

telesperience

How Telecoms Security Affects the Telesperience

March 2009

What is telecoms security?

Telesperience defines telecoms security as:

The technologies, processes and systems that keep CSPs' businesses and their customers secure.

A wide range of technologies are available to manage individual security challenges facing service providers, including software that:

- prevents or detects fraud
- secures networks, computers and devices - for example firewalls, anti-virus protection, software to prevent/detect keyloggers, spyware removal, software to detect anomalous behaviour or traffic patterns, intrusion detection and so on
- secures data – for example, encryption software, digital vaults and other technology employed to secure customer databases (see above)
- provides security assurance – for example, ensuring policies are being adhered to and security technologies are functioning correctly. This type of technology provides a range of auditing and analysis functions.

Security technology employed in the telecoms industry includes software that has been developed specifically for the industry, cross-domain technology that has been adapted for telecoms-specific needs and general security technology. There are thus many types of vendors active in the market – from telecoms-specific vendors (eg fraud management vendors), to companies that produce enterprise security software across many verticals (as is the case with data-level security vendors), to vendors of consumer-side security products (for example, anti-virus software vendors).

Telesperience telecoms security poll 2009

Key findings

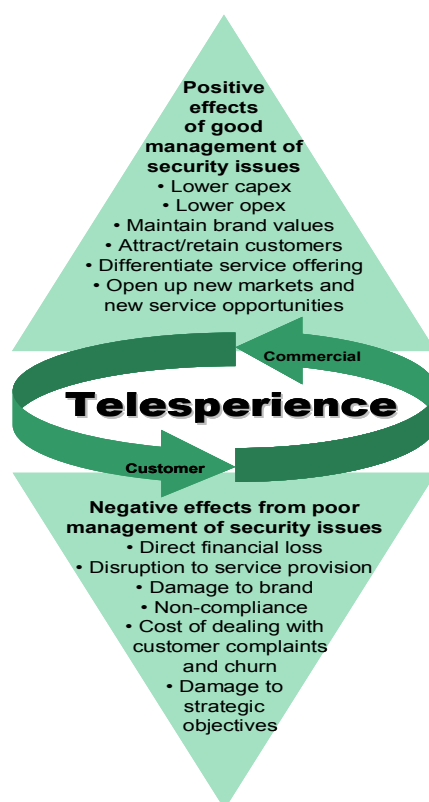
The following key trends emerged from this poll as a result of statistical analysis of responses, from comparing demographic data against responses, and from comments received whilst conducting the poll.

- 76% of consumers are concerned about telecoms security.
- 71% would consider moving service provider to one that offered enhanced security.
- 96% of consumers are concerned about ID theft.
- 92% are concerned about fraud or monetary loss.

- Security fears are a barrier to usage of services. In particular to the uptake of e-commerce services and especially in the older demographics. Older people are more concerned about security than average, and manage the perceived risk by not adopting technology.
- Young men are the least likely to be concerned about security. Women are generally more concerned about security than men.
- People who use only one service are less concerned about security than those who use multiple services and are also less likely to move service provider to one that offers enhanced security.
- Users of services are less concerned about the security of that service than non-users.
- There is a high level of awareness of data security issues, but the risk surrounding newer services is less well understood and/or less recognised.
- Concern about security appears to be rising – many respondents commented that their level of concern has risen, or that they have only recently become concerned. Customers also say enhanced security is a service differentiator (see Figure 7).

Security issues have both a negative and positive effect on the telesperience, as shown in Figure 1.

