ISPA response to DCMS Consultation on Cyber Security Incentives

About ISPA

ISPA is the trade association for providers of internet services in the UK, we have over 200 members, 90% of which are SMEs. Our members cover the whole spectrum of access provision using FTTP, FTTC, wireless, satellite and hybrid solutions at a wholesale and retail level, and all play a critical role in delivering broadband and internet services across the UK to consumers and businesses.

Introduction

ISPA welcomes the opportunity to respond to the DCMS Call for Evidence on their proposed review of cyber security regulation and incentives. As an association representing companies that provide reliable and secure connectivity that have long prioritised security, ISPA's membership would like to note several points around:

- Recognition of the existing work and regulations in place to improve cyber security
- Acknowledgement that there is already a strong commercial incentive to invest in cyber
- Need for greater coordination across Government and regulators
- Need to streamline certifications to boost understanding and recognition
- Requirement to understand the impact of human factors, and the need to educate throughout businesses
- Impact of ongoing changes to internet standards, e.g. at IETF-level which risk undermining the ability of ISPs to monitor traffic
- Exploring the value of targeted incentives to support wider adoption

Increased prioritisation of cyber security

ISPA has regularly surveyed its membership to gain a better understanding of investment levels and priority given to cyber security within the business. From our most recent survey in 2018[1], we found that an overwhelming majority (94%) of ISPs surveyed indicated they expect to increase their investment in cyber security over the next three years. This represents a 15% increase compared to data collected in 2016 showing the increased importance already being placed in cyber security over the last few years.

Existing regulation

The increased prioritisation from members has been matched by a maturing of the overall regulatory framework. The introduction of the Networks and Information Systems (NIS) Regulations and the General Data Protection Regulation (GDPR) have seen a huge increase in awareness in the public

[1] https://www.ispa.org.uk/wp-content/uploads/ISPA-Cyber-Security-Survey-2018.pdf

domain as well as investment from industry. Given the scale of these regulatory changes, the short period of time since their implementation, and the proposed Telecoms Security Requirements (TSRs) which will already layer on top of this, there is a clear need to allow time for the existing frameworks to bed in before further regulation is considered. ISPA would be keen to see the outcome of Government's review into the impact of NIS and GDPR once completed.

ISPA would encourage policymaking in this area to be based on strong evidence. Given the existing trends to improve and prioritise cyber security, as well as significant regulation in this space continuing, ISPA's membership believes that any future interventions should be carefully considered, with awareness of this context to avoid confusion, complication and duplication. For global companies operating in the UK, there may be incompatibilities or grey areas between global and respective national cyber security frameworks which adds further complexity and chills investment.

Commercial incentives to invest

ISPA's membership would challenge the assumption highlighted by this consultation that there is no, or insufficient, commercial incentive to invest in cyber security for businesses. Within the ISP community there is a clear commercial interest to provide secure and reliable products with our members competing on security. Our members' business depends on providing reliable and secure communications which often includes the provision of security products and services. These can be provided at an additional cost or as part the overall service. We would welcome further support from Government to raise awareness of the importance of cyber security to businesses and consumers so that security becomes another aspect of choosing an ISP.

Regulatory cooperation and duplication

The complex network of Government departments and agencies involved in the creation and implementation of cyber security policy means that guidance and requirements are often published by many different organisations. The layering of regulation and guidance makes ever more complicated to navigate.

In this context, ISPs of all sizes can find navigating cyber security frameworks a challenge; however, smaller ISPs in particular can find keeping up to date on developments in cyber security policy a challenge. Without care, this complexity could serve as a barrier to entry to the market, dissuading new entrants and frustrating Government ambitions to foster competition. The Government and regulators should seek to coordinate advice and standards in a single place to ensure effective implementation of policy.

Moreover, ISPA would urge Government to streamline the number of organisations involved in the cyber security landscape, with more clarity around remits and relationships between them to minimise this confusion, including on areas such as breach reporting.

Multiplicity of certifications

Entrenching a culture of strong cyber awareness and prioritisation across the economy is a key objective for Government and one which ISPA strongly supports. It is important that initiatives to encourage this are not merely reduced to a 'box ticking exercise' but thoroughly communicated throughout.

Whilst cyber security certifications prove a useful tool to demonstrate cyber competence to businesses, there is a concern across ISPA's membership that the plurality of certification schemes creates confusion and encourages this 'box ticking' culture. The number of certifications, their overlapping nature, and the lack of wider understanding about what they stand for and how they interrelate.

This indicates a need to educate businesses more widely about the certifications and products that already exist in the market so they can make informed decisions. Moving businesses beyond pure compliance to active and risk-based approaches should be the standard aimed for across the UK.

ISPA would also propose that these schemes are simplified and streamlined to make this more accessible. Furthermore, and in the context of the UK leaving the EU, an effort should be made to align with international standards.

Cyber awareness and device security

As stated, a culture of strong cyber security is necessary throughout businesses for them to remain protected. Whilst ISPs are focused on protect their networks, there are still dangers borne out of human action. This will only be tackled through education rather than further regulation from Government.

Further to this is the impact of the increasing number of devices being used within businesses and in the home. The Government's steps to institute a base level of security in IoT devices through their secure by design programme is welcome. ISPA would urge that any interventions taking into account the behaviour of users and security of their devices are proportionate and in line with international standards.

Impact of ongoing changes to internet standards, e.g. at IETF-level

UK ISPs have long played a prominent role in supporting the online safety agenda and keeping customers safe online, through measures such as parental controls to help users manage what content they can see, protection from malware and other cyber security threats.

The role that ISPs currently play is due to be heavily influenced by a number of ongoing discussions around the definition of internet standards, primarily at the level of the Internet Engineering Task Force (IETF). While ISPs support the general aim of further securing and encrypting connections, there is a risk that, with the current direction of travel, ISPs ability to continue playing a role in securing networks will be diminished. These, and similar developments, need to be taken into account when the UK Government develops the regulatory cyber security framework.

Conclusion

Overall, ISPA would like to emphasise the need for all regulation and policy interventions involving cyber security to be better coordinated. Whilst it is clear that cyber security is an ever increasing priority, there is a need to ensure the landscape is easy to navigate for businesses. The existing, overlapping layers of regulation and oversight from many different bodies and areas of Government have made this difficult and, therefore, must be addressed in any action going forward. Similarly, certifications should be made simpler and easier to understand with education campaigns to ensure these messages have furthest reach.

The impact of any review into cyber incentives and regulation must therefore take this into account and ensure to use an evidence based, proportionate and coordinated approach.