New Telecoms Security Regulations and Code of Practice consultation – CCUK response

Comms Council UK

1. Comms Council UK (CCUK) is a membership-led organisation that both represents and supports telecommunications companies that provide services to business and residential customers in the UK. We keep Britain talking in its various guises by providing or reselling voice services over data networks (VoIP) as well as other "over the top" applications including instant messaging and video.

Contact

For more information, please contact:

Comms Council UK
team@commscouncil.uk
020 3397 3312

2. Our membership is a mixture of network operators, service providers, resellers, suppliers and consultants involved in a sector that is diversifying rapidly. Comms Council UK (formerly known as ITSPA) represents its members at a policy level, builds coalitions to collaborate on industry initiatives and provides a platform to help members prepare for change, learn about new trends and develop new business relationships.

Introduction

3. CCUK recognises that secondary legislation rarely receives the public consultation and engagement with the Government such as we are experiencing with the draft Electronic Communications (Security Measures) Regulations 2022 (the "Regulations") and CCUK would like to express its gratitude for the opportunity to make representations on what is a highly complex and technical subject.

4. We also recognise that the Public Bills Office and many civil servants are not telecommunications experts and appreciate how certain provisions may have been drafted in good faith, but have potential consequences which may not be readily apparent except to those vested in the industry. With that in mind, we trust that the following – while critical of certain aspects of the proposals – is a constructive response intended to improve the draft Regulations and the Code so it better represents the intent of Government.

5. This response is broken into four sections; three of which represent significant issues with specific Regulations which the CCUK membership wishes to raise as a priority. The fourth relates to the inflationary pressure the Regulations and Code will drive; CCUK does not take a position on that – it is for Government to balance the cost of living with national security, not the industry, however, there will be price rises driven as a direct consequence of the proposals.

Regulation 12 – updates

6. At a fundamental level, CCUK understands the intent of Regulation 12 to require an in-scope provider to apply a patch (or, as appropriate, a hardware change) which addresses a security compromise (as defined in the Telecommunications (Security) Act 2021 (the "Act")) within fourteen days of it being available, unless the Board-level authority appointed pursuant to Regulation 10 creates a written record of the reasons why that is not appropriate.

7. We understand the purpose of the regulation in relation to critical security vulnerabilities which can compromise critical national infrastructure or national security. However, we would also make the point that the market is relatively self-correcting in this respect. User demand to protect their data or the integrity of their services dictates such mitigations are deployed rapidly, and in our experience, is something that is done rapidly by any credible or at-scale operator.

8. However, a typical communications service provider may have several vendors, some of which may issue multiple updates a day. The administrative burden for an enterprise whose turnover is £632,001 a year (i.e. just over the micro-entity threshold) to review and make decisions on potentially hundreds of updates is unworkable and creates a moral hazard.

9. Some providers may be incentivised to 'blindly' apply patches which in turn may cause service failures, instabilities or even create their own security compromises – in this sense, the medicine may be worse than the disease.

10. Further, good technical practice dictates a timescale longer than fourteen days for all but the most critical of patches. It is very common (especially in central and local government and enterprise contracts) for maintenance to telecommunications services to require notice (itself anywhere from three to twenty-eight days being a regular requirement) and application to a sandbox environment for regression testing. Indeed, a provider is unlikely to countenance giving notice of a maintenance window until it has itself completed regression testing in its own test environment – and essentially, testing the roll-back position. DCMS may remember a day-long outage of the O2 data network in 2012 which was a result of a failed update to the Home Location Register, and the roll-back failed too. There is a lot of industry-learning which underpins the process we describe above; not dissimilar to the aviation industry, the way things are done today is because bad things happened in the past.

11. This leads to a situation which undermines the intent of the Regulation; every single patch will automatically be subject to the Board-level "exception" because of the technical reality of testing and implementing in a safe and responsible manner.

12. Regulation 12 is too prescriptive to cater for the array of updates a provider can be faced with – in fact, we would suggest it is too long for the most critical of updates to

a zero-day vulnerability, while simultaneously being far too short for the balance of updates, which can range from moderate to inconsequential – such is the wide definition of a 'security compromise' in the Act, many updates theoretically improve security but do not substantively in reality deliver on the underlying purpose of the Act. These inconsequential updates are often batched up to a quarterly or biannual 'feature-drop' as opposed to being applied as they become available.