Figure 1 The risks and opportunities associated with telecoms security management
[Source: Telesperience 2009]

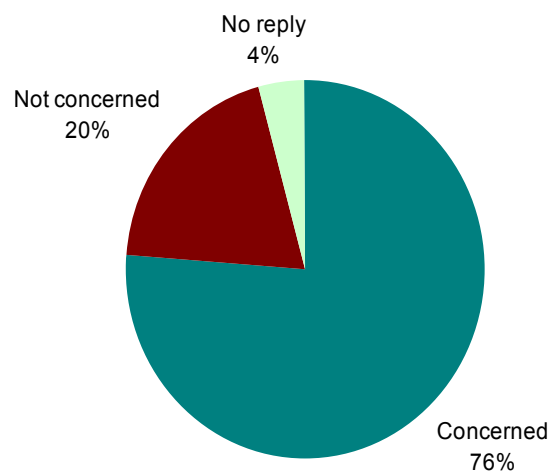


Detailed findings of the telecoms security poll

Question 1: Are you concerned about telecoms security?

We asked respondents how concerned they were about telecoms security as a general gauge of concern before we prompted them with questions about specific services or types of risk. Overall 76% said they had concerns about telecoms security (see Figure 2).

Figure 2 Telecoms consumers' concern about security

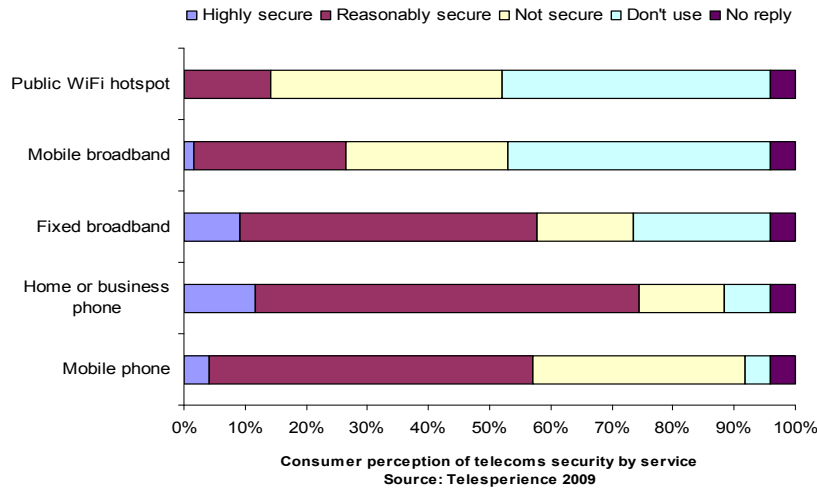


Telecoms consumers' concern about security
Source: Telesperience 2009

Question 2: How secure do you think telecoms services are?

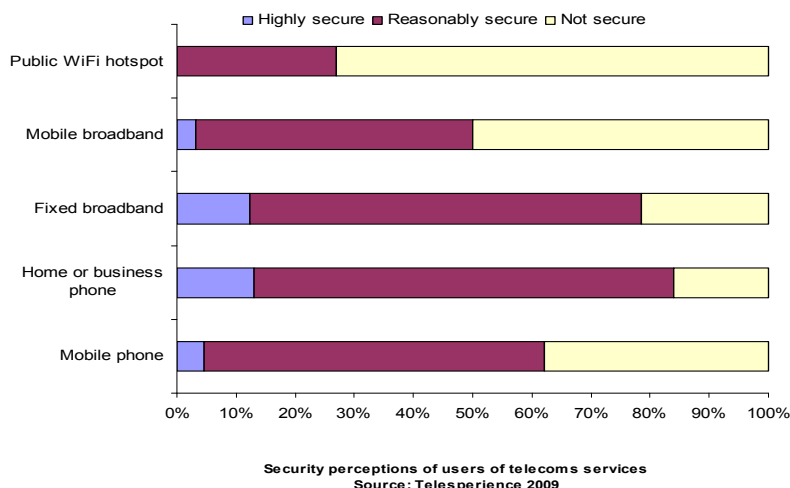
Consumers perceived some telecoms services to be quite safe, but this was highly variable according to service type (see Figure 3). Overall, services that consumers were most familiar with – such as home and business fixed phones – were perceived to be the most safe. Mobile phones and both fixed and mobile broadband services were perceived as being considerably less secure; while WiFi hotspots were seen as the least secure.

