
#### 3.1.2 Distribution of responses with regard to types of provider

The Directive 2002/58/EC differentiates between electronic communication network providers and electronic communication services providers as well as public communication network providers. However, these terms are not well known in the industry, and would have been

especially confusing in those countries which do not have to transpose the Directive. Consequently, the questionnaire for providers offered the options “telco” (telecommunication company), “ISP” (Internet Service Provider) and Content Provider.



Number of responding telcos, ISPs and content providers – by region –



The chart above shows the distribution across the different types of providers in the different regions. Regardless of the region, ISPs provided by far most of the responses. This is not surprising, given that the nature of the questions is most relevant in this space. It should be noted that the questionnaire offered the possibility to choose multiple options, i.e. many providers claimed to act as a telco and as an ISP, occasionally in a combination with content provisioning.

The regional distribution across the types is more or less in line with the regional distribution of the total number, except for the fact that in the Northern region, comparatively less telcos provided an answer. One reason might be that convergence between Internet service provisioning and telecommunication is more advanced in that region, and many providers see themselves predominantly as ISP.



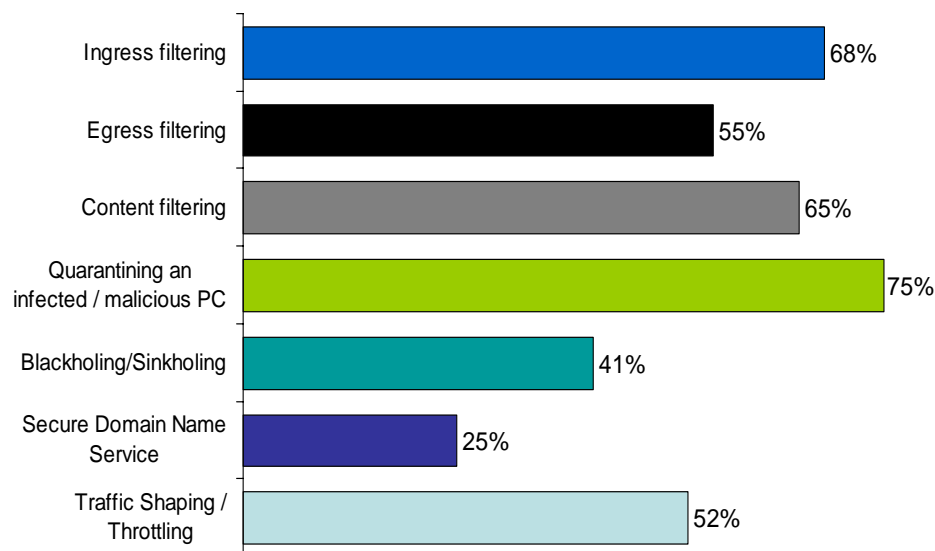
## 3.2 Security measures taken by providers

### 3.2.1 Technical measures

The first – and also most important - question analyzes the technical and organizational measures that providers in Europe take to improve security of their services, according to Article 4 of Directive 2002/58/EC.



Which of the following measures do you take in order to improve security of your services?  
– Technical Measures –



- Not surprisingly, ingress filtering ranks very high, i.e. providers are filtering incoming traffic, trying to keep security threats off their network.
- Providers are less engaged in protecting other networks from malicious traffic on their own network, i.e. egress filtering ranks lower.
- The number of providers that quarantine infected PCs on their network is very high.
- Blackholing / sinkholing and traffic shaping / throttling are used by only around half of the providers. These can be considered more advanced – and more costly – mechanisms.
- The figures for the different security measures vary widely, from a few percent for Secure DNS, to a high number of percent for quarantining a malicious PC. Other measures are used only by more or less half of the providers.

A closer look at the responses reveals that all providers do at least one thing, most of them do 3-5 things in combination, and some of them indicate that they have all 7 proposed countermeasures in place. There is no pattern visible whether certain measures are always used together. It depends on a number of parameters, such as the nature of the providers business (international carrier, serving corporate customers or serving consumers), its maturity (e.g. incumbent national carrier, startup, spin-off), or the type of its connections (Tier 1/2/3). ENISA has not requested such detailed information within this questionnaire. An analysis against the two categories that could be collected – region and type (telco/ISP/content) – did not reveal any additional information.

Moreover, it also depends on the type of threat against which a provider sets up its defenses. A provider who offers Voice over IP services is concerned about Quality of Service (QoS) and will favor traffic shaping / throttling, to make sure that enough bandwidth is available. A provider who offers a large amount of cheap consumer connections will have a high number of clients with absolutely no security expertise. A higher level of not-patched, not-secured PCs can be expected, leading to more infections which Trojans, so that Quarantining PCs could be the preferred choice. In fact, the high number of providers who quarantine infected PCs is a positive sign should be an encouragement for those who do not do it yet. A large corporate customer will have its own security department and will not want its connection to be suddenly shut off nor throttled, but might not mind some simple ingress filtering, to protect it against the worst.

This complexity makes it difficult to issue any specific conclusion regarding technical measures. Some conclusions, however, should be allowed. Egress filtering is used by only half of the respondents, and the other measures rather protect the providers own resources. Providers seem more concerned about protecting their own network than they are willing to protect other networks from malicious activity on their side. It would be beneficial to either reward those who do more to protect others or pinpoint those who are rather careless in inter-connected environments. To do this, it would be necessary to track continuously what technical measures are taken, and to what extent these measures are fruitful. “Good practice” or “best practice” examples could be rewarded with a seal, which providers would use to market security and stability of their services. Once this is accepted, media would have a chance to publicly criticize those who are careless. Such a scheme would require the duty for providers to report technical measures on an ongoing basis.

Conclusion: The technical measures that providers implement vary widely. They depend on the type of threat against which each provider focuses its defense and the specific nature of the business the provider is in. However, technical measures can be improved.

- 1) To increase transparency and introduce comparability, providers could be required to report on the technical measures which they implement to secure their services.
- 2) There should be an incentive for providers to contribute to the overall security of interconnected networks rather than protecting merely their own resources. Egress filtering could be encouraged.

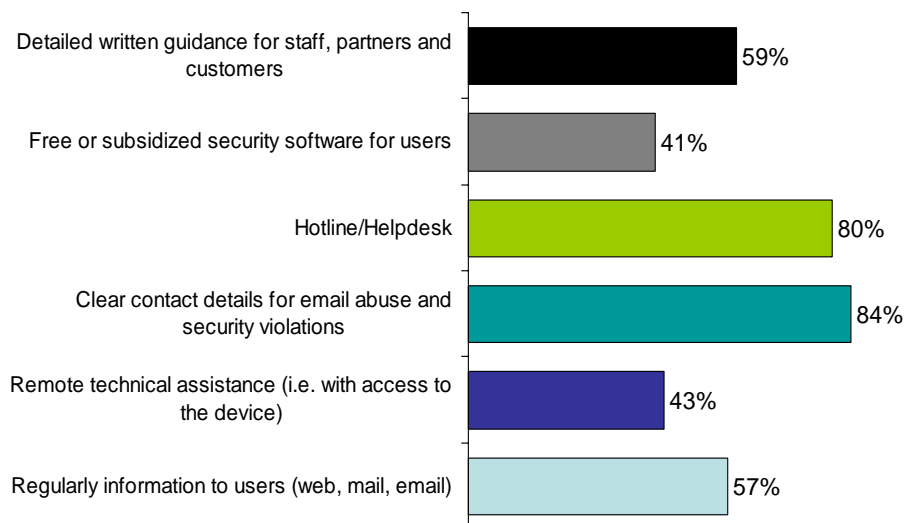
An additional technical measure could be DNSSEC. As a way of guaranteeing the authenticity of DNS (Domain Name System) information, it is a powerful mechanism and would help reducing a number of problems, including spam. DNSSEC is so far only implemented in Sweden. It has to be put in place by the national domain name registrar, i.e. for the whole country, before providers can rely on it. A further distribution of DNSSEC would be laudable.

### 3.2.2 Organizational measures

The organizational measures complement the technical measures (see chart below).



Which of the following measures do you take in order to improve security of your services?  
– Organizational Measures –



- The most wide-spread ones are “clear contact details” and “hotline”, although 16% of all providers do not provide clear contact details.
- As a security measure, only 59% offer detailed written guidance for staff, partners and customers. Assuming that some providers offer it only for staff, some only for partners, and others only for customers, the percent for each group would actually be even lower.
- Remote technical assistance achieved a comparatively low rank here.
- No clear pattern of organizational measures is visible. Most providers use a combination of different measures.

The choice of measures that providers take obviously depends on a number of reasons. Providing a hotline and offering contact details is essential for the core business of the provider. A successful provider will most likely have a Customer Relationship Management (CRM) process

in place. Leveraging or extending this process for security problems requires only minor additional resources (e.g. an additional email address, or a change of guidelines for hotline staff). In fact, it should be worrying that 16% do not provide clear contact details.

The lack of written guidance is quite typical for information security and IT in general. Implementations are often seen as more important than documentation. However, it is widely accepted among security professionals that clear and documented guidance is a prerequisite, and should not be an afterthought.

The fact that remote technical assistance achieved a comparatively low rank here is not surprising, given the resources – both in terms of deployed technology and trained staff – that such a service requires. However, a related question should be raised here: What happens in cases of emergency? Most technical and organizational measures are proactive in nature, and this is laudable. But if a reaction is necessary, are mechanisms in place to help users recover from the incident and resume work? Especially regarding the low level of written guidance, this is questionable. Guidance is needed for cleaning computers from malicious code of different types, for using redundant connections during a worm outbreak, for reporting significant or repeated abuse of resources, for loss of valuable devices, or for recovery after web site hacking.

Guidance should also cover topics like secure configuration of single computers, secure configuration of home networks, simple and safe configuration of computers and networks for small enterprises, redundant connection of small medium enterprises, and secure operation of a web presence. Moreover, keeping users informed about security problems on a regular basis improves the user's knowledge, increases transparency, and helps the user trusting the service provided.

