HM Government

Guiding Principles on Cyber Security

Guidance for Internet Service Providers and Government

December 2013

Contents

Industry Contributors

The Internet Services Providers' Association (ISPA) is the UK's Trade Association for providers of internet services. With over 200 members, ISPA brings together the UK internet industry to provide essential support through innovation, knowledge and experience in order to benefit the UK economy and society. Promoting collaboration and constructive dialogue between its members and the wider internet community, ISPA is an all-important driving force for the industry.

BT is one of the world's leading communications services companies, serving the needs of customers in the UK and in more than 170 countries worldwide. Our main activities are the provision of fixed-line services, broadband, mobile and TV products and services as well as networked IT services. In the UK we are a leading communications services provider, selling products and services to consumers, small and medium sized enterprises and the public sector.

Sky is the UK and Ireland's leading home entertainment and communications company. Around 40% of all homes have a direct relationship with Sky through its range of TV, broadband and home telephony services. Sky is the UK's biggest investor in television content, investing more than £2.5 billion a year. Sky is also the UK's fastest-growing home communications company and favourite 'triple-play' provider of TV, broadband and home phone.

TalkTalk is the UK's leading value for money TV, broadband and phone provider with 4 million customers across the UK. TalkTalk operates it's the UK's largest Next Generation Network which covers 95% of UK homes. TalkTalk is one of seven partners behind YouView, the internet-connected TV service, along with the BBC, IVT, BT, Channel 4, Arqiva and Five. YouView launched to UK homes in 2012 and in August 2013 TalkTalk announced it had signed up over 500,000 customers to the service. TalkTalk is also the only provider to provide a whole home parental controls service, HomeSafe®, to its customers free of charge.

We've come a long way since making the first ever mobile call in the on 1 January 1985. Today, more than 403 million customers around the world choose us to look after their communications needs. In 25 years, a small mobile operator in Newbury has grown into a global business and the seventh most valuable brand in the world. We now operate in more than 30 countries and partner with networks in over 50 more.

Virgin is a leading international investment group and one of the world's most recognised and respected brands. Conceived in 1970 by Sir Richard Branson, the Virgin Group has gone on to grow successful businesses in sectors ranging from mobile telephony, travel, financial services, leisure, music, holidays and health & wellness.

Virgin employs more than 50,000 people around the world, operating in over 50 countries. Global branded revenues of £15bn ($24bn) in 2012.

Introduction

As part of the UK's Cyber Security Strategy, the UK internet industry and Government recognised the need to co-develop a series of voluntary Guiding Principles to improve the online security of the ISPs' customers and limit the rise in cyber attacks.

Cyber security for these purposes encompasses the protection of information, processes, and systems, connected or stored online, and takes a broad view across the technical, people, and physical domains.

These Guiding Principles recognise that the ISPs (and other service providers), internet users, and UK Government all have a role in minimising and mitigating the cyber threats inherent in using the internet. While the internet offers considerable social and economic benefits by enabling open communication and open exchanges of information, there is a risk that our data and infrastructure could become compromised or damaged. The impact of this is already being felt, and will be felt even more as our reliance on the internet grows.

The Guiding Principles have been developed to respond to this challenge by providing a consistent and best practice approach to help inform, educate, and protect ISPs' customers from online threats. They are aspirational, developed and delivered as a partnership between Government and ISPs. They recognise that ISPs have different sets of customers, offer different levels of support and services to protect those customers from cyber threats, and have different business models based on their commercial offerings. The Guiding Principles represent a series of principles that all ISP signatories, in partnership with Government, should be aspiring to reach as a minimum.

The Guiding Principles build on, and compliment, existing sources of internet safety advice and guidance, for both businesses and consumers, and will continue to consider and learn from similar initiatives that have been developed overseas; and will sit alongside separate initiatives, for example those in relation to the protection of children online. We will implement the Guiding Principles through a partnership between the UK internet industry, Government, relevant independent bodies, such as Get Safe Online, within existing legal frameworks and respecting customer privacy, and against the backdrop of relevant international commitments around internet safety and cyber security.

They cover the following three areas:

- Section 1: ISPs' activities to help their customers protect themselves from cyber threats.
- Section 2: Government activities to help protect consumers and businesses from cyber threats.
- Section 3: Government and ISP activities in partnership to help protect consumers and businesses from cyber threats.