Figure 3 Consumer perceptions of telecoms security by service [Source Telesperience 2009]



As can be seen from Figure 3, for newer services such as WiFi hotspots a considerable number of respondents told us they weren't using these services (and therefore offered no opinion as to their security). When non-users were excluded, the proportion of those concerned about the security of the service was lower (see Figure 4).

Figure 4 User perceptions of telecoms security by service [Source Telesperience 2009]



In every case, users of a particular service perceive it to be more secure than non-users (see Figure 5). This could indicate that security is a barrier to uptake of new services amongst some demographics. However, in the case of WiFi hotspots both users and non-users have a high level of concern about how secure it is.

It should also be noted that fixed technologies are perceived by all consumers and by users to be safer than mobile technologies.

- 32% more consumers¹ perceive fixed broadband to be secure than perceive mobile broadband to be secure.
- 29% more users² perceive fixed broadband to be secure than perceive mobile broadband to be secure.

This is a concern that firms offering mobile broadband are going to have to address if they are to compete with fixed service providers. Conversely, it is a concern that fixed broadband suppliers could exploit to retain customers as a counter argument to the benefit of mobility.

Figure 5 Difference between general consumer and user perceptions of telecoms security by service [Source: Telesperience 2009]

Service	Consumers who perceive service to be secure*	Users who perceive service to be secure*	Difference %
Home or business phones	78%	84%	+6%
Fixed broadband	60%	79%	+19%
Mobile phones	59%	62%	+3%
Mobile broadband	28%	50%	+22%
WiFi hotspot	15%	27%	+12%

Note: * this is the total of those who say these services are highly secure or reasonably secure

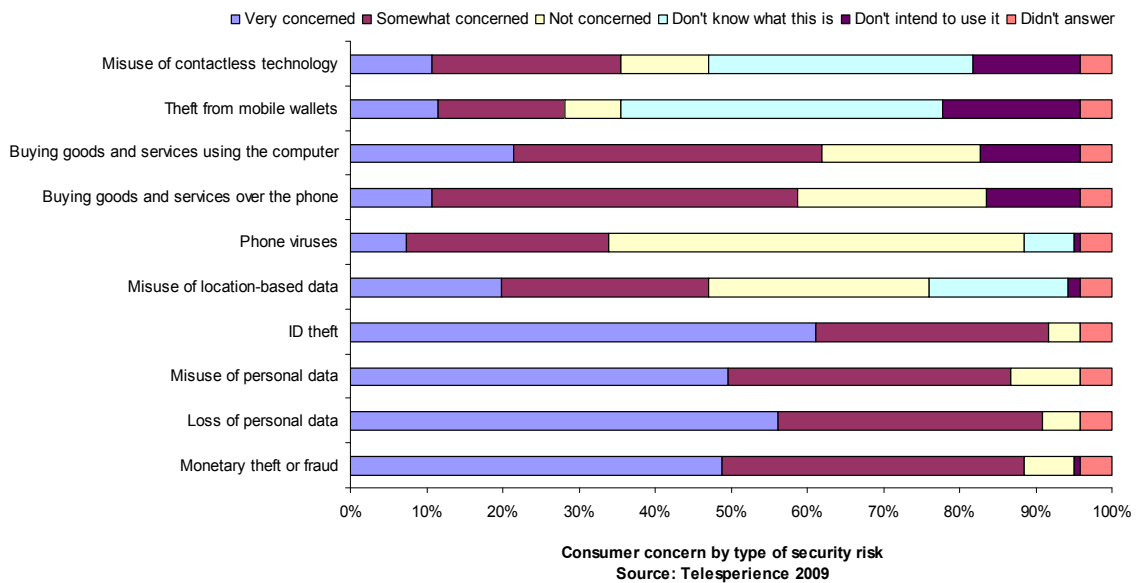
Question 3: How concerned are you about the following types of security risk for services you use now or intend to use in the future?

