Evolved Intelligence

Innovation in an interconnected world

Published November 2017

Consumer trust hanging in the balance with the threat of SS7 attacks

Market research into consumer awareness and response to SS7 threats and the potential consequences for mobile operators

Key takeaways

- 80% of subscribers would lose trust in their mobile operator if it was subjected to an SS7 attack, with 25% saying they would likely change mobile operator as a result.
- However, having been subjected to an SS7 attack, the number of subscribers changing mobile operator increases to 33%.
- Trust in the mobile network provider is a differentiator, with 59% of subscribers likely to move to a mobile operator that can remove all threats from signalling attacks.
- However, having been subjected to an SS7 attack, 72% of subscribers said they would look to move to a mobile operator that could remove all threats from signalling attacks.
- 59% of respondents believe communications via their mobile device is either secure or very secure.
- Privacy and security was ranked the fourth main concern for consumers when last choosing a mobile operator, behind price, coverage, and data speeds. The relative low concern over signalling vulnerabilities was highlighted by only 25% of respondents.
- Education and experience around the SS7 threat greatly raises the concern over privacy and security – with approximately 50% of subscribers changing their view and placing it is one of their top three concerns when next choosing a mobile operator – many of them ranking it second behind price.
- 36% of affected subscribers following an attack would stop using or reduce usage of mobile services.
- An attack reduces overall usage of services, voice, data, text and particularly banking and payments services.

Introduction

Mobile operators have invested vast quantities of time and money developing their brand identity across a range of areas, from offering the fastest high-speed 4G network, the latest services and providing access to the best devices, to offering the most innovative tariffs. In addition, they have struck exclusive content partnerships, and strive to deliver the best customer support.

These investments are designed to ensure customers buy into their brand, and receive an experience worthy of their brand name. Happy customers equal loyal customers, and happy, loyal customers place an overwhelming sense of trust in their mobile phone provider.

So what happens when a mobile operator's SS7 network is attacked and customer communications are compromised?

This White Paper is based on research undertaken in August 2017 by Evolved Intelligence and Mobilesquared into the German and UK mobile markets. The aim of the research was to understand the consumer awareness of the SS7 threat and any consequential effects on trust, mobile service usage and churn.

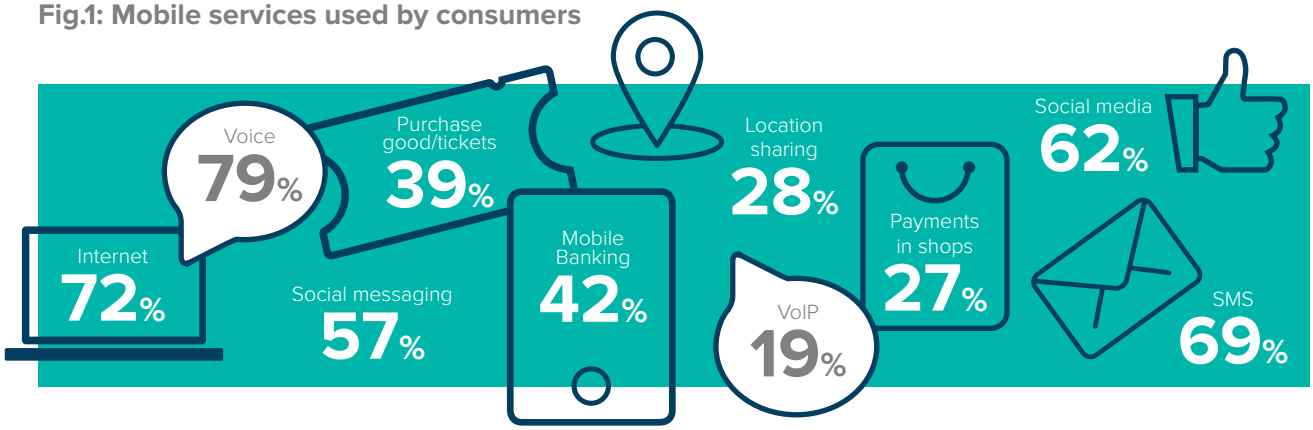
Section 1. Trust

Customers are loyal, with 49% remaining with their existing mobile provider for more than 3 years, according to the consumer research. What's more, 65% of consumers said they were satisfied to very satisfied with their mobile phone provider, while 60% said that they were very likely to recommend their provider. This indicates that almost two-thirds of consumers have bought into the brand ideology of their mobile phone provider.

What has intrinsically driven this trusted relationship between the consumer and their mobile operator is the smartphone, which relies upon the provision of high-speed broadband to allow the user to access apps and websites which contain their personal and sensitive data.