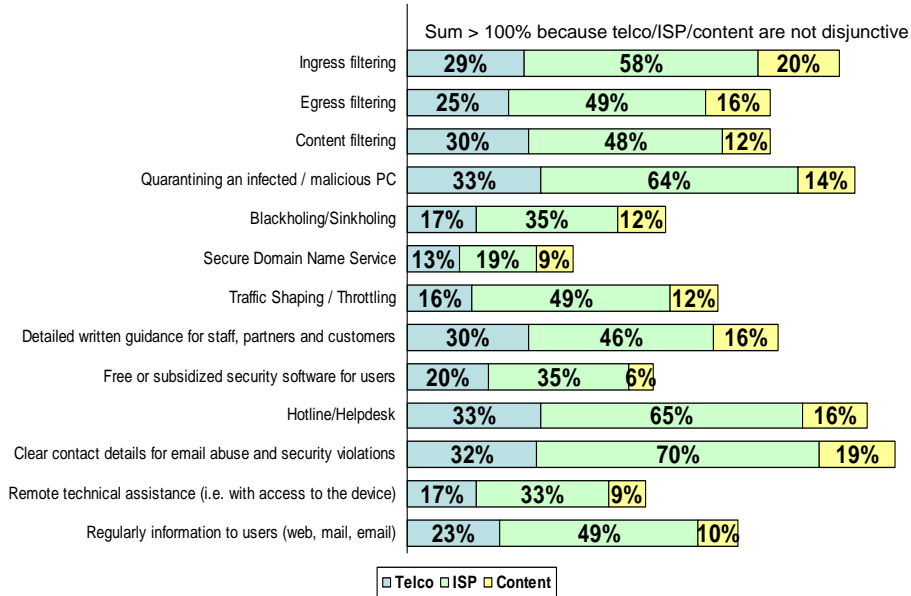
Conclusion: With regard to organizational measures overall guidance could be improved.

- 1) The importance of clear documentation and regular communications on information security as well as collection and dissemination of best practices (e.g. by ENISA) should be emphasized.
- 2) This includes guidance to consumers as well as guidance to working staff, in particular with regard to incident response and emergency planning.
- 3) The need for contact details for email abuse and security violations should be stressed.

### 3.2.3 Measures by type of provider



Which of the following measures do you take in order to improve security of your services? – Overview



Looking at an overview of both technical and organizational measures, and at the same time analyzing these with regard to different types of providers, does not reveal much new information. Some organizational measures are obviously more widespread, because they are easier – and cheaper – to implement. Remote technical assistance and quarantining are less popular among content providers, because content traffic is more diverse in nature than network traffic (i.e. more protocols, more filter criteria). Amongst telecommunication companies, a hotline is slightly more popular than clear contact details – understandable, given that telcos can offer hotlines easily. Overall, the telecommunication companies, ISPs, and content providers answer this (and other) questions in a balanced manner, so subsequently this split will not be discussed further.

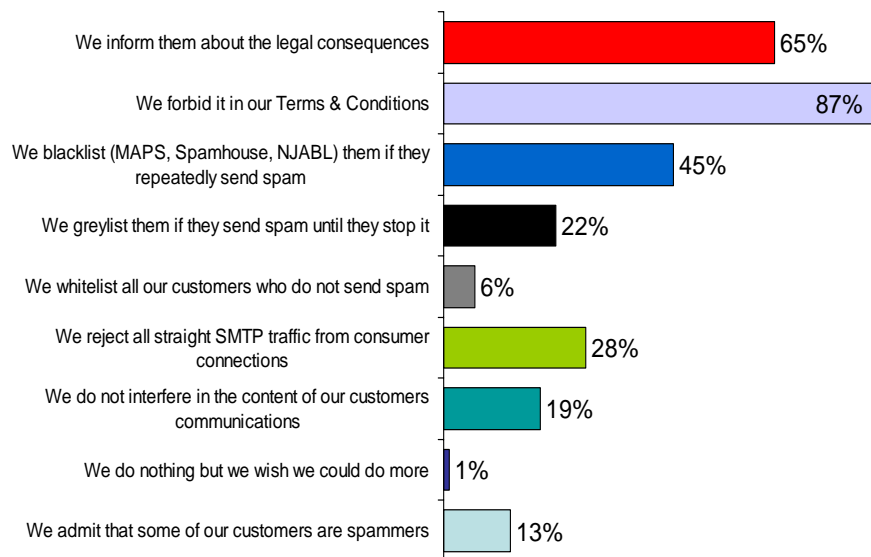
### 3.3 Anti-Spam measures taken by providers

Dealing with a few spammers on the own network or dealing with huge amounts of spam coming from other networks are two quite different problems. Hence such anti-spam measures taken by providers are discussed separately.

#### 3.3.1 Outgoing Emails



What measures did you put in place to prevent your customers from **sending** unsolicited communications (spam)?



- Most providers forbid sending unsolicited emails (spam) in their Terms & Conditions.
- More than 20% less providers inform customers about the legal consequences of sending spam.
- Enforcement of anti-spam clauses is low. Some providers reject all straight SMTP traffic from consumer connections, i.e. they allow every user only to access the mail servers of the provider, and sometimes restrict email access to special software or to web access.
- Other providers prefer not to interfere with the content of their customers' communications, which would mean that there are no technical measures that would prevent a customer from sending large amounts of emails.
- 13% of the providers admit that some of their customers are spammers.

Turning a blind eye on spam can be financially beneficial for a provider. According to an MSNBC report (<http://msnbc.msn.com/id/3078642/>), ISPs can get “premium, rather than normal rates to sell bandwidth to known spammers. In exchange, the ISP agrees to suffer more than normal complaint rates.” Providers who pursue such a strategy might be few, but it might even not be the strategy of the provider. As the report points out, “engineers, abuse staff and technicians all want the spammers off the network, but you have the sales staff looking at the money.”

On the other hand when analyzing these measures, it is important to take into account the geographic origin of spam. Most spam originates in countries outside Europe. For example, on February 24<sup>th</sup>, 2006 the list of the 10 worst spam origin countries on <http://www.spamhaus.org/statistics/countries.lasso> showed only one European country - the UK on position #8, accounting for only 3% of spam issues on this list. On the other hand, on the list of the most affected countries on <http://www.trendmicro.com/spam-map/default.asp>, 5 of the 10 countries were EU Member States, suffering from about 16% of the world’s spam.

Conclusion: Providers in Europe are less concerned about outgoing emails, i.e. they are less concerned about their customers sending spam. They rely on legal instruments such as Terms and Conditions. In addition to better information about legal consequences, enforcement could be further improved to prevent spam originating from Europe.

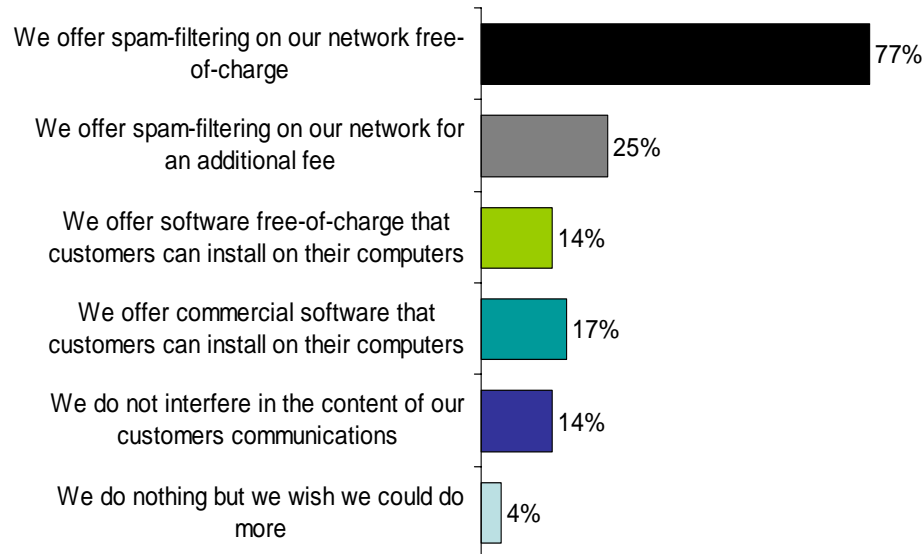
Note: Some of the measures listed in the table above - blacklisting, greylisting and whitelisting - are relevant for outgoing emails in the sense that a provider would report a spammer on its network to an organization that maintains blacklists (of which MAPS, Spamhaus, NJABL are some better known and reputable ones), temporarily block a spammer on its own network or maintain a whitelist of its own customers. At the same time, a provider would also subscribe to such lists to protect email recipients on its own network. Here – with regard to incoming emails – providers are much more active.

### 3.3.2 Incoming Emails

Protecting one’s own customers is of major importance for providers, and indeed most of them invest voluntarily and significantly in such protection, as the following chart shows.



### What measures did you put in place to protect your customers from **receiving** unsolicited communications (spam)?



There are several options for filtering spam and as the chart shows, providers use them at varying degrees:

- The provider can offer such service free of charge. This allows a rather quick reaction to the spam problem.
- The provider can charge a fee for this service. This lowers the financial burden for the provider, but it takes more time to see an uptake of spam filtering.
- The provider can filter on its own network. This is comparatively cheap and allows updating spam signatures and filtering rules quickly.
- The provider can offer software for download; the customer installs and configures it to its own liking.
- All combinations of the above options are possible.

Looking at how many providers offer any kind of spam protection at all, the figure of 81% is not as high as it could have been expected, because many offer several ways in parallel. This figure matches well with the 4% who wish they could do more and the 14% who do not want to interfere in the content of their customer's communications. One reason for this non-interference could be that some providers focus on large corporate customers. Typically, these prefer to retain control over such measures and seek to implement measures themselves.

Most of the providers realized that legal protection against incoming spam is not sufficient, and that there is also not enough incentive for users to invest in spam protection themselves. Consequently, and in order to protect a core asset - the customer, many providers saw free-of-charge spam protection as the only viable solution.



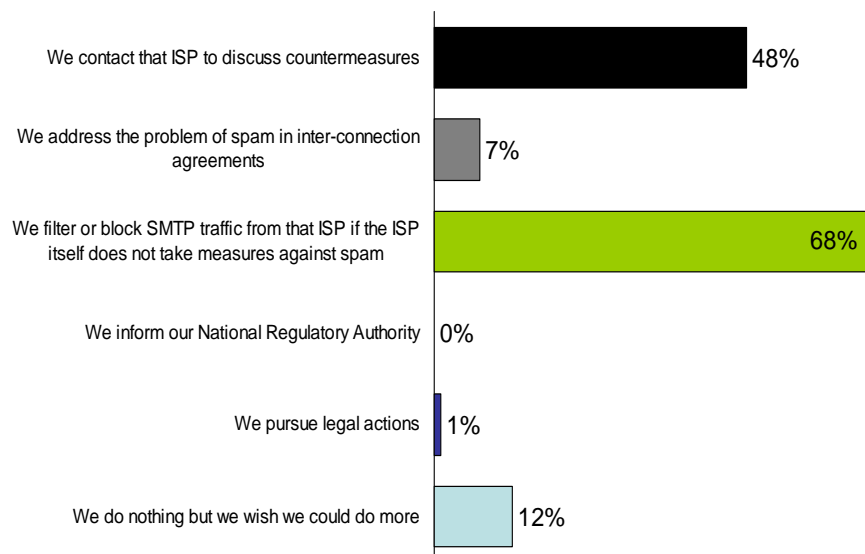
It should be noted, that the economic model behind spamming is still successful. Sending millions of emails to get few responses makes sense for spammers as long as sending emails costs virtually nothing. One way to change this could be to charge a very low amount per email / per recipient (e.g. less than €0,01). For most users, such costs would be negligible in comparison with other fees, but for spammers this would mean a significant financial hurdle. However, such a large scale change is very difficult to orchestrate and hence unlikely.

