

## **Communication and Information Technology Commission**

# **ASSESSMENT OF THE STATUS OF SPAM IN THE KINGDOM**



## *Table of Contents*

1. Purpose of this Document.....	3
2. Our Approach .....	4
3. Executive Summary .....	5
4. Identification of Stakeholders .....	7
4.1 SPAM Activity Lifecycle Analysis .....	7
4.2 Obtaining Personal Details .....	7
4.3 Media Stakeholders .....	8
4.4 Mail Host Stakeholders: .....	9
4.5 Reporting Process Stakeholders .....	10
4.6 Enforcement Process Stakeholders.....	12
4.7 Conclusion.....	13
5. Stakeholders Feedback .....	14
5.1 SAMA .....	14
5.2 DSPs .....	14
5.3 MSPs .....	15
5.4 Bulk SMS Licensees.....	15
5.5 Solution Providers .....	16
5.6 ISPs.....	16
5.7 Companies .....	17
5.8 Universities.....	17
5.9 MOI .....	17
5.10 CITC.....	18
5.11 KACST / ISU .....	18
5.12 Stakeholders Major Concerns and Recommendations .....	18
6. Questionnaire-Based Survey Results.....	22
6.1 SPAM Definition.....	22
6.2 Magnitude of the Problem .....	22
6.3 The Manner in Which Stakeholders Currently Address SPAM.....	27



## **1. PURPOSE OF THIS DOCUMENT**

The purpose of this document is to report the findings of the study conducted to ascertain the magnitude of SPAM in Saudi Arabia. The focus of the study was to obtain a good understanding of the issue of SPAM within Saudi Arabia.

The document was compiled using the statistics that were gathered from stakeholders via different means including questionnaires, interviews, and meetings. The document covers email, mobile and fax SPAM. The document also highlights some of the stakeholders' concerns and recommendations regarding SPAM, as well as the measures taken by these stakeholders to control SPAM in their networks.



## 2. OUR APPROACH

We used a three step approach to collecting the required information on the status of SPAM in the Kingdom. These three steps were:

- Agree on an initial definition of SPAM that could be used as the basis for collecting information;
- Identify and agree to the likely sources of SPAM related statistics and the stakeholders who could be of assistance in this regard; and
- Collection of the SPAM statistics from the identified stakeholders.

Each of these steps is described in more detail below:

### Definition of SPAM, and Related SPAM Indicators

SPAM was defined in our research as unsolicited bulk messages and communications containing commercial, abusive or objectionable content and which are sent out in bulk to people or individuals without their consent by email, fax, or instant messages such as SMS. The basic SPAM indicator used was “SPAM rate” which is defined as the percentage of SPAM compared to the total number of received messages.

### Identification of Sources for SPAM Related Statistics

Key sources were identified and considered relevant in the collection and reporting of SPAM in Saudi Arabia. For example, organizations that were able to report on the volume of SPAM mail received or filtered as a percentage of their total emails were considered for email SPAM. ISPs that were using anti-SPAM filtering tools and were able to report on the SPAM mail filtered by the tool as a percentage of total emails were also considered for email SPAM. For SMS SPAM, Mobile Service Providers who own the gateway and/or servers through which SPAM SMS messages are delivered were considered for SMS SPAM.

### Collection of SPAM Statistics

After defining the basic SPAM indices and the potential sources for data related to SPAM, various methods were used for collecting SPAM related data. The method varies with the type of SPAM. For email SPAM, the key method used for collecting the data was questionnaires and interviews targeted at selected organizations and ISPs. Some interviews and discussion were held with third party service providers such as security solution providers in order to obtain the available information on SPAM. For SMS SPAM, the key method used for collection the data was questionnaires and interviews targeted at Bulk SMS and Mobile Service Providers to obtain relevant SMS related information. Some additional statistics were also collected by service providers on their SMS gateways focusing on the number of SMS messages received by mobile phones in Saudi Arabia.



### 3. EXECUTIVE SUMMARY

SPAM represents a major annoyance and threat to ICT applications users and is spreading into all means of communications. As many countries, regional and international organizations, bodies, and working groups have taken steps to deal with the issue of SPAM, Saudi Arabia has taken the initiative to develop an anti-SPAM framework. Towards this end, and besides considering other countries' experiences and international bodies' recommendations, it was necessary to assess the current state of SPAM in the Kingdom.

The purpose of this report is to describe the findings on the magnitude of SPAM in the Kingdom of Saudi Arabia, including its use for Phishing and spreading viruses, awareness of SPAM, the current anti-SPAM measures used, and its impact on the various stakeholders in Saudi Arabia. SPAM measurement is key to evaluate the evolution of SPAM and the effectiveness of the anti-SPAM framework in the Kingdom.

To achieve this purpose, all pertinent stakeholders were identified and a framework for the collection of SPAM-related statistics was developed. This framework covers email, SMS and fax and is focused on three aspects. First, the definition of SPAM and related SPAM indicators where "SPAM rate" is defined as the percentage of SPAM compared to the total number of received messages. Second, the identification of sources for SPAM related statistics where, in addition to interviews, filters and anti-SPAM tools used by organizations and ISPs were the main source for determining email SPAM while gateways and servers owned by Mobile Service Providers were used to calculate SMS SPAM. Third, the collection of SPAM statistics achieved by inspecting published reliable data and by conducting survey, interviews and discussions with relevant personnel including CITC, KACST, MOC, MOI, SAMA<sup>1</sup>, companies, financial services institutions, Internet Service Providers, Data Service Providers, bulk SMS licensees, mobile operators, solution providers and others.

Although the SPAM rate differs depending on where the SPAM is being measured, SPAM appears to be a serious problem in the Kingdom of Saudi Arabia. According to the data gathered by ISPs, the average eMail SPAM rate in the Kingdom was 54%. Other sources such as Anti SPAM Product vendors suggest that the SPAM rate ranges between 40% and 60%. For instance, Symantec reports SPAM rate to be 59% for the year 2006. Message Labs report the SPAM for the year 2006 to be 48% and for the year 2007 (till July) to be 43%. On the other hand, Fax SPAM was not considered to be a major source of SPAM with less than 6% SPAM rate. The Direct Marketing Messages constitute the major type of SPAM received in the Kingdom reflecting the most majority of commercial SPAM in the globe. As for the SMS SPAM, mobile operators reported that the SMS SPAM rate ranges between 1.25 and 1.75%. The main findings are summarized in the table below.

SPAM emails, in addition to being an annoyance to individuals, cause capacity, bandwidth, and staff performance problems. While most of the companies believe that the primary impact of SPAM was on their email server resources, network, and time wasted, ISPs considered that their customers were most affected by SPAM. Bandwidth and productivity were also highly affected.

---

<sup>1</sup> -CITC: Communications and Information Technology Commission

-SAMA: Saudi Arabian Monetary Agency

-KACST: King Abdulaziz City for Science and Technology

-MOC: Ministry of Commerce

-MOI: Ministry of Interior



	Email SPAM Rate	Domain SPAM Type	Fax SPAM Rate	SMS SPAM Rate	Using RBLs	SPAM Tools deployed
<b>Average</b>	54%	Commercial	6%	1.25%-1.75%	17%	83%

Considering the impact of SPAM in the Kingdom, it appeared that most organizations, with the exception of Banks, did not expend much effort in educating their employees and customers on how to deal with SPAM. Most banks conduct awareness programs to their employees and customers.

Noticeably, almost 83% of stakeholders have tools targeted at combating SPAM. However, it is worthwhile noting that ISPs focus on filtering the email traffic hitting the mail servers hosted in the ISP's Data center. They do not filter all traffic (especially outgoing traffic) due to the existing constraints in budgets, resources and the shortage of technically capable staff. Indeed, ISPs employing Real-time Blackhole Lists (RBLs) reported lower SPAM rates.

With the absence of a formal complaints reporting process, it is not surprising that most organizations deal with SPAM internally or even ignore the SPAM complaints. On the other hand, the observation is different in the case of banks where half of them have procedures in place to report phishing complaints to CITC and SAMA.

When it comes to industry, it was obvious that there is no code of conduct for ISPs or e-marketing in Saudi Arabia. Moreover, half of the Service Providers do not have any provisions in their Acceptable Use Policy (AUP) covering SPAM.

As recommended by the well know international bodies, to combat SPAM, different areas shall be addresses, such as legal, enforcement, technical, awareness, industry assistance, etc. According to the majority of stakeholders, the legal side is of most importance to combat SPAM in the kingdom while having a proper code of conduct between service providers would help substantially in preventing SPAM.

As indicated by the study, SPAM constitutes a serious problem as being an annoyance to people, organizations and service providers. As mentioned, there is little awareness of SPAM, no codes of conduct for service providers and eMarketers. Moreover, stipulations provided through licenses granted to ISPs, bulk SMS service providers and Bluetooth providers are not audited or enforced.

This justifies the need to develop an Anti-SPAM framework for the Kingdom of Saudi Arabia. By developing an anti-SPAM framework coupled with robust enforcement, ensuring industry assistance, running awareness programs, implementing technical solutions, ongoing monitoring of SPAM rates, and focusing the control on commercial SPAM we can reduce the amount of SPAM significantly in the Kingdom of Saudi Arabia.



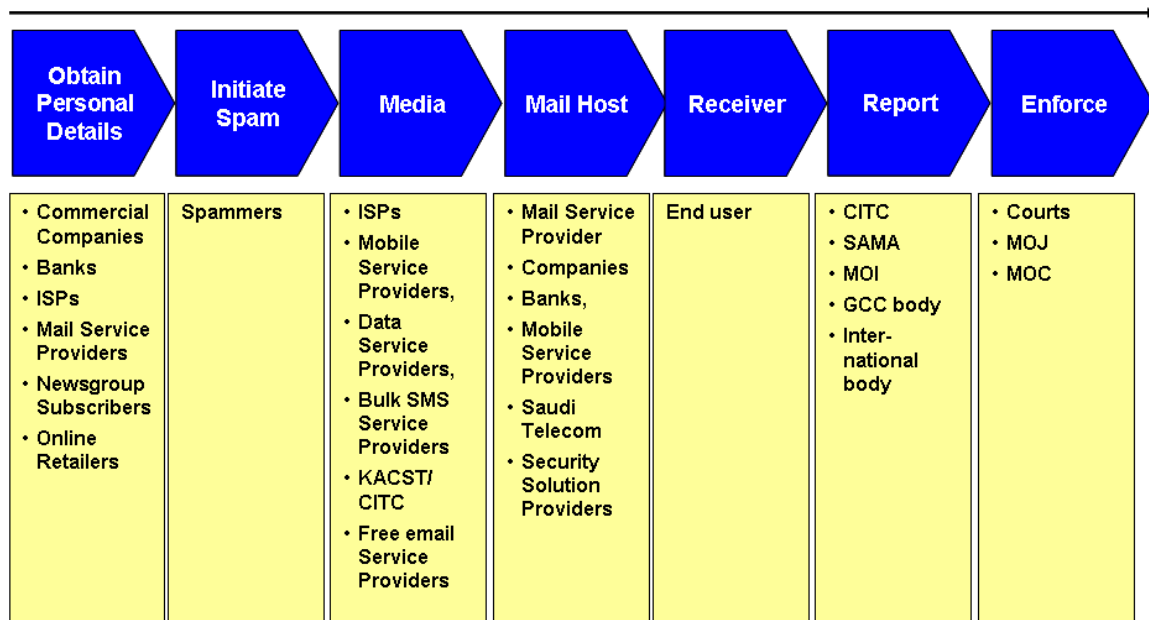
## 4. IDENTIFICATION OF STAKEHOLDERS

### 4.1 SPAM ACTIVITY LIFECYCLE ANALYSIS

This analysis goes through a typical spam activity lifecycle, where:

- 1) The recipient address (email, fax number, mobile number) is captured and stored in a repository for a specific purpose
- 2) The spammer harvests specific address details, which is then used for spamming activities
- 3) The spam message is carried by certain media (ISPs, Mobile service providers etc)
- 4) The message is received by a mail host (mail service provider, banks, etc)
- 5) The end-user (receiver) receives the message
- 6) If required, the receiver reports the SPAM to the appropriate authority
- 7) The designated authority enforces the applicable laws (prosecution and sentencing)

Key stakeholders are involved in each of the SPAM Activity Lifecycle stages. The 7 stages are depicted below:



Profiles and examples of some of the stakeholder groups identified above are presented in the following sections.