Although the research reaffirmed voice as the biggest service (79%)used on a mobile device today, followed by browsing (72%) and SMS on (69%), up to 42% of users demonstrate implicit trust in their mobile device by using services such as mobile banking and making purchases from their mobile device (see Fig. 1).

Fig.1: Mobile services used by consumers



The smartphone has also fundamentally changed how people communicate. The average consumer will typically use four channels to communicate with friends and family, but these channels can be condensed into voice (traditional voice, Skype, Viber, in-app call, etc) and messaging (SMS, email, chat, WhatsApp, Messenger, Twitter, etc).

Consumers are communicating more and over a greater variety of channels. Research by Mobilesquared[1] has revealed that interaction between a business and its customers is also on the increase. Voice continues to be the go-to channel for inter-business and customer communication, while SMS has become one of the most effective channels for a business communicating to its customers.

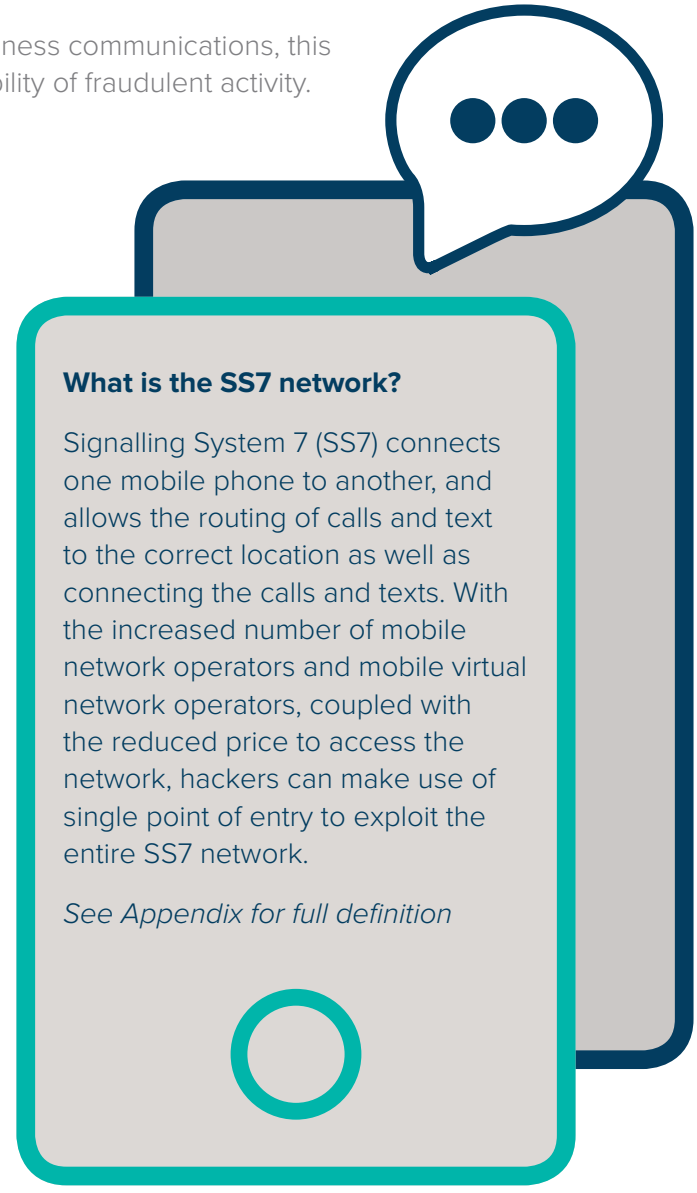
Part of the appeal of both voice and SMS by both businesses and customers alike, is the fact they are viewed as trusted channels. SMS is now the preferred channel for two-factor authentication used by digital service providers such as Facebook, Google and Microsoft, and viewed as the only secure channel to send urgent account information from a bank.

As consumers become more trustful of business communications, this makes them more susceptible to the possibility of fraudulent activity.

Such a threat is becoming all-too-real, with the emerging risk to customers from attacks using the SS7 network to intercept both voice calls and SMS messages. This can materialise as tricking the customer into believing they are communicating with a legitimate source, or silently monitoring communication between a consumer and a legitimate source.

Security messages such as two-factor authentication (2FA) from banks to their customers, are vulnerable to interception, allowing the criminal to carry out a traditional phishing scam to access the customer's personal details, then via SS7 they can intercept communication from the bank to approve a funds transfer.

And it's not just voice and messaging that is under threat. Criminals and Government agencies are using the SS7 network to access user location data and monitor a user's whereabouts. These invasions into privacy pose a real security risk and have a tangible effect on trust.



