Internet Telephony Services Providers' Association

ITSPA response to The Culture, Media and Sport Committee an inquiry into Cyber Security: the protection of personal data.

About ITSPA

The Internet Telephony Services Providers' Association (ITSPA) represents over 90 UK businesses involved with the supply next generation communication services over data networks to industry and residential customers within the UK. Our traditional core members are VoIP providers. ITSPA pays close attention to both market and regulatory framework developments on a worldwide basis in order to ensure that the UK internet telephony industry is as competitive as it can be within both national and international markets.

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

A subsidiary of TalkTalk (Tipicall Ltd) is a member of ITSPA and has not contributed towards this response.

Introduction

Outlined below is a short response from ITSPA to the Committee's inquiry into the protection of personal data. ITSPA members take data protection and cyber-security extremely seriously as it is central to the integrity of our members businesses. We are extremely active as an organisation promoting best practice around VoIP security, educating members around fraudulent scams and engaging with law enforcement organisations in tackling telecoms fraud.

This response outlines some concerns that members have around the issue of encryption and it being seen as the quick fix for data security, without considering the wider implications.

The TalkTalk hack and subsequent data loss - and to a lessor extent the Vodafone hack only a few days later – bring the issue of data security and telecommunications into the news, but it's important to point out that cybercrime is a much wider issue.

> *"The cyber threat remains one of the most significant – and growing – risks facing UK business.* ***81% of large businesses and 60% of small businesses suffered a cyber security breach in the last year****, and the average cost of breaches to*

business has nearly doubled since 2013."[1]

Most of the issues faced by communications providers are identical to those of business in general and the defences against cybercrime are not specific to telecommunications; they're applicable to all online systems where customer data is kept. When considering policy in this area it is therefore important not to single out an individual sector. Indeed the largest data losses are from healthcare (27%), education (17%), government (16%) and retail (12%) with the technology sector responsible for 2.6% (Trend Micro, 2015)[2].

Internet Telephone Service Providers

Because VoIP uses the same protocols as the Internet, ITSPs and their customers are susceptible to attacks from the Internet, consequently ITSPA members are very familiar with hacking and online fraud. However, the main locus of attack for ITSPs is financial; hackers try to breach VoIP networks and their customers in order to make expensive phone calls and benefit from the revenue sharing opportunities it presents. ITSPs therefore prioritise their development and management resources on systems and procedures to prevent a breach, rather than hope to limit damage if a breach occurs. This motivation is rooted in the knowledge that once breached, damage is inevitable and almost instant – large databases can be downloaded or destroyed in minutes.

The need for proportionality

Maintaining the security of data is a balance between the operational need for access and the risk of loss. There is no known method of totally securing data and still being able to access it. Each anti-hack countermeasure deployed by a data holder adds complexity, system limitations and cost and balancing these competing objectives against risk is increasingly difficult.

Not all customer data is equally sensitive and companies that hold customer data are different in scope, scale and technical expertise. It would be disproportionate for companies that hold small amounts of basic information on customers – name address, telephone number etc – to

[1] HMG/Marsh 2015 report: UK Cyber security, the role of insurance in managing and mitigating the risk

[2] US study: http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data

be required to have the same measures in place as those that hold large volumes of very sensitive information etc. – PIN numbers, credit card details etc.

Encryption – Issues to consider

In the media, much emphasis has been placed on the use of encryption as a line of defence against data loss. This is only very partially true – encryption is not a panacea. When it is useful, the system has already been compromised, the data is already lost and can be worked on at the criminal's leisure or sold on to more sophisticated criminals with the tools to decrypt it. Encryption is not perfect and through cryptanalysis it can be broken. For example, knowing that you are looking at a list of tens of thousands of postcodes that are encrypted with the same key can provide sufficient information to decrypt the entire list. Moreover, the encryption key itself then becomes a prime target for hackers.

Encryption is most useful when it is used to protect data transport over a hostile medium e.g. when data is exchanged between two parties over the Internet or a laptop being taken out of the office or situations where physical hardware can be stolen. But inside private networks it is far less useful. This is because customer data is in constant use by multiple users - for billing, reporting, and customer support and by customers for information and updates. Customer databases need multiple entry points and authorisations for both human and machine access. Encrypted information is unencrypted on the fly by the computer which processes it. If the hacker gains access to that computer as a user the data is automatically unencrypted and visible. Any breach that allows an attacker access to a component such as remote code execution and login access would also give them access to the encrypted data and the encryption key. There are very few remote attack forms where encryption would prevent data loss once the hacker has penetrated the system.

In these circumstances, encrypting data adds extra load on processors and systems, adds system and managerial complexity and cost and mostly does little more than provide a false sense of security. In reality, encryption of data inside networks is of most use not for the protection of the data, but from subsequent media accusations of security laxness.

Finally, encryption does not protect against the database deletion or interference.

Despite these reservations, for a limited number of risks, data encryption can bring some security value to a system, but for most it has no benefit whatsoever. Therefore, it certainly isn't a replacement for the other security measures – protecting access to systems, minimising SQL injection or code execution vulnerabilities. It has to be considered a last line of defence, added on top of all other reasonable measures.

And this is its greatest weakness: encryption is being promoted as a silver bullet measure that is cheap to implement and protects against a vast array of risks. This is simply not the case. It provides no protection in too many cases, and even when it does, it can still fail. Its greatest threat is providing a false sense of security that leads to a relaxed attitude towards the other measures that are more important. The priority for data security is in preventing the hacker gaining any form of access to start with.

ITSPA is, as always, welcome to discuss these issues further with the Committee and its individual members as and when required.