### 4.2 OBTAINING PERSONAL DETAILS

A number of organizations, such as Banks, Retailers, ISPs, MSPs, Telcos, Mail Service Providers etc. capture and store details of customers or subscribers. These details are mostly captured for specific purposes, which are typically authorized by the associated person. A number of these organizations are bound by internal Privacy policies, which prevent them from using the information for any purpose other than the purpose for which the information was collected. In some cases, some of these organizations may take the approval of the associated person to use these contact details for the purpose of eMarketing. Some of these organizations may also sell contact details of their subscribers to other bodies, who then use it for SPAMming purposes.

The availability of this store of contact information and personal details is often a key source of contact information for SPAMmers.



### 4.3 MEDIA STAKEHOLDERS

Having collected relevant information, the SPAMmer then sends the spam messages over certain media to the receivers. The media used for this purpose could vary, and could involve media owned by stakeholders such as Internet Service Providers, Mobile Service Providers, Data Service Providers, Bulk SMS service providers etc. These stakeholders are relevant because at times the media owner may knowingly or unknowingly provide the platform for the spammer to carry out his activities.

Stakeholder	Reason	Examples
ISPs	<p>ISPs are the carriers of electronic communications. Mainly emails.</p> <p>ISPs can provide the spammer with the mean to deliver his spam, also, generally they are the first point of contact by receivers, when they started having their mailboxes full of junk</p> <p>ISPs effort is essential in reducing the volumes of junk emails by applying appropriated filtering measures at their email servers.</p>	<ul style="list-style-type: none"> <li>• NESMA National Co. for Advanced Technology Ltd.</li> <li>• MeduNet</li> <li>• Arabian Internet and Communications Services Company (Awalnet)</li> <li>• Saudi Telecom Company (Saudi Net)</li> </ul>
Mobile service providers	SMS can be used as another form of SPAM as shown before in the statistics.	<ul style="list-style-type: none"> <li>• Saudi Telecom Company (STC)</li> <li>• Ithad Itsalat Company (Mobily)</li> </ul>
Data service providers	Any possible controls implemented at the DSPs level can restrict the flow of incoming and outgoing SPAM.	<ul style="list-style-type: none"> <li>• Saudi Telecom Company (STC)</li> <li>• Bayanat Al-Oula for Network Services (Bayanat Consortium)</li> </ul>
Bulk SMS service providers	Bulk SMS is a major form of spam. It is used to promote goods and services, sales, etc.	<ul style="list-style-type: none"> <li>• eCallPlus Company Ltd.</li> <li>• Mediacall Company Ltd</li> </ul>
CITC	<p>CITC manages the internet gateway for the whole Kingdom. All internet content viewed from the country is filtered for content that contradicts the national values or laws of the Kingdom of Saudi Arabia</p> <p>Access to pornographic sites is strictly prohibited and always filtered out by CITC. Other</p>	<ul style="list-style-type: none"> <li>• CITC</li> </ul>



Stakeholder	Reason	Examples
	categories are also controlled to a lesser degree, such as drugs, alcohol, gambling, terrorism, phishing, and extreme cases of abusive religious or political sites.	
Free eMail service providers (to be confirmed)	Free email service providers deal with the largest volumes of SPAM in the world. While none of them is based in KSA, most people have access to their mail services, and it can be used free of charge for any purpose.	<ul style="list-style-type: none"> <li>• Yahoo</li> <li>• Hotmail</li> <li>• Gmail</li> <li>• Lycos</li> </ul>

#### 4.4 MAIL HOST STAKEHOLDERS:

The SPAM mail is then received by the host of the mail box belonging to the receiver. The mail host could be either a mail service provider or organizations that provide corporate mail service to their employees. These stakeholders are relevant because they often employ filters and such devices to control the spam addressed to their mail service subscribers.

Stakeholder	Reason	Examples
Mail service providers	Mail and websites hosting companies provide email services to companies and individuals for a fee. There is no additional cost on the number on emails sent or received by subscribers of these companies, and they can make a good ground for spammers.	<ul style="list-style-type: none"> <li>• Most ISPs provide mail services as part of the subscription packages</li> </ul>
Companies	<p>Most companies run their own email servers, and although there might be a clear policy that prohibits using a company's emails for send out spam, company emails can still be used for massive emailing and chain emailing.</p> <p>Also companies have to tackle the huge amounts of spam received by their email servers. Companies are deeply involved in fighting spam, as it eats up a good chunk of human effort and can cause sever financial losses.</p>	<ul style="list-style-type: none"> <li>• Aramco</li> <li>• Saudi Industrial Corporation (SABIC)</li> </ul>



Stakeholder	Reason	Examples
Banks	Banks are commercial enterprises, which, in addition to what all companies go through in terms of email spam, are also subject to phishing attacks. Phishing emails can cause a potentially huge damage to the bank's revenues and reputation if they weren't addressed promptly.	<ul style="list-style-type: none"> <li>• SAMBA</li> <li>• The Saudi British Bank (SABB)</li> </ul>
Security solution providers/Infrastructure Service providers	While Security Solution providers provide content filtering tools in order to filter out possible spam before it is delivered to the end user, infrastructure service providers include anti-SPAM capabilities into their product features.	<ul style="list-style-type: none"> <li>• Symantec</li> <li>• Microsoft</li> <li>• IBM Internet Security Systems (ISS)</li> </ul>
Universities	Universities' networks are generally vulnerable to hackers using the universities' machines as botnets. As such, universities computers become zombies where SPAMers find it attractive to launch their attacks.	<ul style="list-style-type: none"> <li>• King Fahad University for Petroleum and Minerals (KFUPM)</li> <li>• KSU</li> </ul>

#### 4.5 REPORTING PROCESS STAKEHOLDERS

Once the receiver receives the SPAM message, he may wish to report this incident to a suitable organizational unit within the Kingdom, particularly if some damage was caused as a result of the SPAM.

Typically the organizational unit to whom the receiver can report SPAM would vary by kind, origin and content of the SPAM. For example, the receiver may report such SPAM messages to Banks, the company that he/she works with, or relevant Government agencies. A list of such stakeholders is provided below.

Stakeholder	Reason	Examples
Government Agencies	CITC is entitled to protect the interests of users in respect of public telecommunications services and the Internet and propose regulations related to the telecommunications sectors. When SPAM violations fall under the Saudi electronic transaction Act (e-transaction Act) (e.g. Privacy issues) or the "Anti e-crime Act"	<ul style="list-style-type: none"> <li>• Communications and Information Technology Commission (CITC)</li> </ul>



Stakeholder	Reason	Examples
	(e.g. unauthorized access to computers and networks), CITC is the authority SPAM victims have to report to.	
	SAMA, the central bank of the Kingdom of Saudi Arabia, supervises Commercial banks and is focused on banking regulations.  In case the bank customers fail to secure their own money during Internet transactions (e.g. Phishing using SPAM), SAMA might be the authority the bank customers report to. In fact, the SAMA Committee resolves certain disputes between banks and their customers.	<ul style="list-style-type: none"> <li>• Saudi Arabian Monetary Agency (SAMA)</li> </ul>
	The MOI might be one of the authorities to whom the spam receivers are reporting; since MOI is in charge of public security, border police, special security and investigation forces, and criminal investigation.	<ul style="list-style-type: none"> <li>• Ministry Of Interior (MOI)</li> </ul>
ISPs	Notifying ISPs (especially if the spammer is a customer of the same ISP) might help ISPs to gauge the spam problem on their networks and make decisions about how to prevent further spam.	<ul style="list-style-type: none"> <li>• Awalnet</li> <li>• Atheer</li> <li>• SaudiNet</li> </ul>
GCC Agency	International and regional cooperation is a must for combating SPAM. The GCC could offer effective coordination and integration between GCC Member States in areas of interest such as: legal, industry, and technology.	<ul style="list-style-type: none"> <li>• Not decided yet</li> </ul>
Statistics Agencies	Agencies maintaining spam statistics are stakeholders since reporting SPAM cases will help them compile statistics that may be useful in setting future security policies and countermeasures	<ul style="list-style-type: none"> <li>• MessageLabs</li> <li>• Security Solution providers, like Symantec</li> <li>• eMail Service Providers</li> </ul>
International Bodies	Reporting to a relevant international body may be required	<ul style="list-style-type: none"> <li>• APWG</li> </ul>



Stakeholder	Reason	Examples
	in case spamming was initiated from outside Saudi Arabia	<ul style="list-style-type: none"> <li>• MAAWG</li> <li>• SPAMHAUS</li> </ul>

#### 4.6 ENFORCEMENT PROCESS STAKEHOLDERS

Once the report is submitted and it is determined that the SPAMmer was guilty of sending the SPAM to the receiver, the SPAMmer is punished by a stakeholder responsible for enforcement of the Anti-SPAM regulations.

The enforcement agencies could vary by severity and type of SPAM sent, and would typically include agencies like Courts and/or relevant Ministries. At this stage, the responsibility for enforcement of Anti-SPAM regulations has not been formally defined, though some of the relevant stakeholders likely to be involved are listed in the table below.

Stakeholder Name	Reason	Examples
Courts	Courts will hear spam-related cases and make decisions based on applicable laws in Saudi Arabia.	<ul style="list-style-type: none"> <li>• Shoura Council</li> <li>• Grievances Court (Diwan Al-Mazalem)</li> <li>• Sharia court</li> </ul>
Police	The Police, will either on the courts' instructions or of their own accord (if considered a criminal offence) take action against offenders	<ul style="list-style-type: none"> <li>• Police</li> </ul>
Government Agencies	MOC is in charge of commercial companies marketing regulations. As SPAM violations might fall under consumer protection applicable law in the Kingdom, they could be involved in enforcing the Anti-SPAM related regulations.	<ul style="list-style-type: none"> <li>• Ministry Of Commerce (MOC)</li> </ul>
	MOI is responsible for maintaining law and order within the Kingdom, and key enforcement agencies report to them	<ul style="list-style-type: none"> <li>• Ministry of Interior (MOI)</li> </ul>
	MCIT is responsible for setting regulation projects relevant to communications and IT. In particular, MCIT is responsible for enforcing the IT criminal law; any SPAM violation falling under this	<ul style="list-style-type: none"> <li>• Ministry of Communications and Information Technology (MCIT)</li> </ul>



Stakeholder Name	Reason	Examples
	law will engage MCIT as a stakeholder.	