What is the SS7 network?

Signalling System 7 (SS7) connects one mobile phone to another, and allows the routing of calls and text to the correct location as well as connecting the calls and texts. With the increased number of mobile network operators and mobile virtual network operators, coupled with the reduced price to access the network, hackers can make use of single point of entry to exploit the entire SS7 network.

See Appendix for full definition

[1] Source: Mobilesquared consumer + enterprise research August 2017

For the purposes of this White Paper, we shall focus on interception as highlighted in Table 1.

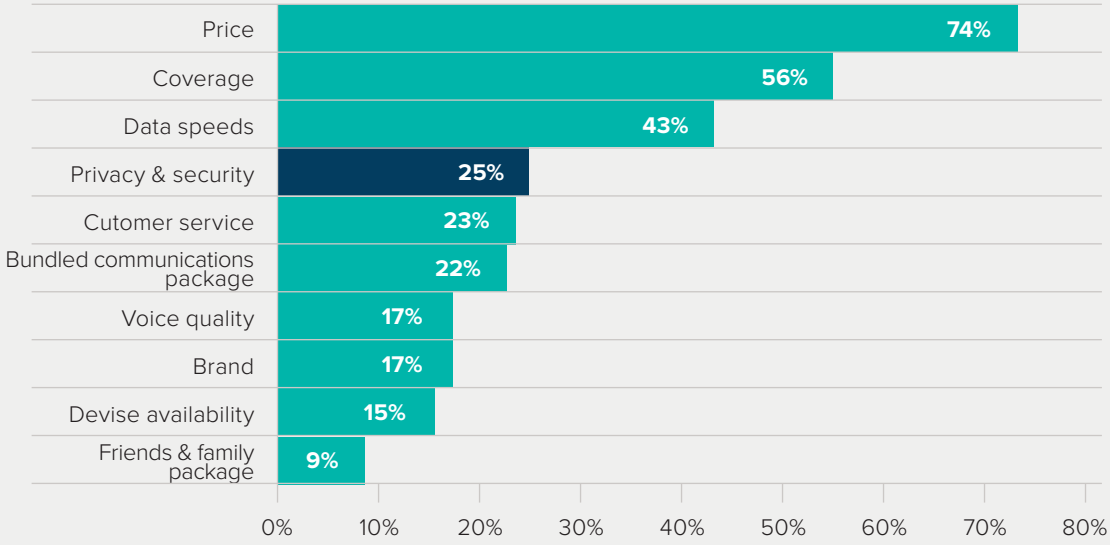
Table 1: What is interception?

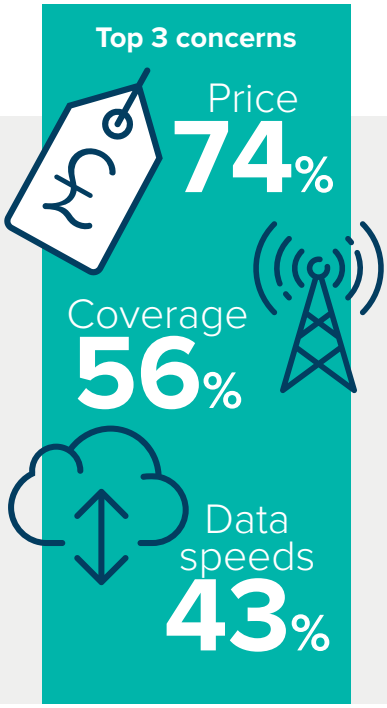
	**SMS/text message intercept:** a third-party intercepting SMS passwords or texts.
	**Location intercept:** the unauthorised access of a user's location data for malicious intent.
	**Hacking:** information being accessed by a third-party without the user's permission.
	**Voice intercept:** a call the user believes is with the dialled party (e.g. a bank) that has been intercepted by a criminal third-party (for example) as a means to extract personal data or approve transactions, or a third-party unlawfully listening in on a conversation.
	**Voicemail hacking:** someone listening to your voicemail without permission.

Section 2. Results: Consumer awareness and trust

The importance of trust between the customer and mobile operator was abundant throughout the consumer research in both the German and UK markets. For instance, 59% of respondents believe communications via their mobile device were either secure or very secure. The belief that their communications were already secure was highlighted by the fact that only 25% of respondents identified privacy and security as one of their top three concerns when last choosing a mobile operator – ranking it fourth behind price, coverage, and data speeds (see Fig.2).

Fig.2: What were your top 3 concerns when choosing a mobile operator?