Conclusion: From a technical perspective, there is no 100% protection against spam. Technical protection against incoming spam can be improved, but only marginally. Unless economic models for spam change dramatically, there is probably not much more that providers can do next to applying the variety of countermeasures to the largest extend possible.

### 3.3.3 Spam coming from outside the EU



What sort of measures do you take if you detect spam coming from an ISP based in a non-EU country?



- Less than half of the providers contact the foreign ISP which has been identified as the source of the spam.
- Two thirds filter or block SMTP traffic from that ISP if spam keeps coming from a non EU country.
- Few pursue legal action and only some address the problem of spam in inter-connection agreements.
- No ISP seems to report spam to NRAs.

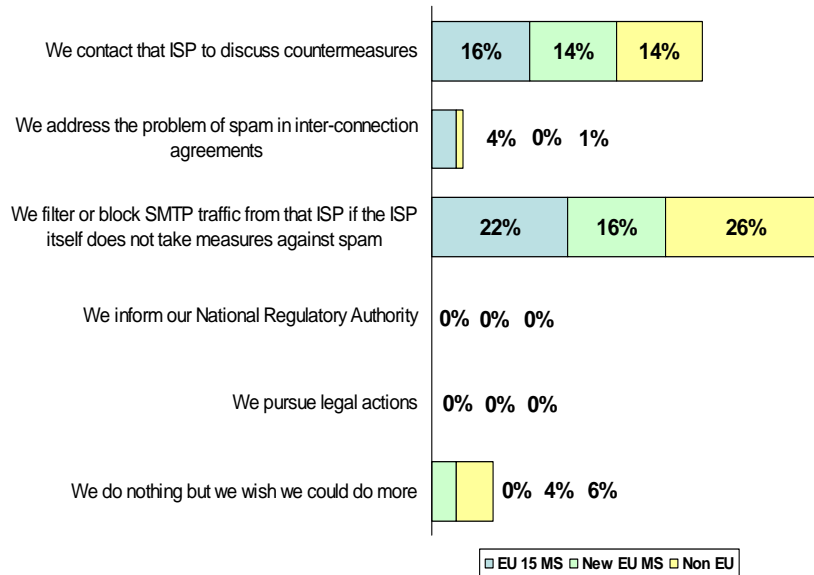
The results are somewhat surprising, since providers pay great attention to prohibiting spam in the Terms and Conditions which form the contractual basis with their own clients. It seems that providers have little incentive to be proactive and address spam in inter-connection agreements, or no hope that such provisions could improve their situation with regard to spam.

The lack of information regarding NRAs is worrying. Regular reports to the NRA which lists such providers could increase transparency and help to improve the situation. In this context, the London Action Plan (LAP), which also incorporates the EU initiative of a Contact Network of Spam Authorities (CNSA), could play a role.

Conclusion: Reporting large scale email abuse to competent NRAs should be encouraged. Building on that, NRAs could take a more active role. ENISA could help raise awareness in this regard.



### What sort of measures do you take if you detect spam coming from an ISP based in a non-EU country?

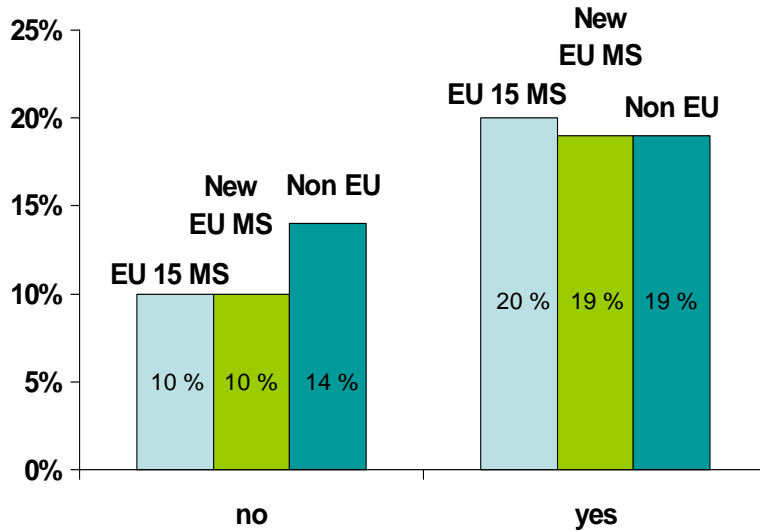


While regarding most questions there is not much difference in the response from EU 15 Member States, new EU Member States and non EU states, in this particular case some variations are visible. Addressing spam in inter-connection agreements has been reported mostly by EU 15 Member States, while new EU Member States and non EU states are skeptical, expressing that they do nothing but wish they could do more. Obviously, such states (9 responses altogether) would benefit from some additional encouragement and support.

### 3.3.4 Unsolicited communications for the purpose of direct marketing



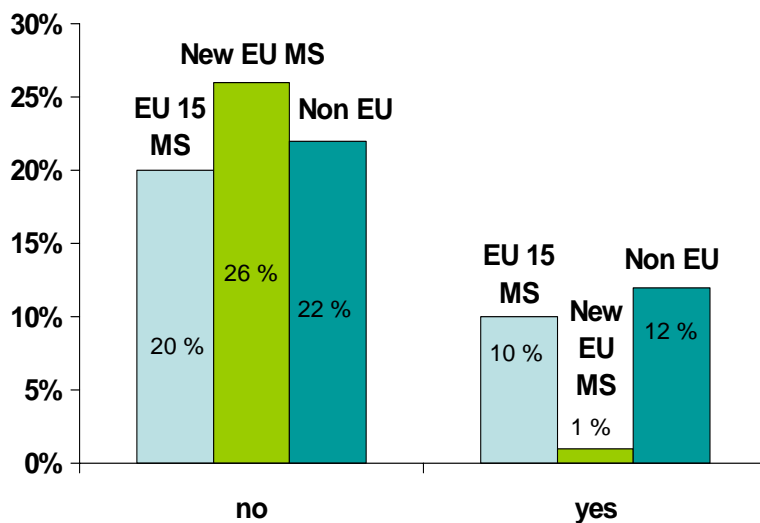
Does legislation in your country allow unsolicited communications for purposes of direct marketing only with the consent of the subscriber (opt-in)?



- Almost two thirds of the respondents said that legislation in their country supports unsolicited communications for purposes of direct marketing only with the consent of the subscriber. This is commonly called opt-in.
- The other third said that this is not the case.



Does legislation in your country allow unsolicited communications for purposes of direct marketing unless the subscriber expressed the wish to no receive these communications (opt-out)?



- Two thirds of the respondents replied that their country does not unsolicited communications for purposes of direct marketing unless the subscriber opts out, 23% said that this is allowed.
- Most countries among the new EU Member States said that it is not allowed.

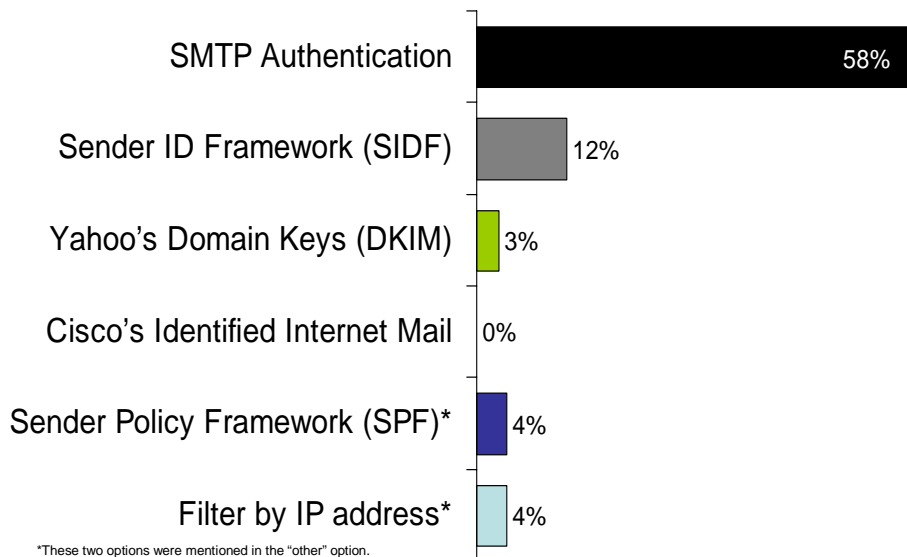
Obviously, opt-in is preferred over opt-out in Europe, but the picture here is not absolutely clear. The terms opt-in & opt-out are not explicitly stated in the Directive, although the Directive uses the concept of consent. The scenarios described in the Directive are also more complex than could be asked in the context of this survey. Some variations regarding the national implementations of different scenarios such as “natural vs. legal person”, “existing business relationship” and “professional vs. private email address” make it difficult for providers in Europe to pursue or support only one strategy. Depending on the scenario, the situation of opt-in versus opt-out is not that clear-cut, because among the EU 15 Member States like Spain, France and the UK ask for opt-in in some situations while allowing opt-out in others.

Conclusion: With regard to the different choices of opt-in versus opt-out, the terms of the Directive 2002/58/EC could be further clarified.

### 3.3.5 Message authentication



How do you prevent senders of electronic mail from disguising or concealing its identity?



None of the upcoming authentication mechanisms for email users has reached any significance yet. In fact, providers use a wider variety of mechanisms than anticipated. Two more options (“Sender Policy Framework” and “Filter by IP address”) were mentioned repeatedly and had to

be added to the list. Overall, SMTP authentication is still the method of choice for preventing senders of emails from disguising or concealing the identity (as requested by the Directive).

ENISA’s next survey might analyze more in detail to what extent the different types of SMTP authentication (e.g. auth login, auth plain, TLS, Kerberos) are being used. Given the variety of possible user identification methods, consideration should be given to technical interoperability and standardization issues (e.g. of sender authentication).