#### 4.7 CONCLUSION

There are a number of stakeholders involved in the SPAM activity life-cycle. Each of them plays different roles in the context of the SPAM life cycle.

In order to be effective, it is imperative that the Anti-SPAM policy framework should address most, if not all, of these stakeholders.



## 5. STAKEHOLDERS FEEDBACK

The following list represents the stakeholders who were included in the research (questionnaire based survey and/or interviews) conducted by the Ernst & Young team during the assessment of the current state in the Kingdom:

- Saudi Arabian Monetary Agency (SAMA);
- Data Service Providers (DSPs);
- Mobile Service Providers (MSPs);
- Bulk SMS Licensees;
- Solution Providers;
- Internet Service Providers (ISPs);
- Companies;
- Universities;
- Ministry Of Interior (MOI);
- Communications and Information Technology Commission (CITC); and
- King Abdulaziz City for Science and Technology (KACST) / Internet Services Unit (ISU).

### 5.1 SAMA

#### 5.1.1 BACKGROUND

SAMA, the central bank of the Kingdom of Saudi Arabia, supervises Commercial banks and is focused on banking regulations. SAMA issues national currency, acts as a banker to the government, supervises commercial banks, and manages the Kingdom's foreign exchange reserves. SAMA is in charge of the Banking Act and provides Internet Banking Security guidelines.

#### 5.1.2 IMPORTANCE OF THE STAKEHOLDER

SAMA provides Internet Banking Security guidelines and is in charge of the Banking Act. Phishing attacks are typically reported by Banks to SAMA initially, who then forwards them separately to MOI and CITC, who are responsible for blocking access to these sites and taking penal actions as applicable.

### 5.2 DSPTS

#### 5.2.1 BACKGROUND

Data Service Providers (DSPs) are media stakeholders who provide Internet Connectivity and act as gateways for ISPs and some corporations to connect to the Internet. Three DSPs were contacted as they are currently licensed by CITC:

- Integrated Telecommunications Company (ITC),
- Saudi Telecommunications Company (STC), and
- Bayanat Al Oula.



### 5.2.2 IMPORTANCE OF THE STAKEHOLDER

Three DSPs provide the backbone for all ISPs operating in the Kingdom. ISPs sign contracts with DSPs for the provision of Internet connectivity. Any possible controls implemented at the DSPs level can restrict the flow of incoming and outgoing SPAM.

## 5.3 MSPS

### 5.3.1 BACKGROUND

Two mobile service providers were contacted in the study, the Saudi Telecom Company (STC) and Mobily. Saudi Telecom Company (STC) is the first mobile service provider. Besides mobile service, STC offers landline, data services and internet services. The data services include Fax, WAP and Jawalnet. The Company also offers roaming services to their subscribers.

The second mobile service provider is Mobily, the official brand name of Etihad Etisalat. Mobily provides GSM and 3G based telecommunication services such as voice calls, MMS, LBS, international roaming, GPRS and GPRS EDGE roaming, etc.

### 5.3.2 IMPORTANCE OF THE STAKEHOLDER

As SMS/MMS can be used as another form of SPAM to promote goods and services, MSPs play an important role as they provide the backbone for all Bulk SMS licensees in the Kingdom and can filter the messages and block SPAMers.

## 5.4 BULK SMS LICENSEES

### 5.4.1 BACKGROUND

A Bulk SMS license enables companies to send bulk SMS messages to subscribers. More than 90 bulk SMS licenses have been granted by CITC to Bulk SMS providers in the Kingdom, for example:

- BAB.Com;
- Tawasul;
- Saudi Research and Publishing Company;
- First Gulf Co;
- Saudi Research and Publishing Company;
- VODATEL;
- Electronic Concepts;
- Sky Telecom Co.; and
- Others.

Eight Bulk SMS providers were interviewed while 13 answered the questionnaires.

### 5.4.2 IMPORTANCE OF THE STAKEHOLDER

Bulk SMS licensees are authorized to send bulk SMS as per the terms and conditions outlined in the license granted by CITC. Some of the Bulk SMS messages might be considered as



SPAM and thus it is considered critical regulate the operation of Bulk SMS licensees and define the acceptable boundaries.

## 5.5 SOLUTION PROVIDERS

### 5.5.1 BACKGROUND

Solution providers play an important role in the battle against SPAM. They provide the technical solutions that are critical to reduce SPAM. Two solution service providers were met while others were contacted via email and over phone such as:

- Symantec: offers BrightMail 6 which can be deployed as Mail Gateway, in lined with Mail Servers and on Mail Servers;
- Sophos: offers security software such as anti-virus, anti-spyware, anti-spam and Network Access Control for desktops, e-mail servers, and other network gateways;
- ISS: provides security products and services that preemptively protect enterprise organizations against Internet threats;
- CLEAR SWIFT: provides MIME Sweeper for SMTP 5.2 ( which can be deployed as Mail Gateway) and MIME Sweeper for Exchange (which can be deployed as Plug-in for Internal Exchange Mail Servers/MDAs);
- SurfControl: offers Email Filter and MailControl products which can be deployed as Mail Gateway; and
- Others.

### 5.5.2 IMPORTANCE OF THE STAKEHOLDER

Security Solution providers provide filtering tools and awareness material in order to filter out SPAM before it is delivered to the end user. Filtering tools should keep in pace with SPAMers' new techniques especially when SPAM is used as a vehicle to send viruses, malware and Phishing attacks.

## 5.6 ISPS

### 5.6.1 BACKGROUND

ISPs provide Internet connections to corporations, individuals and governmental agencies, and hence, they are the carriers of electronic communications, mainly emails. Two ISPs were interviewed while 15 ISPs had participated in the survey. A number of ISPs were licensed by CITC, for example:

- Nesma;
- Zajil;
- MeduNet;
- Awalnet;
- SPSNET;
- Shabakah Net;
- Sahara Net.;
- Jeel Internet Solutions;



- MeduNet;
- Saudi Net; and
- Others.

### **5.6.2 IMPORTANCE OF THE STAKEHOLDER**

ISPs provide the infrastructure where the Internet traffic goes through. ISPs can deploy filters that reduce SPAM and can block well-known origins of SPAM using black/white lists. Moreover, ISPs may have a role in raising the awareness on SPAM, receiving complaints from victims, and taking remedial actions against SPAMers.

## **5.7 COMPANIES**

### **5.7.1 BACKGROUND**

Most companies receive massive advertisements emails of products and services. As a result, companies are most likely to be a victim of SPAM messages including fax. Thirty six companies were included in the study and meetings were conducted with two of them.

### **5.7.2 IMPORTANCE OF THE STAKEHOLDER**

Companies are mostly the victims of SPAM. Their heavy use of email makes them more vulnerable to SPAM threats. On the other side, company networks might be used to send SPAM as well. Having filters, policies and awareness programs is critical to reduce the amount of SPAM sent and received.

## **5.8 UNIVERSITIES**

### **5.8.1 BACKGROUND**

Some universities in the Kingdom, such as King Fahd University of Petroleum and Minerals (KFUPM), King Saud University, King Faisal University and others rely heavily on Internet and email as a way of communication between management, instructors and students. Two universities were interviewed and participated in the survey.

### **5.8.2 IMPORTANCE OF THE STAKEHOLDER**

Universities' networks are generally vulnerable to hackers using the universities' machines as botnets. As such, universities computers become zombies where SPAMers find it attractive to launch their attacks.

## **5.9 MOI**

### **5.9.1 BACKGROUND**

The Ministry of Interior (MOI) is the owner of the Anti e-Crime Act which aims at creating legal and regulatory standards to combat information, computer and internet crimes through specifying /determining the relevant crimes and punitive actions for each crime or violation.

### **5.9.2 IMPORTANCE OF THE STAKEHOLDER**

MOI is the owner of the Anti e-Crime Act. As such, the MOI plays an important role in combating SPAM. MOI has recently established a new division in charge of investigating



eCrimes. Cooperation between MOI, CITC, SAMA and other stakeholders is critical for ensuring that SPAM is efficiently combated.

## 5.10 CITC

### 5.10.1 BACKGROUND

The CITC is the commission regulating the telecommunications sector in the Kingdom. It enjoys the juridical personality and financial independence to achieve its objectives stipulated in the Telecommunications Act, its Bylaw and the Ordinance of the Communications and Information Technology Commission. CITC is charged with protecting the interests of users in respect of public telecommunications services and the Internet and proposing regulations related to the telecommunications sectors.

### 5.10.2 IMPORTANCE OF THE STAKEHOLDER

CITC administratively manages the telecommunication spectrum in the whole Kingdom. All internet content viewed from the country goes through extensive filtering for content that contradicts the national values or laws of the Kingdom of Saudi Arabia. Access to pornography, gambling, and drugs related sites is strictly prohibited and always filtered out by CITC. CITC, as the agency regulating the telecommunication sector in the Kingdom, receives complaints from SAMA and commercial companies. CITC, as part of its CERT initiative, will be monitoring the Internet in Saudi Arabia to ensure that the users receive early notices when a security threat is identified. Additionally, the CITC might play a role in combating SPAM.

## 5.11 KACST / ISU

### 5.11.1 BACKGROUND

King Abdulaziz City for Science & Technology (KACST) is an independent scientific organization of the Saudi Arabian Government, established in 1977 under the name of Saudi Arabian National Centre for Science & Technology (SANCST) and later in 1985 renamed as 'King Abdulaziz City for Science & Technology (KACST)'. The ISU is a department at KACST which used to be in charge of the Internet Service in Saudi Arabia and currently provides internet service to academic and research institutions.

### 5.11.2 IMPORTANCE OF THE STAKEHOLDER

KACST is carrying out its mission in the promotion of science & technology in the Kingdom by coordinating and cooperating with various universities, agencies and institutions concerned with research and technology, and encouraging the Saudi experts to undertake research that will help the development and evolution of the society. KACST was used to regulate and supervise the Internet before it moved to CITC. KACST is now an "Academic ISP" responsible for providing standard and cutting-edge internet services and related labs and technologies to universities, research centers, and governmental agencies.

## 5.12 STAKEHOLDERS MAJOR CONCERNS AND RECOMMENDATIONS

Interviews were conducted with the identified stakeholders, using structured questionnaires, in order to obtain feedback on their views and concerns on the status of SPAM in Saudi Arabia.

The major concerns and recommendations of the various stakeholders with regard to SPAM have been summarized in this section.



