OECD Digital Economy Papers No. 99

Spam Issues in Developing Countries

OECD

https://dx.doi.org/10.1787/232156241342

OECD

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

26-May-2005

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE ON CONSUMER POLICY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/CP/ICCP/SPAM(2005)6/FINAL
Unclassified

Task Force on Spam

SPAM ISSUES IN DEVELOPING COUNTRIES

JT00185109

English - Or. English

FOREWORD

The OECD Task force on Spam discussed this document during its meeting in March 2005, and recommended it for declassification to the CCP and ICCP Committees through a written procedure, which was completed on 6 May 2005.

The report was prepared by Mr. Suresh Ramasubramanian, Consultant to the OECD. It is published under the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

FOREWORD 2
TABLE OF CONTENTS 3
EXECUTIVE SUMMARY 4
INTRODUCTION 6
Why spam is so popular - the "transfer of cost" syndrome 6
SPAM ISSUES IN DEVELOPED AND DEVELOPING ECONOMIES 7
Impact on ISPs 7
Bandwidth 7
Costs 7
Accountability for spam issues 8
ISP resource and organisational limitations 8
Effect on users 12
Costs 12
Software piracy and its impact on viruses that propagate through spam 13
Education of users 13
Legislative and regulatory framework 14
ACTION REQUIRED BY DEVELOPING ECONOMIES AGAINST SPAM 17
Putting in place technical solutions 17
Open Source software solutions 17
Formation of CSIRTs and CERTs 18
Training of ISP personnel in security and spam handling 19
Anti-spam policy setting and enforcement for ISPs 20
International co-operation, and the role of regional organisations 21
International co-operation on an ISP to ISP level 21
International co-operation at an industry and end-user level 22
Legislative and regulatory framework to deal with spam 23
User education 24
WHAT DEVELOPED ECONOMIES CAN DO TO HELP 26
Facilitate industry co-operation and anti-spam workshops 26
Source funding to NGOs that train developing economy ISP and network administrators 26
Work with developing economies to educate people on spam and security issues 27
Helping developing economies with anti-spam legislative and regulatory frameworks 28
Establish centres of expertise and information sharing 29
CONCLUSION 30

EXECUTIVE SUMMARY

Spam is a much more serious issue in developing countries than in OECD countries, as it is a heavy drain on resources that are scarcer and costlier in developing countries than elsewhere. In this paper, it will be seen that several issues faced by the victims of spam in developing countries are the very same ones that are faced by their counterparts in more developed countries. The only difference is that the effects of spam are magnified, and are felt much more strongly in developing countries than elsewhere. ISPs and network providers in developing countries lack the capacity and resources to deal with sudden surges in spam that occur from time to time, and this often causes their mail servers to break down or function at a sub-optimal level. Indeed, their capacity to cope with even normal (though fairly high) levels of spam is much weakened because resources such as hardware, bandwidth and software licenses tend to cost much more as a percentage of a developing country ISP's budget. Similarly end users, both consumers and business, may lack knowledge of potential resources available to them to take effective action, and even those resources that they do have available cost relatively more.

The genesis of this paper was the emphasis given by the OECD Task Force on spam on ensuring that its work on spam also included an outreach element encompassing non-member countries. This also reflected the deep concern felt by representatives of developing economies, and strongly expressed at the ITU/WSIS Thematic Meeting on Spam held in Geneva in July 2004, about how spam and net abuse were bleeding the Internet economy in their countries of scarce and costly bandwidth, and that they were ill equipped to deal with these issues, both in terms of technical know-how, money and equipment for ISPs to deal with spam and net abuse.

Developing country representatives have often expressed the view that Internet users in their countries were suffering much more from the impact of spam and net abuse, and were becoming wary of even using the Internet. As a consequence of this widespread fear and distrust of the Internet, some people were not prepared to access even e-governance resources being made available to them by their governments.

OECD is studying the problems of spam specific to developing economies, its impact on these economies, and suggested means and measures that can be taken to mitigate the impact of spam on developing economies.

This paper will attempt to discuss the challenges faced by developing economies in fighting spam. Its main emphasis is on issues facing Internet Service Providers. Beginning with a review of the economic and technical issues of spam, it goes on to suggest several technical and legislative solutions, backed by the education and empowerment of users, giving them access to secure computing resources and making them more sensitized to net abuse issues. The paper goes on to examine what developing economies can do to combat spam on their own, and examines the various possible ways in which developed economies can contribute their expertise and resources to help developing economies fight spam.

The solutions proposed in the paper are carefully selected so as to be scalable, with the highest possible return on investment in money, and even more importantly, in human resources. The ubiquitous resource shortage and other conditions specific to developing economies (such as a current lack of regulation and enforcement) have also been kept in mind, as have the advantages available to developing economies – such as a large pool of competent human resources available at a comparatively low cost and

will prove a valuable resource for developing economies that helps them increasingly mitigate spam locally, at the lowest possible cost, and with maximum knowledge of local conditions so that any anti-spam solution implemented – whether legislative, technical or user level – can be properly customised to reflect local conditions. Another important part of the solution – international co-operation at multiple levels (ISP to ISP, government to government, business to business) has also been discussed. Further, the paper also suggests several possible and currently operational venues and forums for such co-operation.

INTRODUCTION

Why spam is so popular - the "transfer of cost" syndrome

Unsolicited bulk email messaging, also known as spam, thrives for one major reason - the costs incurred by the spammer sending the spam are extremely low. In contrast the costs incurred by an ISP, a business or an individual to receive, store and download spam far outstrip the costs incurred by the spammer. In contrast, traditional off-line marketing methods, such as bulk postal mail and telemarketing, are based on a sender pays model, where the sender bears all the costs, and the cost to the recipient of this advertising is negligible.

The e-mail system, when formed, never envisaged the probability that it would be abused so there is a strong design legacy of operation on a trusted network, and a largely open access policy that allowed all participants on the network free access to computing resources, SMTP relay services etc., on each others' machines, as a gesture of courtesy and goodwill. Another feature of the e-mail system when it was first developed, and which remains a legacy to this day, is the ability of users to remain anonymous. While anonymity is still an essential feature of today's Internet, especially in the context of free speech or other legitimate reasons for anonymity, the possibilities of anonymous e-mail are increasingly being adopted by spammers.

Spammers and other Internet abusers adopt a wide variety of tactics in an effort to cover their tracks and avoid detection. These include techniques such as rapidly cycling through a huge list of anonymous proxy servers, or infecting thousands of PCs around the world with viruses in order to set up a "zombie army" of computers that can be remotely controlled to send out spam, perpetrate distributed denial of service (DDoS) attacks, compromise servers etc.

These techniques ensure that spammers can abuse the resources of others, namely the computing power and bandwidth of thousands of people around the world in order to send out their spam. This allows for very large amounts of spam to be injected into the global e-mail stream at negligible cost to the spammer. The spammer need not pay for anything except an Internet connection and the cost of bulk mailer software to distribute sales pitches.

SPAM ISSUES IN DEVELOPED AND DEVELOPING ECONOMIES

Impact on ISPs

Bandwidth

There is still limited availability of bandwidth in many developing countries, often associated with high costs. High volumes of incoming and outgoing spam are a severe drain on the meagre available bandwidth and therefore impact developing economies relatively more than would be the case for similar volumes of spam in developed economies.

Costs

The costs of handling, sorting and delivering this e-mail to users' mailboxes are borne by the receiving ISP. Data provided below is the average estimate of the spam filtering costs incurred by Outblaze Limited, a large Webmail provider based in Hong Kong, China, that has over 40 million users around the world on domains such as lycos.com and operamail.com. The costs presented below are for filtering spam on just one of their mail server clusters – they have several such clusters around the world. Given that Outblaze hosts e-mail for over 40 million Webmail users, the problems created by, and costs of fighting spam are magnified, and become immediately more obvious.

The bandwidth cost that is presented below is an average estimate that has been prepared from the cost of hosting servers in a managed data-centre in various developed countries. These costs will be far higher in developing countries, especially in countries where the major form of international and even local connectivity is by satellite (for example, several countries in the interior of Africa and Asia, such as Nigeria and Nepal), rather than through surface laid / submarine copper and fibre optic cables.

It must be noted that salaries paid by ISPs to hire administrators and support staff for anti-spam and other operations will be lower in developing economies, but as a quick scan of these figures shows, that is not that much of a factor in the cost equation. It must be noted that all filtering technology used at Outblaze is based on and developed using freely available open source tools, so that the only cost is in hiring competent administrators and programmers to write and customise new filters. If licences for a proprietary spam filter had to be purchased, the costs would be correspondingly higher.

- Bandwidth costs = USD 600 / MB / month
- Bandwidth consumption for mail = 70 MB / day
- Incoming mail rejected as spam = 80%
- Percentage of accepted mail that is spam that gets past filters = 15%
- Monthly bandwidth cost of spam = USD 6 300
- Monthly storage cost of spam = USD 5 400
- Monthly salary expenses for mail / abuse administrators = USD 75 000
- Plus the costs of support for users upset at being spammed

That last item amounts to several hundred thousand dollars to a few million dollars a year at a large ISP in a developed economy, even with technical support outsourced to India or the Philippines. In fact, as

the cost of spam handling finally gets passed on to the ISP's users, up to 10% of a user's ISP bills may go towards combating spam and providing technical support for spam-induced problems.

