Comms Council UK's response to Ofcom's 'General policy on ensuring compliance with security duties' consultation

About Comms Council UK

Founded in 2004 (and formerly known as ITSPA) Comms Council UK is a UK, membership-led organisation that represents companies who provide or resell business and residential customers voice services over data networks (VoIP) as well as other "over the top" applications including instant messaging and video. The membership is a mixture of network operators, service providers, resellers, suppliers and consultants involved in a sector that is diversifying rapidly from just voice services to other innovative IP applications.

Contact

For more information, please contact:

Comms Council UK
team@commscouncil.uk
020 3397 3312

Presumption of the Will of Parliament

The new security regime is complex and only partly in force. While overarching duties are in place (sections 105A-105D of the Act) and it is correct that Ofcom consult on elements which are currently in force, Comms Council UK would question whether it is appropriate or necessary for Ofcom to fetter its discretion with instruments that are not yet passed, or to second-guess or presume the will of Parliament.

The draft regulations which the Secretary of State may make under sections 105B and 105D as well as the draft code under section 105E are not in force; they have not been laid before Parliament – indeed, the are presently being consulted upon. The consequence is that some of the consultation's subject matter risks being obsolete at best, or inappropriate at worst.

This notably applies to parts of the discussion on testing (Section 4 of Annex 5 of the Consultation) and Accountability (in section 5 of Annex 6) given that proposed Regulations 14 and 10 goes to these subjects, as does the Code. Matters going to tiering, such as section 3 of Annex 5 also fall into this category.

Ofcom will likely need to reconsult if any part of the draft Regulations or Code changes that have been presumed in the Consultation. Comms Council UK considers that the correct approach is for Ofcom to consult only on powers it has, not powers it might or might not have in the future.

In this case we recognise that the subject matter at hand is intertwined with the widely drafted and in force general duties at the start of section 105 of the Act, which obfuscates the issue. However, as a general point of principle, we would be concerned if Ofcom were to regularly second-guess, fetter itself or otherwise presume the will of Parliament when carrying out its duties.

Reporting Regime

The previous reporting regime was highly problematic and very difficult for a provider to navigate and Comms Council UK is disappointed that the previous thresholds for reporting have largely been copied over.

For example:

- What is national mainstream media coverage? Given that BBC Solent can be streamed online nationally, does that qualify? As far as Comms Council UK is aware, The Sun is not readily available in Liverpool – does that mean it is not a national source? Ofcom needs to be more prescriptive as to precisely what it means in this regard, preferably with a set list, or a quantitative criterion such as the scope of a broadcast licence.
- What are trade news sources? Does Nigeria Communications Week count? Again, Ofcom need to be more prescriptive. The telecommunications industry is naturally furtive; any ambiguity is going to be read in the favour of the entity with the security compromise trying to avoid reporting.
- What is a major cyber security breach? The loss of bank account details for one individual will be construed as major by that individual, but in the context of cyber security breaches, the loss of just one customer's data is hardly recognised as major.
- What is an End User when businesses are considered? Is it Subscriber? i.e. the counterparty which could represent 5,000 hosted PBX handsets? What number of potential 'users' do you ascribe to a 200 channel SIP Trunk, given they are sized on concurrent calls not end users. Equally, with a hosted PBX, meeting rooms, warehouse phones etc all obfuscate the number of end users. Guidance is needed on how to calculate end users for businesses – again, any ambiguity is going to lead to underreporting.
- The section "Outages affecting the ability of a user to contact the emergency services" is contradictory to Table 1. A literal reading of 'any security compromises affecting networks or services involved in connecting emergency calls' covers any network connecting an end user to 999/112. This renders the first two rows of Table 1 and the first bullet under "General" redundant.
- Ofcom may wish to be cautious with "any single security compromise that affects the provision of wholesale services to both fixed and mobile communications providers".

While this removes the ambiguity on who must report an outage where a switchless reseller is the provider to an End User and not a network, as well as ambiguity in calculating affected end users for wholesale services, it introduces other issues.

- If a major wholesale network had an outage, a smaller network subtended from it should, based on General Condition [A2] have appropriate resilience in place and fail over to alternative carriers, or at least an alternative switching centre of that wholesaler – when this works, it should be irrelevant to the regulator.
- The statutory definition of 'security compromise' is drafted so widely that common-or-garden, vanilla packet loss is a security compromise. We doubt Ofcom really intend for every wholesaler to report every lost packet amongst the terabits of traffic they convey between them each hour. Rather we suspect the requirement needs some additional detail or criteria to ensure that Ofcom are not overwhelmed with meaningless and irrelevant reports.

These criteria make more sense (although retain some problems) when viewed from the prospective of a major vertically integrated residential network. They become especially problematic when the 440+ other Public Electronic Communications Networks are considered.

Comms Council UK can speak from experience of advising members on these criteria – they are difficult to comprehend and rather impenetrable, which is less than ideal given the timescales to report incidents

in. We are more than happy to walk Ofcom through some real-world examples of the issues in interpreting these criteria if it would assist.

We would also suggest that the urgent reporting number is not published in the guidance, but instead made available via the Numbering Management System or other password protected area or made available on demand (like the Do Not Originate List), lest Ofcom personnel are woken up by pranksters in the middle of the night.

Testing

Ofcom has the power to mandate a form of testing by way of section 105O of the Act. However, it has not chosen to be more prescriptive in the scenarios in which it might mandate such testing.

For example, as it stands, the Government has signalled by way of draft Regulations its intent to exempt micro-entities from the Regulations. Yet there is nothing in the Consultation that would suggest Ofcom would fetter its mandatory testing such as requiring a micro-entity to procure expensive tests – such tests which may be at a cost which puts it out of business. The very existence of such an unfettered ability to mandate a small business to undertake such a disproportionate burden is itself a barrier to entry.

A sophisticated provider may well point to section 3 of the Act and make the compelling argument that Ofcom's general duties limit its ability to mandate disproportionate testing by way of section 105O; however, prospective new entrants and new entrants may only go as far as the guidance, which needs to make this need for proportionality clear therein.

Resilience Requirements

The draft guidance given in Annex 6 makes it clear that measures taken by providers should be appropriate and proportionate, however this is an extremely subjective matter. As touched up on earlier in this response in relation to a data breach, an individual's loss of service would likely be considered a minor breach to a large provider but to the individual, who is perhaps running an emergency callout or a medical service, it could have significant and long ranging consequences.

In contrast, a seemingly insignificant compromise by a major network could have an extreme impact once extrapolated across a large range of resellers and remain unreported. A relatable and simple example would be dropped prefixes on ported numbers as a result of a database upgrade. This is something which still occurs far too frequently, but many would not consider a significant and reportable resilience incident.

The 'appropriate and proportionate' approach is of course entirely welcomed and sensible, however, to avoid the risk of under reporting we would consider some more detailed guidance in this area useful. In particular where providers fall into Tier 3 where proportionality is likely to be more ambiguous. Perhaps some real-world use case examples could be useful in this guidance.

For example, the guidance points to NICC documents ND1643 and ND1653, the latter requiring significant and extensive testing which would be a considerable burden on all but the largest networks but taken at face value all tiers of networks will feel compelled to comply when reading the guidance alone.