All stakeholders mentioned the fact that there is currently no law in Saudi Arabia to regulate SPAM. However, there are some SPAM-related provisions that are scattered over different laws and licensing requirements/agreements. For this reason, there are no regulations regarding the collections, use, and trade of personal contact details such as email addresses and phone numbers. Some stakeholders also highlighted the lack of cooperation between various agencies in combating SPAM. For instance, SAMA, MOI, and CITC have developed an informal procedure to cooperate regarding SPAM/Phishing related issues. However, there is no formal process in place for handling complaints and forwarding them to the appropriate authorities. It was also raised that there is no code of conduct for ISPs or e-marketers in Saudi Arabia.

SPAM emails, in addition to being an annoyance are causing capacity, bandwidth, and staff performance problems. During the meetings held with the various stakeholders, many points were raised and some stakeholders suggested some technical controls as well.

Some stakeholders suggested that CITC should promote the establishment of Commercial Secure Mail Hosting providers who receive emails on behalf of companies and filter them before delivering them to the mail servers of the companies.

### **ISPs**

ISPs highlighted their shortage of technically capable staff. They indicated that they are understaffed and thus are not capable of addressing the SPAM issue extensively. ISPs also indicated that they install tools/filters to protect the mailboxes of the customers who decide to use the email servers of the ISPs. As such, ISPs do not filter all the traffic flowing through their networks due to the existing constraints in budgets, resources, and capacities. However, one of the findings is that ISPs who have deployed RBLs on their routers or Gateways, report a lower SPAM rate, as do their clients.

### **DSPs**

DSPs highlighted their shortage of technically capable staff. They indicated that they are understaffed and thus are not capable of addressing the SPAM issue extensively. DSPs also indicated that they do not have existing controls for SPAM emails and they strongly advise that SPAM filters should be decentralized at the ISP level and below since these filters might introduce degradation in the quality of service offered by DSPs if installed on their backbones. However, DSPs agreed that RBLs might be deployed on their routers to ensure that known SPAMers cannot send emails to users in the Kingdom, yet they stressed on the fact that these blacklists need to be very accurate since they might result in blocking legitimate traffic.

### **MSPs**

Mobile Service Providers (MSPs) suggested that SMS SPAM regulations should focus on bulk SMS licenses and should exclude advertisements. They also suggested that it is important to control websites' registries as an ancillary element to setup accountability and to control websites sending SMS SPAM.

MSPs receive daily huge numbers of SMSes originating from outside Saudi Arabia. Some of these messages are SPAM messages. Although their current systems do not contain sophisticated filters to identify SPAM SMSes, MSPs have developed some controls to ensure that bulk SMS sent internationally are inspected and blocked if deemed SPAM. Additionally, the MSPs are upgrading their systems to ensure that they can apply smarter controls to combat SPAM. The Mobile Operators reported that the SMS SPAM rate ranges between 1.25% - 1.75%.

### **Bulk SMS Service Providers**



Bulk SMS providers suggested the development and enforcement of an Anti-SPAM law with severe penalties as the best way to control SMS SPAM. Moreover, in order to know the Bulk SMS providers who originated the message, Bulk companies suggested that this could be achieved by tracking the premium numbers included in the messages sent. The tracking should be done in coordination with STC and Mobily.

## **SAMA**

SAMA took many initiatives targeted at fighting Phishing, whether by encouraging the banks to join international organizations to fight phishing, or by coordination the efforts with CITC to block access to the phishing source website. SAMA also does regular follow-ups with banks which have been subject to phishing attacks, after closing the phishing website to assess any possible damage that could have happened as a result. Additionally, SAMA stated that they have strict measures to be undertaken by banks operating under SAMA's license and the Saudi Banking Law. SAMA does conduct regular audits to ensure that all financial institutions are adhering to SAMA's regulations.

Moreover, SAMA has published security guidelines for the banks on its website [www.sama.gov.sa](http://www.sama.gov.sa) and has recorded 72 phishing attacks on Saudi Banks during the last Year.

SAMA also mentioned that the current cooperation in law enforcement is not efficient as SAMA has to coordinate between MOI and CITC in order to issue an order for blocking a phishing website through CITC. The bureaucracy sometimes causes severe delays before an action could be taken against the offenders.

## **MOI**

MOI suggested that either CITC or the newly established eCrimes Fighting Unit is to be contacted for reporting SPAM. Then, the case would be forwarded to the Bureau of Investigation and Prosecution who might use the technical skills of other agencies including CITC.



## Universities

Universities recognized that their networks and machines are attractive to SPAMmers since they can turn them into Zombies<sup>2</sup>. Thus Universities have deployed various security controls to mitigate the issues of SPAM. However, some of the universities do not allow the students to use their Laptops to access the Internet using the University networks due to the shortage of existing resources. Once this access is granted, the threats of SPAM might increase and thus additional security controls might be needed. Universities also suggested that a Cybercrime law should be in place to combat SPAM. Universities also suggested that an awareness program for SPAM is very critical to educate people.

## KACST-ISU

The ISU division in KACST indicated that currently they do not filter the bandwidth provided to universities to clean it from SPAM however, they might consider the idea of offering filtered bandwidth to universities especially that universities do not have the required technical resources needed to deploy those technically complex solutions.

ISU stressed on the importance of signing agreements with other countries and already existing international enforcement agencies. ISU suggested the cooperation with regional bodies in the GCC. Moreover, it also suggested that the reporting mechanism should be clear and straightforward while enforcement should be very simple and international cooperation is critical to achieve this.

## Companies

Most companies use anti-SPAM softwares to filter SPAM emails. Although some companies have huge databases of customer related information on their databases, these companies have not invested heavily to protect the secrecy of this information and thus prohibit SPAMers from harvesting this information. This is also due to the fact that the protection of this information is not enforced by law.

Companies that are hit by SPAM have not developed programs to educate users on how to use the Internet while minimizing the entities who know their email addresses and thus minimize the probability that SPAMers can discover their email addresses.

## Banks

Banks suggest that control measures and a clear reporting procedure should be enforced in case the SPAM is originated using a local ISP. Additionally, a formal procedure for reporting Phishing complaints is being developed currently in conjunction with the Banks as are user education and awareness guidelines.

---

<sup>2</sup> A Zombie computer (often abbreviated zombie) is a computer attached to the [Internet](#) that has been compromised by a [security cracker](#), a [computer virus](#), or a [trojan horse](#). Most owners of zombie computers are unaware that their system is being used in this way. Zombies have been used extensively to send [e-mail SPAM](#).



## 6. QUESTIONNAIRE-BASED SURVEY RESULTS

This section highlights the findings that we generated using the statistics provided by Stakeholders in the answers to our questionnaires. Our findings are divided into three main categories:

- SPAM definition,
- Magnitude of the problem, and
- The manner in which stakeholders currently address SPAM.

### 6.1 SPAM DEFINITION

As illustrated in Figure 1 below, the majority of stakeholders in Saudi Arabia agree on the definition of SPAM that we have proposed in our questionnaire. The definition of SPAM used in the survey was: unsolicited<sup>3</sup> bulk<sup>4</sup> messages and communications containing commercial, abusive or objectionable content and which are sent out in bulk to people or individuals without their consent by email, fax, or instant messages such as SMS.

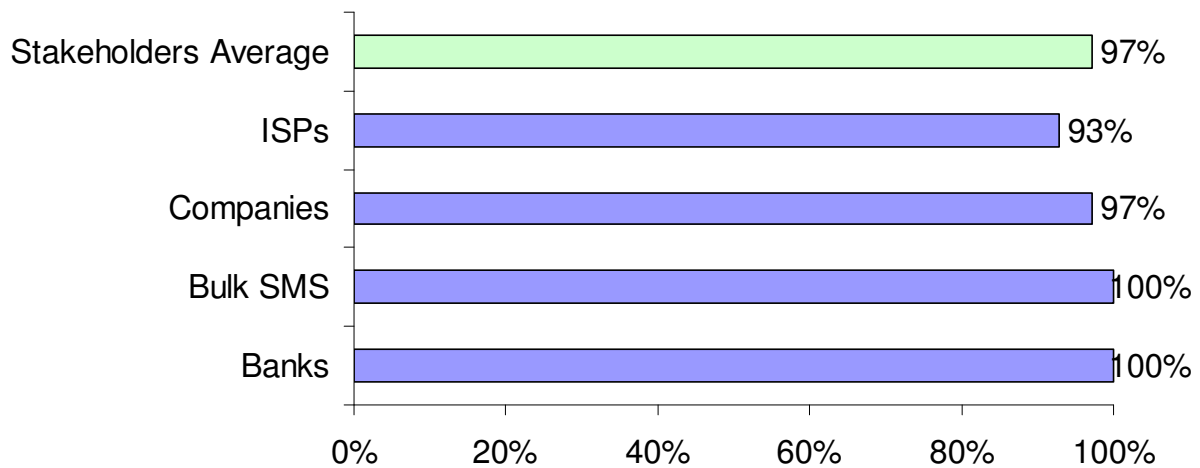


Figure 1: SPAM Definition Agreement

### 6.2 MAGNITUDE OF THE PROBLEM

This section of the report shows the magnitude of the SPAM problem in the Kingdom.

Using data provided by the panel of ISPs whose support was enlisted for the purpose of this project, it was concluded that the average eMail SPAM rate in the Kingdom was 51%<sup>5</sup>. Statistics collected from other sources such as companies, was ignored since it was considered that:

<sup>3</sup> Electronic messages that was sent without the stated or inferred consent of the recipient and are of an advertising or promotional nature

<sup>4</sup> Messages that are sent in numbers exceeding a predefined threshold in a predefined period of time

<sup>5</sup> Multiple ISPs participated in the survey for the duration of 8 months. However, we only considered the statistics of the months where multiple ISPs provided us with accurate numbers. Also, this number represents the SPAM average across these months.

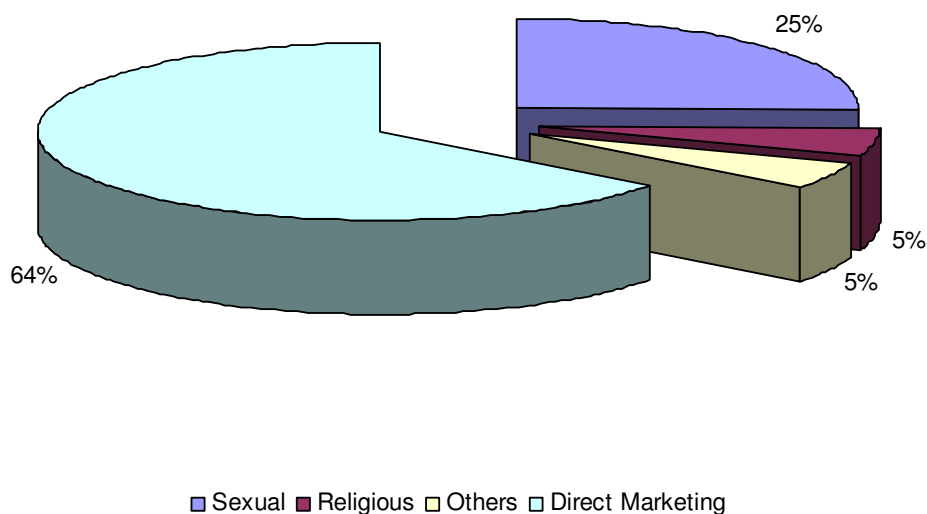


- Some of the companies provided guesstimates since they did not procure reporting tools that can generate such information readily.
- Other companies have reported their statistics, however, their SPAM rate was skewed by the fact that some ISPs do deploy RBLs on their gateways and thus block a substantial amount of SPAM messages before they reach these companies.