Thus ISPs are faced with a large cost centre, rather than a profit centre, as a result of spam. The costs of receiving, storing and downloading spam, the opportunity costs of hiring administrators solely to do spam filtering, when their talents could be devoted to other tasks within the company, are all high. However, it is a necessary cost, due to the associated savings in bandwidth, server infrastructure, and most of all, in retention of customers who would otherwise shift their services to another ISP just because it offered better filters.

In addition to costs faced by ISPs, businesses would also be faced with costs to filter spam, costs associated with hiring administrators to deal with spam, and productivity and other costs associated with spam reaching end user e-mail boxes. For developing economies these costs may be relatively the same for large businesses as in developed economies. However, factors such as the high cost of software licenses, combined with the scarce knowledge resources in some developing economies may often mean that it is difficult to locate and hire well-trained mail systems and anti-spam administrators.

These problems get exacerbated for smaller businesses that may not be able to afford either licensed software or systems administrators, trained or otherwise. A common situation noticed in developing economies is that a consultant is hired to perform initial installation and configuration of the mail server, and to set up mailboxes on it, but further maintenance of the server (such as application of security updates) does not take place at all. As a result of these resource and staffing constraints, several businesses in developing economies tend not to use e-mail very much, thus losing what can be a powerful tool to boost communications and productivity. Several businesses that are not heavy users of e-mail, tend to use e-mail addresses provided by a free Webmail site like Lycos or Hotmail, or have their ISP host their mail server for them rather than doing this in-house.

Accountability for spam issues

ISP resource and organisational limitations

ISPs with lax anti-spam and security policies soon find that their network starts getting overrun by spammers.

Spam will form more and more of their incoming mail stream, thus making e-mail practically unusable for their users. Open relays, open proxies and trojan / virus infected machines on their network will become major spam sources.

This leads to saturation of the ISP's existing bandwidth and far higher expenses on buying new bandwidth, as they have to provide more and more bandwidth solely because they have to factor in bandwidth wasted by spam and worm traffic.

ISPs in developing economies like India, that have comparatively more bandwidth and adequate data centre facilities, may find themselves infested by spammer customers – not just local spammers, but, in several cases, spammers from developed economies. Spammers from the United States and Europe who find that they are *persona non grata* at ISPs in their region often decide to shift base to a developing economy, or outsource their operation to a local spammer. Obviously, those ISPs who accept to take spammers on their network in exchange for financial compensation lose out in the long term: despite the cash flow initially generated, they then see higher bandwidth and storage costs hit them due to the volume of spam increasing, while at the same time losing customers annoyed at the spam they receive and the likely slower connection they enjoy due to bandwidth being busy handling spam.

ISPs in developing economies are quite often quite hard to contact for a combination of reasons, some of which are briefly described below.

One major issue is inaccurate, outdated or incomplete "Whois"[1] for domains and IP addresses - IP addresses and domains are supposed to have complete and up-to-date records in the Whois database maintained by the domain registrars and Regional Internet Registries (RIRs). However, this is often not the case – this is something that RIRs and individual domain registrars are trying to correct, but the problem is widespread.

Local Tier 1[2] ISPs often do not sub-allocate (SWIP[3]) IP blocks that they allocate to their customers. That is, they do not explicitly register smaller blocks at the RIR as assigned to a particular customer and instead have one large omnibus record for all their IP space. In other words, the Tier 1 ISP does not modify the IP Whois records that they maintain in the RIR's Whois database to indicate allocation of a block of IPs to their customer. So, from an outside perspective, what is actually a conglomeration of smaller ISPs that buy bandwidth and lease IP addresses from a large ISP instead appears to be just the one large ISP. The small ISPs are not visible as the actual tenant of that IP address.

Another alternative to sub-allocating IP blocks to customer ISPs is to maintain a publicly accessible Referral Whois "RWhois" database of IP assignments made to their customers. While most large ISPs worldwide that do not sub-allocate IP blocks at the RIR level do this, even this is not a common practice among ISPs in developing economies.

Developing countries often have a single incumbent monopoly ISP, who is therefore responsible for providing Internet and e-mail services to the entire country. In all such cases, spam issues that would otherwise be traceable to various customers of a large tier 1 ISP – typically smaller ISPs or web hosts that buy bandwidth from them – can only be traced to the tier 1 ISP and no further. On top of this, 'worms' and other attacks can spread more easily to the whole country if there is a monopoly ISP / bottleneck, despite any advantages that a central gateway point normally offers for spam filtering.

Consequently, the Tier 1 ISP becomes the *de facto* point of contact for complaints about spam or other net abuse originating from, and for spammer sites hosted by all the customer ISPs / Web hosts under it.

A simple analogy would be the management of a large complex of apartment buildings that does not let their tenants publish their addresses and phone numbers in the city telephone directory (comparable to an ISP sub-allocating IP Whois records for its customers in the RIR maintained Whois database). Nor do they maintain a central directory of their tenants (comparable to operating an RWhois server).

So, any letters addressed to a tenant in this complex gets delivered only to the building management, which then has to contact the owner of the apartment and deliver the letter to him. Further, as this analogy has to apply to an ISP with spamming customers, when the tenant of an apartment is wanted by the police for an offence, they have to contact the building management and find out just where in the complex the man they want lives, rather than just looking up the directory and going straight to his apartment. As there are several hundred apartments in the complex, the apartment managers find all their time taken up with delivering mail, directing visitors and handling police requests for all their tenants, instead of publishing a central directory and letting postmen and visitors contact the tenant directly.

Quite frequently, neither the Tier 1 ISP nor their customers have a dedicated team to deal with spam issues, and do not even maintain postmaster and abuse accounts, which all sites that operate mail servers are required[4] to maintain. In addition, the ISP must assign staff who are reasonably fluent in English to monitor their postmaster and abuse mailboxes, as most of the spam complaints reaching them will be in

English. The reason why ISPs need to employ bilingual employees, who are fluent in both the local language as well as in English, on their abuse desk, is that ISP abuse desks will receive complaints from Internet users around the world, about their customers. This is in addition to complaints from the ISP's own users complaining that they are being spammed.

Abuse desk staff at an ISP will find themselves receiving, and having to reply to anywhere between several dozen to a few hundred spam complaints a day in English, depending on the extent of the spam problem they have on their network. The spam problem spans a wide variety of countries, so that the sender can be in one country, the source in another and the victim of spam in a third, entirely different country. A Chinese ISP may host an American spammer, who then spams the users of a Swedish ISP. The Swedish Internet users, and their ISP's abuse desk, will typically complain to the Chinese ISP in English.

Even ISPs that do maintain postmaster and abuse mailboxes are handicapped by the fact that they are forced to handle spam complaints for all their customers, because of their lack of transparency in IP sub-allocation, or because their customer ISP is unresponsive to spam complaints, so that these complaints get copied to the tier 1 ISP.

This leads to the ISP's postmaster and abuse mailboxes being flooded with spam complaints, severely taxing their staff's time and resources, so that spam complaints are often handled after a very long delay, if not simply deleted *en masse* by ISP's staffers who are overwhelmed and overworked.

Quite frequently, the ISP's staffers may be reasonably competent in systems and network administration, but are quite unaware of standard operating procedures, tools and techniques when dealing with spam issues, so that each spam issue that does get taken up for action is handled in an extremely slow and inefficient manner.

In addition, ISPs have been alleged to be quite willing to ignore spam complaints and continue to host a spammer, so long as the spammer continues to pay his bills (and possibly a premium on top of the regular rate for hosting), and, in certain cases, have been known to continue to give the spammer new IP addresses as his old addresses begin to get blocked. This is a trend that appears to be much more pronounced in developing economies that are starting to become a haven for spammer hosting, primarily because any foreign customers – frequently foreign spammers – are a regular source of hard currency for them, and they may even charge premium rates to keep the spammer connected.

A possible explanation could, of course, be that the ISP, if large, has several resellers, and the spammer merely moves his hosting to another reseller at the same ISP, without the ISP's knowledge. However, it does appear that some ISPs make a conscious decision to host known spammers, or are unwilling to face the loss of revenue caused by disconnecting a high paying customer, even though he may be a spammer.

It should be noted that these so-called "pink contracts"[5] are by no means unique to ISPs in developing economies. Large ISPs in developed economies have allegedly flirted with pink contracts, and in some cases, been exposed by whistleblower ex-employees and anti-spam organizations, gaining some rather embarrassing media attention in the process.

All these factors - lack of traceability and accountability in the Whois records, no standard operating procedure or trained staff to handle spam incidents, as well as the occasional pink contract, ensure that the spam problem at ISPs in developing economies tends to get out of hand.

As a result, e-mail and network administrators who are responsible for stopping spam at various ISPs, e-mail providers and corporate mail systems around the world, and the operators of widely used public "block lists"[6] of IPs and domains, such as spamhaus.org, may well elect to block large swathes of IP space,

or even block entire ISPs as a last ditch measure to stop spam originating from, hosted at or otherwise tracing back there, after complaints to the ISP have been ignored or perhaps addressed unsatisfactorily.

