verizon

Verizon response to Ofcom's consultation on the review of security guidance

Introduction

1. Verizon Enterprise Solutions ("Verizon") welcomes the opportunity to respond to Ofcom's "Review of Security Guidance - Consultation on updating Ofcom's guidance on security requirements in sections 105A to D of the Communications Act 2003"[1] (hereinafter the "2017 Security Guidance consultation").

2. Verizon is the global IT solutions partner to business and government. As part of Verizon Communications – a company with nearly $131 billion in annual revenue – Verizon serves 98 per cent of the Fortune 500. Verizon caters to large and medium businesses and government agencies and is connecting systems, machines, ideas and people around the world for altogether better outcomes.

3. Please note the views expressed in this response are specific to the UK market environment and regulatory regime and should not be taken as expressing Verizon's views in other jurisdictions where the regulatory and market environments could differ from that in the UK.

4. We note that Ofcom did not include any questions in its 2017 Security Guidance consultation. As such, we have structured our response thematically, as follows:

    - General comments
    - Security and availability
    - Incident reporting
    - Audit and enforcement

Response to the 2017 Security Guidance consultation

General comments

5. Firstly, Verizon agrees that security is of utmost importance in the sector, and we are committed to ensuring that our networks are secure and reliable. Security is critical to Verizon's business, and, as a business-to-business (B2B) provider, it is key to the service which is demanded by our highly empowered large business customers. Accordingly, we have detailed and robust policies, processes and technologies in place to protect both our own network and our customers, many

[1] https://www.ofcom.org.uk/__data/assets/pdf_file/0024/103596/consultation-review-security-guidelines.pdf

of which are aligned with relevant parts of industry standards and frameworks. Much of these are bespoke to our highly complex business and our diverse customer base. We are confident that our security strategies are extremely robust and should satisfy Ofcom's regulatory expectations.

6. That said, we are disappointed that Ofcom is seeking to broaden the scope and increase the prescriptiveness of its guidance on compliance with s.150A-D of the Communications Act 2003. Ofcom is unnecessarily breaking away from the ENISA Technical Guideline on Minimum Security Measures[2] which recognises that:

    - there are no one-size-fits-all solution to security;[3]
    - different organisations have different systems and as such guidance must be flexible to recognise this;[4]
    - there should be an avoidance of duplication with international standards and best practice;[5] and
    - pan-EU and international communications providers (CPs), like Verizon, need flexibility as it is impractical and not cost effective to comply with different security specifications for each jurisdiction in which they operate.[6]

7. We would therefore strongly encourage Ofcom to adopt a more principles-based approach in which the high level aims or areas which need attention are highlighted in the Ofcom guidance, yet the practice is the responsibility of the CP who has the operational experience and knowledge of their own business in order to make informed, appropriate and efficient choices. A principles-based approach is also more likely to encourage compliance rather than becoming unreachable or impractical for small and large providers respectively.

Security and availability

Specific standards, testing, certificates and other guidance documents

8. Ofcom references a number of standards, policies, certifications and tests,[7] and places strong emphasis on being able to provide evidence of these in order to demonstrate compliance. Verizon strongly disagrees with this approach.

[2] Available at: https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures
[3] See section 5.1.4 of the ENISA Technical Guideline on Minimum Security Measures.
[4] See section 5.1.1 of the ENISA Technical Guideline on Minimum Security Measures.
[5] See section 5.1.3 of the ENISA Technical Guideline on Minimum Security Measures.
[6] See section 5.1.4 of the ENISA Technical Guideline on Minimum Security Measures.

9. We are concerned that Ofcom is making it even harder to demonstrate compliance with s.105A by placing further weight on only one set of standards, and assuming that CPs that do not have these specific requirements are non-compliant unless they can prove otherwise. As stated above, Ofcom should not assume this to be the case, as CPs such as Verizon have a clear focus and incentive for ensuring high-quality and robust security standards, albeit in a way which is most suited to the organisation's size, focus, and geographical reach.

10. Ofcom says that it does not intend for the security guidance to become a "tick box" exercise;[8] however this is indeed what Ofcom is proposing. Ofcom is not following the ENISA guidance which suggests that NRAs should ensure that guidance is flexible, and takes account of difference in size, operations and global reach of CPs.[9]

11. While suggesting generic standards may make an external security audit or compliance check more straightforward for Ofcom, it does not necessarily do anything to improve security or increase resilience. It arguably serves only to increase costs and the regulatory burden for CPs, who may well meet or exceed minimum standards with their own internal controls which are already well-established. Ofcom should ensure that it does not cause some CPs to shoulder an undue burden or be placed at a financial disadvantage just because they choose to rely on their internal bespoke controls rather than seek external certification.

12. In this respect Ofcom needs to be flexible about the type of evidence it will accept to demonstrate compliance, and look at the wider context of the type of customers and market a CP operates in. For example, the customers of a mass-market consumer CP are likely to have a different view on security and resilience, relatively speaking, to the customers of a B2B CP who are typically government departments and large corporates.