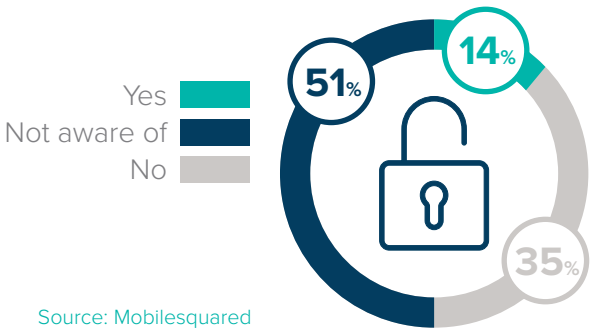




Source: Mobilesquared

According to the consumer research, 14% of respondents claim to have experienced a privacy or security breach (see Fig.3). That figure could be considerably higher, given that 51% said "they were not aware" of such activity, leaving just 35% stating that they had not experienced interception-based issues.

Fig.3: Have you experienced any privacy/ security issues on your mobile phone?



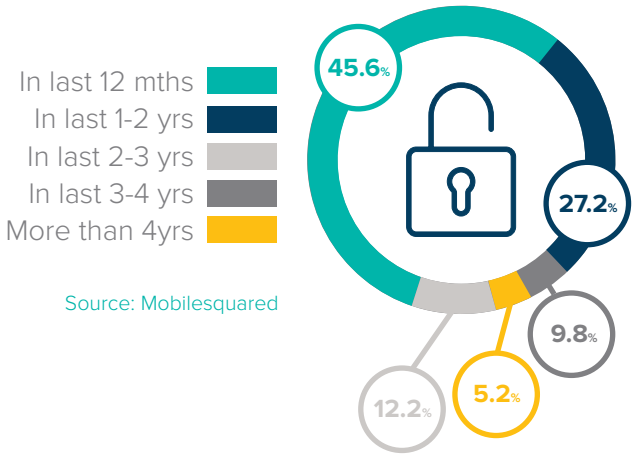
Source: Mobilesquared

Section 3. Results: Attack victims: The 14%ers

Fourteen percent might not seem like much, but in the markets included in the research, that accounts for more than 9 million users in the UK and 16.8 million users in Germany. What's more, an attack affecting 14% of a mobile operator's subscriber base could have a devastating impact on its business.

What is extremely revealing is that consumers believe the level of interception-based attacks is on the increase. Based on the users that claim to have experienced such an attack, more than two-thirds have taken place in the last 2 years, with the majority occurring in the last 12 months. This indicates that attacks are happening on a more frequent basis, and will potentially affect more mobile users in the coming months and years (see Fig. 4) as criminals look to exploit mobile network vulnerabilities.

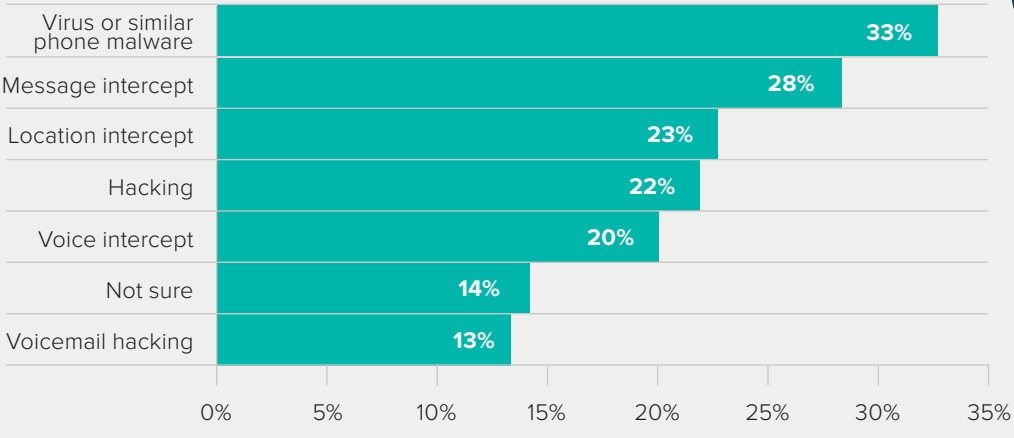
Fig.4: Have you experienced any privacy/ security issues on your mobile phone?