This is justified by arguments (or even facts) such as that spammers based on an ISP can generate more spam in an hour than the rest of the ISP's legitimate customers may send out in a whole week, and that it is much easier to keep track of a single block entry for a large chunk of contiguous IP space, aggregating all the individual blocks on IPs adjacent to each other that are sending out spam. It has also been observed that this kind of large-scale blocking may serve as a deterrent to stop ISPs from providing services to spammers, once they notice that large-scale blocks are affecting all the rest of their legitimate customers.

Whatever the rationale behind large-scale blocking, it is a fact of life that is all too familiar to most ISPs in developing economies and one that they sometimes tend to resent and in some cases, blindly lash out at, rather than attempt to remedy the situation that caused the blocking to occur in the first place.

An example is what happened when a Malaysian ISP got blocked, and its CEO wrote an article in a local newspaper; vehemently criticising the widespread spam blocking that was being targeted at the company. Soon after this, two detailed letters appeared in the newspaper, both pointing out that the company was hosting an international spam operation that was listed in public block lists, at that time (see http://www.jeffooi.com/archives/2003/08/internet_commun.php). The company immediately published a follow-up letter in the newspaper, declaring that they were proactive about spam, and then proceeded to terminate several spammers that they were hosting, and that were listed in the blocklists.

However, while negative publicity can be a powerful motivator for an organisation to redress problems, it is not a feasible or scalable approach to addressing long-term problems. ISPs must plan for and put in place systems for long-term mitigation of spam problems on their network, without which they have to potentially contend with negative media publicity, besides a poor reputation among their peers and the Internet community at large, This image problem, as well as the spam problem that caused it, triggers a vicious cycle of increased block-listing of the ISP, and increased spammer hosting and spam origination at the ISP. This could explain the long-term presence of ISPs in block-lists.

The situation gets even worse when the ISP that is blocked is an incumbent monopoly, as this has the effect of cutting an entire country off from e-mail access – though, to be sure, there is always the option of just using the blocked ISP to connect to the nternet, and then using a free Webmail service like lycos.com or hotmail.com for e-mail access.

A case in point is the blocking of Radiografica Costarricense SA (racsa.co.cr), a government-owned monopoly ISP in Costa Rica that got entirely blocked for 48 hours by the spamhaus.org blocklist in late 2001. Costa Rican newspapers extensively covered the reasons behind this block[7] (http://www.amcostarica.com/112301.htm). Some steps were taken in 2004 to filter out spam and block spammers, three years after their blocking incident hit the headlines and mainly because of the implementation of new government regulations.[8] http://www.amcostarica.com/080904.htm. It needs to be emphasised here that over-aggressive filtering is irresponsible and detrimental to the future of e-mail as a whole. ISPs, as a community, are ultimately responsible for delivering e-mail to their users and have the power to block e-mail. They also bear the responsibility for delivering wanted, non-spam e-mail to their users – mail from their friends and relatives, from mailing lists that they subscribe to, bills when they buy on an e-commerce portal like eBay, tickets that they have booked on line, while at the same time keeping out the huge tide of Unsolicited Bulk Email (that is, spam) from their users inboxes – mail that the majority of their users don't need and have not asked for, but which keeps getting sent to them and clogging their mailboxes.

The challenge of blocking spam while at the same time allowing non-spam e-mail is a fine tightrope that ISPs and spam filter providers walk, and they owe it to their users, and to the Internet community at large, to be unbiased, free and fair in their blocking policies. They must also be responsive to requests for unblocking, and must lift the blocks they have put in place as far as is feasible, when they can see that legitimate mail is being blocked, and that the ISP is making a good faith effort to keep their systems clear of spam and spammers.

It must be noted that there are several block lists available for people to use, ranging from professionally managed and widely used ones like Spamhaus and MAPS to extremist and illogical blocklist that list all IP addresses belonging to a particular country as spam sources.

A site that a blocklist lists as a spam source may also be a site that sends e-mail an ISP's users want, and expect to receive. Administrators at ISPs that use block lists as a guide to filter incoming e-mail to their users are similarly encouraged to make local exceptions (sometimes called "whitelists" as a counterpoint to "blacklists") to allow e-mail that their users want from block listed sources.

In the final analysis, it must be clearly seen that block lists, especially the professionally managed ones, should not be considered hostile to ISPs, even to ISPs that they block. ISPs who are faced with their IPs getting block listed must treat blocklist entries as the symptoms of a spam problem they have, and which they have to eradicate.

Effect on users

Costs

The cost of downloading all the spam that is received in a mailbox is borne by the user. Users in developing countries usually rely on dialup Internet access at home, or share access at cyber cafés with connections which are often slow and expensive, as they often pay by the byte for traffic that is downloaded. In addition, unlike many developed economies where competition has led ISPs and telecommunication service providers to provide Internet access packages which are not based on per minute usage charges, many developing economies still use per minute charging for dial-up access. As broadband develops and diffuses in these countries these cost impacts may change but the volume of spam traffic may also change to reflect the ability to send spam more easily to a particular geographic area, and due to the fact that increased penetration of broadband services means that more and more insecure and unpatched[9] home PCs come on line for several hours a day, and then get infected by viruses and spam emitting trojans.

The telephony infrastructure in developing economies is also inadequate and expensive, which means that someone who tries to login and download their e-mail may find their Internet connection keeps getting disconnected, and they have to make several telephone calls, and login to their ISP each time to get their day's quota of e-mail. This is an activity that would take a few seconds on a broadband connection – while on a dialup it may take up to half an hour of frustration and multiple redials. All this effort and expense is completely wasted when the user finds that the downloaded e-mails are to a large extent random spam or viruses. Furthermore, the amount of data carried due to spam encumbers the network and therefore slows connections.

Of course, there are other, sometimes less quantifiable but much more substantial costs faced by the user - corruption or destruction of data on PCs by a virus, mental anguish caused by spam with objectionable content, loss of life savings when a user falls for a scam that is e-mailed.

Business users in developing economies are also likely to face higher costs from spam than counterparts in developed economies. This is because connections to the Internet are more expensive, for example through leased lines, and technical assistance may be scarcer and therefore more expensive.

Software piracy and its impact on viruses that propagate through spam

Users in developing economies are particularly vulnerable to malicious spam and viruses as they often find that licenses for operating systems and for many antivirus programs are unaffordable. For example, a licensed copy of Windows XP costs USD 199 and a year's license for a popular antivirus program would cost USD 75. This is almost a month's salary for several PC users in developing economies. This often results in Internet users in developing economies using illegal pirated versions of Windows, and dispensing with such "added extras" as antivirus software. A recent survey[10] by the BSA of computer users in several developed and developing countries has shown this trend – users in some countries are quite likely to buy cheaper (and most likely pirated) copies of software that they see advertised in spam. Such software is not only difficult to keep updated because it lacks proper licences, it may also be a source of viruses, so that the buyer of such software is infected from the moment the software is installed on the PC.

It must be noted that people who use pirated software do not have access to security and antivirus updates. They are therefore forced to use a system that lacks critical security features, and has several vulnerabilities that are regularly targeted by viruses.

An interesting side effect of slow and expensive Internet connectivity in developing economies is that even users who have licensed versions of software are not very eager to download several MB worth of updates on a slow and unreliable 56kbps dialup, leaving it on the whole night and paying telephone and ISP charges on a per hour or even per byte basis. Their only alternative is to order a CD full of updates to be shipped to them.

By the time the CD reaches them, there is a high probability that their PC could have been already become infected and turned into a spam source sending out thousands of copies of the virus, as well as copies of spam advertising everything from pirated software to child pornography, all with the user's e-mail address, and that of friends listed in their address book, spoofed into the "from" address. Add to this the additional Internet connectivity charges users may have to bear because of excess virus traffic sent through their PC.

For the business user, a virus outbreak that leaves an office LAN filled with infected PCs that are connected directly to the Internet over an expensive leased line tends to have a harmful effect on the company's next bandwidth bill.

Education of users

Internet and e-mail users in developing economies are frequently unaware of basic Internet safety, or, as described above, they may be unable to practice basic Internet safety like maintaining a well-patched and upgraded system for various reasons.

Another major issue is "phishing" - credit card and identity theft targeted at users of banks and e-commerce sites. The impact of phishing is slightly less than it could be in developing economies because much banking and trade is carried out the old-fashioned way – offline, face to face or using letters / faxes etc., rather than over the internet. However, the risk is still there, and worsens every day. While there are sporadic attempts at educating users, mostly through newspaper articles, there appears to be little or no impact on the problem, so far. An added difficulty in developing countries is that most users tend to be less technically sophisticated, and less used to Internet fraud than people in developed countries, so that they

are more likely to become victims to scams that target gullible Internet users or encourage spam by purchasing products advertised by spammers, that are quite likely to be fake and/or hazardous to use.

