ISPA Response to Ofcom Consultation on Security Guidance for Communications Providers

Introduction

ISPA welcomes the opportunity to submit comments on the review of guidance on security requirements for Communication Providers (CPs) consultation. We represent a number of companies that fall under the remit of the guidance and are subject to the security requirements set out by Ofcom and other public sector organisations.

Security is undoubtedly an incredibly important issue and ISPA members fully recognise this. It is an integral part of their business and company reputation, and CPs have been consistently working with existing bodies to continue to build the protection of their systems. As reported in our 2016 survey of members, 79% increasingly prioritise cyber security given 92% of respondents are subject to cyber-attacks on at least a monthly basis. ISPA members are not only acutely aware of the risks they face, but also continue to proactively work to mitigate them - 84% of those surveyed having reported incidents and 92% providing advice and tools.

In recent years, the regulatory framework has been considerably strengthened through the establishment of the National Cyber Security Centre (NCSC), the introduction of Privacy and Electronic Communications Regulations, and the impending implementation of GDPR, the NIS Directive and e-Privacy Regulations. This is in addition to stringent ISO accreditation. Any action that Ofcom takes in this area needs to clearly complement and enhance these already existing provisions around data protection, breach reporting and information provision as any duplication would increase compliance costs for our members without making a meaningful contribution to security.

In this response, we wish to raise concerns over Ofcom's approach as set out in the updated guidance which we feel will:

- create unnecessary complexity;
- duplicate reporting across other regulatory bodies;
- raise concerns around handling and guaranteeing sensitive data;
- put an unnecessary and unjustified additional burden on our members.

We will also outline a principles-based approach which we feel public bodies should consider when forming any regulation in this area.

ISPA concerns with Ofcom guidance

Unnecessary complexity

ISPA calls for a more streamlined approach to incident reporting that places little burden on communications providers already complying with regulations set out by the ICO. The call for 24/7 reporting mechanisms and the proposed three-hour window to report urgent incidents to Ofcom seems an unnecessary and unjustified addition to existing and effective requirements. These requirements are only set to increase with the implementation of GDPR and NIS Directive.

Duplication

These guidelines represent a duplication of the already significant demands on CPs, and that this duplication, and the lack of consistency between regulations, will put unnecessary and potentially overwhelming pressure on providers, especially smaller companies. This is particularly significant in relation to cyber incident reporting where CPs are already required to report breaches to the ICO within 24 hours under the Privacy and Electronic Communications Regulations (PECR). These regulations are set to be updated in the e-Privacy regulations and the reporting requirements of NIS Directive and GDPR will again create overlap.

Increased data sharing

We are concerned about the increase in data sharing that will be generated by the implementation of this guidance. Members' main concern regards the lack of assurance from Ofcom about the security of their data once shared with the regulator, with no indication from Ofcom on its intentions for the use of said data. This is especially pertinent given the sensitivity of the data involved in incident reporting. We feel the creation of any additional risk needs to be fully justified and the case here has not been made.

Justification

The National Cyber Security Centre (NCSC) was created last year to provide consistent and consolidated cyber security advice and support to businesses in the UK. Members have been working closely with the NCSC since it opened and recognise that it represents a significant improvement in how Government handles cyber security and the expectations put on industry, including an active cyber defence agenda. There are also new and existing reporting requirements under PECR and soon under GDPR that will have some impact on CPs. With these additional obligations and the creation of the NCSC, we fail to see the justification for Ofcom needing expanded reporting requirements. Clearly the security of communications services is

of great importance, however, this guidance seems to overlook the standard of protection, the regulation and the reporting requirements already present in the sector already and instead of reflecting this, places disproportionate demands on CPs.

Principles approach

While suggesting generic standards and meeting external certification may make an external security audit or compliance check more straightforward for Ofcom, it does not necessarily do anything to improve security or increase resilience. ISPA therefore recommends that security requirements are upheld using a principled approach rather than a prescriptive set of demands. This is in line with the EU Network and Information Security Agency (ENISA) on network security. ENISA advises National Regulatory Agencies such as Ofcom to adopt flexible approaches in relation to specifying standards. ISPA recommends Ofcom's approach is thus based in principles including flexibility, necessity, proportionality and data security.

Flexibility – There should be an acceptance that specific government standards programmes and other accreditations, such as Cyber Essentials Plus mentioned in the guidance, are not the only way to secure against cyber risk, and a more flexible approach is necessary to assess a provider's security systems to determine compliance.

Necessity – Given the existing regulation already in this area for CPs, Ofcom should ensure that all new guidance is strictly necessary for the protection of services. This would help guard against the duplication of demands from several bodies putting an increased burden on providers.

Proportionality – The demands on providers to maintain security should be proportionate not only to the risk presented, but also the size and focus of the provider itself. As such, regulators should be mindful of the differing impact security demands will have on different businesses before they impose unilateral demands on the whole sector.

Data Security – All interventions should be considered in relation to its impact on data security and thus include necessary measures to protect against data breaches resulting from the required sharing of confidential data with regulators. This closely relates to necessity and the importance of only imposing demands on providers when the information sharing is entirely essential for the regulator.

Harmonisation – Many CPs work not only in the UK but across borders where they are subject to varying demands of regulators in individual states. ISPA calls for more harmonisation across borders especially with EU member states. It is not practical for pan-EU or global providers to meet the national-specific standards or certification requirements for each jurisdiction. Ofcom should ensure that it does not cause some providers to shoulder an undue burden or be placed

at a disadvantage just because they choose to rely on their internal bespoke controls rather than seek external certification. There should be an awareness of the complexity involved in navigating multiple different requirements across countries and an attempt made to maintain consistency. We would argue that Ofcom is not following the ENISA guidance which calls for flexibility and recognition of the difference in size, operations and global reach of ISPs when designing and implementing NRA guidance.

Conclusion

ISPA feels that there is already considerable regulation in this area on CPs, who are striving to maintain excellent cyber security standards, fully cooperating and engaging with the relevant authorities already. As such, this guidance adds an additional, unnecessary burden upon providers which Ofcom has failed to justify. We suggest that all new regulation in this area should clearly enhance rather than duplicate existing provisions, to strengthen security rather than diverting resources with increased compliance costs. Furthermore, interventions should be designed using the principles approach outlined here and avoid setting out further prescriptive demands on CPs.