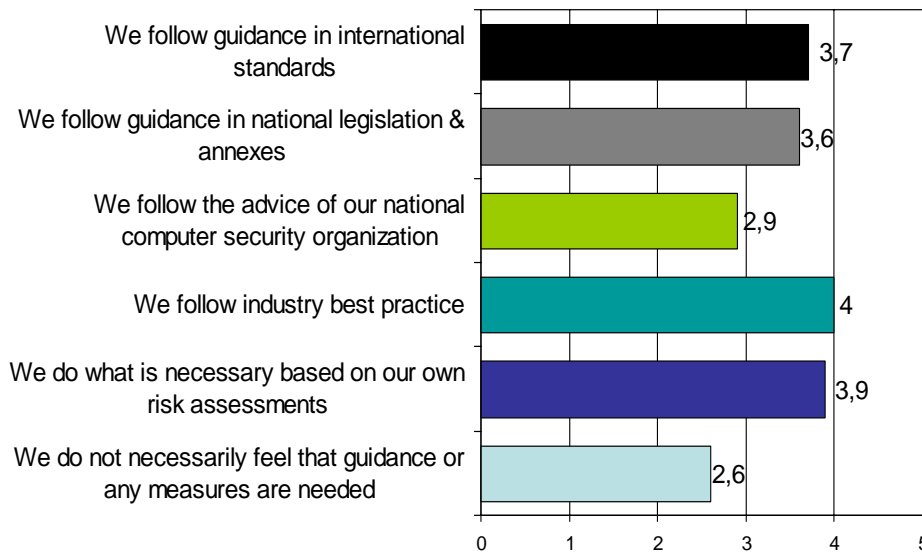
Conclusion: Given the variety of possible user identification methods, consideration should be given to technical interoperability and standardization (e.g. of sender authentication).

### 3.4 Appropriateness of measures taken by providers

The Directive 2002/58/EC requires that security measures are appropriate to the risk presented, having regard to the state of the art and the cost of their implementation. Especially the “state of the art” is difficult to articulate, and it is certainly not defined by a single entity. Consequently, the questionnaire tried to avoid a black/white approach, and asked *how* providers take state of the art (and cost) into account.



How do you take into account state of the art and cost of the implementation to ensure an appropriate level of security? (Importance)



Note: The questionnaire asked for “priority”, this chart displays “importance”. “Importance” = 6 minus “Priority”, e.g. “priority = 2” is “importance = 4”. Empty answers (priority = 0) are not taken into account. The way the question was asked makes extreme values (e.g. 1 or 5) unlikely, because for each answer there is in most cases someone else who has a quite different opinion. Typically, this balances the average answer somewhere in the middle (e.g. 2-4).

- Providers indicated that following industry best practice and using their own risk assessments is most important for them to balance state of the art and cost of security measures.
- Guidance in international standards and guidance in national legislation and annexes follows suit, while the advice of national computer security organizations is deemed less important.
- The lower end of the scale is the option “do not need guidance”.

Obviously, even though providers certainly do not ask for more regulation, they do appreciate guidance in particular with regard to the question which measures are considered appropriate. This would enable them to keep costs down while at the same time they would comply with legal requirements.

It is interesting to compare this answer of the providers with the answer that the NRAs gave. While providers obviously need and appreciate some sort of guidance, NRAs assume that providers work on their own.

Conclusion: Article 4 of Directive 2002/58/EC refers to state of the art and cost of security implementations. Additional guidance is welcome, in particular around industry best practices, and should be supported at EU level.

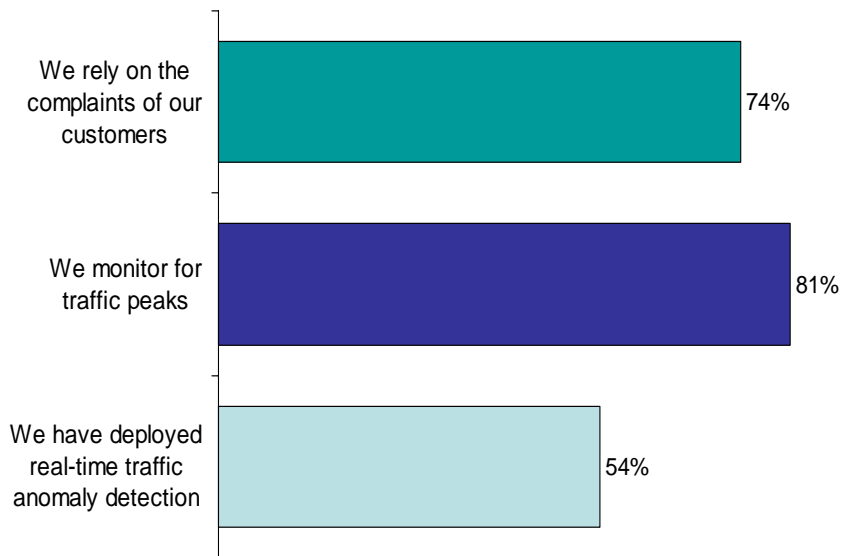
## **3.5 Security breaches and anti-spam violations**

### **3.5.1 Discovering problems**

Article 4 of Directive 2002/58/EC requires providers to inform subscribers of particular risks of a breach of the security of the network. In order to do so, a provider has to become aware of such a risk.



### How do you become aware of security or spam problems?



- 81% of the providers monitor for traffic peaks. Use of real-time traffic anomaly detection can be considered a subset of this and is in place at 54% of the providers.
- The remaining almost 20% of providers do not have any proactive mechanism in place to become aware of security or spam problems, and merely rely on complaints of their customers.
- Reliance on customer complaints is relevant for 74% of the providers.

The picture is not consistent here. Relying on customer complaints is certainly not sufficient. On the other hand, most providers do monitor for traffic peaks and at least half of them use real-time traffic anomaly detection. Overall, it seems that proactive behavior of providers prevails, but it can certainly be improved.

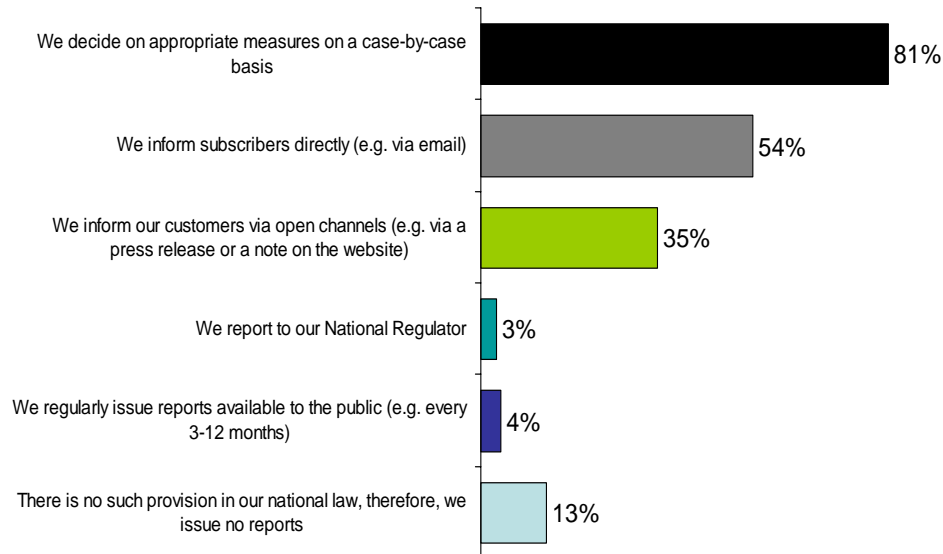
Conclusion: All providers should be proactive and monitor their networks for risks of security breaches. Providers could also be asked to report which networks they monitor.

### 3.5.2 Reacting to problems

After a provider has become aware of a particular risk of a security breach, the more important question is how the provider reacts.



### If you become aware of a particular risk of a breach of the security of your network, what do you do?



- Most providers (81%) act on a case-by-case basis.
- Many providers (54%) inform subscribers directly, fewer (35%) prefer open channels. The total number of providers who use either direct or indirect channels to inform users is about 58%.
- Very few issue reports to the public or report to the national regulator.
- More than a tenth of the providers even assume that there are no legal duties, and hence do not issue any reports.

It is discouraging, that most providers act on a case-by-case basis, i.e. obviously not in a structured way following documented procedures. The number of providers that actually report on the risk of security breaches is almost negligible. Regarding the obligatory information to subscribers, it is obvious that providers prefer direct communication (i.e. in a closed user group). An open audience (e.g. via a press release to the public) is less desirable for them, since this has a higher chance of negative publicity.

It should be noted that “risk of a security breach” and “security breach” is not the same. It can be expected that providers would be even more reluctant to report security breaches which actually happen than to report those situations where there is merely a risk of a breach. Mechanisms for reporting that support confidentiality of the information (e.g. via the CERT community) could alleviate the situation for providers.

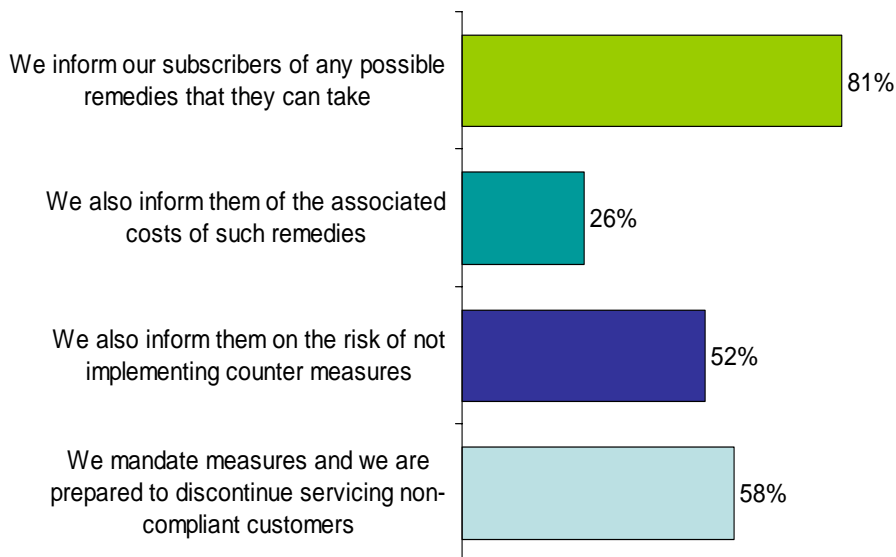


The Directive 2002/58/EC already requires providers to inform subscribers of a particular risk of a security breach. Since there is otherwise no incentive for providers to report on actual security breaches, it could be necessary to make such reporting also mandatory.

