Cyber Security Working Group

Introduction

The reliance on the digital economy means the Government and regulators are pursuing a more preventative, interventionist and collaborative approach to cybersecurity to further trust and resilience following high profile incidents. A recently updated five-year cybersecurity strategy doubled Government spending and a new central body has launched to drive and direct policy in this area. ISPs are a crucial part of the cyber security chain and 2017 will see greater regulatory compliance demanded of businesses as the UK Government sets out how it plans to implement significant European regulations, such as the GDPR and NISD in 2018. Unlike more commercial issues, cyber security is an area where the ISPA membership is often in agreement.

Topics/Themes

Cybersecurity

- Role of ISPs in protecting networks and customers
- Regulatory compliance (NIS Directive implementation, Investigatory Powers Act)
- Public/business awareness of cybersecurity
- Skills gap

Cybercrime

- Creating a more hostile environment for cyber criminals
- Cooperation with law enforcement

Communications data

- Implementation/compliance around Investigatory Powers Act

Objectives

1. ISPA to intensify contact and relationship with key stakeholders, including Ofcom and DCMS
2. To ensure ISPA is a lead voice in the cyber security debate through proactive ISPA cyber security initiatives and work
3. To ensure members are aware of ongoing and upcoming regulatory compliance developments
4. To ensure ISPs are viewed as responsible, secure actors by policymakers and stakeholders

Upcoming developments

- Active cyber defence, making it harder for
- Legislative compliance (GDPR, NIS Directive, etc)
- Parliamentary inquiries into the Future of Policing and National Security