Legislative and regulatory framework

Many developing economies have yet to consider adopting legislation against spam. In addition, many do not have consumer protection laws, computer crime, privacy or network security laws or regulations which could be used to take action against spammers. This implies that many of these countries are not only limited in taking action against spammers targeting their users but also against spammers using their countries as a base to send spam internationally.

Several developing nations, such as India, have laws that prohibit hacking, stalking or harassment over the Internet etc., but even then, the implementation of these laws is in the hands of the local police or other law enforcement organisations, who may be inadequately funded, ill equipped and poorly trained to keep abreast of cyber crime trends, let alone spam-related issues.

People pursuing anti-spam or any other Internet-related litigation are frequently forced to use a patchwork of other laws in order to build their case against the miscreant – such as tort law (breach of contract), trespass to chattel, criminal fraud, obscenity etc.

Meanwhile, unscrupulous e-mail marketers in developing countries take advantage of the absence of any valid law to confuse the issue, in an attempt to convince the people they are spamming that these e-mails are not spam. One such disclaimer, taken from the Web site of an Indian e-mail marketing company, is reproduced below:

> *Since India has no anti-spamming law, we follow the US directive passed by the 108th US Congress (CAN-SPAM Act 2003), which states that email cannot be considered Spam if it contains contact information, which all our email list does, and a remove mechanism.*

That disclaimer is quite a stretch, even in terms of the CAN-SPAM act – never mind the fact that US law is not applicable in India. Previous versions of this disclaimer used to mention the defunct HR 1618 Title III of the 105th US Congress – the so-called "Murkowski Bill", which was a bill proposed in 1998 by Senator Frank Murkowski of Alaska, one of the first anti-spam bills that required that spam be labelled as such.

This bill lapsed without passing into law after that session of congress ended, but became quite famous until about 2001 or so, because spammers kept including disclaimers in their spam, stating that their spam was compliant with the Murkowski "anti-spam law". Such disclaimers soon began to be used, for example a variant as used in India in 2001:

> *Since India has no anti-spamming law, we follow the US directive passed in Bill.1618 Title III by the 105th US Congress, which states that mail cannot be considered spam if it contains the following information*

In the OECD area 23 countries have implemented spam legislation whereas to date only a handful of non-OECD countries have appropriate legislation in place. Nevertheless, the corpus of existing legislation provides a ready solution for countries that wish to take action against spam. However, unlike many developed economies, developing countries often do not have supporting institutions which are necessary to implement legislation effectively. The OECD "Spam regulation compendium" should also provide a useful central source for developing countries to use, in deciding how to craft an anti-spam law, taking into account local characteristics, and balancing the right to privacy and freedom of expression with the need to

deal with spam. Enforcement is in particular difficult in developing economies given lack of technical expertise in the area of enforcement.

Another issue is that of increased co-ordination between different anti-spam regulators, even within the same national jurisdiction. Spam being such a multifaceted issue, there is a regulatory role for several regulatory agencies responsible for consumer protection and telecommunications, which are in charge of tackling spam. In some countries, various other regulators are involved, for instance data protection authorities. At the same time, most regulators on their own do not have the legal, technical, human or financial resources to effectively handle spam complaints. To ensure that spam is most efficiently tackled, co-ordination and joint work must therefore become normal practice nationally.

Additionally, care must be taken that ISPs do not abandon all effort to proactively crack down on spam or other net abuse complaints, in an effort to cut down on compliance costs or for whatever other reason. Stray incidents of such behaviour are beginning to become apparent at several ISPs, and may well materialise in other countries that have, or implement strict data protection regulations.

For example, here are two auto responders received in response to abuse complaints, from different EU-based ISPs:

> ***Belgium***
> *Moreover, Art. 18-21 of the law of 11 March 2003 specifies that when providers only carry data, which is the case with hacking, they are not required to take any action. Complaints must be forwarded directly to the competent authorities. We will therefore not be able to identify or take action against our customers in the event of hacking complaints. However, you may file a complaint with the legal authorities or the Computer Crime Unit if you wish.*
>
> ***Germany***
> *Dear user,*
>
> *…. has received your message. Unfortunately it is not possible for us as a provider to take legal measures preventing any further abuse.*
>
> *In accordance with the actual legal appointments for privacy ….l renounces on the storage of IP addresses since the 1st of September 2004 by supply of telephone services.*
>
> *If you want to trace the abuse please refer to the police. In founded cases like the suspicion of an offence, we can save IP addresses on directive of the responsible authority for criminal prosecution to persecute these cases. Therefore these organs have to apply for a strict tracing progress and justify it plausible.*

Data protection laws are increasingly being interpreted as a mandate to ISPs not to store any user information such as IP addresses that might be used to track or trace users' online activities.

While the goal of preserving users' privacy is laudable, measures such as this can also be interpreted as preventing the ISP, on receipt of a complaint about net abuse (spam, hacking or similar activities) from one of their IP addresses, from actually being able to find out which customer was logged on to that IP address at the time the abuse occurred. So, by inference, they cannot locate the source of the net abuse - the actual malefactor, or possibly their customer whose PC was compromised and abused to send out spam or participate in a DDoS attack.

ISPs are thus motivated not to log or trace spam activity from their network without a court order, to comply with data protection laws.

Therefore, any planned anti-spam or anti-net abuse laws must also make it easy for the ISP to track and trace information about their users, with strict non-disclosure norms that comply with data protection and other privacy legislation. Such laws must not be allowed to be interpreted as a mandate for inaction. They must be implemented in ways that safeguard the privacy of users, while at the same time allowing the prompt tracing and removal of sources of net abuse, and quick enforcement of anti-spam and anti net abuse policies by the provider.

If ISPs decide that they will only begin tracking an abuse issue upon reception of a court order or other requests from law enforcement authorities, the time taken to trace a reported spam or net abuse issue increases exponentially.

The complaint has to be received and processed by law enforcement, following which they have to locate a contact at the ISP from whose network the abuse originated. The law enforcement body would then forward the complaint on to their point of contact at the ISP, quite frequently the ISP's legal department. The complaint then has to be routed internally within the ISP to reach the appropriate team (abuse / postmaster or systems administration) that deals with these cases.

By the time all this takes place, the spam / DDoS attack or other network abuse will have long been concluded, or will have achieved its objective. The spammer will have sent out all his spam, and the target of the DDoS attack will already have suffered a massive disruption of their services. Further, all evidence of the spam, hacking or DDoS may well have been erased by the malefactor, and he may shift to a completely different IP address, so that it will be difficult to trace him once a request to do so has been received. This is a worrying trend, and future anti-spam / data protection legislation has to address these issues.

Anti-spam and other cybercrime related laws must also provide a comprehensive safe harbour provision for ISPs and network providers that holds them harmless from the consequences of an illegal act committed by one of their users, and allows them a reasonable and well defined amount of latitude in investigating spam or other net abuse issues.

An illustration of what can happen if the concept of safe harbour is not built into such a law is the recent case in India where the CEO of baazee.com, which is an Indian auction site now owned by eBay, was arrested as a publisher of obscene material, after someone advertised a pornographic CD for sale on the Baazee website. Similarly, with the current IT act, there is a good chance that the CEO of an ISP may be arrested if somebody misuses e-mail and Web hosting services that the ISP provides to operate a scam. The Indian ministry of IT is currently in the process of setting up a committee with representatives from industry lobbyist associations, the legal community, law enforcement and the local telecom regulator, in order to suggest amendments to the law that will introduce data protection and privacy wording, as well as a safe harbour guarantee that will avoid future arrests such as the one of baazee.com's CEO.

ACTION REQUIRED BY DEVELOPING ECONOMIES AGAINST SPAM

Putting in place technical solutions

Technical solutions to spam, though not perfect, are possibly the best suited to obtain fast results in mitigating the impact of spam on the user, but not necessarily reducing the volume of spam. The best possible solution that can be hoped for is that large amounts of spam that are sent to the ISP's users are rejected at the ISP's mail gateways and prevented from entering the ISP's network. ISPs that do even basic filtering of spam on their MXs (Mail Exchangers, servers that handle inbound e-mail traffic for a domain) will see a tremendous drop in spam that reaches their customers' mailboxes – about 50% of the incoming spam can be filtered out using a very basic and easy to deploy set of filters. Needless to say, filtering out the remaining spam gets harder and harder.

Purchasing licenses for spam filtering software is not very expensive now, even for ISPs and networks in developing countries. Alternatively, such ISPs can outsource their spam filtering, or their entire e-mail service, to third party providers of spam filtered e-mail such as Brightmail, Postini and Outblaze.

Further, ISPs in developing countries must actively explore some way of making secure computing software easily available to their users. For example, they can distribute a current set of Windows security updates and a trial version of an antivirus program with the setup CD they distribute to new users.

They can also aggregate the demand for spam filtering and antivirus software that exists among their end users, to distribute licenses for spam and virus filter software at cheaper costs, taking advantage of bulk discounts from security vendors.

It must be noted that end user spam filtering software that runs on the e-mail user's PC and filters incoming e-mail for him after it comes in, is not an efficient solution by itself – the spam has already been delivered to the user's mailbox, and the ISP has already borne the costs of receiving and storing this spam. However, e-mail users must be encouraged to install such software on their PCs as a second line of defence. Desktop anti-spam programs supplement the spam filtering that ISPs deploy on their mail systems, so that any spam that slips past the ISP's defences is quarantined by the anti-spam program, thus providing better protection to the user.