13. It should also be noted that the application of a patch often requires network down-time. It is not a ridiculous proposition to say that Regulation 12 drives providers to routinely turning off the UK's telecommunications infrastructure to apply patches within an arbitrary deadline. Imagine if a town's electrical substation had to be turned off for an hour every week for maintenance that could otherwise be batched up and applied less frequently, and you have a parallel to the direction of travel here. In an increasingly 24/7/365 economy, especially the digital economy, this is likely to frustrate citizens.

14. To reiterate, the fundamental premise, being (as we understand) that providers should not leave critical vulnerabilities without remedied is one we agree with. The question is about taking Regulation 12 to the next level of detail and differentiating between the criticality of vulnerabilities and patches. There already exists a well-respected and widely adopted framework which the Government could leverage for this purpose: Common Vulnerabilities and Exposures[1], which we note is funded by the US Department for Homeland Security and has inherent credibility as a result.

Regulation 3(3)(h) – The reliance on UK resources

15. The underlying intent of the Government, in securing the operation of UK networks in the event of a state-actor or terrorist materially affecting, or totally compromising, the international gateways is again, not one we disagree with. The question is about the wording and the proportionality.

16. Firstly, the proposed law applies to a service provider with a turnover of just £635,000. Using Ofcom's own average revenue per domestic residential fixed connection of £37 a month[2], that's a service provider with just 1,431 residential customers. In terms of a provider with small business customers, that number is materially less as the average spend is likely higher.

17. Frankly, in the event of (for example) all of the UK's submarine cable landing stations being compromised, the performance or otherwise of a provider with just 1,431 residential customers is, in comparison to the whole, irrelevant. That's 0.005% of UK

[1] https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures
[2] §5.4 of "*Quick, easy and reliable switching: Statement and consultation on a new landline and broadband switching process and improved information for mobile switching*" published by Ofcom on 28th September 2021

households[3].

18. If BT, which provides the 'National Grid' of telecommunications through Openreach, were to experience consequences because of such a compromise, the impact would be near-universal to the citizens of the UK. The draft Code makes a valuable distinction on other rules at turnover thresholds of £50m (112,790 average residential customers) and £1bn (2.25 million average residential customers).

19. In an ideal world, the UK would be the centre of excellence for telecommunications equipment vendors; Cisco and Juniper would be based in Milton Keynes and not California. AWS would have built their first availability zone in London not Dublin and early adopters (noting the UK's membership of the European Union and the 'certainty' that brought at the time) of cloud computing, which innovated for the benefit of UK citizen-consumers, would not have core infrastructure in Ireland. Covid-19 would not have driven the more rapid adoption of telecommunications services embedded in enterprise-software, such as Microsoft Teams or Google's Gsuite – organisations which, given their software-minded approach, have core infrastructure serving the whole of the UK and EU from two or three locations – Dublin, Amsterdam and Frankfurt are not an uncommon position. Indeed, from one resilience perspective, that is preferable – Regulation 3 drives the industry to be concentrated solely in AWS London, instead of being more diversified as it is today. Ultimately, DCMS need to balance the risk of a compromise to international connectivity to creating a target in the limited number of cloud compute resources based in the UK.

20. Finally, in consideration of this point (and expanded upon in the fourth section below), the UK was once the most liberal telecommunications market on Earth. This has fostered competition and lowered our telecommunications prices to one of the most competitive levels of any country. Achieving further efficiencies has meant that customer service is off-shored – not necessarily to India, but maybe realising economies of scale across multiple markets with a central call centre, or leveraging daylight hours around the world to provide 24/7 support, for example. Regulation 3, as drafted, forces a reversal of this trend to on-shoring all capabilities and brings with it inflationary pressure by having to pay a substantial uplift to resource that capability 24/7 with a night shift. The UK economy has long been accused of having productivity problem – reversing otherwise efficient support models only adds to that issue.

21. The solution is for the obligations need to scale with turnover – as used elsewhere in the Code. We would suggest that Tier 3 operators are only required to 'consider the potential of an interruption to international connectivity in their network design, mindful of their statutory obligations regarding un-interrupted access to the

[3] Office of National Statistics Households Dataset as at 2021

emergency services'.

22. Tier 2 operators may be better-suited to reasonably ensure that they can operate a basic service, noting that they will be isolated from (for example) third line support from Cisco or Juniper. From the impact we describe above for a Tier 1 operator, given their likely UK market share, the current drafting is probably closer to what is needed, but again, Cisco et al are not going to relocate their Centre of Excellence to the UK from California – therefore certain faults that develop during a period of no international connectivity cannot be rectified.

23. Incidentally, in the absence of international connectivity, international direct dial services will not work, therefore the concept of 'operating as normal' is impossible and the Regulation or Guidance requires some fettering regardless. Nor will patches be able to be downloaded and applied, so the fourteen (or whatever the outcome following the first section of this response is) days target would have to fall away.

Regulation 4(4) - Encryption

24. As with the other Regulations discussed above, we understand the underlying intent – the Government does not want sensitive traffic sent over the public internet without any form of encryption. We agree – telecommunications networks need to ensure that a malicious actor cannot intercept the content of signals.

25. However, Regulation 4(4), due to its reliance on the broad definition of 'network provider', itself just a restatement of Public Electronic Communications Network ("PECN") defined in the Communications Act 2003, creates significant issues.

26. The Regulation needs to differentiate between a conduit and a provider. At present, an internet exchange such as LONAP or LINX, which themselves meet the PECN definition, would be required to apply encryption to signals received at the ingress point, then decrypt at the egress point. Even though they are just a conduit for communications between two other networks.

27. That's like asking the Royal Mail to add a security seal itself to every letter that leaves a credit card company and remove it just before it goes through the letterbox – instead of simply asking the sender and receiver to have arrangements to ensure a nefarious person in the sorting office, or others, cannot read the PIN number through the envelope.

28. The consequence would be a material increasing in latency and packet loss as the processing overhead of many superfluous encryption and decryption routines slow the transmission of data. This would lead to unusable applications, e.g., extensive lag in video games, or worse, constant time outs as users attempt to access services which configured to drop a port after too long a wait.

29. The solution is to differentiate, perhaps in the Code or other guidance, between types of networks and between encrypted signals and secure conduits.

30. For example, with the planned commencement date of October 2022, the Regulations would come into force at a time where British Telecommunications plc still operates a significant TDM estate. They say it will be decommissioned by 2025, but many in the industry suspect it will be until at least 2027. TDM cannot be encrypted – however, its infrastructure is somewhat secure by design. Its "conduits" are secure – just as two voice operators' interconnects over LINX or LONAP are if they deploy IPSEC or other tunnelling protocol. In that scenario, LINX or LONAP being mandated to encrypt again adds nothing.

31. It is possible that the meaning of 'or otherwise' in Regulation 4(4) is meant to capture the scenario that we outline, but the Code does not appear to allow for our 'conduit' interpretation as at §3.28 it talks about encryption where possible in transit, yet §3.29 mentions TLS and IPSEC which in turn do support our interpretation, providing that certain conduit providers like internet exchanges, are afforded certain exemptions in the definition of 'network provider'.

32. To conclude, we would suggest that Regulation 4(4) uses different language than 'network provider' and instead binds 'network providers which are transmitting or are receiving signals other than as a simple conduit for those signals must use [..]'. This will also need elaboration in the Code or other guidance so that conduit cannot be misconstrued to undermine the intent of the Regulation.

Inflationary Pressure

33. The UK was one of the most liberal telecommunications markets on Earth – the Act changes that paradigm and creates barriers to entry. It is possible some operators will choose to exit the market as a direct result of the Regulations and Code, reducing choice and competition, which in turn removes one of the checks and balances on the very aggressive pricing enjoyed by UK consumers for their services.

34. Those that remain will have an increased cost-base – in terms of on-shoring operations currently run at a significantly lower cost abroad, diverting capital away from innovation into compliance matters (such as encryption or reviewing and applying patches, penetration testing) all of which, in a perfect market, gets passed onto the consumer. CCUK can assure DCMS that no-one can ever credibly refer to telecommunications as 'margin-rich' or 'profit-intensive', therefore the perfect market academic theory is likely to resemble reality.

35. We are aware of a few service providers that have stated that current central and local government contracts are not sustainable at the current price point if the Regulations come into force; a double-whammy of an increase on the burden of the Treasury and on consumer pockets at a time of an (generationally at least)

unprecedented increase in the cost of living.

36. As we said at the start, the balance of the tension between national security and cost of living is one for Government to consider and decide in the round, all we can do as an industry is point out that the policy will increase prices at a rate in excess of inflation.

ENDS