We presented ten risk scenarios to consumers and asked how concerned they were about each. They told us they were most worried about ID theft (see Figure 6). This might indicate a recognition that theft or fraud can be a one-off event, and that there are mechanisms in place to protect them – for example, compensation if credit cards are used fraudulently. However, there is currently little help for victims of ID theft, it can also be much harder to resolve, and its consequences can be both greater and longer lasting.

¹ Consumers are all respondents to the survey.

² Users are only those respondents actually using a service.

Figure 6 Consumer concern by type of security risk [Source: Telesperience 2009]



We asked consumers how much they feared each of the risk scenarios we presented to them. They told us they were very concerned or somewhat concerned by each scenario as follows:

- Monetary theft or fraud – 92% are concerned
- Loss of personal data – 95% are concerned
- Misuse of personal data – 91% are concerned
- ID theft – 96% are concerned
- Misuse of location-based data – 49% are concerned
- Phone viruses – 35% are concerned
- Buying goods or services over the phone – 61% are concerned
- Buying goods or services using a computer – 65% are concerned
- Theft from mobile wallets – 30% are concerned
- Misuse of contactless technology – 37% are concerned.

The high level of concern about ID theft and loss of data probably also reflects the level of coverage this has received in the general press. In other words, there is a higher awareness of this risk. However, as can be seen from the figures, there is still a much lower level of concern about location-based data. This technology is receiving a mixed reception by the general press as it is introduced. Where the service is limited to a particular geography – eg a shopping centre – and is an opt-in service then generally reception has been either neutral or positive. Technology that tracks people over wider areas has received less positive press. It is far too early to say how this situation will develop, but it is important for service providers to pre-empt negative connotations by addressing security concerns before services are launched. Too much negative press about a particular service could retard uptake of the entire technology.

Lower levels of concern about the security of new services should likewise not be misinterpreted. This does not necessarily represent an intrinsically lower level of concern, but is due to ignorance about the service and the security issues surrounding it, and the fact that many consumers are not yet using the service. As services that use location-based data increase, it is highly likely that concern will increase.

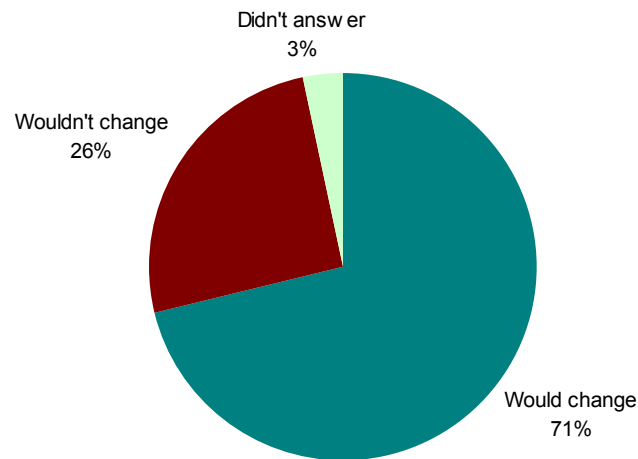
It is therefore very important that service providers train and inform customers about how to stay safe while using telecoms services. No matter how many security measures a service provider puts in place, reckless behaviour by users will undermine these and create a security risk for the consumer.

Unfortunately, the service provider might very well be blamed for issues that are not really its fault. Likewise they may also end up fielding considerable numbers of support calls at vast expense. Proactively working to increase awareness and promote sensible behaviour will therefore enhance both the customer and commercial telesperience.

Question 4: Would you be prepared to change service provider to one that offered you an enhanced level of security?