Further, economies of scale make it much more efficient for an ISP to filter spam across the board on its mail system, and stop spam from entering all their users' mailboxes, rather than requiring all its users to download and install a spam filter that then does this on each user's PC. ISP-wide spam filtering also lets an ISP track "trends" in spam so that a persistent spam source can be blocked, or addressed by other means, such as those detailed in the section about co-operation between ISPs.

Open Source software solutions

In developing economies there are several local and international initiatives that encourage the use of Free / Libre and Open Source Software (FLOSS) alternatives to expensive legal versions of non-free software. FLOSS software is free to download, use and customise – several of these customisations are usually released in the public domain and, quite frequently, integrated into the next release of the software.

FLOSS software thus has a broad base of developers around the world, who continuously write new features and improve the security of existing features of such software.

FLOSS operating systems like Linux are widely used and recommended by e-mail and Internet providers around the world as robust, secure and scaleable server platforms. Linux, as well as other FLOSS operating systems such as FreeBSD, are used to run some of the best mail server software (again FLOSS licensed) in the world, such as Sendmail, Postfix and qmail. These are widely used by some of the largest e-mail providers in the world. For example, Yahoo uses qmail, Outblaze uses Postfix, and AOL extensively uses a heavily customised version of Sendmail.

In addition to this, there are some excellent FLOSS anti-spam utilities available, both for mail server operators and for users. Some of these, which are widely considered to be best of breed, are Spamassassin and ASSP (Anti Spam SMTP Proxy). ClamAV is a popular and well-written open source antivirus filter that can be seamlessly integrated into several popular anti-spam filters and mail servers.

The effective license cost of these operating systems and utilities is zero – compared to the high cost of buying and licensing proprietary server operating systems, mail servers and anti-spam software. This makes FLOSS software an extremely useful tool for ISPs in developing economies.

Besides migrating their server infrastructure to Linux, several ISPs, universities, corporations and Internet cafés have set up Linux PCs for their employees and users, both to save on site wide licenses for Windows or other non-free operating systems, and to cut down on the cost of fighting virus infections on PCs.

Several Internet users who may not want to switch from Windows can be encouraged to switch to alternative, freely available e-mail, browser and office suite programs such as Mozilla and Open Office instead of Internet Explorer, Outlook and MS Office. A welcome side effect of such a switch is that these programs, less popular than their mainstream counterparts, are far less regularly targeted by viruses.

Formation of CSIRTs and CERTs

Computer Security and Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs), at the organisational, national and regional levels help organise an effective and efficient response to individual computer security incidents, widespread security vulnerabilities (such as the spread of a worm or virus) and incident co-ordination throughout the region.

They thus serve as a region-wide clearinghouse of information about computer security related incidents, and can bring together several parties (including their counterparts in other economies) whose joint efforts may be required for damage mitigation and control.

Another important role of CSIRTs / CERTs is education and training of ISP personnel, systems and network administrators to raise awareness and encourage development of best practices on computer security issues.

Some developing countries such as India do have CERT teams in place, but their role needs to be expanded, and regional ISPs made more aware of the utility of having access to CERT-provided alerts and security co-ordination. Those developing countries that do not have CERTs should definitely consider setting up CERTs. Several CERTs around the world are organised by university computing departments and government IT research labs that have the know-how and facilities to carry out extensive research into computer and network security issues. CERTs work in close co-ordination with ISPs and network administrators in their area of coverage.

Training of ISP personnel in security and spam handling

ISP personnel in developing countries are, quite often, comparatively less skilled, not because of an actual lack of knowledge, but because they may not be as well trained in issues specific to practical systems and network administration, and tend not to remain abreast of current trends in their field of work, such as by participation in mailing lists, newsgroups and online discussion forums on these subjects.

Administrators can also benefit from attending network operator groups (a series of workshops, tutorials and conferences that teach practical aspects of systems and network administration, and bring ISPs together with their peers from other ISPs, and with engineers who have designed and built the equipment (routers, operating systems etc), that they use to run their network.

Network Operator Groups (NOGs) are available for several regions, and hold regular meetings at various cities in these regions. Some of these are listed below, along with the regions they cover (typically aligned along RIR jurisdictions):

NANOG (North America) – http://www.nanog.org
APRICOT (Asia Pacific / Oceania) – http://www.apricot.net
RIPE (Europe, Middle East, North Africa, parts of Asia) – http://www.ripe.net
AFNOG (Africa) – http://www.afnog.org
SANOG (South Asia) – http://www.sanog.org

Most of these network operator groups organise tutorial and conference sessions on systems and network security and anti-spam operations, taught by people who are acknowledged by their peers as experts on the topics on which they are presenting papers or on teaching. These NOG tutorial and conference sessions are heavily subsidized by corporate sponsorship, and include fellowships that cover the cost of deserving applicants' registration and accommodation. The tutorial and conference papers that are presented at NOG meetings serve as a valuable online reference source for practicing network and ISP administrators.

RIRs such as APNIC and RIPE etc. also hold frequent training programmes and "hostmaster consultations" at several major cities in their areas of coverage. Venues for RIR training programmes include meetings such as SANOG and APRICOT, or other events such as those organised by local ISP associations. At these meetings, administrators can learn best practices about IP assignment and other issues that the RIR deals with, directly from the RIR personnel, and also approach them for discussions on specific issues that they face in relation to IP management, reverse DNS, Whois record updating and sub-allocation on their networks.

The NOG meetings have another advantage in that they provide a common meeting ground where the regional RIR, CSIRTs and other organisations concerned with spam, network security and ISP operations in participating economies can hold their own meetings and training programmes, or organise tutorials and conference tracks for the NOG.

For example, APCAUCE (http://www.apcauce.org) organises regular anti-spam tutorials and conferences at APRICOT and SANOG. Not for profit organizations such as the US-based NSRC (Network Startup Resource Center, http://www.nsrc.org) and PCH (Packet Clearing House – http://www.pch.net) help teach systems and network security, efficient routing techniques and other subjects relevant to ISP operations.

However, there is a major issue that has been observed in several developing countries – ISPs there are under staffed, and under funded – and typically reluctant to let their network administrators take a few

days off work to attend a conference, especially if the conference is in a foreign country, as the conference fees, airfare and mission costs and obtaining foreign currency, can be expensive. For example, if a typical ISP systems or network administrator in India were to fly to Malaysia or Singapore – both less than three hours away by air, to attend a network operators conference, he would expect to spend at least two or three months salary in airfare, room and board and conference attendance fees.

Add to this the fact that citizens of most developing countries have to obtain a visa for international travel, whereas most developed countries have reciprocal visa agreements with other country, that allow their citizens to obtain visas on arrival, or do not require visas at all for short term trips.

Given the expenses involved, quite frequently the ISP elects to send someone from senior management to attend the conference. As the issues being taught and discussed at the event are typically more relevant to practicing systems and network administrators rather than to management, these attendees do not derive all that much benefit from attending the event.

Thus, senior management will not be able to take back enough knowledge from the conference, (where one of their more technical colleagues would have derived maximum benefit from the event), to apply effectively at their workplace, and to teach their colleagues. It has often been observed that people who attend and participate in such a conference typically, if they can find funding for it, are quite willing to volunteer to help teach the skills they have learnt at subsequent conferences.

All this contributes to the outreach of the conference, but this is not enough, especially given the situation in developing economies, where ISPs are cash strapped and may elect not to send their administrators to such conferences.

The solution to this is to increase the penetration of such events. Both industries and governments in developing economies must actively work to ensure that international systems and networking conferences come to their countries, so that administrators at local ISPs will not have to travel long distances to attend one of these meetings.

For example, APRICOT 2004 was extensively supported by the Malaysian Ministry of Communications and Multimedia, and hosted by PIKOM, an industry association of ISPs and Internet firms in Malaysia. At the same time, the materials for such conferences should be shared as much as possible, for example, through centralised Web sites or portals.

Anti-spam policy setting and enforcement for ISPs

ISPs must strive to discourage spammers from abusing their services to send out spam. Unfortunately, there is a strong perception among at least some ISPs that anti-spam policy enforcement teams are cost centres rather than profit centres, and that customers, even spammers, are valuable sources of revenue.

This leads to a strong tendency among ISPs not to disconnect spammers, and to ignore complaints, until it is much too late, and the ISP's mail servers are being blocked by dozens of large ISPs and block lists around the world. The ISP may then realise that their hosting of spammers is causing them more trouble than the revenue that spammers bring in is worth, and finally take action.

Training administrators in spam filtering and network security is a good first step to stop spam from coming into an ISP's mail servers and to its users' mailboxes. However, the other side of the coin is “outbound spam” caused when the ISP's users are spammers.

ISPs who wish to take action against spammers on their network must have a strong anti-spam policy in place, and make it part of the “terms of service” or “acceptable use policy” document that a user must sign or otherwise agree to (for example, by clicking the “I Agree” button at the end of a page full of terms and conditions) when he signs up for the ISP's services.

An Acceptable Use Policy is in the nature of a contract between the ISP and its user, and the ISP may reserve the right to unilaterally terminate the contract and cease providing services to a customer who, it deems, has violated any part of its Acceptable Use Policy.

Even if the country the ISP is based in does not have an anti-spam law, the ISP may elect to mandate in its Acceptable Use Policy that its customers must not send unsolicited bulk e-mail (otherwise known as spam), and must not use their network to facilitate spam in any manner, such as hosting a Web site that is advertised by spam that may originate from elsewhere. The ISP can then take action to deny services to a spamming customer, citing breach of contract as the reason. A useful resource that ISPs looking to write a new anti-spam policy can refer to, is a compendium of ISP Acceptable Use Policies maintained by Spamhaus, and available at http://www.spamhaus.org/aups.html.

Spammers often look for smaller ISPs without adequate acceptable use policies, especially where issues such as poorly maintained Whois records and IP ownership data means that complaints get directed to the abuse staff of a much larger ISP which is several levels upstream from the small ISP. So, the spammers find that they have a lead time of several days at the same small ISP during which their website or spam sending server remains online. If and when the smaller ISP is forced to terminate them, the spammer can simply sign up for the services of another small ISP, that may have its servers co-located in the same large ISP's data centre, so that the spammer simply has to relocate his servers across a room in order to get them connected to the Internet again,

International co-operation, and the role of regional organisations

In the fight against spam as for other Internet issues, it is essential that we combine the relevant skills of various bodies to best effect, to maximise success.

Action for international co-operation could usefully take place through the relevant regional organizations, public and private, successfully addressing problems that may be common, or unique to several countries in the region.

At a regulatory and government level, much can be achieved by regional organisations like ASEM or APEC, as well as the ITU and with inputs from ISPs, eminent experts in the field of systems and network security, and anti-spam organisations.

International co-operation on an ISP to ISP level

ISPs in developing economies must integrate themselves further with their peers in other economies. This is best done when they actively attend NOG meetings in their region, and participate in NOG-related activities such as BoFs (Birds of a Feather sessions) and SIGs (Special Interest Groups), informal discussion sessions at which people get together to talk about topics that especially concern them.

Another excellent method for ISP administrators to get in touch with their peers around the world is to use the INOC DBA phone system (http://www.pch.net/inoc-dba/) - a closed VOIP phone network that directly connects senior network administrators at different ISPs and network providers around the world.

Besides all this, one of the easiest and most essential steps that ISP staffers and management must take is to join and actively participate in mailing lists and discussion forums that are targeted at the ISP and

network administrator community. There are several such mailing lists that discuss spam, as well as issues such as security, network administration, ISP policy etc, that have a direct or indirect bearing on the spam issue.

Some of these lists include:

- The Spam Prevention Discussion List – http://peach.ease.lsoft.com/archives/spam-l.html which is a popular, but high volume mailing list that is read by systems and network administrators, and citizens concerned about the spam issue, from around the world.
- APCAUCE Discuss List – http://www.apcauce.org/mailman/listinfo/discuss/
- NANOG-L - This list, as well as the lists of other regional NOGs such as SANOG, are set up to discuss network operator issues – mostly concerned with networking and routing rather than with spam. Indeed, spam is off topic here, but several aspects of networking and security that have a direct bearing on spam are not – http://www.nanog.org
- Full Disclosure - http://lists.netsys.com/mailman/listinfo/full-disclosure is an excellent source of information and early breaking news about systems and network security issues.

ISP associations in developing economies must be prepared help member ISPs deal with spam issues, and work out ways to ensure mutual assistance in fighting spam. ISP associations are also encouraged to develop joint codes of conduct and draft acceptable use policies that can be used as a guideline for policy setting and enforcement by member ISPs. For this, they can seek assistance from APCAUCE, which holds regular conference tracks where ISPs from developing economies in the region can meet their peers from ISPs in other economies, blocklist providers and anti-spam technologists, who can help them, discuss and draft viable anti-spam policies.

Larger ISPs can also invite distributed content providers like Akamai to set up a cluster at their data centre. Akamai provides ISPs around the world with fast, "local" access to several major websites such as Google and Yahoo. More germane to this paper, the websites of Microsoft – including their Windows Update site, as well as the sites of several antivirus and security software vendors, are "Akamaized" - available over Akamai. This gives the ISP's users faster local access to security update and antivirus sites, so that they can quickly download security updates and anti-spam software. Akamai clusters can benefit a larger number of ISPs in the country if they are collocated at "Internet Exchange Points", sites where ISPs from around the region can interconnect with each other.

International co-operation at an industry and end-user level

Businesses must reach out to ISPs and ISP associations, associations of computer users, such as local PC user groups, as well as international organisations such as ISOC that have a worldwide presence and a focus on several ICT issues that are substantially congruent with other stakeholders in this issue. Businesses must also reach out to the user community, directly as well as through other organisations that can potentially reach out to Internet users in the country. The focus of such efforts must be to educate and empower users, and to sensitise them to issues that affect their well being on the Internet, while at the same time making their Internet experience much more productive for them.

First and foremost, vendors of operating systems, antivirus and security software can work with ISPs, chambers of commerce and user associations to provide easier access to secure computing facilities, such as licensed antivirus software and regular security updates. This is especially necessary in countries that

have an active grey market that sells non-branded PCs, which, as mentioned earlier in this paper, often get shipped with insecure pirated software. This has a twofold effect – a second line of defence for the user against spam and viruses, as well as, in the long term, a significant drop in the amount of viruses and spam originating from compromised PCs and workstations.

ISPs must co-ordinate their spam filtering efforts with other industries such as hotels, airlines and banks that have extensive e-commerce operations and routinely use e-mail as an essential tool in their business model, in order to reach out to potential new customers and keep in touch with existing customers. Such companies typically send out large volumes of -email a day – newsletters, bank statements, billing invoices for online transactions etc. Especially in the case of large and reputable companies that use e-mail extensively, the last thing they want to do is to spam, or be considered spammers and subject to the same filtering as spammers.

It must however be noted that spam is not an issue of content – it is an issue of consent and permission, the right of a user to determine what he wants in his mailbox, and to explicitly request being added to an e-mail marketing list rather than having the marketing content forced on him. Legitimate companies that send out high volumes of e-mail must be careful not to send out spam, and to adopt an opt-in model for their mailing list management so that the chance of their sending out unsolicited bulk e-mail *(i.e.* spam) is minimised. They must therefore co-ordinate with ISPs, and with their marketing partners, to ensure that they do not send spam, and that e-mail that the ISP's users actually want to receive does not get trapped by the ISP's spam filters.

Chambers of Commerce, and nationwide associations of chambers, can make ideal venues for co-operation between ISPs and the e-mail sending industry, especially as all stakeholders in the spam problem – senior executives from the industry, ISPs, regulators, and law enforcement – tend to be closely involved with chambers of commerce either as members or as regularly invited speakers at previous chamber of commerce seminars.

Technically aware Internet users can group together to form local PC user groups, which can coordinate with end user groups in other cities as well as other countries. Internet users can also join international organizations such as ISOC, so that they can organize education campaigns about spam, drive efforts to implement anti-spam laws, and on a personal level, help people in their immediate area about secure computing, and help them cope with and filter out spam in their inboxes.

Legislative and regulatory framework to deal with spam

Several countries have already called for the development of an international framework to fight spam. Some have even suggested the signature of a ‘Global MoU’ on spam, and possibly, in the future, something structured on the lines of the Berne Convention or the Geneva Convention. However, such instruments will take a very long time to put in place, and moreover would be rendered meaningless if not backed by a strong legislative and regulatory set of anti-spam measures at the national level, which would then allow international co-operation to be effective.

Therefore, countries that have not done so yet must expedite the implementation of a comprehensive legislative and regulatory framework to deal with spam, as well as associated computer crime issues, such as hacking, forgery of e-mail headers or other information, etc.

Adequate data protection measures must be put in place, along with anti-spam legislation, in order to protect the privacy of users, and reining in overzealous marketers who share user data with each other for marketing purposes, without the user's consent.

The EU Data protection directives, the Australian anti-spam law and their associated regulatory and enforcement mechanisms are excellent examples of such laws.

These legislative and regulatory measures must be backed by a well trained, equipped and funded enforcement arm that is capable of investigating the often complex issues associated with spam and computer crime, and proceed to take action against offenders.

Furthermore, there is broad consensus in the OECD that a liberalised regulatory framework for electronic communications and telecommunications in particular, is advisable for the long-term benefit of users and of the network. This is true in relation to spam: a liberalised ICT regulatory framework would allow market entry for global ISP networks with large R&D capabilities or for local players affiliating with them. This would encourage transfer of information security capabilities, knowledge and skills helping in expanding the knowledge infrastructure.

User education

Massive and widespread public education and awareness campaigns, using simple and easy to understand material such as cartoon strips, posters and ads will be needed, preferably in the local language, as not many Internet users in developing economies are likely to be comfortable with English. For example, the Dutch government teaches password security and elementary protection against hackers using a Donald Duck cartoon strip, and the Japanese government educates teenagers against premium rate call-back scams using Japanese language comic strips.

Several local newspapers do carry articles on what not to do with e-mail that arrives in their inbox asking them to click on an attachment to see a Britney Spears picture, and warn users that Microsoft will not send them e-mail asking them to install “security patches” that turn out to be viruses. In any case, a much more widespread education campaign will be needed, as will the adoption by ISPs of strong anti-spam and antivirus filtering systems.

E-mail users in developing countries may also not be aware of the ethical issues surrounding spam, and may think that spam is just the usual barrage of ads for pornography and assorted scams that they keep receiving in their e-mail.

They have to understand that spam is unsolicited bulk e-mail, and learn the principles of ethical e-mail marketing. This will help them refrain from sending out spam themselves, advertising legitimate products or businesses like auto repair shops, holiday resorts and restaurants. Such spam is quite often in a local language (Chinese, Korean, Russian, Hebrew) to people who are not even in the same country, and cannot speak or read a single word of the language the spam is in.

Such an education campaign will help suppress a thriving local spam industry, where people advertise e-mail marketing services. Such services typically sell CDs with “ten million e-mail addresses”, all of dubious provenance, and most of which do not exist at all, having been randomly generated by the spammer. These CDs also ship with bulk mailer software that may forge headers and abuse open relays and proxies to send out spam. This may make users of such spam software unknowingly violate local laws against computer crime and hacking, even if there are no specific anti-spam laws in their country.

As ignorance of a law is not normally regarded as a valid excuse for breaking the law, this may result in innocent people, whose only crime is that they believed the glib claims of a spammer and wanted to promote their business on the Internet, go to jail or have to pay heavy fines.

Developing countries have a major advantage when it comes to running education and awareness building campaigns, due to the way people access the Internet: often, users have limited Internet access at

home, so they connect to the Internet at work or school, or use one of several commonly available community access points, such as cyber cafés or public libraries.

Targeting educational initiatives at such locations makes it possible to disseminate leaflets, screen films etc., which teach basic Internet security and anti-spam principles to a large number of users at a time. This makes it easier to localise/centralise information and education materials at these community access points, to reach a maximum of users through a single outlet. User organisations such as PC user groups and ISOC can also co-operate with ISPs and businesses to maximise the outreach of educational campaigns, by co-ordinating the campaign at a state or national level.

Education efforts must emphasise and highlight localised spam issues such as cases where a local business acquires a list of e-mail addresses of people in their city and then sends a marketing pitch, which may in that country be considered as spam. Knowledgeable end users, user organisations that are focused on spam and ICT issues can talk to reporters and run a story on spam, citing the business' spam as a violation of privacy. They can also co-operate with local ISPs and businesses to organise educational campaigns, and also to address localised spam issues. This will influence increased media coverage of spam issues with a local emphasis, so that such issues can be promptly addressed by businesses. The negative image that spam currently has will make local e-mail marketers realise that media reports about their sending out spam may not be viewed in a positive light, and will motivate them to bring their e-mail marketing efforts into compliances with international best current practices such as opt-in e-mail, proper unsubscribe mechanisms and the respect due to user privacy.

Another option they have is to file a lawsuit or perhaps a public interest petition, pleading that privacy and anti-spam legislation be enacted in the country, to prevent users from receiving spam. For example, a lawyer in India recently sued several local banks and insurance companies for repeated telemarketing calls to his cellular telephone, despite several requests from him to take his cellular telephone number off their marketing lists. He further sued his cellular phone provider for allegedly releasing personal data about him to the telemarketing firms, as well as not doing anything to block or stop the telemarketing calls. Filing a similar lawsuit against spam, and circulating petitions requesting that anti-spam legislation be enacted will help build up popular support for better anti-spam regulation, and also make local businesses and marketing firms aware of the fact that spam is not an acceptable or a legal marketing tactic. It will also attract media attention to local spam issues – attention that spamming businesses may prefer to avoid.

WHAT DEVELOPED ECONOMIES CAN DO TO HELP

Facilitate industry co-operation and anti-spam workshops

Developed economies should help facilitate industry level (ISP to ISP) co-operation with developing economies. The goal of this effort is to bring together ISPs from developed economies, such as AOL, Outblaze and Demon Internet (to name a few) that have considerable experience in anti-spam operations and help them share their knowledge with ISPs in developing economies.

Steps must be taken to facilitate the regular organisation of a round table meeting, real or virtual, of ISPs from developed and developing economies, along with other stakeholders in the anti-spam effort, such as blocklist maintainers, spam filter developers, anti-spam technologists such as ASRG members, etc.

At such a forum, ISPs from around the world can get together to discuss issues of mutual interest, such as spam blocking and blocklisting, offshore hosting of spammers, "botnets" of zombie / trojan infected computers and phishing from both technical and policy perspectives.

This is a much needed step, as most such conferences so far have been on geographical lines – EU, Asia Pacific, North America etc., while spam is an international problem. This will ideally be a web based conference, in order to ensure maximum participation from around the world without putting people to the expense of international travel. As already discussed, factors such as financial constraints and visa requirements tend to limit the participation of actual stakeholders in the spam issue in international conferences that involve physical face to face meetings.

Source funding to NGOs that train developing economy ISP and network administrators

There are several not-for-profit NGOs that are focused on training systems and network administrators from developing economies in key operational issues like systems and network security, spam filtering, deployment of secure open source mail servers as alternatives to pirated software, etc. These NGOs also help source donations of old hardware (PCs, servers, switches, routers, satellite connectivity equipment ...) to help provide Internet connectivity to developing economies that lack Internet access.

Case study 1 - The Network Startup Resource Center – http://www.nsrc.org

The NSRC helps source donations of software, hardware, Internet connectivity etc. to help ISPs and organizations in developing economies get started on deploying secure and efficient Internet access at the lowest possible cost.

Case study 2 - The Packet Clearing House – http://www.pch.net

PCH helps developing economies optimize their scarce Internet connectivity by helping them build "peering points", where local ISPs can interconnect their networks, ensuring that traffic between local ISPs remains local, routed via the shortest possible path between two ISPs rather than taking a roundabout route through international connectivity links. Local traffic getting routed through international links is all too common when ISPs in a country don't peer with each other, and leads to Internet access within a country becoming slow, and drives up bandwidth costs.

As mentioned in the section on improving international co-operation among ISPs in developing and developed economies, PCH also maintains the INOC-DBA closed VOIP telephone network, which allows participating ISP administrators to pick up an INOC-DBA phone and talk with their counterparts at other ISPs around the world.

Providing grants to these NGOs or otherwise giving them access to donated software and equipment will be an effective method of helping developing economies, as these NGOs have the most experience in deploying anti-spam filters, secure systems and networks in developing / under-developed economies, often having to start from scratch or make considerable improvisations to take into account primitive local conditions such as a fluctuating power supply and extreme temperature conditions.

Work with developing economies to educate people on spam and security issues

ISPs, governments, banks and e-commerce providers in developed economies such as Japan, the Netherlands and the United States have considerable experience in educating Internet users on the dangers they face because of spam, phishing, insecure computers, viruses, as well as scams such as Nigerian scam letters, pyramid schemes and porn dialler programs that trick users into installing software that will make their PC's modems dial expensive international phone calls to access pornographic content.

This last problem – porn dialler software – is an issue quite like the premium rate call-back scams that are perpetrated on mobile phone users. Regulatory bodies in the United Kingdom and elsewhere have been cracking down on dialler scammers, who often induce people to download their diallers using porn spam, spyware that hijacks PCs and downloads diallers, or pop up advertisements for porn sites, etc.

UK experience suggests that when possible, a self-regulatory or co-regulatory body, managed by industry with government backing, often proves to be the most effective way of dealing with such abuses: this is especially true as industry is generally keen to maintain a reputation for providing high quality service, and is the best equipped with technology and personnel to tackle misuse and block miscreants. The authorities have generally remained in a supportive role, extending the necessary basic regulatory support, while relying on industry to ensure that their sector remain fully trustworthy.

However, regulators and ISPs in developed economies will need to co-ordinate further with local telecommunication service providers, as well as with telecommunication service providers in small, remote countries that are used by porn dialler scammers, in order to eradicate this menace. It must be kept in mind that several telecommunications and ISP providers who are suddenly faced with problems such as these are not very well trained or equipped to adequately resolve them, so that their users become easy prey for such online scams.

In 2004, members of the EU, through the CEPT regional grouping in ITU, have successfully pushed for wording in ITU's Telecoms standards resolutions so that all ITU Administrations are advised when

they are the subject or recipients of such misuses, and to spread best practice on how to deal with 'auto-diallers'.[11]

National authorities now need to implement this and other proposed anti-net abuse measures in a sensible and speedy way, ideally co-ordinating with regional CERT teams, ISPs and other expert stakeholders in the issue, so that any net abuse situations that arise are quickly dealt with, and any potential abusers blocked, before the abuse begins to cause widespread damage.

Helping developing economies with anti-spam legislative and regulatory frameworks

OECD countries have already organized in the Spam Task Force to put together a 'Spam toolkit', which will include a 'Spam regulation compendium' that will exemplify how to devise a spam law, and refer to existing structures. The OECD Task Force hopes that this toolkit will serve other countries around the world as they consider how to tackle spam themselves – outreach to the developing world is a particular concern of the Task Force.

Australia is a leader in this effort, and has, over the last two years, signed MoUs with regulators and governments in several countries that wish to study and implement aspects of the Australian anti-spam law. Their current efforts are for instance to help Pacific islands and nations in their anti-spam endeavours.

The FTC, together with the UK Office of Fair Trading (OFT), also have put forward the London Action Plan (LAP), agreed at a workshop on spam enforcement held in London on 11 October 2004 in association with the OECD and ICPEN (the International Consumer Protection and Enforcement Network): this initiative is open to any participants, public or private, and is intended to foster the exchange of best practice in enforcement techniques, training spam enforcers, etc.

The end goal of the LAP is to build an international network of anti-spam specialists and regulators, and develop good working practices between them, so that cross-border cases of spam can be jointly investigated. More than 20 regulators and many industry representatives are now involved in the LAP, from all continents:

(http://www.ftc.gov/opa/2004/10/spamconference.htm).http://www.ftc.gov/opa/2004/10/spamconference.htmhttp://www.ftc.gov/opa/2004/10/spamconference.htmhttp://www.ftc.gov/opa/2004/10/spamconference.htmhttp://www.ftc.gov/opa/2004/10/spamconference.htm

In addition, if anti-spam laws include a provision that permits private right of action, victims of spam, whether ISPs or users, will be able to file suit against spammers which will put pressure for creating a well-organised law enforcement body to deal with anti-spam issues and enforce a country's anti-spam laws.

Regulators, lawmakers and law enforcement authorities from developed countries who have considerable experience with anti-spam legislation, and its enforcement against spammers, are quite proactive in sharing their experience with their peers in developing economies. However, they need to reach out to developing countries that have major spam problems in order to help them build comprehensive anti-spam laws.

There is also a need for law enforcement authorities from around the world to work together on developing a mechanism that will help trace international spam operations that may be based out of the United States, have their Web server hosted in China, send out spam through a mail server in India and use a payment gateway in the Bahamas to process orders from people who buy products advertised in the spam message.

Speeding up the law enforcement process and opening up communication channels is critical, given the fact that most of the profits derived by a spammer from a single e-mail blast flow in within the first few days after the spam has been sent out.

Another reason is that the anonymity of the Internet makes it much easier for a spammer to cover his tracks, set up a new domain with a different fake address and send out an entirely new spam.

Further, several Internet providers may not retain mail server log files beyond a week, unless they have specific reason to do so, such as an intention to collect evidence against a spammer in order to sue him, or in compliance with a subpoena that has been served on them by law enforcement officers investigating a particular spammer.

Therefore, spammers are best tracked down when investigators have fresh spam available, and can immediately reach out to ISPs and other organisations around the world, without undue delays caused by not knowing whom to contact.

Development of a legislative and regulatory framework in developing economies, backed by a framework for international co-operation between governments, as well as on an ISP to ISP level, will have a drastic effect on enforcement costs of regulatory and law enforcement authorities in developed as well as developing countries, and speed up their investigation of spam issues.

Establish centres of expertise and information sharing

There have already been suggestions that a central information portal for ISP staff should be developed, which would consist of anti-spam tips, standard or best practice procedures, etc. Different initiatives to enhance and diffuse best practice, whether by the OECD or other bodies, can play an extremely useful role in allowing market players, policy makers and enforcers to leap frog the learning curve and quickly implement ready solutions to help eliminate spam.

CONCLUSION

In conclusion, the differences in the impact of spam in developed and developing countries are not outstanding. The particular problems developing countries are facing, however, may be different, due to the lack of technical, financial and knowledge resources in these areas.

Firstly, the effect of spam on Internet access can be even more dramatic, considering that in developing countries:

- The available bandwidth is lower.

- Most of the users connect through dial-up or in cyber cafes.

- ISPs often are not aware of the dangers connected to spam and viruses, or do not have the resources to fight them.

Furthermore, it is difficult to apply technical solutions (filters and anti-virus software, etc.) because they may often be relatively expensive, but also the legislative framework is incomplete:

- There is no appropriate anti-spam legislation in place.

- Legislation for consumer protection and data privacy is often fragmentary, and not sufficient to face the challenges of the Internet environment.

- Even when some legislation is in place, there are not the necessary resources or authorities to enforce these laws against spammers.

As a result, many spammers - for whom it has become difficult or too risky operating from a developed country - may decide to “migrate” to developing countries, where they know they can enjoy a certain degree of impunity.

The goal of any viable effort to help developing countries fight spam must work towards optimising the use of whatever limited resources are available locally, as well as any further resources that are obtained as grants in aid from developed economies.

Efforts to mitigate spam must consist in a two-pronged attack – any spam initiative that is organised in a country must have two foci:

Incoming spam that clogs the mailboxes of local Internet users.

Outbound spam, that originates from or is facilitated by local ISPs.

- Preventive measures against spam that originates from the ISPs' networks.
- Enforcing anti-spam laws and policies on spammers based out of that country.

Several solutions described in this paper are short term in scope and implementation, with immediately visible benefits. They can be rapidly achieved by local ISPs and NGOs, with the assistance and co-operation of their peers from developed economies. The equally necessary efforts on developing comprehensive anti-spam legal and regulatory frameworks, and on maintaining high-level channels for co-operation, can proceed at a government-to-government level, at a slower pace, with regular inputs from ISPs, NGOs and other stakeholders in the problem.

As has been noted in this paper, developing economies often lack a proper legislative and regulatory framework, and there is an urgent need to help them develop and build such a framework, and facilitate cooperation between law enforcement bodies in different countries that are charged with investigating spam violations and implementing anti-spam laws against international spam gangs.

ISPs in developing economies must be convinced of the need to filter spam coming into their users' mailboxes, crack down on spam originating from their network, and develop policies that prohibit spam, so that they can stop providing services to any spammers that are hosted on their network.

Another key priority is the development of a grassroots awareness campaign on spam targeted at Internet users in developing countries that helps them understand the effects of spam, prevents them from being cheated by fraudulent schemes advertised in spam, and stops them from becoming spammers themselves by educating them about ethical e-mail marketing practices.

Once ISPs and users in a developing country are educated and aware of anti-spam and Internet security issues, enforcement of anti-spam laws in that country becomes much easier than in a country where awareness of these issues is hazy, at best, so that people unwittingly break laws because they are not aware of them, or are simply not aware that such laws exist, so that they may not report spammers to law enforcement authorities for action.

Implementing local solutions depends on creating awareness and building up a large pool of people who are aware of the issues involved and their solutions – trained e-mail administrators, Internet savvy users who refuse to be drawn into the schemes touted to them by phishers and scam artists, local organizations which educate users and work with ISPs to facilitate better interaction between ISPs and the user community.

Developing economies are rich in human resources – talented personnel who are aware of the issues involved, and who will benefit enormously from training and interaction with their peers in tackling spam problems. Deployment of local personnel and low-cost, open source software solutions involves comparatively low amounts of monetary investment. Moreover, such soft investments injected into a developing country's Internet economy are directed towards long-term capacity building and development of a trained pool of local expertise, both of which contribute to improving the operational stability of the Internet in that country.

NOTES

[1] The Whois utility looks up records relating to domain and IP address ownership, administrative, technical and general contacts, in the publicly queryable and authoritative databases maintained by several Network Information Centers (NICs) and Regional Internet Registries (RIRs) such as APNIC for the asiapac region and LACNIC for Latin America, and domain registrars such as Network Solutions and OpenSRS.

[2] In this context, a national Tier 1 is the dominant ISP in the country – at the top of a multi-tiered pyramid that has this ISP selling connectivity to smaller "Tier 2" ISPs, which then resell this connectivity to even smaller ISPs and other networks.

[3] SWIP (Shared WHOIS Project) is a process used by ISPs to submit customer IP reassignment information to ARIN's WHOIS database. It ensures the effective and efficient maintenance of records for IP address space.

[4] Ref RFC 2142 – Mailbox Names for Common Services, Roles and Functions and RFC 2635 - A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam), both available at http://www.rfc-editor.org

[5] A pink contract is a contract from an Internet service provider to a spammer exempting the spammer from the usual terms of service prohibiting spamming. Usually pink contracts come about because ISPs can charge the spammer a great deal more than they would a normal client.

[6] There is another, once commonly used term "blacklist", use of which is discouraged because of the association of this word with suppression of the fundamental right to free speech.

[7] A fairly detailed English language article is available at http://www.amcostarica.com/112301.htm .

[8] See http://www.amcostarica.com/080904.htm

[9] An unpatched computer is one that has not corrected a security flaw in its software.

[10] The survey is available for download from the BSA's website http://www.bsa.org/usa/events/loader.cfm?url=/commonspot/security/getfile.cfm&pageid=20654&hitboxdone=yes

[11] WTSA Resolution 20, revised in Florianopolis 2004.