Conclusion: Having providers report on the risk of security breaches is very important in order to get an overview of the risk that can be expected from a particular problem. This assumes that information on such risk of breaches has been communicated properly. Reporting of actual security breaches, publicly or anonymously, would help even further. Additional research is necessary.



If the risk lies outside the scope of the measures that you as a provider can take, what do you do?



- If the risk lies outside the scope of the measures for which the provider is responsible then more providers are willing to inform their subscribers and suggest possible remedies.
- A fourth of the providers also informs of the associated costs of such remedies.
- More than half of the providers mandate measures and are prepared to discontinue servicing non-compliant customers and hence protect the rest of their customers from such risks.

It is not surprising that providers are more willing to inform subscribers if the risk lies outside of their scope since they do not have to bear the consequences. Where they could help, i.e. regarding associated costs and regarding information about the risk of not implementing counter

measures, much less providers are willing (or able) to do so. In any case, the decision to act is left to the subscriber who often does not have the capability and the skills to balance cost and risk.

However, it should be noted positively that more than half of the providers mandate measures and are prepared to shut off non-compliant customers and so at least protect the rest of their customers. Overall, a thorough evaluation of cost and risk is still not in the focus of providers, even though it has been written into the Directive.

Conclusion: A cost versus risk perspective in the reporting on the risk of security breaches could be encouraged. This also requires research in the area of cost and risk measurements.

### 3.5.3 Provider's perception of legislative requirements

The providers were also asked what national legislation they are required to comply with in the context of information security and spam. The answers were expected in an open format and the full list of responses is listed in the appendix.

- The answers vary widely, ranging from “EU legislation” and “national legislation” to specific quotations of relevant articles.
- Within a country, answers are sometimes contradictory, e.g. some list the laws whereas others say there is “no legislation”. One provider replied “no idea”.
- Laws mentioned cover electronic communications, telecommunications, electronic signatures, information society, competition, consumer protection, criminal law, privacy and data protection.
- In addition to laws, NRAs, ministries and other national bodies are mentioned as issuers of requirements.

The legislative requirements with regard to information security and spam are not clear for all providers. Moreover, it is not always obvious who the relevant requirement-setting entities are. In addition to legislation itself, communication of the legislation can also be improved.

## 3.6 *The Role of NRAs*

### 3.6.1 Security and spam countermeasures

A questionnaire was also sent to the National Regulatory Authorities for electronic communication services. The role of the NRA varies from country to country. Some of them have specific requirements for providers in their country. Others do not have the competency to mandate specific measures, and some of them commented this in the questionnaire. Overall, the sample of answers for several questions was too weak to draw any conclusions. The following is a summary of the findings of these questions.

- Finland, Lithuania, Norway and Turkey offered some ideas of technical and organizational countermeasures that they require from or recommend to their providers: ingress and egress filtering, quarantining an infected PC, blackholing, free or subsidized software and regular information to users.
- With regard to counter measures against incoming and outgoing spam, NRAs replied almost unanimously that there are no requirements or recommendations.
- Regarding the appropriateness of security measures about half of the NRAs indicated that providers should take care of a risk assessment and the other half said that there are no specific requirements. The consequence is the same, providers are on their own.
- NRAs said almost unanimously that there are no recommendations with regard to the state of the art and the cost of security measures.
- Almost all NRAs said that their country allows unsolicited communications for the purpose of direct marketing only with the consent of the recipient. Most NRAs also said that their country does not allow such communication with the possibility of opt-out.

As stated above, the sample of answers of most questions was too weak to draw any specific conclusion. However, a few remarks should be allowed. Many NRAs (on electronic communication) explicitly commented that they are not the ones responsible for spam. Only few forwarded the questionnaire to another authority in their country, got feedback and incorporated it in the final answer. From a technical perspective, such a separation of authority is not necessarily helpful. More and more often, spam carries also a number of security threats and requires exactly the same countermeasures as normal email traffic.

Conclusion: The relationship between those national entities who control electronic communications and those who control transmission of unsolicited emails should be clarified and simplified. Coordination is desirable at Member State or EU level.

The Directive 2002/58/EC requires an appropriate level of security, but there seems to be not enough help as to what “appropriate” means. The same problem applies to the requirements regarding the state of the art and the cost of implementations.

Conclusion: To enhance the effectiveness of the Directive regarding *appropriate security, cost effectiveness* and *state of the art of information security*, then much more detailed guidance is needed.

Note: The NRAs did have a clearer opinion than the providers regarding the opt-in / opt-out question. Most said that their country requires an opt-in approach, only Turkey said that an opt-out approach is allowed. Overall, NRAs showed a better understanding than providers where in some countries (e.g. Spain, Lithuania, and Norway) about half said opt-in and half said opt-out.

### 3.6.2 Nature of requirements



How has your country legislated, specified or communicated these requirements to the providers?

	CS	DE	DK	EE	ES	FI	HU	LT	MT	NL	NO	SE	SK	TK	UK	
National legislation and annexes require providers to implement safeguards						X	X	X	X					X	X	X
Regulators issue recommendations or advice which describe technical safeguards in detail						X										
Legislation and/or annexes refer to (inter)national standards, so these standards are strongly recommended or binding							X									
Industry associations define specific requirements for their constituency (self-regulation)			X													
No specific measures taken	X	X		X	X					X	X	X				

Number of responses: 15

- Only the Finnish NRA indicated that they issue recommendations or advice which describes technical safeguards in detail.
- Almost half of the responding NRAs refer to national legislation and annexes.
- The other half says that the country has not taken any specific measures to legislate, specify or communicate requirements on information security.

Based on the data from this survey, a lack of coordination of guidance and enforcement becomes apparent. While providers seek advice from a variety of sources, most NRAs do not see themselves in a position to help with guidance, because they do not have the mandate to do so.

Requirements are sometimes set by national legislation and annexes. It requires additional research to clarify how precise such legislative guidance can be and which body in the countries – if there is any - oversees the implementation.

Conclusion: Europe needs better guidance regarding technical and organizational measures to improve security of electronic communication networks. NRAs could be more actively involved in providing guidance for providers on technical and organizational measures on security and spam. Better guidance does not necessarily require stricter regulation, but more details, better definitions and international coordination would certainly be helpful.

### 3.6.3 Security breaches



Regarding a particular risk of a breach of security in the network of the provider, what is the provider required to do?

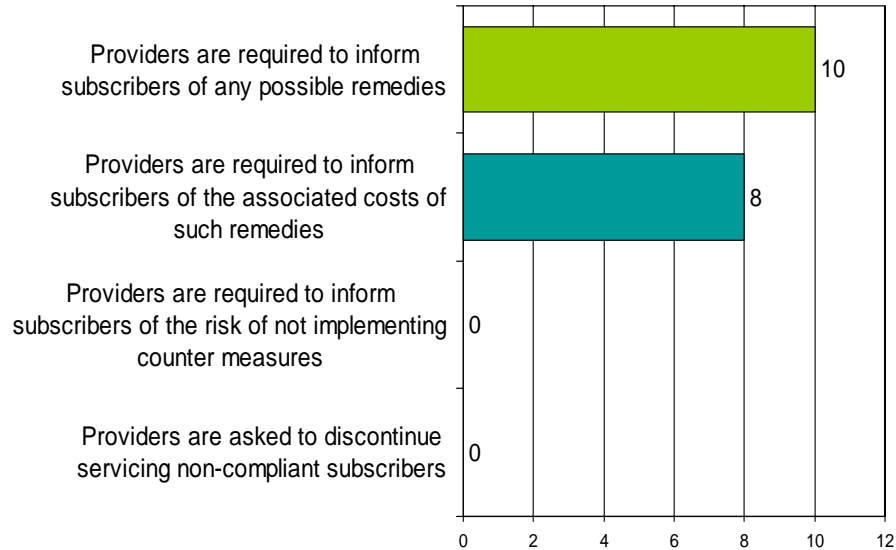
	CS	DE	DK	EE	ES	FI	HU	LT	MT	NL	NO	SE	SK	TK	UK
<b>It is required to inform subscribers directly (i.e. individually)</b>	X					X	X					X	X	X	
<b>It is required to inform subscribers via open channels (e.g. via press release)</b>						X	X					X			
<b>The provider has a duty to report to the NRA</b>						X								X	
<b>It is up to the provider to decide whether and how subscribers should be informed</b>		X		X	X			X		X	X	X			X

Number of responses: 15

There is more variety in the answers on how providers should act in case of a particular risk of a breach of security. The picture that the answers from the NRAs give is very similar to the answers from the providers. The preferred option is to leave providers the freedom to decide what measures they take. Informing subscribers directly ranks also higher than informing the public in general and the role that NRAs see for themselves is minor, with only Finland and Turkey reporting that they expect the provider to inform them. There is no clear pattern with regard to new EU / EU 15/non EU countries.



If the risk lies outside the scope of the measures a provider can take, then are there any further requirements for the provider?



Most of the NRAs answered that providers are required to inform subscribers of any possible remedies and that they also have to inform subscribers of the associated costs. These two requirements are stated in Article 4 of the Directive 2002/58/EC.

It should be noted that providers themselves have a more balanced approach, engaging in all four options, even though two of that are not required by law. So far the Directive 2002/58/EC, Article 4 does not require providers to inform subscribers of the risk of not implementing counter measures nor does it ask for discontinuity of the service for non-compliant subscribers. These two options could also be made mandatory by legislation.

Conclusion: NRAs already oversee electronic communication services in the Member States. The European Commission could find a way to involve NRAs more actively in information security matters, for example as recipients of reports on the risk of security breaches.

## 4 Appendix

### 4.1 Request from the European Commission



EUROPEAN COMMISSION  
Information Society and Media Directorate-General

The Director-General

Brussels, - 3 XI 2005  
INFSO B3/FC/ZG/sl D (2005) 6463 18

NOTE FOR THE ATTENTION OF MR ANDREA PIROTTI  
EXECUTIVE DIRECTOR OF THE EUROPEAN NETWORK AND INFORMATION SECURITY  
AGENCY

**Subject: Industry measures taken to comply with national measures implementing provisions of the regulatory framework for electronic communications relating to the security of services**

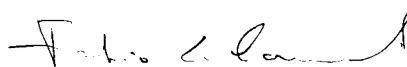
Under the regulatory framework for electronic communications, service providers have to take technical and organisational measures to safeguard the security of their services. Questions on the implementation of such security requirements are gaining in importance as several threats to such security have developed in recent years resulting in e.g. spam, viruses, spyware and other forms of malware.