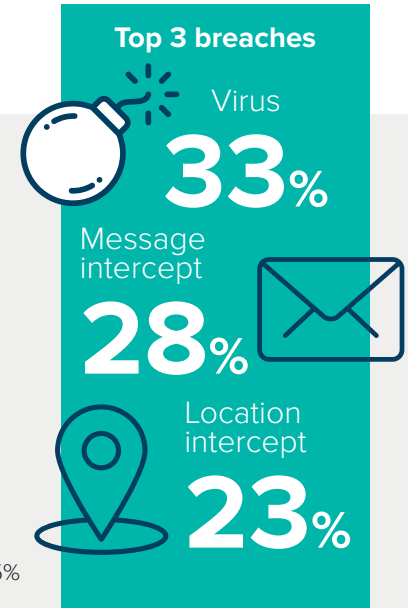


Source: Mobilesquared

Of these 14% of respondents, the most common issue was a virus, or similar malware accessing phone data, followed by message intercept (see Fig.5). Location intercept was the third most common breach, followed by hacking, voice intercept, and voicemail hacking. A further 14% of respondents were sure they had experienced some sort of issue without knowing exactly what it was.

Fig.5: What kind of privacy attack occurred on your mobile phone?





Source: Mobilesquared

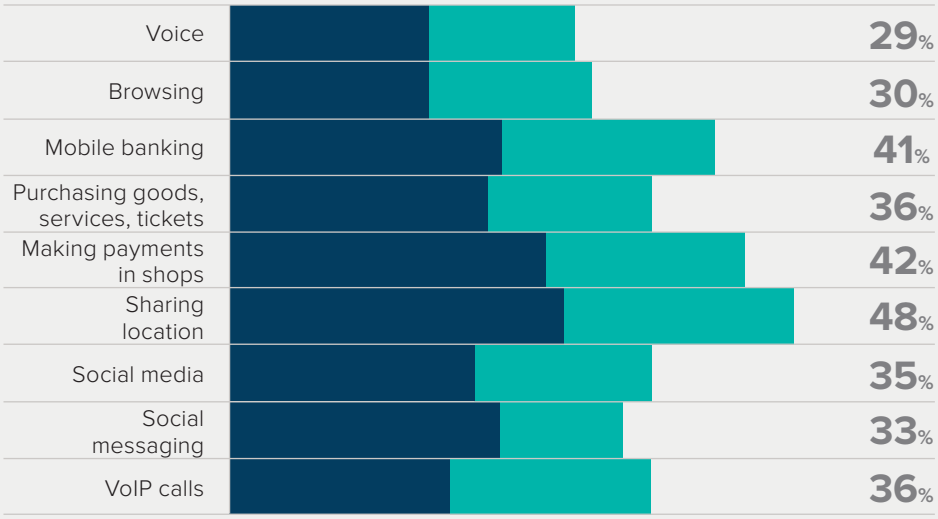
The impact of the breaches on customers was immediate, with 41% stating they either no longer trusted their mobile operator, or trusted them less. Moreover, 33% of the affected customers either changed mobile operator because of the attack or intend to change as soon as possible (see Fig.6). Clearly, an attack of this nature has had a hugely detrimental impact on the customer's relationship with their mobile network operator, resulting in an immediate loss of trust.

Fig.6: How has the attack affected your relationship with your mobile operator?

Having been victim of an attack, not surprisingly, 72% of these users said they would look to move to a mobile operator who guaranteed their privacy and security.

The impact on trust and subsequent churn is undoubtedly the mobile operator's biggest concern following an attack, but data usage will be hit as well.

Fig.7: How did the attack affect your mobile usage?



