Internet Telephony Services Providers' Association

ITSPA evidence contribution to the House of Lords Science and Technology Committee Internet Security report

1.1 The Internet Telephony Services Providers' Association (ITSPA) is the UK VoIP industry's trade body, representing over 80% of UK businesses involved with the supply of VoIP services to industry and residential customers within the UK. We act as the representative voice of the VoIP industry to Ofcom, the Home Office and the DTI, as well as to EU institutions. Internet industries are global, and consequently the regulation of them must aim to follow suit. ITSPA has members in Australia and Europe, and pays close attention to the development of VoIP regulatory frameworks on a worldwide basis in order to ensure that the UK internet telephony industry is as harmonised as it can be with international developments.

1.2 ITSPA welcomes the Lords inquiry on this subject and the Internet. By responding to this call for evidence ITSPA hopes to offer clarity on what Internet telephony providers in the UK are doing to promote personal internet security, thereby giving the enquiry an informed base to work from.

1.3 ITSPA has recently met with the Cabinet Office, the Home Office and ACPO Association of Chief Police Officers) regarding issues of traceability, where ITSPA emphasised that members hold assurances of personal internet security for customers as paramount.

1.4 ITSPA is committed to combating the threats to personal internet safety presented by internet telephony, but firmly believes that the VoIP (Voice over Internet Protocol) industry is only one part of an extremely broad sector obliged to formulate a response to such threats. Our response will focus on VoIP issues and so must not be viewed as a comprehensive discussion of personal security issues.

A full list of ITSPA members can be found at http://www.itspa.org.uk/

Defining the problem

• What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

2.1 The motivations to attack Internet telephony users are very similar to those associated with conventional phone attacks: to benefit financially via toll fraud or identity and information theft, and to gain notoriety, by disrupting service and inconveniencing users. Furthermore, as computers running VoIP software are more like computer than phone in structure they are also potentially vulnerable to the unauthorized access, privilege escalation and "system" misuse, viruses and worms, and denial of service attacks exploiting network protocols that are typical of networked computers.

2.2 Potential threats are identified by security companies and trade bodies like ITSPA, and communicated widely through both the trade press and mass media. ITSPA has identified three threats that are currently of particular concern; phone spam, 'vishing' and CLI spoofing. However, although we take every care to acknowledge and protect against these risks, it is important to emphasise that none of them are currently creating significant problems for UK consumers.

2.3 Phone spam, sometimes known as SPIT (Spam over Internet Telephony), is not yet a major problem but it has nonetheless received a great deal of attention from VoIP providers and the trade press. VoIP systems, like other Internet applications such as e-mail, are susceptible to attack by telemarketers or phone system abusers who initiate unsolicited and unwanted communications. Unlike e-mail however, the technology to filter or block unwanted calls is potentially extremely complex.

2.4 A further worrying new trend is that increasingly cyber criminals are targeting home users with ‘vishing’ attacks. Despite deriving the name from ‘phishing’, an e-mail based scam, ‘vishing’ is essentially a traditional telephony process made financially viable by new telephony technology. It uses VoIP to send a large number of calls to standard PSTN equipment using originating equipment that would have been prohibitively expensive in the past. The Committee should note that despite the wide exposure it receives, this problem is often covered in a misleading way by the media and it does not currently present a major worry to UK consumers.

2.5 ITSPA members have also noted the difficulties posed by CLI spoofing. CLI (Caller Line Identification) or Caller ID is made up of two separate entities: the calling number and the subscriber name. CLI spoofing is the practice of causing the telephone network to display a number on the recipient's caller ID display which is not that of the actual originating station; usually for nefarious purposes.

2.6 The problems posed by CLI spoofing are three-fold. It can be used to trick subscribers into calling expensive numbers by giving a caller ID the user does not recognise – encouraging them to ring back. This practice has become incredibly common in some countries, notably Japan. CLI is often used for caller identification, and there are public expectations to this effect. However, there are now web sites that allow anyone to make a call with any caller ID, making it impossible to use such data as a reputable identification source. Finally, there are issues posed by the frequent use of caller ID for authentication. Major mobile companies until recently had voicemail systems which would allow access to voicemail based solely on a caller's CLI. Someone wishing to check someone else's voicemail simply had to call their mobile number with the caller ID set to be the same as the number they were calling, allowing them to obtain access without any further form of authentication. Although it is important caution is exercised on this issue, it is must be recognised that UK networks have traditionally strictly observed caller ID checking procedures. This is unlike the situation in the US where telecommunications companies have not validated caller ID on entry to the network from 'end-user' connections for some time.

2.7 When new threats arise, ITSPA members can bring up concerns amongst its working groups and push the issue onto the agenda at Council meetings. This allows for discussion of preventive tactics and the development of a coherent industry solution to the problem. ITSPA’s has a technical working group where such concerns can be investigated at length and where the right technical experts can resolve the various problems. ITSPA members are also heavily involved in wider industry groups such as the NICC, which try to tackle the various concerns that affect the VoIP industry. CLI is an important part of the NICC agenda.

• What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

3.1 The scale of the problem varies according to the particular threat discussed. Although phone spam is subject to much industry discussion, there is little evidence as yet of widespread difficulty. Vishing and CLI spoofing are a concern but not to the point where the industry is struggling to cope. With the VoIP market growing rapidly, ITSPA understands it is imperative that there is careful monitoring of security issues.

3.2 ITSPA has endeavoured to tackle these problems at the earliest possible stages, and in doing so has successfully mitigated the damage they have caused to VoIP users in the UK.

Internet Telephony Services Providers' Association

• How well do users understand the nature of the threat?

4.1 ITSPA works tirelessly to ensure that there are high standards of consumer awareness and believes that its members have a responsibility in providing clear education for consumers and simple products for consumers to use to address the security threats that present themselves in the online world. However, users also have a responsibility to protect their computers and the equipment that they are using. There is evidence to suggest that because of the rapidity with which the nature of threats can change, the precise nature of some security risks are not comprehended by all users.

4.2 By working in a flexible self-regulatory environment, the VoIP industry is better placed than others to deal with the constant changes in the nascent Internet world. ITSPA is able to quickly assimilate the nature of potential industry risks and convey this information to customers, unburdened by potentially cumbersome external regulation.

Tackling the problem

• What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

5.1 Although hardware and software both have very important roles to play in curtailing computer security risks, the importance of consumer knowledge cannot be over-emphasised. Many Internet crimes perpetrated via Internet telephony rely on consumers being fooled, rather than an attack on the computer or its software. Both vishing and CLI spoofing are avoidable difficulties. ITSPA suggests that making the public more motivated to act on security concerns is a crucial step in fighting Internet crime.

5.2 ITSPA notes that many UK ISPs have run specific campaigns promoting security information to the public. We are also encouraged by initiatives such as Get Safe Online, which has received widespread media coverage and should go some way to protecting consumers against internet threats. ITSPA would like to see the government continuing to support such actions, and persist in including industry sponsors from the communications sector in discussions with the Cabinet Office, DTI, SOCA and other relevant bodies or departments. We would also like to be involved in setting up similar initiatives for internet telephony in the future if it were thought that such a step would help consumers.

5.3 ITSPA believes that it would be crucial for any campaign to focus closely on the ever-changing threat posed by Internet scams. Whilst initiatives that target specific difficulties would have a positive impact in the short-term, the adaptability of cyber-criminals makes it fair to assume that there would be no realistic quick fix. Consequently, a program aiming to target Internet crime by changing consumer attitudes is likely to be successful in proportion to how entrenched the message of caution is on consumers. While awareness has been raised, there are still some steps that need to be taken.

• What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

6.1 The public is generally increasingly aware of computer security threats, though more vulnerable members of society who are less exposed to the Internet are still at great risk. However, the major problem seems not to be simply lack of awareness, but of action. Recent statistics have suggested that only half of the consumers surveyed for the report said they would ignore 'phishing' e-mail messages. Even more alarmingly, almost one in 25 said they would respond to an unsolicited e-mail about their online bank accounts. These figures are in response to a relatively established scam. ITSPA is concerned that new tactics like 'vishing' may potentially have an even more destructive effect if not acted upon.

6.2 ITSPA believes that it is clear that much work remains to be done. Security initiatives should not only be considered in terms of raising awareness amongst sections of society who may not be as immersed in Internet culture, but also to encourage positive action on the part of all private users. ITSPA is extremely concerned that the prevailing attitude appears to not take proper account of security risks, and works hard with its members to ensure consumer attitudes are appropriate for the problems faced.

• What factors may prevent private individuals from following appropriate security practices?

7. There is a series of factors that may constrain use of adequate security by private Internet users. The main problem seems to be the lack of impact industry initiatives designed to encourage use of appropriate security practices are having. Despite a number of high-profile company campaigns and a genuine wish amongst many consumers to learn more about computer protection, the majority remain ignorant as to where to turn and what to do to make their computers secure. This is not simply a function of the complexity inherent in computers but is also indicative of the ingenuity of Internet criminals making it difficult for many to follow rapid developments in hi-tech attacks.

Governance and regulation

• How effective are initiatives on IT governance in reducing security threats?

8. The UK Government has played an invaluable role in reducing security threats through various policy and advice initiatives, such the Get Safe Online scheme already mentioned.

ITSPA is optimistic that the upcoming Internet Governance Forum, which will discuss Security as one of its topics, will be a continuation of the positive impact government initiatives have had in developing personal internet security.

• How far do improvements in governance and regulation depend on international co-operation?

9.1 ITSPA is concerned by the recent Ofcom consultation in to VoIP, which fails to account properly for the flexibility of Internet markets and the associated risks of over-regulating UK industry. The Internet is a truly global entity and consequently it is of great importance that any governance initiatives recognise this.

9.2 If regulation of the Internet is to be successful and worthwhile, it must be done in a spirit of international co-operation and harmonisation. ITSPA believes that Ofcom's measures will ultimately fail to make a positive impact because foreign providers can continue operating (within the UK) outside of the regulatory framework whilst the competitiveness of UK-based firms suffers. As previously mentioned ITSPA has members in Europe and Australia, with the latter adopting a considerable amount of the ITSPA Code of Practice as part of the national regulatory framework. We feel that this approach of co-operation and convergence between countries will ultimately create the healthiest markets and most suitable regulatory framework to govern them.

Our full response to the Ofcom consultation can be found at; http://www.itspa.org.uk/

• Is the regulatory framework for Internet services adequate?

10.1 ITSPA firmly believes that the current system of self-regulation in the VoIP industry is perfectly adequate for anticipating, identifying and communicating the risks associated with Internet crimes.

10.2 Although ITSPA has been in existence for less than 2 years, it has played a major role in ensuring that the VoIP industry has grown in a rapid but stable fashion. Not only have businesses been well placed to deal with security difficulties, they have also been successful commercially as a consequence of ITSPA membership.

10.3 ITSPA would also encourage the Committee to note that for the past 10 years the Internet industry as a whole in the UK has been a model example of self-regulatory success. A clear endorsement of the success of this framework is the approach to self-regulation adopted in the UK's Communications Act 2003 and applied by the UK's national regulatory authority, OFCOM.

10.4 Imposing external regulation would inevitably make the process of communicating security threats to customers a slower one. As speed is of the essence when dealing with online crime, ITSPA believes neither consumers nor the industry would gain from any change of framework being imposed.

• What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

11.1 ITSPA believes that to excessively regulate this area would create a barrier to developing information security systems and standards, and that a flexible approach is needed in order to be responsive to problems as they arise. Given that the current state of affairs, ITSPA would suggest that any change to the existing arrangement must be considered with extreme care to determine whether it would be truly necessary.