While the 2006 work programme of ENISA is effectively expected to cover the measures taken by providers of electronic communications services to comply with these security requirements, the review of the provisions of the regulatory framework is already about to start (call for input in December 2005, first Communication expected in June 2006).

To maximise the value of ENISA's contribution, I would like to ask if the Agency could start working on this subject as early as possible, so that deliverables could be provided in January or February 2006. This would allow them to be used in the context of the Review.

You will find attached a more detailed description of the work to be undertaken. If you have any questions on this dossier, please contact Philippe Gérard (DG INFSO B1, tel: +32.2.296.86.44; email: [philippe.gerard@cec.eu.int](mailto:philippe.gerard@cec.eu.int)).

Please let me know if this is agreeable to you.



Fabio Colasanti

Cc: P. Zangl, Directors INFSO; P. Scott, M. Niebel, Ph. Gérard, Assistants

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.  
Office: BU 24 03/43. Telephone: direct line (32-2) 296.86.44.

E-mail: [philippe.gerard@cec.eu.int](mailto:philippe.gerard@cec.eu.int)

## **Annex – Work on industry measures taken to comply with national measures implementing provisions of the regulatory framework for electronic communications relating to the security of services – Technical description (21 October 2005)**

### **Background**

Under the regulatory framework for electronic communications, service providers have to take technical and organisational measures to safeguard the security of their services. Several threats to such security have developed in recent years – and continue to develop - resulting in e.g. spam, viruses, spyware and other forms of malware.

### **Objective and scope**

The work consist of the collection and analysis of information (including national legislation and self-regulatory measures) from Member States on measures taken by providers of publicly available electronic communications services to comply with the legal requirement in Article 4 of Directive 2002/58/EC on Privacy and Electronic Communications to take technical and organisational measures to safeguard the security of their services, if necessary in conjunction with the provider of the public communications network with respect to network security.

This extends to measures to fight against unsolicited electronic mail (spam), “spyware” and other forms of “malware” that affect the provision of electronic communications services and networks (according to the Directive 2002/58/EC on Privacy and Electronic Communications).

### **Results and format**

The results of this survey will differentiate between technical and organisation measures taken.

The survey and the actual information will be made available in the form of a collection of legislation and self-regulation, and of a comparative analysis of measures taken by measures taken/industry sector/size of the company/Member States concerned.

### **Deadline**

The results should be handed over to the Commission in January or February 2006.



## 4.2 List of Conclusions

- Conclusion: The technical measures that providers implement vary widely. They depend on the type of threat against which each provider focuses its defense and the specific nature of the business the provider is in. However, technical measures can be improved.
- 1) To increase transparency and introduce comparability, providers could be required to report on the technical measures which they implement to secure their services.
  - 2) There should be an incentive for providers to contribute to the overall security of interconnected networks rather than protecting merely their own resources. Egress filtering could be encouraged. .... 10
- Conclusion: With regard to organizational measures overall guidance could be improved.
- 1) The importance of clear documentation and regular communications on information security as well as collection and dissemination of best practices (e.g. by ENISA) should be emphasized.
  - 2) This includes guidance to consumers as well as guidance to working staff, in particular with regard to incident response and emergency planning.
  - 3) The need for contact details for email abuse and security violations should be stressed. .... 12
- Conclusion: Providers in Europe are less concerned about outgoing emails, i.e. they are less concerned about their customers sending spam. They rely on legal instruments such as Terms and Conditions. In addition to better information about legal consequences, enforcement could be further improved to prevent spam originating from Europe..... 15
- Conclusion: From a technical perspective, there is no 100% protection against spam. Technical protection against incoming spam can be improved, but only marginally. Unless economic models for spam change dramatically, there is probably not much more that providers can do next to applying the variety of countermeasures to the largest extend possible. .... 17
- Conclusion: Reporting large scale email abuse to competent NRAs should be encouraged. Building on that, NRAs could take a more active role. ENISA could help raise awareness in this regard..... 18
- Conclusion: With regard to the different choices of opt-in versus opt-out, the terms of the Directive 2002/58/EC could be further clarified. .... 20
- Conclusion: Given the variety of possible user identification methods, consideration should be given to technical interoperability and standardization (e.g. of sender authentication). .... 21
- Conclusion: Article 4 of Directive 2002/58/EC refers to state of the art and cost of security implementations. Additional guidance is welcome, in particular around industry best practices, and should be supported at EU level. .... 22
- Conclusion: All providers should be proactive and monitor their networks for risks of security breaches. Providers could also be asked to report which networks they monitor. ... 23
- Conclusion: Having providers report on the risk of security breaches is very important in order to get an overview of the risk that can be expected from a particular problem. This assumes that information on such risk of breaches has been communicated properly.

Reporting of actual security breaches, publicly or anonymously, would help even further. Additional research is necessary..... 25

Conclusion: A cost versus risk perspective in the reporting on the risk of security breaches could be encouraged. This also requires research in the area of cost and risk measurements. .... 26

Conclusion: The relationship between those national entities who control electronic communications and those who control transmission of unsolicited emails should be clarified and simplified. Coordination is desirable at Member State or EU level.... 27

Conclusion: To enhance the effectiveness of the Directive regarding *appropriate security, cost effectiveness* and *state of the art of information security*, then much more detailed guidance is needed..... 28

Conclusion: Europe needs better guidance regarding technical and organizational measures to improve security of electronic communication networks. NRAs could be more actively involved in providing guidance for providers on technical and organizational measures on security and spam. Better guidance does not necessarily require stricter regulation, but more details, better definitions and international coordination would certainly be helpful..... 29

Conclusion: NRAs already oversee electronic communication services in the Member States. The European Commission could find a way to involve NRAs more actively in information security matters, for example as recipients of reports on the risk of security breaches. .... 30

### 4.3 Legislative Requirements

#### 4.3.1 Perception of respondents (providers)

Question: In the context of information security and spam, what national legislation are you required to comply with?

Legislation	No country	As an international network service provider we have to comply with the legislation of the various countries we operate in
Legislation	No country	Legislation within all countries (EU and elsewhere) where we operate a network
Legislation	Belgium	Belgian law ; * Wet van 11 maart 2003 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij ; * Wet van 13 juni 2005 betreffende de elektronische communicatie
Legislation	Belgium	Requirement to provide a protection against unwanted e-mails (spam)
Legislation	Bulgaria	Bulgarian law
Legislation	Bulgaria	According to Bulgarian legislation, which is very incomplete at the moment.
Legislation	Bulgaria	Law Of The Telecommunications
Legislation	Bulgaria	Law for the protection of personal data Law for the electronic document and electronic signature Law for the money transfers, electronic payment instruments and payment systems There is also an on-going Bulgarian project for "Law for the electronic com"
Legislation	Cyprus	Both (spam and security breaches) are illegal by law.
Legislation	Czech Republic	Act No. 480/2004 Coll., Act. No 127/2005 Coll.
Legislation	Estonia	"Information Society Services Act"
Legislation	Germany	German and European law. In particular we are required to comply with: - Bundesdatenschutzgesetz - Teledienstedatenschutzgesetz - Telekommunikationsgesetz - Gesetz gegen den unlauteren Wettbewerb

Legislation	Germany	UWG, others
Legislation	Greece	Greek Law 2251/1994 "Consumer Protection", Greek Law 2774/1999 "concerning the processing of personal data and the protection of privacy in the telecommunications sector".
Legislation	Greece	Rules 630a & 631a /2005 of Hellenic Authority for the Information and Communication Security and Privacy (ADAE)
Legislation	Greece	article 9 of Law 2774/1999 (articles 9,10,12,13), article 13 Directive 2002/58/EC-Draft Bill, article 6 Presidential Decree 131/2003 (on e-commerce- commercial communication), article 4 par.6, article 4a, article 9 par. 10,11,12 and article 10 of Law 2251
Legislation	Greece	We are in compliance with the laws and regulations enforced by the National Regulatory Authority.
Legislation	Greece	Law 2472/1997 - Protection of the person during the processing of personal data Law 2774/1999 - Protection of the personal data in the telecommunications sector Law 2251/1994 - Consumer's protection Presidential decree 131/2003 for electronic commerce
Legislation	Lithuania	Lithuanian law
Legislation	Lithuania	- Law on Electronic Communications [EN]; - the Orders of Minister of Economy of the Republic of Lithuania about Physical security [LT] and about Information security [LT];
Legislation	Lithuania	None
Legislation	Malta	Article 4
Legislation	Malta	Data Protection Act ; Criminal Code
Legislation	Malta	Telecommunications (Personal Data and Protection of Privacy) Regulations (Legal Notice 19 of 2003 as amended by Legal Notice 523 of 2004) and the Telecommunications (Personal Data and Protection of Privacy) Regulations of 2003 (Legal Notice 16 of 2003 as
Legislation	Norway	Norwegian Law
Legislation	Norway	Norwegian Post and Telecommunications Authority.
Legislation	Norway	EU legislation
Legislation	Norway	What ever legislations that are active in Norway
Legislation	Poland	Criminal Law Act on electronically provided services Act on Personal Data Protection; more <a href="http://www.csirt-handbook.org.uk/app/index.php?table_name=app_record&amp;page=0&amp;function=search&amp;execute_search=1">http://www.csirt-handbook.org.uk/app/index.php?table_name=app_record&amp;page=0&amp;function=search&amp;execute_search=1</a>
Legislation	Poland	"Personal Data Protection Law", "Telecommunication Law", "Electronic Services Act", "Database protection act", parts of Criminal Law, some other minor ones
Legislation	Poland	Nothing. We have good legislation but bad practices
Legislation	Poland	None.
Legislation	Spain	Personal data protection
Legislation	Spain	LOPD and LSSI
Legislation	Spain	Here in Spain we are required to comply both with LOPD law (Personal Data Protection Law) and LSSI (Regarding Information Society Services)
Legislation	Spain	LOPD ( <a href="http://www.agpd.es">http://www.agpd.es</a> ), LSSI ( <a href="http://www.lssi.es">http://www.lssi.es</a> )
Legislation	Spain	Law 34/2002 for Information Society Services and Electronic Commerce (July 11th., 2002) and RD 424/2005 for Universal Service Regulations (April 15 th, 2005).
Legislation	Spain	Spanish
Legislation	Spain	At least UK, Spain and European Directives. Spanish relevant legislation is: Organic Law 15/99 of December 13th (Data Protection Act Spain), Royal Decree 994/1999 of June 11th, Law 34/2002 of July 11th on the Information Society and Electronic Commerce a
Legislation	Turkey	No idea
Legislation	United Kingdom	UK Law

### 4.3.2 Transposition Status of Directive 2002/58/EC

As regards transposition generally, all member states have notified measures implementing 2002/58/EC except Greece. In terms of implementation issues, there are ongoing infringement cases regarding the failure to implement spam opt-in/opt-out systems against Latvia, Austria and Slovakia. There is also a case against Germany for various shortcomings with the implementation of the Directive (spam not included). (Source: DG MARKT, November 2005)

In addition, the Bulgarian NRA CRC reported that the Directive 2002/58/EC is transposed in the draft Electronic Communications Act, but that this has neither been adopted by the National Assembly nor promulgated as per the adequate order.