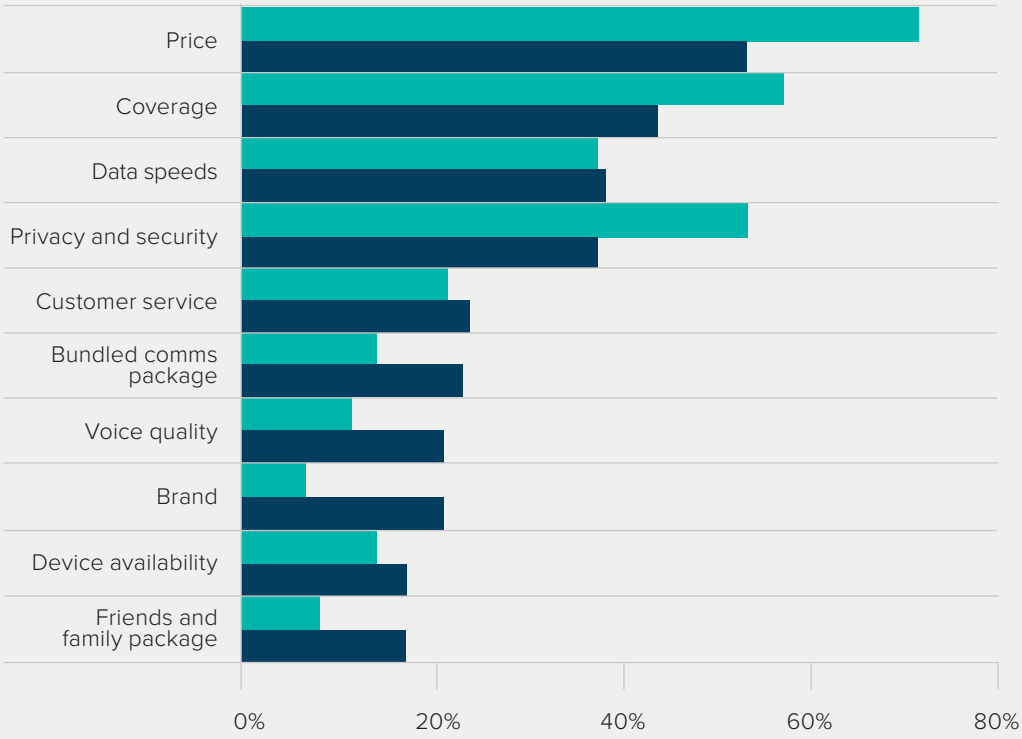
Source: Mobilesquared

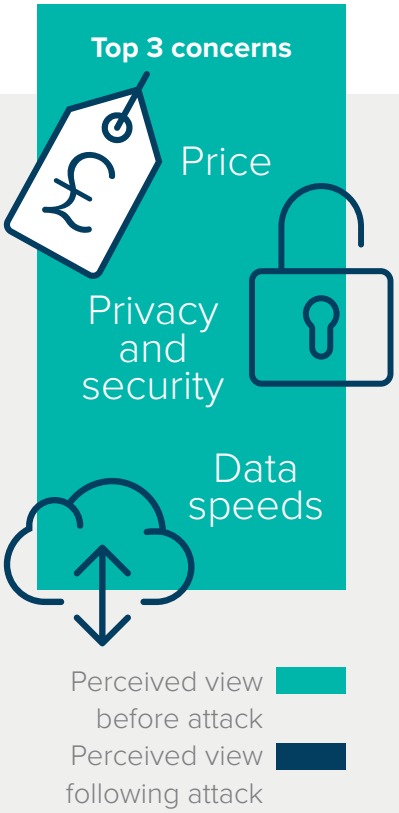
Of those customers affected, on average 15% said they stopped using the services, and 21% said they had reduced their usage (See Fig. 7). Not surprisingly, the services most impacted by an attack are those based on personal data, location, and financially-related information, although the impact is across the board and hits total mobile usage.

Ultimately, the customers that have experienced an attack have revised their requirements from their mobile phone provider. Privacy and security has jumped 71% and has become the second most important factor when selecting a mobile phone provider (see Fig.8).

Being able to reassure customers that their communication is safe will increasingly become a differentiator for mobile operators as the threat of potential attacks rises.

Fig.8: How did your top 3 concerns change after you were victim of an attack?





Source: Mobilesquared

Section 4. Results: What if you were attacked tomorrow?

This section looks at the 86% of respondents that have not been victim to an SS7 network attack. Here we explore how they believe they would react.

With the number of security attacks expected to rise year-on-year, a mobile operator's subscriber base will be under increasing threat. The research highlights that the response of mobile users to new SS7 network attacks will have a significant impact on trust, and – as demonstrated in the previous section increased churn.

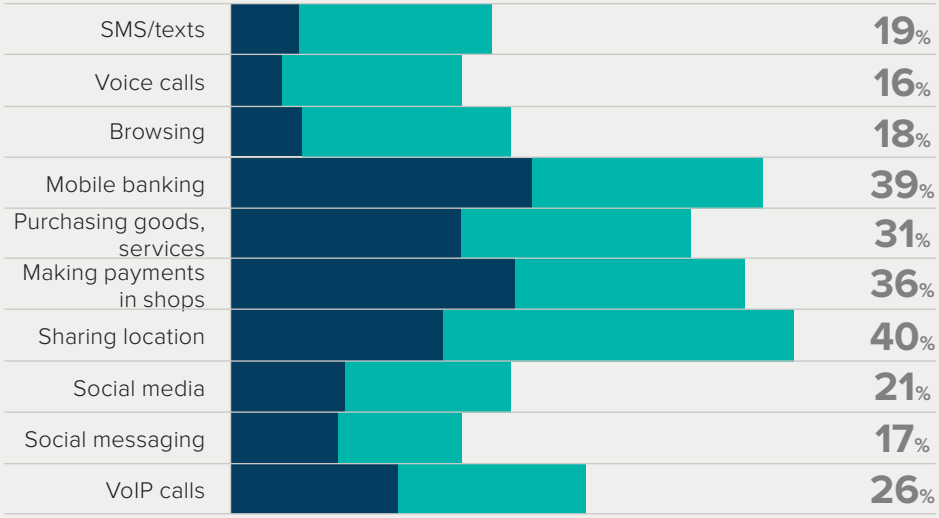
For starters, of the 86% of respondents yet to have experienced an attack, a staggering 80% would lose trust in their mobile operator immediately if they were attacked. This would result in 25% leaving their existing mobile provider (see Fig.9).

