vorboss

Vorboss response to Ofcom’s Resilience guidance consultation and Call for Input on mobile RAN power back up

NON CONFIDENTIAL 1 March 2024

Introduction

Vorboss welcomes the opportunity to respond to Ofcom’s consultation concerning its proposed network resilience guidance. Vorboss is a fixed network operator and internet service provider, investing over £250m in delivering direct internet access to businesses in central London. The resilience and security of our network is central to how we operate. Our response to the consultation is informed by this approach.

We are broadly supportive of the proposals set out by Ofcom in its consultation and our network’s design principles already meet or exceed many of them. While these proposals will go some way to support improved network resilience, Vorboss is concerned about the increasing prevalence of unidentified physical access to Openreach ducting, resulting in damage to fixed telecoms networks. While there are already rules in place which should control who accesses this infrastructure, compliance is low and falling.[1] This is leaving providers’ networks at risk of damage and attack, with no obvious recourse. Low compliance with these rules risks undermining the wider purpose of Ofcom’s guidance. We discuss this further in response to question 5.

The rest of this response sets out Vorboss’ views on Ofcom’s proposed guidance for communications providers and where we consider more needs to be done to support the security and resilience of these networks and the services they provide.

Question 1: Do you consider the measures in the proposed guidance relating to the resilience of the physical infrastructure domains to be appropriate and proportionate?

Vorboss is of the view that the measures proposed in Ofcom’s guidance regarding the resilience of physical infrastructure domains is appropriate and proportionate. We agree that many of Ofcom’s proposed measures are already recognised as the established industry standard to ensure robust and resilient networks and services. Although, there are areas of the proposed guidance where we believe Ofcom could set out its ambitions more clearly. For example, we would welcome Ofcom pointing to specific examples of best practice to inform practical compliance.[2]

[1] The Telegraph, ‘Lazy’ broadband engineers blamed for exposing hospitals and banks to cyber attacks

[2] As mentioned in Section 4.1 of the Guidance.

The Vorboss network has been designed to prioritise security and resilience. Our network architecture avoids single points of failure and internet traffic can easily be diverted through a range of different routes should there be a problem. This ensures that our customers' service uptime is maximised and consistent.

In relation to power outages, Vorboss recognises the need to consider the risks associated with a loss of power and ensure safeguards are in place, deploying battery back-up and generators where appropriate. Ofcom's expectations should be proportionate to the risk and be mindful of the environmental impact of batteries and generators. Communications networks are dependent on power networks – any power autonomy of our network will last for a finite period. Ofcom should support the sector to ensure that communications providers are considered priority users in the event of power outages.

Question 3: Do you consider the measures in the proposed guidance relating to the resilience of the Management Plane to be appropriate and proportionate?

We agree that there are significant benefits of having an out-of-band management function, going beyond network security and reliability. In our view, Ofcom should consider using this opportunity to be more prescriptive in relation to the security and resilience of out-of-band management networks.

Question 5: Do you consider the measures in the proposed guidance relating to communications providers' arrangements for preparing adequate process, skills and training to be appropriate and proportionate?

Vorboss supports Ofcom's view that staff competency is key to supporting resilient systems and processes. We take the training of our staff extremely seriously. As a result, we do not use any third-party contractors for civils engineering work on or in our network. Instead, we have developed our own training academy that provides our installation and civils teams with comprehensive training across all key areas of build. These functions allow us to directly control quality of work and process compliance, rather than relying on third party good practice and contract enforcement.

We are conscious that this structure is not the industry norm and that most network operators utilise third party contractors for physical network build, maintenance and installation. This means that most network operators will have diminished direct control of their compliance with rules that govern access to physical infrastructure, such as Openreach's PIA network.

To this end, Vorboss is concerned about the increasing prevalence of physical attacks on telecoms networks. Recent events, such as the deliberate attacks on full fibre networks in Liverpool[3], London[4],

[3] ISP Review, Vandal's attack Netomnia's FTTP broadband network in Liverpool

[4] The Telegraph, 'Lazy' broadband engineers blamed for exposing hospitals and banks to cyber attacks

Pembrokeshire[5] and Sheffield[6] highlight the need to protect this infrastructure and the public services, businesses, and households it serves.

Network operators must ensure that they know who is accessing their physical network infrastructure, especially where network operators are sharing physical assets. There must then be strict enforcement of 'whereabouts compliance'. This is a contractual obligation requiring all network operators and anyone acting on their behalf to register their activity with Openreach when using the Openreach physical network. Currently, industry compliance is low and falling.[7] This trend must be reversed. Ensuring that industry complies with these low-cost requirements of registering when and where they are accessing the Openreach network means we can more easily identify if an incident resulting in an outage is deliberate, malicious or unintentional damage. To be effective, every time someone enters or accesses that shared network, it must be logged. This is a necessary first step to identifying if unauthorised personnel are accessing our networks.

Further, compliance with Section 105K of the Communications Act rests upon effective whereabouts compliance. Unauthorised access to Openreach's shared physical network, by definition, results in a security compromise where a person is in a position to bring about further security compromise. Driving compliance amongst all users of Openreach PIA must then be a priority.

Whilst Openreach already has the contractual mandate to drive enforcement, whereabouts compliance has been poor throughout the life of the unrestricted PIA remedy. Openreach is also in competition with the network operators that use its ducts and poles. Its position is then potentially conflicted. If it cannot meaningfully enforce high whereabouts compliance standards, Ofcom should consider more direct intervention in light of Section 105K and oversee measures to improve compliance rates.

[5] ISP Review, Targeted attack hits Ogi's full fibre broadband network in Wales

[6] ISP Review, Pine Media suffer targeted attack on Sheffield full fibre network

[7] The Telegraph, 'Lazy' broadband engineers blamed for exposing hospitals and banks to cyber attacks