Moreover, the Swiss NRA reported the following: "In general, thanks to our central position on the sidelines we can take a flexible approach to the provisions of 2002/58/EC. We do have some specific anti-spam measures in the pipeline. These are based on a revision of the Telecom Law which is at present making its way through parliament. The proposed spam measures are given more detail in a draft new Decree on Telecom Services which is based on the revised law. If and when the revised law is passed, the revised decree will go through a public consultation and the present proposals could very well be dropped, modified, replaced, added to etc. before we arrive at a final result. There is no firm date for the entry into force of the new legislation. If anti-spam measures make it through to entry into force then we will deal with the technical solutions in more detail in suitable Technical and Administrative Regulations."

## 4.4 Questionnaires

### 4.4.1 Questionnaire for Providers

Provider name                                      Telco                       ISP                       Content Provider   
Contact name                                      Phone                      Email                      Remain anonymous

#	Question	Legal Reference
1.	In the context of information security and spam, what national legislation are you required to comply with?	
2.	Which of the following measures do you take in order to improve security of your services?  Technical measures <input type="checkbox"/> Ingress filtering <input type="checkbox"/> Egress filtering <input type="checkbox"/> Content filtering <input type="checkbox"/> Quarantining an infected / malicious PC <input type="checkbox"/> Blackholing/Sinkholing <input type="checkbox"/> Secure Domain Name Service <input type="checkbox"/> Traffic Shaping / Throttling  Organizational matters <input type="checkbox"/> Detailed written guidance for staff, partners and customers <input type="checkbox"/> Free or subsidized security software for users <input type="checkbox"/> Hotline/Helpdesk <input type="checkbox"/> Clear contact details for email abuse and security violations <input type="checkbox"/> Remote technical assistance (i.e. with access to the device) <input type="checkbox"/> Regularly information to users (web, mail, email)	Article 4 (Security), §1 The provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, ...

	<input type="checkbox"/> Other (pls. specify):	
3.	<p>Regarding these measures, do you work in conjunction with a public communications network provider?</p> <input type="checkbox"/> yes, we do <input type="checkbox"/> no, we do not <input type="checkbox"/> we are also a public communication network provider ourselves	(cont.) ... if necessary in conjunction with the provider of the public communications network with respect to network security.
4.	<p>How do you take into account state of the art and cost of the implementation to ensure an appropriate level of security? Please prioritize the following options (1,2,3):</p> <p>We follow guidance in international standards</p> <p>We follow guidance in national legislation &amp; annexes</p> <p>We follow the advice of our national computer security organization</p> <p>We follow industry best practice</p> <p>We do what is necessary based on our own risk assessments</p> <p>We do not necessarily feel that guidance or any measures are needed</p>	(cont.) Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.
5.	<p>How do you become aware of security or spam problems?</p> <input type="checkbox"/> We rely on the complaints of our customers <input type="checkbox"/> We monitor for traffic peaks <input type="checkbox"/> We have deployed real-time traffic anomaly detection Others (pls. specify)	(cont.)
6.	<p>If you become aware of a particular risk of a breach of the security of your network, what do you do?</p> <input type="checkbox"/> We inform subscribers directly (e.g. via email) <input type="checkbox"/> We inform our customers via open channels (e.g. via a press release or a note on the website) <input type="checkbox"/> We report to our National Regulator <input type="checkbox"/> We regularly issue reports available to the public (e.g. every 3-12 months) <input type="checkbox"/> We decide on appropriate measures on a case-by-case basis <input type="checkbox"/> There is no such provision in our national law, therefore, we issue no reports	Article 4 (Security), §2 In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk ...
7.	<p>If the risk lies outside the scope of the measures that you as a provider can take, what do you do?</p> <input type="checkbox"/> We inform our subscribers of any possible remedies that they can take <input type="checkbox"/> We also inform them of the associated costs of such remedies <input type="checkbox"/> We also inform them on the risk of not implementing counter measures <input type="checkbox"/> We mandate measures and we are prepared to discontinue servicing non-compliant customers	(cont.) and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

<p>8.</p>	<p>What measures did you put in place to prevent your customers from <b>sending</b> unsolicited communications (spam)?</p> <p><input type="checkbox"/> We inform them about the legal consequences</p> <p><input type="checkbox"/> We forbid it in our Terms &amp; Conditions</p> <p><input type="checkbox"/> We blacklist (MAPS, Spamhouse, NJABL) them if they repeatedly send spam</p> <p><input type="checkbox"/> We greylist them if they send spam until they stop it</p> <p><input type="checkbox"/> We whitelist all our customers who do not send spam</p> <p><input type="checkbox"/> We reject all straight SMTP traffic from consumer connections</p> <p><input type="checkbox"/> We do not interfere in the content of our customers communications</p> <p><input type="checkbox"/> We do nothing but we wish we could do more</p> <p><input type="checkbox"/> We admit that some of our customers are spammers</p> <p>What measures did you put in place to protect your customers from <b>receiving</b> unsolicited communications (spam)?</p> <p><input type="checkbox"/> We offer spam-filtering on our network free-of-charge</p> <p><input type="checkbox"/> We offer spam-filtering on our network for an additional fee</p> <p><input type="checkbox"/> We offer software free-of-charge that customers can install on their computers</p> <p><input type="checkbox"/> We offer commercial software that customers can install on their computers</p> <p><input type="checkbox"/> We do not interfere in the content of our customers communications</p> <p><input type="checkbox"/> We do nothing but we wish we could do more</p>	<p>Article 13 <b>Unsolicited communications</b></p> <p>1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.</p>
<p>9.</p>	<p>Does legislation in your country allow unsolicited communications for purposes of direct marketing only with the consent of the subscriber (opt-in)?</p> <p><input type="checkbox"/> yes <input type="checkbox"/> no</p> <p>Does legislation in your country allow unsolicited communications for purposes of direct marketing unless the subscriber expressed the wish to no receive these communications (opt-out)?</p> <p><input type="checkbox"/> yes <input type="checkbox"/> no</p>	<p>3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.</p>
<p>10.</p>	<p>How do you prevent senders of electronic mail from disguising or concealing their identity?</p> <p>We implement the following sender authentication mechanisms</p> <p><input type="checkbox"/> SMTP Authentication</p> <p><input type="checkbox"/> Sender ID Framework (SIDF)</p> <p><input type="checkbox"/> Yahoo's Domain Keys (DKIM)</p> <p><input type="checkbox"/> Cisco's Identified Internet Mail</p> <p>Other (pls. specify)</p>	<p>4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.</p>
<p>11.</p>	<p>What sort of measures do you take if you detect spam coming from an ISP based in a non-EU country</p> <p><input type="checkbox"/> We contact that ISP to discuss countermeasures</p> <p><input type="checkbox"/> We address the problem of spam in inter-connection agreements</p> <p><input type="checkbox"/> We filter or block SMTP traffic from that ISP if the ISP itself does not take measures against spam</p> <p><input type="checkbox"/> We inform our National Regulatory Authority</p> <p><input type="checkbox"/> We pursue legal actions</p> <p><input type="checkbox"/> We do nothing but we wish we could do more</p> <p>Other (pls. specify)</p>	<p>(cont.)</p>
<p>12.</p>	<p>If one or several questions above did not offer appropriate answer options, please use</p>	

this space to explain. Please also indicate the number of the question.	
---	--

#### 4.4.2 Questionnaire for NRAs

Country \_\_\_\_\_ Name of the regulatory authority \_\_\_\_\_  
 Contact name \_\_\_\_\_ Phone \_\_\_\_\_ Email \_\_\_\_\_

The EU Directive 2002/58/EC requires EU Member States to have provisions in place to increase information security of their communication networks and in particular to fight spam. National Regulatory Authorities oversee the work of electronic communication providers. ENISA would like to understand how EU legislation is transposed into national laws and regulations and what exactly you as an NRA are expecting providers in your country to do.

#	Question	Legal Reference
1.	<p>Which of the following <b>measures</b> do you require or recommend providers in your country to take in order to secure their services?</p> <p>Technical measures</p> <p><input type="checkbox"/> Ingress filtering      <input type="checkbox"/> Egress filtering      <input type="checkbox"/> Content filtering</p> <p><input type="checkbox"/> Quarantining an infected / malicious PC      <input type="checkbox"/></p> <p>Blackholing/Sinkholing</p> <p><input type="checkbox"/> Traffic Shaping / Throttling</p> <p><input type="checkbox"/> Secure Domain Name Service</p> <p>Organizational matters</p> <p><input type="checkbox"/> Free or subsidized security software for users      <input type="checkbox"/> Hotline/Helpdesk</p> <p><input type="checkbox"/> Remote technical assistance (i.e. with access to the device)</p> <p><input type="checkbox"/> Regularly information to users (web, mail, email)</p> <p><input type="checkbox"/> Other (pls. specify):</p>	<p><i>Article 4 (Security), §1</i>          The provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security.</p>
2.	<p>How has your country legislated, specified or communicated these <b>requirements</b> to the providers?</p> <p><input type="checkbox"/> National legislation and annexes require providers to implement safeguards</p> <p><input type="checkbox"/> Regulators issue recommendations or advice which describe technical safeguards in detail</p> <p><input type="checkbox"/> Legislation and/or annexes refer to (inter)national standards, so these standards are strongly recommended or binding</p> <p><input type="checkbox"/> Industry associations define specific requirements for their constituency (self-regulation)</p> <p><input type="checkbox"/> No specific measures taken</p>	<p>(cont.)</p>
3.	<p>How do you take into account the <b>state of art and the cost</b> of implementation?</p> <p><input type="checkbox"/> Technical annexes etc. are revised and updated regularly (e.g. yearly)</p> <p><input type="checkbox"/> There are varying requirements depending on the size of the provider</p> <p><input type="checkbox"/> There are regularly issued industry guidelines</p> <p><input type="checkbox"/> No specific measures taken</p>	<p>(cont.) Having regard to the state of the art and the cost of their implementation ...</p>
4.	<p>How do you define an <b>appropriate level</b> of security?</p> <p><input type="checkbox"/> Adherence to international standards on information security is mandated</p> <p><input type="checkbox"/> A national information security entity provides appropriate guidance</p> <p><input type="checkbox"/> It is up to the provider to carry out a risk assessment and to define the level of security needed</p> <p><input type="checkbox"/> There is a national list of organizations that are considered to be more</p>	<p>(cont.) ... these measures shall ensure a level of security appropriate to the risk presented.</p>