Fig.9: How would a breach affect your relationship with your mobile operator?

Similarly, having been made aware of the threat, the research suggests that 59% of users would look for a mobile operator that could safeguard privacy and security, and protect their communications (SS7 protection) when looking to switch providers. Clearly, in addition to the 25% of users that will churn, a significantly larger percentage of customers – if not all the subscribers – will raise their privacy and security concerns having been made aware of their mobile operator's network vulnerabilities.

And it doesn't stop there. As already highlighted with actual victims, reduced usage will be part of the fall-out following a mobile network attack. On average 11% would stop using the services, and 15% would use them less. As Fig.10 shows, it's not only the banking, payments or location services that will be hit, but everyday services like messaging, voice and social media.

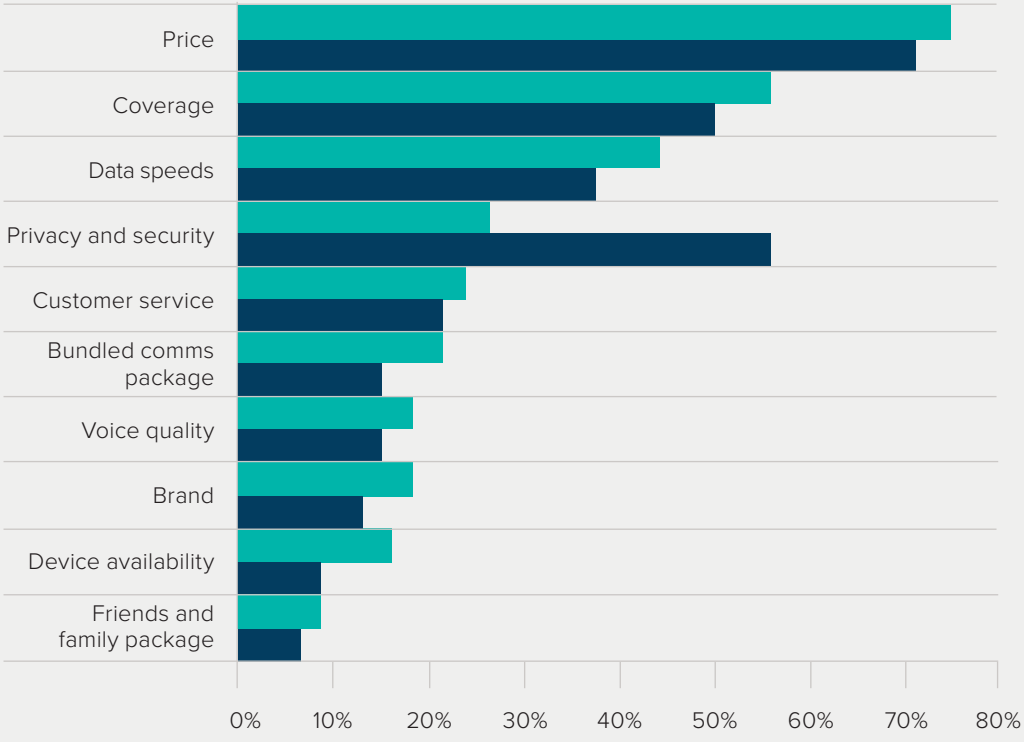
Fig.10: How would your mobile usage change following an attack?

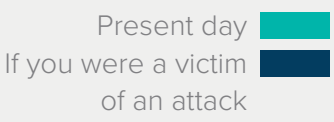


Source: Mobilesquared

So, what will these mobile customers now look for when selecting their next mobile operator? Similar to those customers identified in the previous section, privacy and security will become the second biggest concern after price (see Fig. 11).

Fig.11: What are your top 3 concerns, post implied attack?





Source: Mobilesquared

Section 5. Conclusion

As highlighted in this White Paper, the public awareness of the threat from SS7 vulnerabilities in the mobile network is growing through increased media coverage, but also because of a wave of high-profile global cyber-attacks such as WannaCry, Petya, and Yahoo!.

