Verizon response to Ofcom's consultation on the Security Procedural and Resilience Guidance

Introduction

Verizon is grateful for the opportunity to feed into Ofcom's consultation on the Procedural Guidance for the Telecommunications (Security) Act 2021 and the Resilience Guidance.[1]

Verizon is a global player. Outside of the United States, Verizon provides a broad range of global communication products and enterprise solutions, predominantly to large business and government customers. We are established in most European Union ("EU") Member States ("MSs") and the UK, and provide services in over 150 countries worldwide.

This paper covers the following areas:

- Verizon's commitment to security and our policy principles; and
- Specific comments on the guidance.

Verizon's commitment to security and our policy principles

Verizon is fully committed to the ongoing security and integrity of its networks globally; it is one of our key priorities. Our customers in the UK are governments and global and large enterprises, and therefore expect the highest levels of security. We therefore continually evaluate our risk profile, including supply chain risks, and we take appropriate measures to partner with trusted vendors and suppliers. As our network and the external environment evolve, we will continue to evaluate and take appropriate steps to address security risks through the use of consistent, global security processes.

Verizon believes that the following policy principles are essential to build an appropriate and effective policy framework reflecting the dynamic nature of cybersecurity. Policies should:

- define principles rather than prescriptive measures and avoid country-specific measures; allowing companies the flexibility to define their own consistent global security policies and procedures in order to achieve those principles;
- be risk-based, flexible, robust, embrace collaboration and promote innovation-friendly and technology-neutral solutions;
- foster voluntary public private partnerships, as collaboration is and will continue to be essential to build effective cyber resilience;

[1] Published 8 March 2022, https://www.ofcom.org.uk/consultations-and-statements/category-1/ensuring-compliance-with-security-duties

- draw on existing, interoperable and global best practices and voluntary industry standards and certifications that improve security while enabling growth in international commerce through digital means; and
- promote horizontal rather than sector-specific regulation when regulation is proven to be necessary.

Verizon supports the overall objective of the new security regime to build a highly secure telecommunications market in the UK, but our policy policy principles lead us to the view that, as a global company, we want to continue being able to have robust global policies and measures in place, without the unnecessary complexity of prescriptive UK-specific measures which add no additional security benefit, but only additional burden.

Specific comments on the guidance

We have some specific concerns in relation to the draft Procedural Guidance. These are:

- **Intense rolling programme of information requests** - Ofcom will use its statutory information gathering powers to issue a series of information requests focused on sections of the Code of Practice. For Tier 1 operators, this will be issued every six months, and for Tier 2 operators, these will be issued every nine months. We understand that Ofcom intends to issue draft versions of the requests - we strongly support this approach. We are however concerned that the rolling programme of information requests will be very resource-intensive for both operators and Ofcom. Operators will be heavily resource-impacted by having to work towards compliance with the lengthy new regime under the Code of Practice. For Ofcom, we understand that the UK Government indicated that there are eleven Tier 1 operators (seven fixed, four mobile), but there will likely be a much greater number of Tier 2 operators given the wide range of the currently proposed threshold (£50m - £1bn annual relevant turnover). We question whether this is the most appropriate use of resources, and we consider that Ofcom should instead allow Tier 2 operators to focus their efforts on meeting the compliance requirements instead of responding to complex information requests. Tier 2 operators are smaller and will have less resources so it is appropriate for them to have a lower reporting burden overall. We also suggest that information requests regarding compliance with the measures should only be issued after the relevant implementation period set out in the Code of Practice has elapsed. Lastly, we recognise that Ofcom has acknowledged the risk of becoming a central risk point by retaining copies of sensitive security information and documentation from a large number of important UK telecoms providers. We stress that this is a critical concern for Verizon and we would welcome further information as to how information will be transferred and stored securely by Ofcom.

- **TBEST penetration testing** - Ofcom highlights its voluntary TBEST penetration testing in the consultation. While it says participation is voluntary, the documents suggest that it is being strongly encouraged. While TBEST may be a good test, we question whether it is the only form of compliance and whether it is appropriate for global operators who already carry out their own internal and external penetration tests (as Verizon does). Furthermore, we understand that operators will need to fund the TBEST themselves - again we question whether this is necessary if

operators already invest in the expense of their own tests. We are disappointed to see that international standards such as the ISO 27000 series are not referenced, as these require audit requirements which require additional expense, and are generally recognised in other international regimes (such as per the EU guidance set out by ENISA).[2] Many international operators who must ensure compliance with different security regimes in different jurisdictions simply cannot justify the expense of localised testing when global testing exists. It would be burdensome and expensive to require such operators to duplicate these efforts. We strongly urge Ofcom to be flexible in its assessment of testing, and to appreciate the complex compliance requirements that international operators must meet.

- **Security compromise reporting to regulator and customers** - The guidance contains the thresholds for reporting security compromises to Ofcom but also sets out certain criteria where operators should also inform end-customers of security compromises where there is a "significant risk of a security compromise occurring" and where such a compromise "may adversely affect users". We suggest that further clarification around these measures should be issued by Ofcom. We would also note that the security reporting landscape is very complex, especially for those telecoms providers who also provide other services such as cloud services and managed services. One particular incident may require notification to both Ofcom under the Telecommunications (Security) Act, to the ICO under the NIS Regulations (both under the current scope and under the expanded scope that was recently proposed by the Government in its cyber resilience consultation [3]), and to the ICO again if it involves a personal data breach. That is not to mention any reporting required contractually to enterprise customers, who depending on their sector, may need to report to their own sectoral regulators. We urge Ofcom to take an active part in the debate as to whether these separate reporting regimes make sense, or whether a streamlined approach with a central reporting portal for all regulators would be achievable.

Conclusion

We consider that the concerns and suggested changes we have raised above would result in a reduction in some of the burden of the new security regime. We also look forward to clarification on a number of points. We look forward to working with Ofcom on this regime in a pragmatic fashion, and we look forward to engaging further on this matter with you in the coming months.

17 May 2022

[2] ENISA Technical Guideline on Minimum Security Measures.
https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc
[3] Published 19 January 2022,
https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience