Ofcom's role in cyber security

UKNOF
Edinburgh

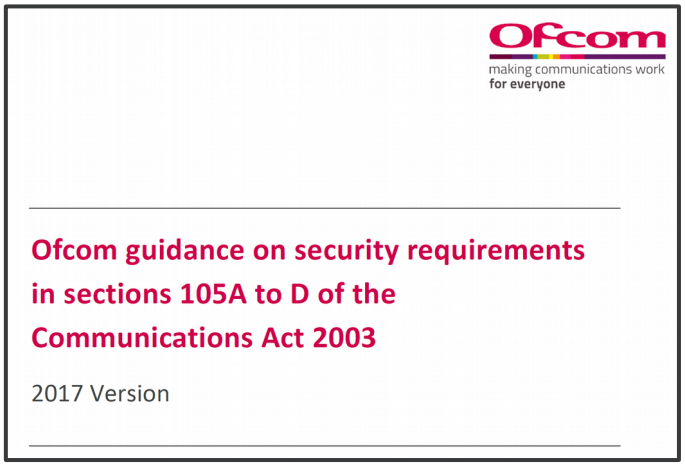
Huw Saunders

Director, Network Infrastructure

Ofcom and cyber security

Area of growing importance across all sectors, with new legislation to match

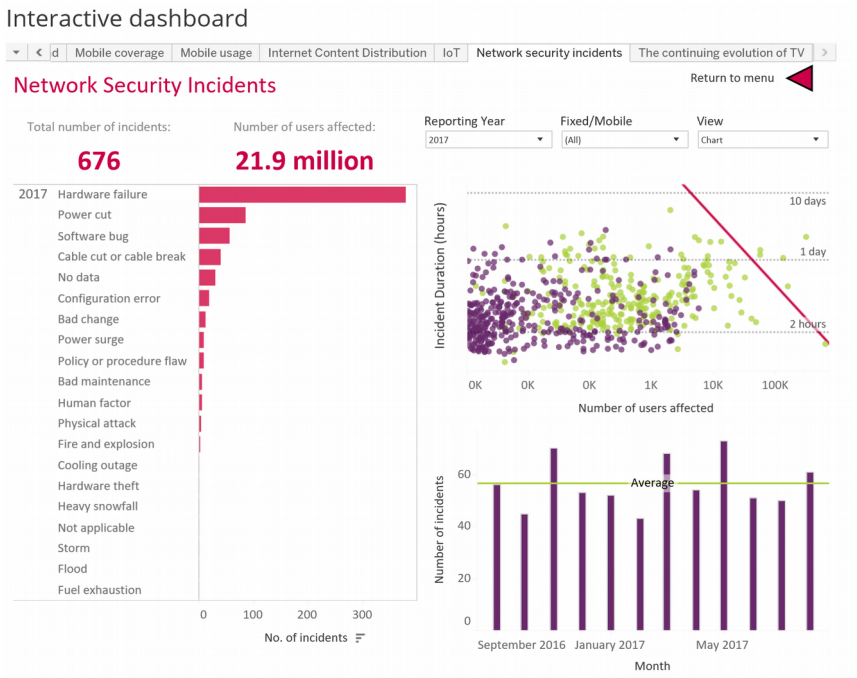
- Involvement in broader security obligations since 2011
- Long considered cyber to be in scope but this area is now getting more attention:
  - Increasing threat
  - Government cyber strategy
  - More pro-active approach – TBEST etc
  - New legislation - NIS



Comms Act - Section 105A-D

Security obligations for communication network and service providers

- **Security measures**
  "…providers must take… measures appropriately to manage risks to security…"
- **Report incidents**
  "…provider must notify Ofcom of a breach of security which has a significant impact on the operation of…"
- Ofcom's role
  - Issuing & updating guidance
  - Following up & investigating reported incidents & any other concerns as needed
  - Publishing a summary of incidents

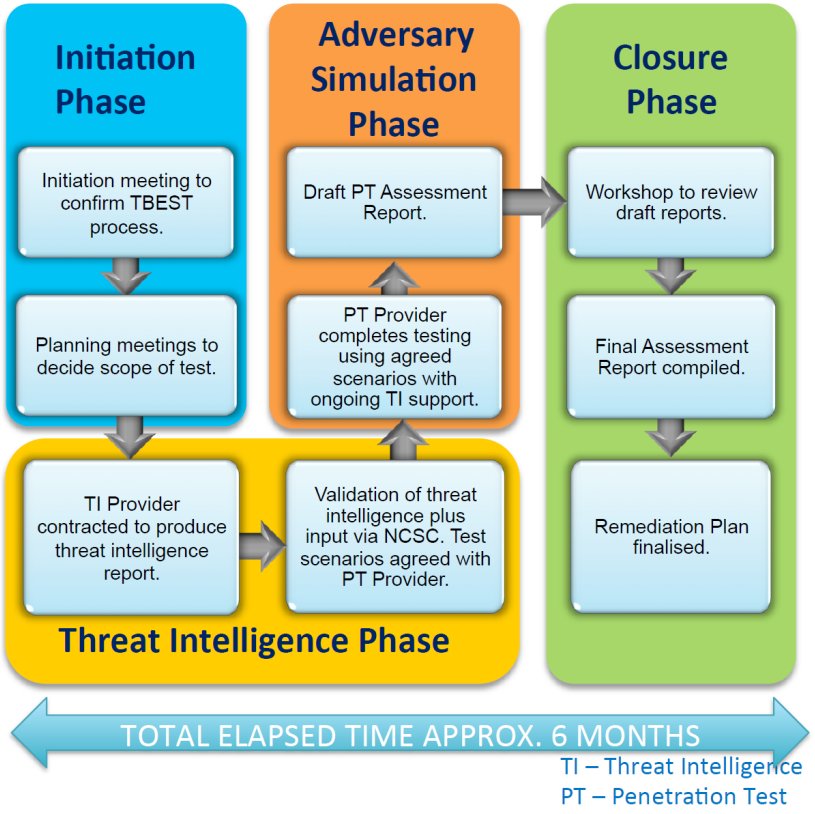


What is TBEST ?

CBEST, used by the Finance sector to enhance the sectors ability to protect against cyber threats, was identified as Cyber Security best practice. Established in 2015, CBEST has a proven track record of conducting safe yet realistic simulated attack on the people, processes and technology that may compromise a firm's cyber security controls.

It uses threat intelligence to align the simulation to the latest sophisticated and persistent attacks against critical systems and essential services. The aim is not only to test a firm's defences, but also its ability to detect and respond to a range of external attackers as well as people on the inside.

In 2016 DCMS initiated a programme of work with NCSC, Ofcom and key stakeholders from Industry to review whether CBEST can be adapted for the Telecoms sector. This resulted in the draft Telecoms version TBEST.



Network and Information Systems Regulations 2018

New Regulations that introduce security duties on infrastructure sectors

- Made law in June 2018
- Transposes the EU NIS Directive into UK law
- A strong cyber focus, but obligations cover security more widely
- *"aims to raise levels of the overall security and resilience of network and information systems across the EU"*
- Establishes need for:
  - National cyber strategy
  - National CSIRT
  - NIS SPOC & Technical Authority
  - Security and reporting obligations

Sectors in scope of NIS Regulations:

- Electricity
- Oil
- Gas
- Air Transport
- Water Transport
- Rail Transport
- Road Transport
- Healthcare
- Drinking Water Supply & Distribution
- **Digital Infrastructure**

- Online Marketplace
- Online Search Engine
- Cloud Computing Service

Digital Service Providers

Ofcom ask of UKNOF Attendees

The NIS legislation mandates that if you are in scope of the Directive that you nominate your company to Ofcom

- View Ofcom's guidance on the NIS Directive - https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/guidance-network-information-systems-regulations
- Review the NIS Directive legislation - http://www.legislation.gov.uk/uksi/2018/506/pdfs/uksi_20180506_en.pdf
- If you exceed the thresholds and are in scope then inform Ofcom at nis@ofcom.org.uk
- Contact mike.lee@Ofcom.org.uk of you have any questions

NIS Thresholds for DNS, TLD and Internet Exchanges

Top level domain (TLD) Name Registries
TLD Registries who service an average of 2 billion or more queries in 24 hours for domains registered within the Internet Corporation for Assigned Names and Numbers (ICANN). [Note the threshold specified is an annual average and shall be based on the best available historic data from the preceding 12 months; and the threshold specified excludes growth of traffic load due to malicious activity such as DDoS attacks]

Domain Name System (DNS) Service Providers
DNS Service Providers who provide DNS resolvers offered for use by publicly accessible services, which service an average of 2,000,000 or more requesting DNS clients based in the UK in 24 hours; or DNS Service Providers who provide authoritative hosting of domain names, offered for use by publicly accessible services servicing 250,000 or more different active domain names. [Note. the thresholds specified are on annual average and shall be based on the best available historic data from the preceding 12 months)

Internet Exchange Point (IXP) Operators
IXP Operators who have 50% or more annual market share amongst UK IXP Operators in terms of interconnected autonomous systems, or who offer interconnectivity to 50% or more of Global Internet routes. Note. Global Internet routes means the total number of active entries within the Global Internet Routing Table averaged per calendar year.