Privacy and security is becoming a fundamental issue for consumers as their awareness regarding such threats increases. As the research has highlighted, consumer protection for some consumers has become second only to price in terms of key considerations.

This makes protecting customer communications a core objective for mobile operators, and potentially a competitive differentiator as the threat of attacks and public concern increases.

Failing to protect customers from an SS7 attack, will impact a mobile operator's subscriber base through increasing churn up to 25% of impacted or aware subscribers. Risking losing years' worth of brand investment almost overnight, as well a potentially lowering lower data usage leading to a reduction in ARPU.

Ultimately, a signalling attack will drive a change in customer perception and usage, resulting in brand negativity, loss of subscribers and reduced revenues.

Appendix.
History of the SS7 threat

Signalling System 7 (SS7) connects one mobile phone to another, and allows the routing of calls and text to the correct location as well as connecting the calls and texts. With the increased number of mobile network operators and mobile virtual network operators, coupled with the reduced price to access the network, hackers can make use of single point of entry to exploit the entire SS7 network.

The protocol was originally developed for a closed network of trusted partners – primarily the state-owned telcos of the time. As such, security was never a main design concern.

However, with the increased number of MNOs and MVNOs, and the reduced price to access the network, hackers can make use of single point of entry to exploit the entire global SS7 network.

The threat to mobile networks and their customers from vulnerabilities in the SS7 protocol is nothing new. Experts in mobile security and fraud prevention have warned for years about the very real danger of criminal abuse of SS7 weaknesses to gain access to personal data and, potentially, carry out fraudulent activity.

Through SS7 it is possible to access all communications made via a mobile device. The ability to track, intercept and redirect mobile calls and text messages with relatively inexpensive and commercially available hacking software makes SS7 an incredibly weak link in terms of network security. Government agencies have utilised these loopholes for many years and increasingly, now, so are criminals.

According to Evolved Intelligence, only about 1% of total signalling messages are deemed to be 'suspicious' – and only 10% of those are actually harmful. However, with trillions of signalling messages sent on a daily basis, the number of harmful messages transmitted is immense and the necessity to have rigorous signal management and protection in the network would appear obvious.

However, public awareness of the threat to privacy and security from SS7 vulnerabilities in the mobile network has been growing over the last decade with increased media coverage.

Warnings first emerged of the SS7 loophole in 2008, but it wasn't until Karsten Nohl, chief scientist at Germany's Security Research Labs, demonstrated a hack at the 2014 Chaos Communication Congress in Germany that people really began to listen.

Nohl's work drew international attention in 2016, when he demonstrated the vulnerabilities on the 60 Minutes TV show. Since then researchers have demonstrated how to hack WhatsApp, Facebook & Telegram and further TV shows have shown a US Congressman and an Australian Senator being hacked via SS7. In 2017 O2 Telefonica in Germany confirmed some of its customers had experienced banking fraud via a combination of traditional phishing and SS7 access.

Methodology

Independent research house, **Mobilesquared**, surveyed 2,000 mobile consumers aged 16 and over, split equally between Germany and the UK. Each respondent has double opted-in to be part of an online panel. Research took place in August 2017. Analysis and copy for this White Paper created by Mobilesquared.

About Evolved Intelligence

Evolved Intelligence provides roaming, fraud and security solutions to mobile phone operators and signalling providers world-wide. Solutions are powered by a unique architecture which allows network intelligence to be sited remotely from the network core. Evolved Intelligence has more than 60 service implementations in 50 operators. The company's solutions are also available from several leading signalling providers. Evolved Intelligence is based in Bristol, UK and was formed in 2007.

Evolved Intelligence
Innovation in an interconnected world

About the Author

Gavin Patterson is Chief Data Analyst at Mobilesquared. Gavin brings twenty-five years' experience in technology, media and telecoms journalism, research and analysis, to Mobilesquared. He has authored numerous articles and reports covering diverse mobile markets and strategies, spoken at leading global mobile conferences, and developed Mobilesquared's proprietary data forecasting tool. Before joining Mobilesquared, Gavin held analyst roles including Research Director at Dataxis, and Principal Analyst and Editorial Director at Ovum.

About Mobilesquared

Mobilesquared is a trusted research partner to some of the biggest companies in mobile, working with organisations including; Three UK, O2, Tesco Mobile, Nokia, Qualcomm, and the Phone-paid Services Authority (PSA). We have been covering all areas of mobile including; mobile advertising, marketing, A2P messaging, OTT, RCS, LTE, broadband, 5G, unified communications, mobile payments, premium rate services and mobile technology since 1998. Find out more about Mobilesquared at **www.mobilesquared.co.uk/**

Mobilesquared
Communicating data