Section 1 - Internet Service Providers

1.a Awareness and Education:

Recognising that raising customer awareness of cyber security issues and education on how to manage them is central to engaging customers to practise safe online behaviour, ISPs will:

- Provide either their own education and awareness information and/or sign post to information elsewhere (e.g. Get Safe Online and national campaigns) in a clear and accessible place, such as on their websites, so that customers understand:
    - what basic online threats exist,
    - the symptoms they may experience from them,
    - how to spot potential problems with their computer or account,
    - how to fix problems,
    - how they can report crimes through Action Fraud.
- Seek to partner with other industry sectors to raise awareness amongst internet users of the importance and benefits of behaving safely online.

1.b Customer Offering:

To assist and empower customers to protect themselves from online threats, ISPs will offer tools and/or advice on security solutions and indicate from where solutions can be accessed.

Solutions offered could include some of the following features:

- Anti-virus software
- Anti-spyware
- Anti-spam
- Malware protection
- Firewall provision
- Advice on the back-up of data
- Identity protection
- Safe search and social networking protection

1.c Reporting Mechanisms:

To minimise the impact that cyber security threats have on their customers, ISPs will:

- Provide clear information on their websites and/or via their usual customer communication channels, about how customers and other Internet users can report compromises or threats.
- Have processes in place to escalate credible reports to facilitate risk mitigation. Notify their customers if they have their contact details, and in line with company policy, when they become aware of particularly unusual or novel behaviour which indicates potential compromise to a customer’s computer or account.

Section 2 - Government

Government published its Cyber Security Strategy in November 2011 which can be viewed at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf. This outlined a number of objectives to improve the cyber security of the UK, including public and business awareness and protection. Through this, we have committed to undertake the following key actions:

- We will work to educate and raise awareness amongst businesses of the importance of effective cyber risk management and mitigating cyber threats. Government launched its Cyber Security Guidance for Business in September 2012, targeted at FTSE100 companies, and BIS launched its Small Business Guidance for Cyber Security in April 2013.

- We will provide advice on cyber security. Get Safe Online, a joint public and private sector initiative, provides unbiased advice for consumers and businesses to protect themselves online and raises awareness of the importance of effective cyber security. An upcoming cyber security awareness-raising campaign, to be delivered by the Government and private sector will also be delivered across a range of media, targeted at consumers and SMEs to raise their awareness of cyber security.

- We launched in October 2013 the National Crime Agency (NCA) which includes a national cyber crime capability to deal with the most serious cyber crimes. The NCA will also support police forces across England and Wales to drive up wider national capabilities on cyber crime, including through shaping the training for mainstream policing.

- We will increase the security of Government Online Services. Government has rolled out an advisory tool across the .GOV.UK website and sections of the HMRC website which advises users that their internet browsers are out-of-date. Users can link to advice that is easy to understand, on what risks this poses and how they can update their browser. This initiative is being carried out in conjunction with Get Safe Online.

- We will work with education providers to develop teaching resources and cyber security learning materials to introduce younger internet users to the importance of using the internet safely and sensibly.

Section 3 – Government and Internet Service Providers

Section 1 and 2 of this document outline the activities that the ISPs and UK Government will undertake to help customers better protect themselves from cyber threats. This section captures new areas where UK Government and ISPs will work together on cyber security, and how the ongoing partnership that underpins this activity will be governed.

3.a Areas for joint working between Government and ISPs on Cyber Security:

Members of the partnership will work together to explore a number of issues, these include:

- Law Enforcement Agencies/ISP information sharing and action regarding identified risks and wider cooperation.

- Partnering between Government and the internet industry to raise awareness amongst customers of the importance and benefits of behaving safely online.
- ISPs to explore reviewing themselves against the 10 Steps to Cyber Security as appropriate to its business.
- Investigate potential ways in which issues can be brought to the attention of customers.

3.b Ongoing partnership and Governance:

Members of the partnership will meet on a quarterly basis, drawing in other Government and internet industry stakeholders as required, to implement these Guiding Principles and explore other issues for potential joint working. BIS will continue to lead in drawing this partnership together, in close coordination with the Home Office, OCSIA, the ISPs, and the Internet Service Providers Association.

This partnership will regularly review its progress against the activities outlined in this document. The Guiding Principles are a strategic objective in the UK's Cyber Security Strategy and so this partnership will provide an annual progress report to the OCSIA-led National Cyber Security Programme.

This publication is also available on our website at www.bis.gov.uk

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/13/1327