13. Furthermore, as ENISA recommends, Ofcom should take account of the need for harmonisation for large pan-EU or international CPs.[10] It is simply not practical or viable for a CP of such global reach to have to adapt to each of the specific certificates of each jurisdiction in which they operate. This leads to a patchwork of regulatory requirements and, at worst, it could put such international CPs at a cost-disadvantage compared to national CPs.

---

[7] For example, the ISO27001, the ND1643, the Cyber Security Essentials and Cyber Security Essentials Plus, 10 Steps to Cyber Security, DCMS+NCSC+Ofcom vulnerability testing (TBC) etc.

[8] See paragraph 2.14 of the 2017 Security Guidance consultation.

[9] See section 5.1 of the ENISA Technical Guideline on Minimum Security Measures.

[10] See section 5.1.4 of the ENISA Technical Guideline on Minimum Security Measures.

14. We consider that a high-level principles based approach would be much more effective and successful in ensuring that CPs implement security processes which are fit for purpose. We therefore urge Ofcom to amend the wording of the guidance to make it clearer that the standards or certificates it references in the guidance are only one way of demonstrating compliance, and that internal international policies which follow and surpass the principles of these documents are another way to demonstrate compliance.

15. To be clear, we are confident that our security strategies are extremely robust and should satisfy Ofcom's regulatory expectations.

Vulnerability testing

16. Ofcom's proposals are unclear as to whether or not CPs must undertake vulnerability or network penetration tests. **[✂]** We note a number of issues with the proposed guidance.

17. Firstly, Ofcom suggests that these tests could be good tests of CPs security policies[11] but then says CPs should participate in a joint DCMS-Ofcom-NCSC test which is still in production.[12] We note that no link or timeline is provided for the latter. As a result, this proposal is unclear and impractical – how are providers supposed to demonstrate compliance if the recommended methods are not even available yet?

18. Furthermore, Verizon would be concerned about sharing the results of any vulnerability testing with Ofcom or other relevant bodies. The dissemination of information about potential security vulnerabilities is highly sensitive information would create an unnecessary risk to our network and to our customers with no clear benefit to any party. **[✂]**

19. This further demonstrates that Ofcom should adopt a high-level principle that CPs should carry out some form of vulnerability testing to identify risk areas, without specifying exactly how that should be undertaken. This would eliminate the risk of specifying one example of vulnerability testing which may be overly burdensome for a very small CP, but may be insufficiently complex or robust to test a large complex CP. Again, Ofcom would be going against the guidance on flexibility in the ENISA Technical Guideline on Minimum Security Measures.[13]

Cybersecurity

[11] See paragraph 2.10 of the 2017 Security Guidance consultation.
[12] See paragraphs 2.22 to 2.24 of the 2017 Security Guidance consultation.
[13] See section 5.1 of the ENISA Technical Guideline on Minimum Security Measures.

20. Cyber risks and incidents are a clear threat today, and Verizon is committed to mitigating the risks to our own network and our customers.

21. However, we disagree that Ofcom should add a further layer of complexity and regulatory burden to what is already a crowded legislative and regulatory environment with various external stakeholders (e.g. ICO, DCMS and NCSC). Ofcom is unnecessarily expanding the remit of the security guidance, and in the process, is creating additional resource and financial burden, and increasing complexity and duplication. For example, the ICO alone publishes significant amounts of guidance relating to reducing security risks amongst other topics.[14] Ofcom needs to be aware of the pressure that further expansion of existing guidance puts on CPs trying to keep track across the various initiatives at both a UK and EU level,

22. We therefore urge Ofcom to refrain from including cyber security in its Security Guidance, as we consider that the intention and primary focus should be on the operations and availability of networks, rather than data. Ofcom should have confidence that other regulators such as the ICO regulate and enforce cyber security appropriately, and take comfort in knowing that cyber issues are of high importance to CPs (especially B2B CPs whose empowered customers have strict requirements for such protection).

Incident Reporting

General comments on reporting

23. As we have highlighted in previous responses and correspondence with Ofcom, Verizon has a robust, automated process in place for incident reporting which was developed in the back of our US processes. This process is well-established and proven, and is used for reporting in all EU countries. It captures all of the information that Ofcom requires, and as such, we strongly prefer to continue using this efficient system with no modifications.

24. In terms of incident reporting we would also take the opportunity to reiterate the need for Ofcom to reflect the differences inherent between consumer- and business-oriented CPs. Verizon often acts as an intermediate carrier in a chain between originating and terminating parties. Moreover, as a B2B CP, we do not have contractual relationships with residential end-users of communication services. Therefore if we were to report an incident affecting our network, it may well be the case that Ofcom would receive one or more duplicate reports from other carriers up or down the chain. Such an arrangement would seem to be

[14] https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/

disproportionate and inefficient. It would also appear to leave Ofcom with the task of having to determine which reports concern essentially the same incident.

Incident categories

25. Ofcom proposes to move to three incident categories: urgent, other, and non-major. In relation to "urgent" incidents, we believe that the proposed reporting requirements (24/7 reporting within three hours) are hugely disproportionate. We feel that this is an unnecessary timeline that would only serve to divert resources away from resolving the breach incident at hand. There is also no justification given in the consultation as to why Ofcom requires this information within three hours, nor what it intends to do with this information outside of office hours.