Seventy-one per cent of consumers say they would be prepared to change service provider to one that offered enhanced security (see Figure 7). Of those unwilling to change, most were from demographics where price was still the most important factor in their choice of service provider. (This was the most common explanation offered to us for unwillingness to change.) However, it should be noted that those unwilling to change were highly likely to be people who only used a single service – typically older people who only used a home phone or younger people who only used a mobile phone. Consumers who used multiple services had a high propensity to change service provider.

Figure 7 Inclination to change service provider to one that offered enhanced security
[Source: Telesperience 2009]



Inclination to change service provider to one that offered enhanced security
Source: Telesperience 2009

The fact that so many consumers perceive security to be a differentiating feature of service provision is a commercial opportunity for CSPs. Offering security as a service to risk-averse demographics could be a business opportunity, but is at least a way of differentiating a CSP's brand in a competitive market. Many users are aware that they lack the technical wherewithal to select and implement technology to protect themselves, or don't have the time or inclination to do so. (This includes smaller businesses as well as consumers.) Customers are therefore interested in services that protect them and offer help when security problems occur. Whether they are prepared to pay extra for these services was not tested in our poll, but certainly customers have indicated that enhanced security services would be attractive enough to encourage them to change service provider.

Summary

As new and more complex services are rolled out, and as communication becomes ever-more embedded into daily life, the opportunity to employ security as a competitive differentiator or as a service in itself will increase. Service providers need to put effort into educating customers about security risks, emphasise the security features of their services and consider how they can use security to position their brand. Importantly, if certain next-generation services are to succeed, CSPs need to proactively work to manage security fears before and during the early phases of rollout.

Methodology and further resources

Method

The poll was conducted in March 2009 by Babworth Ltd. It was designed to highlight consumer feelings about telecoms security. The sample size was 122 people broken down as follows:

- Male (57%), Female (43%)
- Under 18 (5%), 18-30 (29%), 31-50 (45%), 51-70 (18%), over 71 (2%).

We used both online polling and street polling to gather our results in order that the views of those people without access to the Internet were also represented in the poll. Most of the people who responded to the survey (80%) were from the UK. Other nationalities were represented due to non-nationals working in or visiting the UK and being captured in the street poll; a very small number of international respondents answered the online poll. Non-UK respondents came from: other European countries, US and Canada, South and Central Asia, Asia-Pacific, Africa and the Middle East.

Further resources

Telesperience 2 has a telecoms security feature. It is available to download from www.telesperience.com.

Re-use of information in this paper

This paper can be freely distributed in the original form. However, re-use of data or diagrams from the paper can only be done if it is for limited internal purposes and a citation is included to the original publication. This should take the form of a source line (Source: Telesperience 2009). In these circumstances permission to re-use is not needed.

You are also advised to read the accompanying blog piece 'UK customers are willing to change service provider to get better security' available from www.microsperience.com. The data and information contained in this piece can be re-used and re-quoted without permission being sought provided it is cited to the original publication (Source: Telesperience 2009).

For external use of any kind – conferences, user groups, customer meetings or publishing in blogs, magazines, reports or other media use – please email enquires@telesperience.com for permission to re-use. Permission must also be sought where the information is to be used in academic work.

Even where you believe fair use applies, you are kindly asked to inform us that you intend to use the information and where it will be used. You should in any case ensure it is sourced correctly.

Permission to use this information will usually be granted provided the information is to be used appropriately, the source is acknowledged and the data is not manipulated to support arguments that it does not reasonably support. We are able to supply original charts and diagrams to companies and organisations at our discretion for use in presentations. Please send an email to the address above stating briefly how you intend to use the information if you are interested in this service.

Please note: the information in this paper is provided for free, but copyright is retained by Babworth Ltd. Failure to gain permission for re-use – except in the specific circumstances stated above – is copyright infringement. If you have a legitimate need to use the information and are in any doubt about whether you need permission please just ask us: permission will usually be granted and your politeness in informing us of re-use is very much appreciated.

This paper was originally published in March 2009 in Telesperience, which is a publication wholly-owned by Babworth Ltd. See www.babworth.com for more details.