Figures obtained from Anti-SPAM product vendors, such as Message Labs and Symantec, appeared quite close to the numbers obtained from the panel of ISPs. Message Labs<sup>6</sup> reported the SPAM rate in KSA for the year 2006 to be around<sup>7</sup> 48.3 % whereas Symantec<sup>8</sup> reported the SPAM rate for the year 2006 to be around 59%. Message Labs reports the SPAM rate for the year 2007 (till July) to be around 42.7%.

The Mobile Operators reported that the SMS SPAM rate in the Kingdom was ranging between 1.25% and 1.75%.

According to the surveyed stakeholders, SPAM eMail received by them was typically of four broad types as shown in Figure 2. The majority of the respondents (64%) considered that Direct Marketing Messages were the most common type of SPAM. 25% of the respondents considered Sexual email to be the most common type of SPAM, while only 5% considered religious SPAM to be a major type of SPAM received. Accordingly, controlling commercial SPAM has the potential to reduce the amount of SPAM substantially.



**Figure 2: Respondents views on most common types of SPAM**

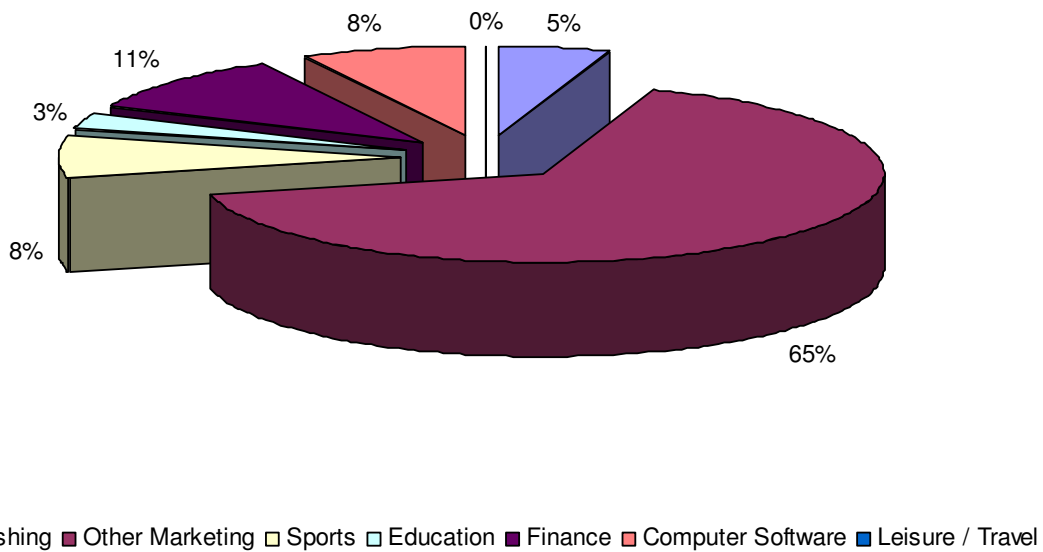
<sup>6</sup> The data provided by Message Labs is based on statistics and analysis on a range of email security threats worldwide. MessageLabs Intelligence is based on live data feeds pulled from its global network of control towers that scan millions of emails daily.

<sup>7</sup> This number was obtained by averaging various SPAM rates collected from different physical sensors.

<sup>8</sup> The data used in this analysis is based on the SPAM messages detected by Symantec Probe Network sensors deployed in over 180 countries.

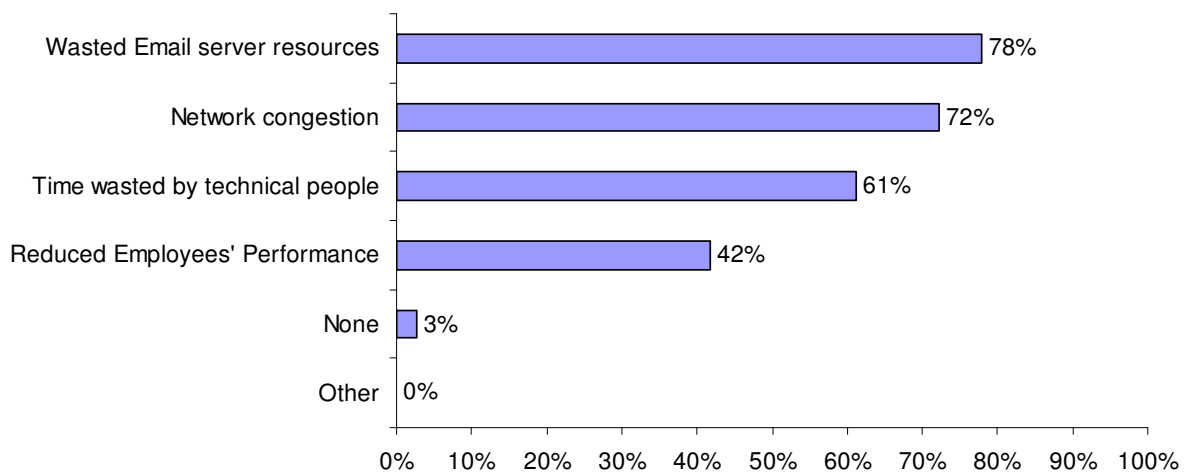


Respondents considered that Finance (11%). Sports (8%) and Computer Software related messages (8%), were the predominant types of commercial SPAM messages. The other types of SPAM were either related to phishing or education. A big part of the SPAM messages received were clubbed under the “Other marketing messages”. Respondents indicated that by “Other marketing messages” they were referring to messages promoting for the illegal sales of products (ex. Viagra).



**Figure 3: Breakdown of respondents views on Direct Marketing types of SPAM**

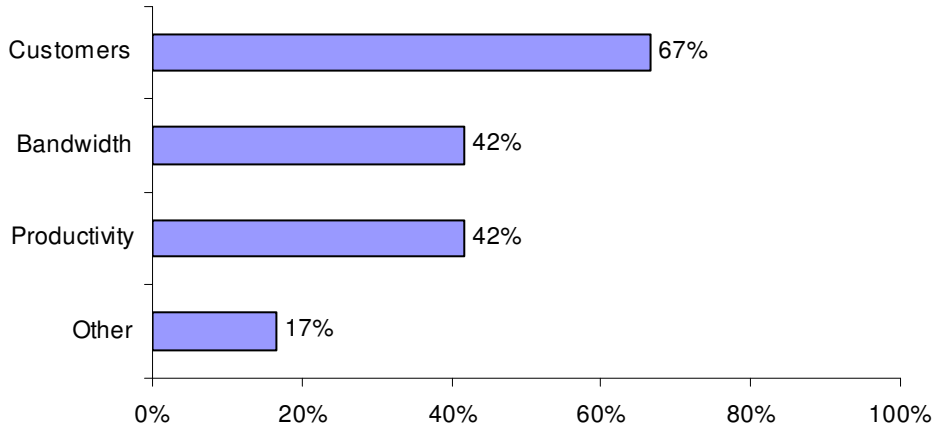
As shown in Figure 4, 78% of companies that responded to the survey believe that the primary impact of SPAM was on their email server resources. 72% believed that it congested their network. Other major impacts included the time spent by their technical people to deal with SPAM (61% of the respondents). Surprisingly, only 42% stated that SPAM reduced employee’s performance.



**Figure 4: Percentage of companies who consider that SPAM impacted them as per the criteria in the graph**

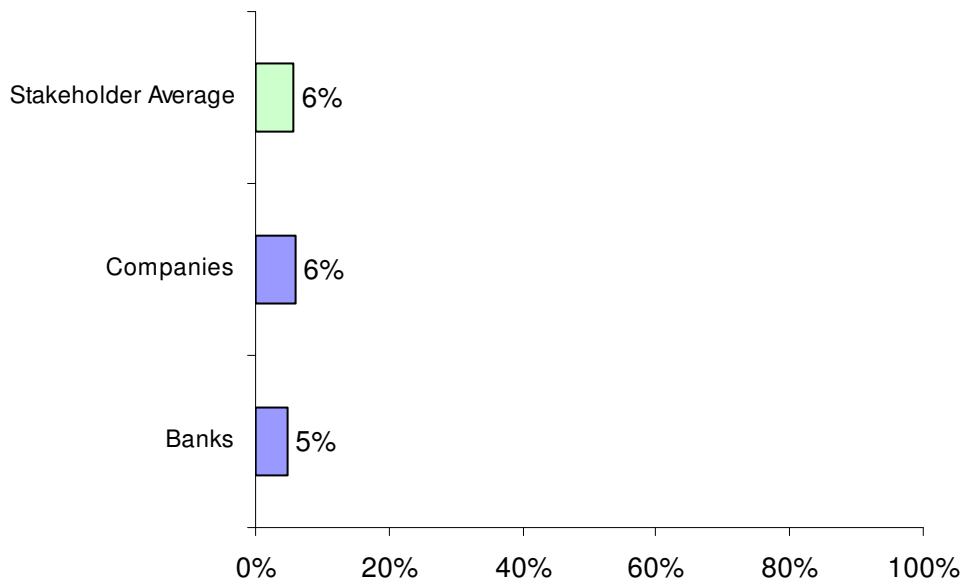


When ISPs were asked to specify the Impacts that SPAM has on their organizations, the results came in as shown in Figure 5. 67% of ISPs believed that customers were most affected by SPAM. Bandwidth and productivity were also highly affected as per 42% of the ISPs. Respondents also reported that the bandwidth consumed by SPAM ranged from 5% to 25% of the total bandwidth.

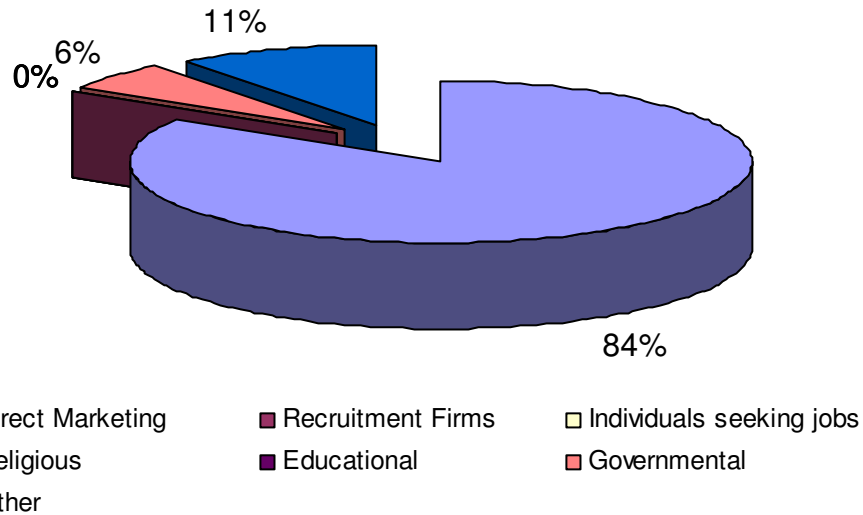


**Figure 5: Percentage of ISPs who consider that SPAM impacted them as per the criteria in the graph**

Fax SPAM was not considered by any of the respondents to be a major source of SPAM in the Kingdom. Figure 6 represents the amount of faxes received that are reportedly considered to be SPAM. According to respondents, fax SPAM is not a major issue in Saudi Arabia. Most of the Fax SPAM received tended to be commercial in nature, with 84% of the respondents confirming that commercial SPAM was the most common form of SPAM received by fax.