26. We also do not consider that Ofcom has a valid and proportionate reason for requiring such a timeline. Paragraphs 3.36 and 3.37 of the consultation suggest that this requirement is only driven by Ofcom's desire to be able to be prepared for any press enquiries related to an "urgent" incident. We do not consider this to be a valid reason to impose such an obligation on CPs, nor is notification a priority in the event of such incidents, where resource should be dedicated to ensure swift resolution instead. Ofcom should be aware that a major incident may require a large coordinated response with may make complying with specific time periods more difficult. We consider that the current requirement to notify major incidents within 24 hours[15] is more proportionate, and we argue that this should be retained in the updated guidance.

27. We agree with the proposed change to 72 hours for "other" incidents, and the retention of the requirements around "non-major" incidents. This provides greater clarity and is proportionate.

Cyber reporting

28. In relation to reporting cyber incidents, we of course agree that cyber incidents are an important area for CPs and the wider industry to tackle. However, we disagree that cyber incidents which do not have a "significant impact on the operation of a public electronic communications network"[16] are in scope of the reporting requirements set out in s.105B.

29. Furthermore, we consider that the main concern is likely to be in relation to customers' personal data, and as such, these types of incidents are already

[15] Paragraph 4.5 of the Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003, dated 8 August 2014.
[16] See s.105B(a) of the Communications Act 2003.

reported to the ICO under the DPA[17] and PECR[18] obligations, and in future, the GDPR and the NIS Directive. Therefore, Ofcom should refrain from adding unnecessary burden by duplicating the requirements for other regulators, or at worse, conflicting reporting requirements. If Ofcom should require this information, then it should look to cooperate with other regulators/bodies in this area and avoid duplication. That said, should such cyber incidents result in network operations outages that meet the relevant criteria, then they would be reported under the current arrangements.

Audit and Enforcement

Audit

30. Ofcom says that it intends to make use of audits (paid for by CPs) "more often than previously"[19] albeit recognising the burden that places on CPs.[20] We consider that without clear criteria for invoking an audit, this change to the guidance has the potential to be extremely burdensome. Furthermore, the threat of increased audits might discourage people from reporting incidents, undermining Ofcom's proposals and duties.

31. Currently Ofcom only says that it will consider the "appropriateness" of auditing in each case. We consider that, as a minimum, Ofcom must consider its general conditions for invasive regulatory action, i.e. objectively justifiable, no undue discrimination, proportionality, and transparent.

32. In addition to these high level principles, we consider that Ofcom needs to be clearer when it is likely to use the auditing powers. Without doing so it is introducing unnecessary and unwelcome regulatory uncertainty. We consider that audits should only be required in the most extreme or serious circumstances, once other avenues (such as informal and formal requests for information) have been exhausted. Adopting a collaborative approach between regulator and industry is likely to build a more successful and motivated security environment (on top of the incentives that CPs already possess in terms of commercial interests). In addition, before considering undertaking an audit, Ofcom should also take account of the results of any audits that CPs may have already conducted which are likely to be sufficient, before deciding to request a further external audit. Furthermore, Ofcom should focus its limited resources on "at risk" areas such as consumer facing CPs where there is limited empowerment for

[17] Section 55 breaches.
[18] Section 5A of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)
[19] See paragraph 4.7 of the 2017 Security Guidance consultation.
[20] See paragraph 4.8 of the 2017 Security Guidance consultation.

consumers to be involved in the design and application of security measures for the services that they use.

33. Finally, Verizon would be concerned about sharing information about possible security risks and/or vulnerabilities in our network outside of our organisation. This information which may be gathered under such an audit would be highly sensitive information, and the sharing of this information would create an unnecessary risk to our network and to our customers with no clear benefit to any party. **[✂]**

Enforcement

34. We generally agree with Ofcom's proposed changes to align with the general Ofcom Enforcement Guidelines as this provides consistency and clarity. However we are also grateful that Ofcom is proposing to clearly set out that informal investigations are more effective.[21] We would agree that this is the best approach as this allows CPs to concentrate on resolving the present issue, learning and implementing solutions to prevent future incidents, without having to dedicate additional time and resource on responding to formal investigation procedures which can be time-consuming, resource-intensive and costly.

35. Furthermore, as above, there is a risk that large operators who offer a number of telecoms and data-based services could be subject to triple enforcement under s.105 of the Communications Act from Ofcom, and the GDPR and the upcoming NIS Directive (once implemented in UK law) from the ICO. We would again strongly encourage regulators to work together to look at how their different pieces of legislation and regulatory powers interact in order to have effective deterrents to unacceptable behaviour without being disproportionally punitive.

Conclusion

36. In summary, while Verizon is committed to working with the appropriate authorities to address issues of network security and resilience, we call for harmonisation, flexibility in the guidance, and a high-level principle-based approach.

Verizon Enterprise Services
September 2017

[21] See paragraph 4.14 of the 2017 Security Guidance consultation.