	<p>critical/sensitive; for them higher protection is a priority</p> <p><input type="checkbox"/> The providers must make a risk assessment</p> <p><input type="checkbox"/> No specific guidance is provided</p>	
5.	<p>Regarding a particular <b>risk of a breach</b> of security in the network of the provider, what is the provider required to do?</p> <p><input type="checkbox"/> It is required to inform subscribers directly (i.e. individually)</p> <p><input type="checkbox"/> It is required to inform subscribers via open channels (e.g. via press release)</p> <p><input type="checkbox"/> The provider has a duty to report to the NRA</p> <p><input type="checkbox"/> It is up to the provider to decide whether and how subscribers should be informed</p>	<p><i>Article 4 (Security), §2</i></p> <p>In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk ...</p>
6.	<p>If the risk lies <b>outside the scope</b> of the measures a provider can take, then are there any further requirements for the provider?</p> <p><input type="checkbox"/> Providers are required to inform subscribers of any possible remedies</p> <p><input type="checkbox"/> Providers are required to inform subscribers of the associated costs of such remedies</p> <p><input type="checkbox"/> Providers are required to inform subscribers of the risk of not implementing counter measures</p> <p><input type="checkbox"/> Providers are asked to discontinue servicing non-compliant subscribers</p>	<p><i>(cont.)</i> ... and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.</p>
7.	<p>What measures is a provider to take to become aware of security or spam problems?</p> <p><input type="checkbox"/> It is sufficient if the provider relies on complaints from customers</p> <p><input type="checkbox"/> The provider is required monitor for traffic peaks</p> <p><input type="checkbox"/> The provider is required to deploy real-time traffic anomaly detection</p> <p>Others (pls. specify)</p>	<p><i>(cont.)</i></p>
8.	<p>Which of the following measures do you require providers to take in order to prevent their customers from <b>sending</b> spam?</p> <p><input type="checkbox"/> The provider has to inform customers about the legal consequences</p> <p><input type="checkbox"/> The provider has to clarify this in the Terms &amp; Conditions</p> <p><input type="checkbox"/> The provider should put a customer on a blacklist (MAPS, Spamhouse, NJABL) if the customer repeatedly sends spam</p> <p><input type="checkbox"/> The provider should greylist a customer who sends spam until he/she stops it</p> <p><input type="checkbox"/> The provider should whitelist all customers who do not send spam</p> <p><input type="checkbox"/> The provider should reject all straight SMTP traffic from consumer connections</p> <p><input type="checkbox"/> There are no requirements or recommendations for providers</p> <p>Which of the following measures do you require from providers to protect their customers from <b>receiving</b> unsolicited communications (spam)?</p> <p><input type="checkbox"/> The provider should offer spam-filtering on the network free-of-charge</p> <p><input type="checkbox"/> The provider should offer spam-filtering on the network for an additional fee</p> <p><input type="checkbox"/> The provider should offer software free-of-charge that customers can install on their computers</p> <p><input type="checkbox"/> The provider should offer commercial software that customers can install on their computers</p> <p><input type="checkbox"/> There are no requirements or recommendations for providers</p>	<p><i>Article 13</i></p> <p><b>Unsolicited communications</b></p> <p>1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.</p>
9.	<p>Does legislation in your country allow unsolicited communications for purposes of direct marketing only with the consent of the subscriber (<b>opt-in</b>)?</p> <p><input type="checkbox"/> yes <input type="checkbox"/> no</p>	<p>3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than</p>



	<p>Does legislation in your country allow unsolicited communications for purposes of direct marketing unless the subscriber expressed the wish to no receive these communications (<b>opt-out</b>)?  <input type="checkbox"/> yes <input type="checkbox"/> no</p>	<p>those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.</p>
10.	<p>How do you prevent senders of electronic mail from <b>disguising or concealing</b> its identity?          We implement the following sender authentication mechanisms  <input type="checkbox"/> SMTP Authentication  <input type="checkbox"/> Sender ID Framework (SIDF)  <input type="checkbox"/> Yahoo's Domain Keys (DKIM)  <input type="checkbox"/> Cisco's Identified Internet Mail          Other (pls. specific)</p>	<p>4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.</p>
11.	<p>If one or several questions above did not offer appropriate answer options, please use this space to explain. Please also indicate the number of the question.</p>	

#### 4.5 Explanation of terms

This list illustrates ENISA's understanding of some more specialized terms that have been used in the context of this study. Definitions by external parties (e.g. Wikipedia) have been checked and sometimes adjusted by ENISA.

Blackholing / Sinkholing	<p>Black-holing or sinkholing: This approach blocks all traffic and diverts it to a black hole, where it is discarded. The downside is that all traffic is discarded - both good and bad - and the targeted business is taken off-line. Similarly, packet-filtering and rate-limiting measures simply shut everything down, denying access to legitimate users. – Source: ComputerWorld</p>
Blacklist	<p>A blacklist is an access control mechanism that means, <i>allow everybody, except members of the blacklist</i>. – Source: Wikipedia</p>
Content Filtering	<p>Content filtering is the most commonly used group of methods to filter spam. Content filters act either on the content, the information contained in the mail body, or on the mail headers (like "Subject:") to either classify, accept or reject a mail. – Source: Wikipedia</p>
Domains Keys	<p>DomainKeys is an e-mail authentication system designed by Yahoo! for verifying the DNS domain of an E-mail sender and the message integrity. The DomainKeys specification has adopted aspects of Identified Internet Mail proposed by Cisco to create an enhanced protocol called DomainKeys Identified Mail, or DKIM. This merged specification is the basis for an IETF Working Group which planned to guide the specification towards becoming an IETF standard. – Source: Wikipedia, shortened</p>
Egress Filtering	<p>Egress filtering is the process of filtering packets from going from the inside to the outside in order to block spoofed packets. When a packet leaves the network with a source address not in the inside range of addresses the packet is blocked. – Source: ENISA's own definition</p>

Electronic communication network	Electronic communications network means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. – Source: EU Directive 2002/21/EC
Electronic Communication service	Electronic communications service means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. – Source: EU Directive 2002/21/EC
Greylist	A mail transfer agent which uses greylisting will "temporarily reject" any email from a sender it does not recognize. If the mail is legitimate, the originating server will try again to send it later, at which time the destination will accept it. If the mail originates from a spammer, the spammer will probably not resend it. – Source: Wikipedia, shortened
Ingress Filtering	Ingress filtering is the process of filtering of packets from outside the network with a source address inside the network. This prevents an outside attacker spoofing the address of an internal machine. – Source: Wikipedia
IP Filtering	IP filtering is the process of filtering traffic by IP address or source and destination port. – Source: ENISA’s own definition
Opt-in	Allowing unsolicited communication for purposes of direct marketing only with the consent of the subscriber. – Source: ENISA, as defined in the questionnaire
Opt-out	Allowing unsolicited communication for purposes of direct marketing unless the subscriber expressed the wish to not receive these communications. - Source: ENISA, as defined in the questionnaire.
Public communication network	Public communications network means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services. – EU Directive 2002/21/EC
Quarantining a computer	Quarantining a computer means isolating a computer into a special network until it has reached a certain security level. The computer is offered to install updates for anti-virus signature files or install software patches. – Source: ENISA’s own definition
Real-time anomaly	Anomaly detection tries to discover malicious behavior by comparing current behavior to learned normal models of behavior. An anomaly

<p>detection</p>	<p>detection approach usually consists of two phases: a training phase which defines what is normal and a working phase which compare new data to the learned model. – Source: Long Fei (Purdue University)</p>
<p>Remote technical assistance</p>	<p>Technical assistance done remotely, using a phone line and/or an Internet connection. It gives access to the device in question, enabling remote input and output. The user requests such assistance and gives his consent to remote access prior to any action.</p>
<p>Secure DNS</p>	<p>DNSSEC (short for DNS Security Extensions) adds security to the Domain Name System (DNS) used on Internet Protocol networks. It is a set of extensions to DNS, which provide origin authentication of DNS data, data integrity, and authenticated denial of existence (i.e. authenticated non-existence reply). DNSSEC was designed to protect the Internet from certain attacks such as DNS cache poisoning. All answers in DNSSEC are digitally signed. By checking the signature, a DNS resolver is able to check if the information is identical (correct and complete) to the info on the authoritative DNS server. – Source: Wikipedia, based on RFC 4033-4035</p>
<p>Sender ID</p>	<p>Sender ID was an anti-spam proposal from the MARID IETF working group that joined Sender Policy Framework and Caller ID. – Source: Wikipedia</p>
<p>Sender Policy Framework (SPF)</p>	<p>Sender Policy Framework (SPF) is an extension to Simple Mail Transfer Protocol (SMTP), the standard Internet protocol for transmitting e-mail. SPF makes it easier to counter most forged "From" addresses in e-mail, and thus helps to counter e-mail spam. Formally, SPF is defined in the SPF Classic specification. – Source: Wikipedia</p>
<p>SMTP Authentication</p>	<p>SMTP authentication allows a requested authentication mechanism, which performs an authentication protocol exchange to authenticate and identify the user. The authentication mechanism can be for example ESMTP AUTH LOGIN / PLAIN, TLS, Kerberos, GSSAPI. – Source: RFCs 2554, RFC 2222, ENISA</p>
<p>Traffic Shaping</p>	<p>Traffic shaping is an attempt to control computer network traffic in order to optimize or guarantee performance, latency, and/or bandwidth. Traffic shaping deals with concepts of classification, queue disciplines, enforcing policies, congestion management, quality of service (QoS), and fairness.</p> <p>Traffic shaping provides a mechanism to control the volume of traffic being sent into a network (bandwidth throttling), and the rate at which the traffic is being sent (rate limiting). For this reason, traffic shaping schemes need to be implemented at the network edges to control the traffic entering the network. It also may be necessary to identify traffic flows at the ingress point (the point at which traffic enters the network) with a granularity that allows the traffic-shaping control mechanism to separate traffic into individual flows and shape them differently. – Source: Wikipedia</p>
<p>Whitelist</p>	<p>A whitelist, is an access control mechanism which means, <i>allow nobody, except members of the white list.</i></p>