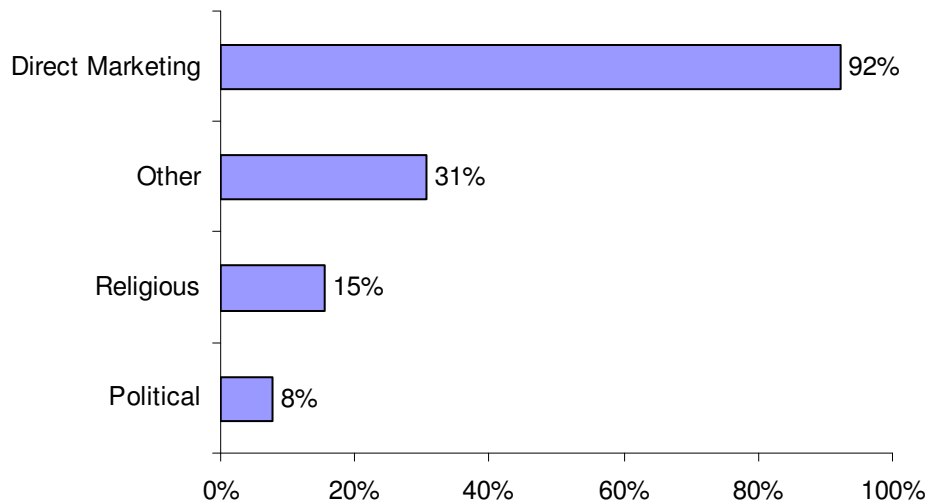


**Figure 6: FAX SPAM received**



**Figure 7: Types of FAX SPAM received**

Bulk SMS providers offer 3 main types of services: product promotions, service promotions, and advertisements on behalf of others. Messages sent through their respective units are usually either Direct Marketing, religious, or political as shown in Figure 8. It is obvious that the vast majority of Bulk SMS Licensees send Direct Marketing Messages.



**Figure 8: Percentage of Bulk SMS licensees who send bulk SMS messages as per the criteria in the graph<sup>9</sup>**

<sup>9</sup> According to the stakeholders, examples of others include, but are not limited to, the following categories: Sports, Entertainment services, Education services, Subscription services from mobile operators.



Interestingly, Bulk SMS Licensees stated that they only receive around 100 complaints per month. Some of them (17%) even state that they don't even receive any complaints. This may be due to the fact that users cannot tell who is the real originator of the SMS that they have received.

The following table summarizes the key findings of the SPAM survey:

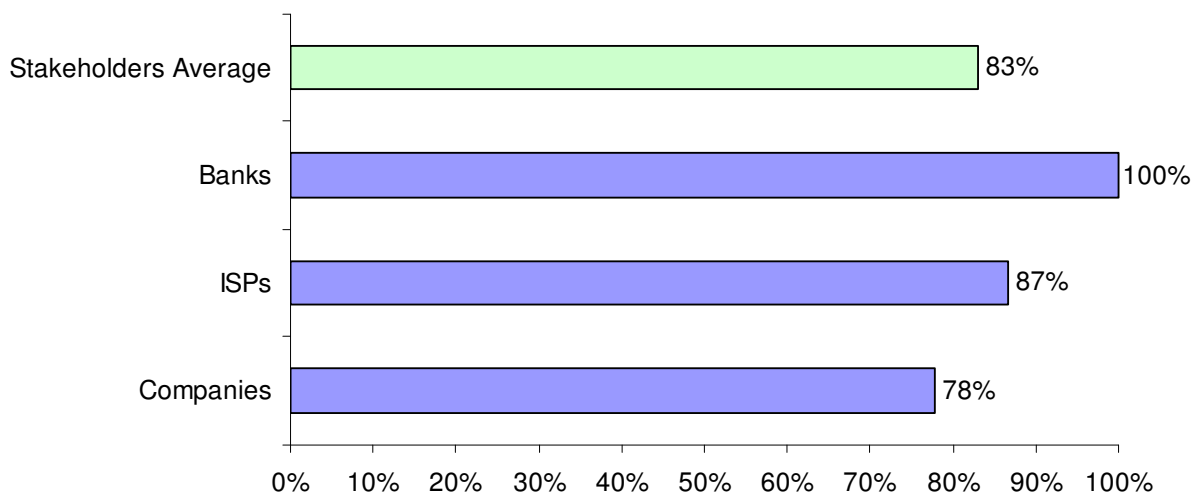
### 6.3 THE MANNER IN WHICH STAKEHOLDERS CURRENTLY ADDRESS SPAM

Addressing the issue of SPAM needs a multi-level approach, not just deployment of tools and filters to prevent SPAM. There is also a need to have proper processes in place to report and deal with SPAM on a higher level as well as the availability of proper awareness and education to end-users and customers. To be able to present a comprehensive view of how stakeholders currently address SPAM in the Kingdom, we have looked into three areas.

First, we looked at the existence of anti-SPAM solutions. This also included the location at which the solution is deployed and how the solution is configured. Second, we looked at processes that are in place to control SPAM. This includes procedures to report SPAM to other agencies. Finally, we looked into whether stakeholders carry out SPAM awareness programs within their organizations.

#### Anti-SPAM Tools

As a result of the survey that we conducted, it became evident that SPAM is a big concern for stakeholders. Different types of solutions are adopted by different stakeholders varying from general security tools that also provide protection from SPAM to advanced anti-SPAM tools and filters. Our statistics show that the average percentage of stakeholders who have controls targeted at combating SPAM is very high (83%). They have deployed anti-SPAM tools/filters on their networks to filter incoming traffic. Figure 9 below shows the percentage across various stakeholders' types.

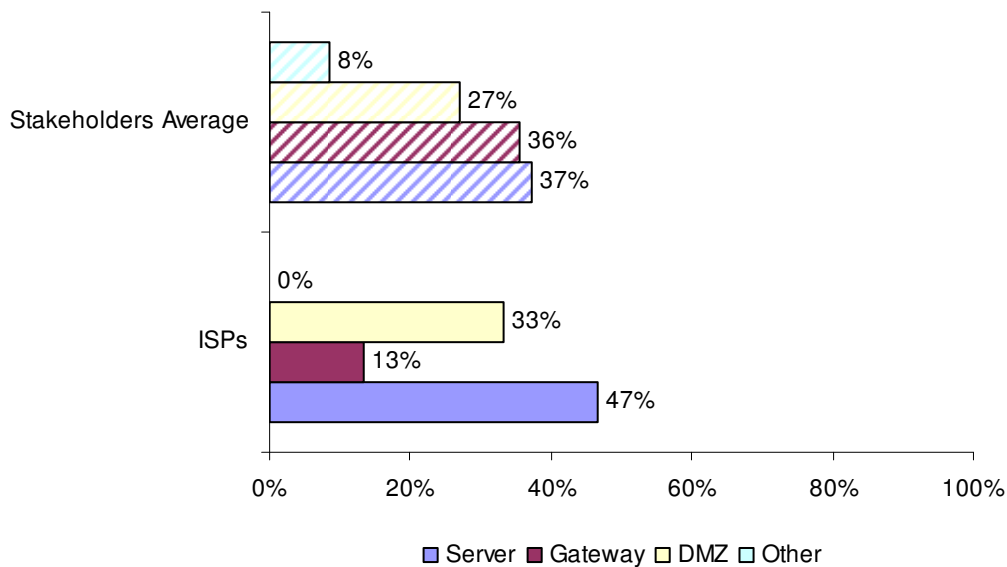


**Figure 9: Percentage of respondents who deployed email Anti-SPAM Tools/filters (Incoming)**



Another important finding that our survey revealed was the location where the anti-SPAM solution is deployed to filter incoming traffic. Stakeholders average show that almost the same percentage of respondents deploy tools on their servers<sup>10</sup> (37%) and on their gateways (36%).

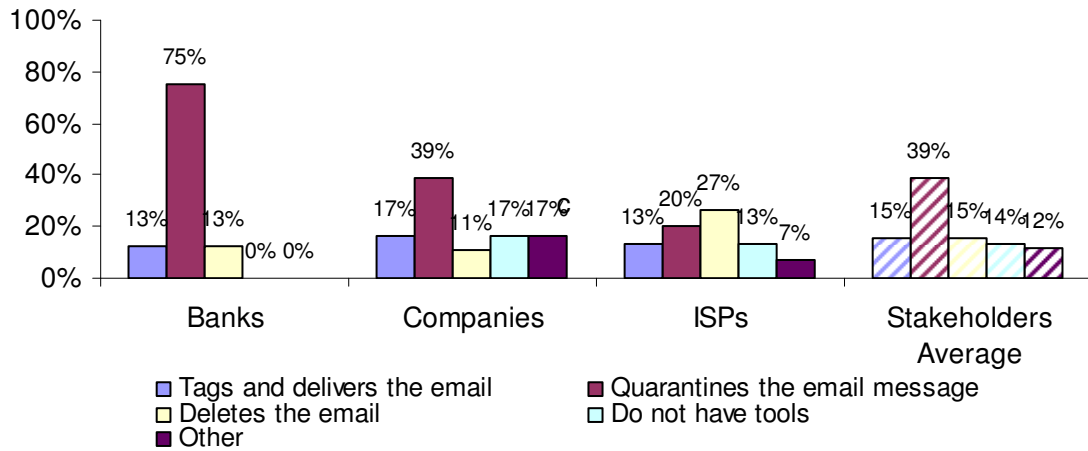
However, as indicated in Figure 10 below, ISPs tend to have a different approach. Most ISPs tend to deploy anti-SPAM solutions on their servers (47%) in order to protect the mailboxes that they host on their servers, while they tend to focus less on protecting or filtering the traffic going through their network. Only 13% of the ISPs tend to deploy anti-SPAM solutions on their gateways. This means that SPAM originating or targeting the clients of the ISPs can pass through the network of the ISPs' without being detected or filtered.



**Figure 10: Percentage of respondents who install their Anti-SPAM Tool/Filters (Incoming) as per the criteria in the graph**

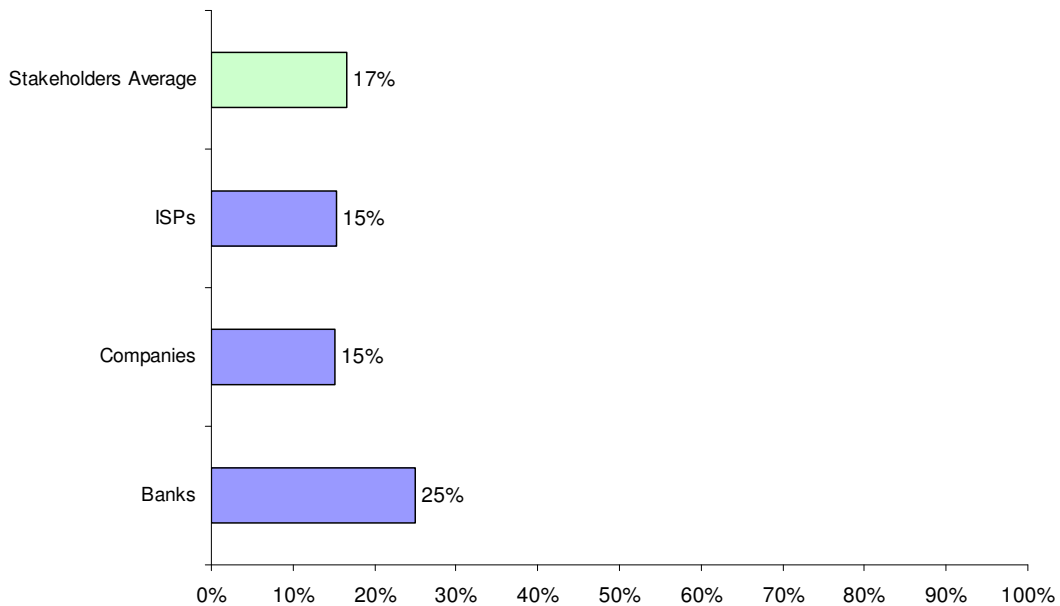
Figure 11 below shows that banks and companies prefer to quarantine the suspected SPAM email messages. ISPs, on the other hand, are divided as to whether to delete the email messages that are suspected to be SPAM or whether they quarantine them.

<sup>10</sup> When the anti SPAM solution is deployed on the server, only incoming and outgoing emails are inspected and cleaned. Whereas, when the solution is deployed on the gateway, then all the traffic flowing out or into the network is inspected and cleaned. For instance, Zombies might send emails that pass unidentified by a server-based solution.



**Figure 11: Percentage of respondents who configure their Anti-SPAM tools as per the criteria in the graph**

Real-Time Blackhole Lists (RBLs)<sup>11</sup> are considered to be efficient in blocking a big percentage of SPAM emails. These lists need to get updated regularly and it also needs regular maintenance in order to ensure that legitimate traffic is not blocked accidentally. In our survey, we also checked if stakeholders utilize RBLs alongside their anti-SPAM solutions. In Figure 12 below, we can see that on average, only 17 % tend to use RBLs separately from their Anti SPAM solutions. A higher percentage is shown in case of banks (25%).



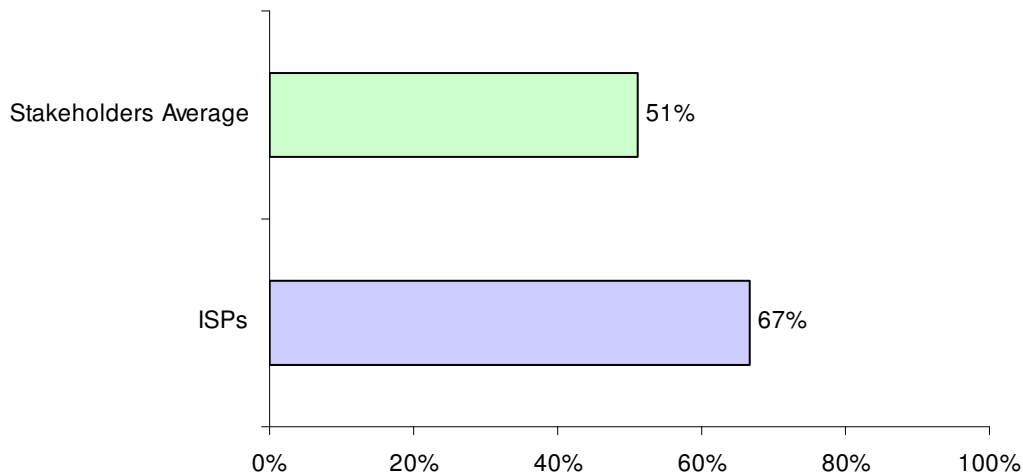
**Figure 12: Percentage of Respondents who use a RBL solution**

<sup>11</sup> Realtime Blackhole List (RBL) is a list of IP addresses whose owners refuse to stop the proliferation of spam. The RBL usually lists server IP addresses from ISPs whose customers are responsible for the spam and from ISPs whose servers are hijacked for spam relay.



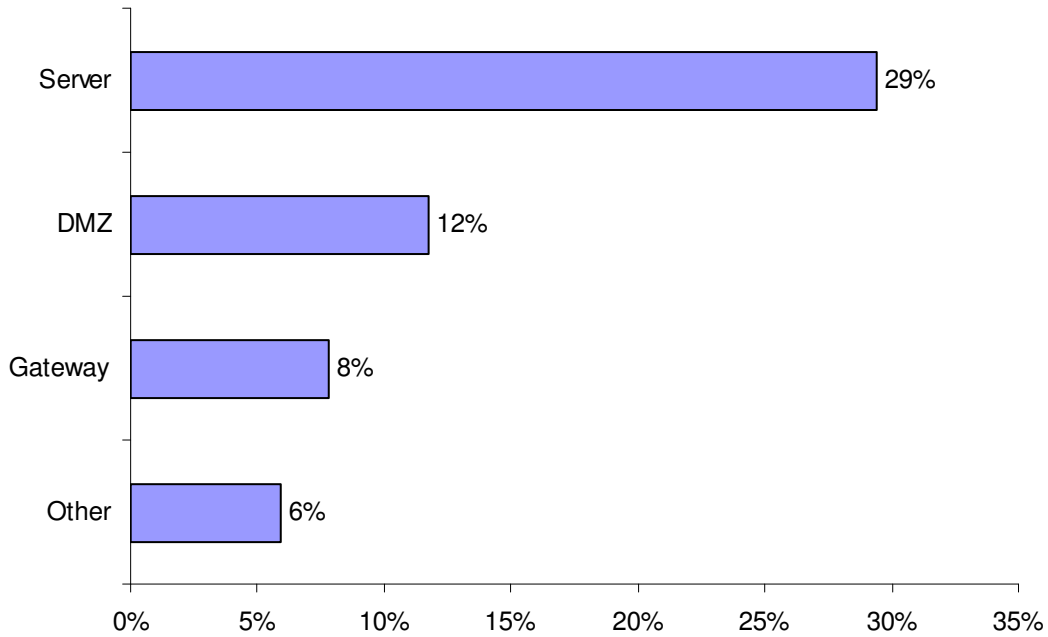
### separately from the Anti SPAM Solution

Looking at the outgoing traffic, our survey revealed that stakeholders are less concerned with blocking SPAM on the outgoing traffic. On average, only 51% of Stakeholders deploy solutions to filter outgoing traffic compared to 83% of stakeholders who filter incoming traffic. This shows that stakeholders are not too concerned about the SPAM that might originate from their networks. In the case of ISPs, in addition to the fact that most of the ISPs do not filter the email traffic sent by their customers without passing through the ISP's email server, Not all ISPs check whether their own mail servers are generating SPAM. Figure 13 below illustrates this point.

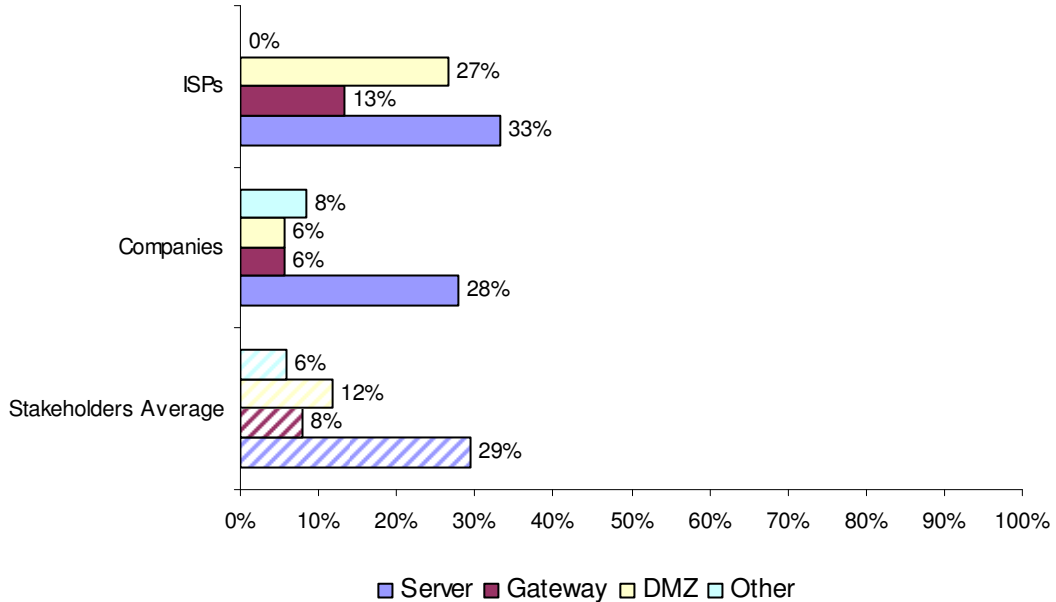


**Figure 13: Percentage of respondents who deployed email Anti-SPAM Tools/filters (Outgoing)**

Looking at the location where the tools are implemented on the outgoing traffic, our survey shows that only 8% of average stakeholders are concerned with protecting the outgoing traffic on their gateways and in the case of ISPs only 13% are concerned with protecting their gateways. This means that if a subscriber installs a mail server, he/she can send SPAM emails undetected. Additionally, this means that SPAM bots can send SPAM emails undetected. Figure 14 and Figure 15 give a clearer picture of the situation.



**Figure 14: Percentage of respondents who installed their anti-SPAM Tools/Filters (Outgoing) as per the criteria shown in the graph**



**Figure 15: Percentage of respondents who installed their anti-SPAM Tools/Filters (Outgoing) as per the criteria shown in the graph by Stakeholders' types**

### Processes to Control SPAM

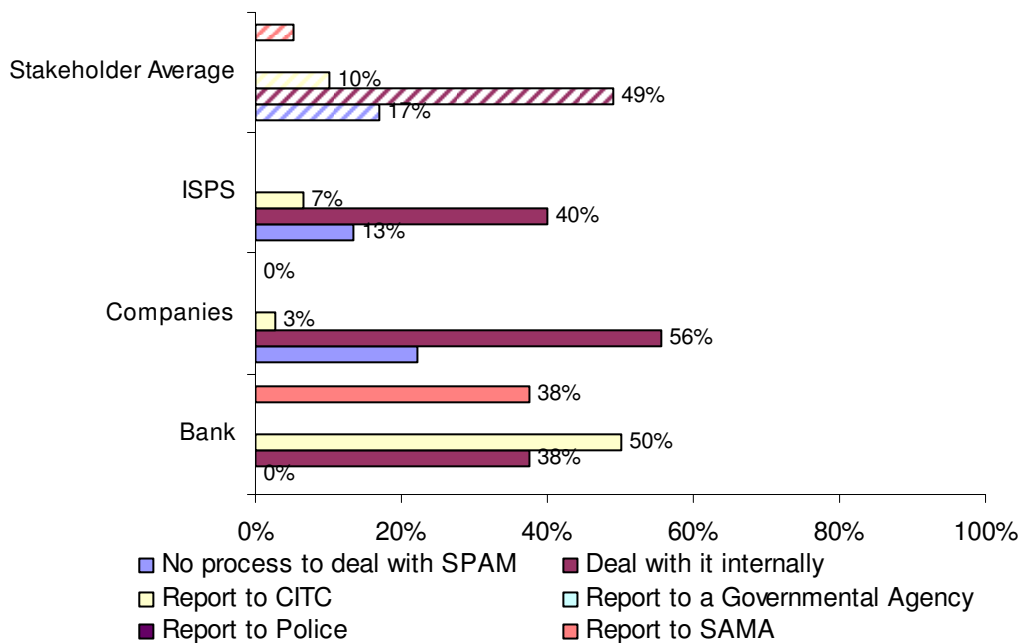
The second aspect that we have covered in our survey was the processes that stakeholders have to control SPAM. This includes dealing with SPAM initially, SPAM reporting



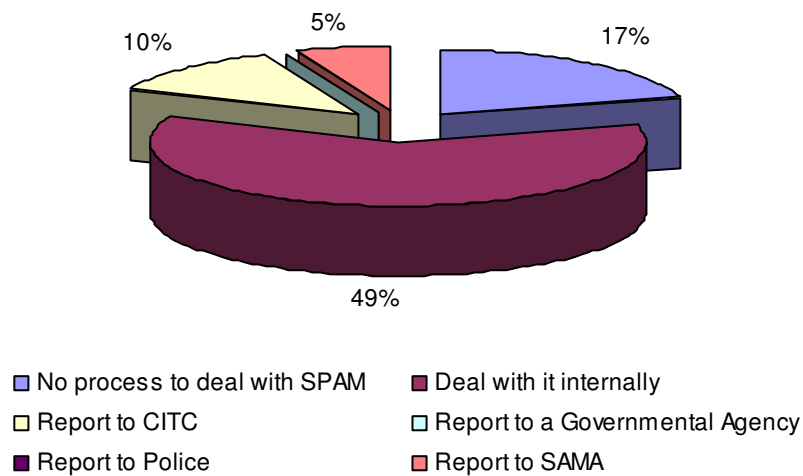
procedures, any Acceptance Use Policy (AUP) with customers and Code of Conduct among entities.

Our survey has showed that in the absence of a formal complaints reporting process, it is not surprising (contrary to Banks) that most of the organizations deal with SPAM internally or do not do anything about SPAM complaints. Around 17% of stakeholders do not even have a proper process to deal with SPAM as we can see from Figure 16 and Figure 17 below.

However, the observation is different in the case of banks. Figure 16 show that almost half the Banks have procedures in place to report phishing complaints to CITC and SAMA. By developing an anti-SPAM framework it is expected that other industry sectors will develop such processes as well to report SPAM.



**Figure 16: Percentage of the stakeholders who take one of the actions listed in the graph when SPAM is detected by stakeholders' type**



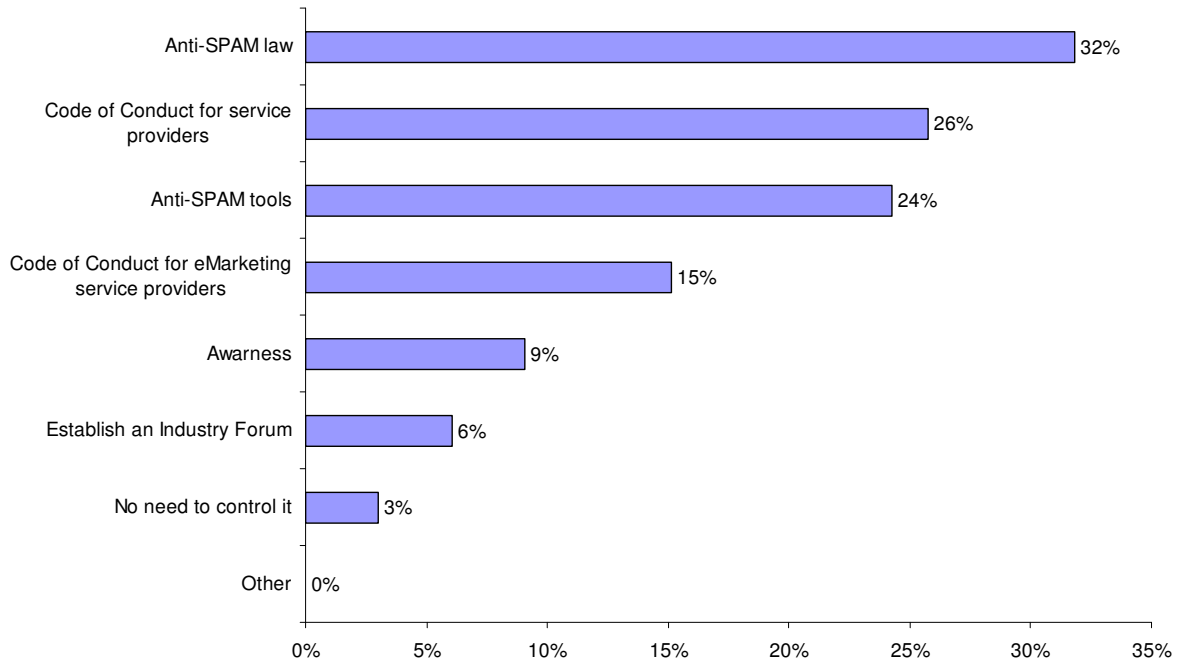
**Figure 17: Percentage of the stakeholders who take one of the actions listed in the graph when SPAM is detected**

In our survey, we also tried to confirm the views of stakeholders on the best method to combat SPAM. As indicated in Figure 18 below:

- 32% of the stakeholders see that having an anti-SPAM law was the most effective manner in which their organizations could combat SPAM.
- 26% of stakeholders also agreed that having a proper code of conduct between service providers would help substantially in preventing SPAM, though interestingly, only 13% of ISPs believed that having a code of conduct amongst them will help in combating SPAM<sup>12</sup>.
- 24% of stakeholders (especially ISPs and Companies) saw that deploying anti-SPAM tools was a sufficient measure to prevent SPAM.
- 15% of stakeholders agreed that having strict eMarketing rules, including possibly a Code of Conduct, between e-Marketing service providers could help in controlling SPAM<sup>13</sup>.

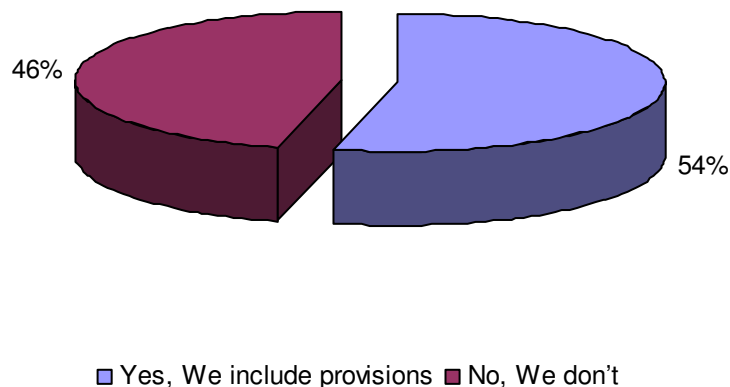
<sup>12</sup> Possibly, this is because ISPs are aware of the fact that having a code of conduct with no enforcement and audit will not help to reduce SPAM.

<sup>13</sup> This reflects the importance of the industry assistance in the battle against SPAM. Although legislation is critical, having an industry-specific guideline which is more customised to a specific industry is of great importance.

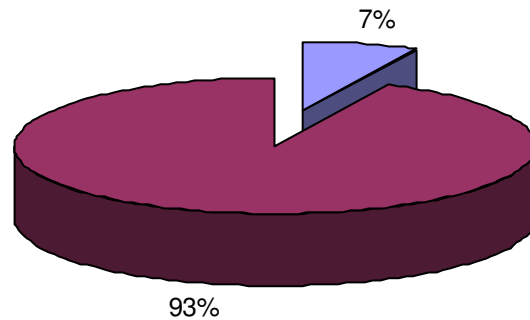


**Figure 18: Stakeholders' View on How to Combat SPAM**

This led us to have a look at two other aspects: Do Service Providers ensure that their customers do not abuse the services offered to them, and do Service Providers cooperate amongst each others in combating SPAM. First, we noticed in our survey that 46% of Service Providers (Figure 19) do not have any anti-SPAM provisions in their Acceptance Use Policy (AUP). The inclusion of such clauses can help greatly in controlling SPAM originating from Saudi Arabia. Second, we have also discovered that 93% of Service Providers (Figure 20) are not aware of any existing code of conduct amongst Service Providers. This means that there is no cooperation between Service Providers to control SPAM.



**Figure 19: Provisions in the Acceptable use section of the contracts restricting sending of SPAM**

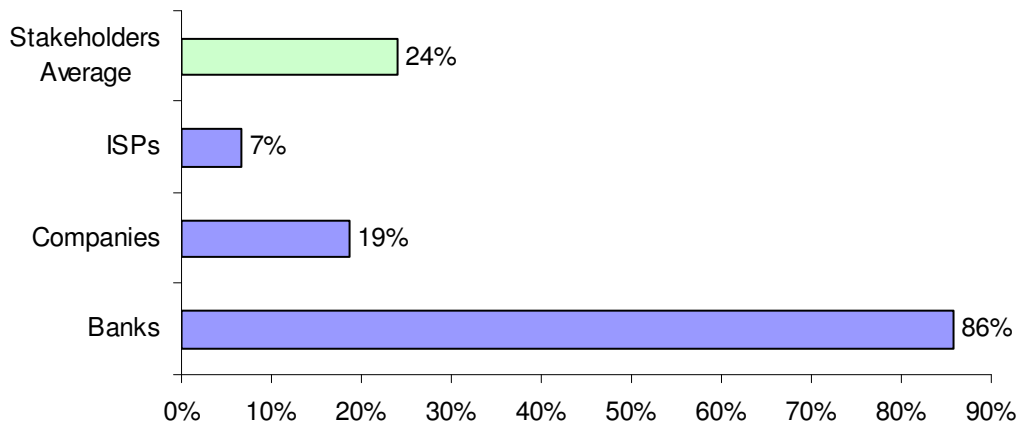


■ Yes, there is a CoC ■ No, there is not

**Figure 20: Existence of an inter-ISP Code of Conduct for SPAM?**

### SPAM Awareness Programs

Finally in this survey we tried to identify the level of awareness that stakeholders provide to their customers/employees. The results were very surprising as we can see from Figure 21 below. The stakeholders' average of 24% shows that organizations are not putting much effort in educating their employees and customers on how to deal with SPAM. However, banks have scored very high (86%) in conducting awareness programs to their employees and customers.



**Figure 21: Stakeholders running an Awareness Program**