Written Evidence to the Cyber Security and Resilience Bill Committee

VIRTUS Data Centres - February 2026

Executive Summary

1. VIRTUS strongly supports the Government's objective of strengthening national cyber resilience and recognises the importance of effective, proportionate incident reporting for genuinely systemic risks. The company already operates to internationally recognised, gold-standard security and resilience frameworks and works closely with customers to maintain high levels of operational and physical security.

2. However, as drafted, the Cyber Security and Resilience (Network and Information Systems) Bill risks imposing new cyber incident reporting obligations on data centre operators that are not aligned with the colocation operating model – which accounts for a significant proportion of UK data centre deployments. In particular, the Bill does not sufficiently distinguish between incidents affecting data centre infrastructure and continuity, and incidents occurring solely within customer-managed systems over which data centre operators have no technical visibility or legal authority.

3. Without clarification, this creates a risk of unworkable compliance requirements, unnecessary duplication for operators already complying with existing accredited assurance regimes, and potential conflicts with contractual confidentiality and non-disclosure obligations. These unintended consequences would complicate the colocation model in the UK and undermine growth ambitions of a sector that is crucial to the overall growth of the economy.

The role of Data Centre Operators in the digital infrastructure ecosystem

4. Data centre operators play a foundational but clearly defined role within the UK's digital infrastructure ecosystem. **Their primary function is to provide secure, resilient physical environments that enable digital services to operate, rather than to operate or manage those digital services themselves.**

5. In the colocation model, which underpins a large proportion of large-scale data centre provision in the UK, operators are responsible for physical infrastructure, including power supply, cooling systems, environmental controls, physical security and building resilience.[1] Customers retain full responsibility for their own IT equipment, networks, software, data and cyber security controls. This distinction is reflected in the Bill's definition of a "data centre service", which focuses on the provision of physical structure and supporting infrastructure rather than the operation of customer IT systems.

6. This separation of responsibilities is central to how the digital economy functions. It allows operators of essential services, cloud providers, managed service providers and other digital

[1] United Kingdom Hyperscale Data Centre Market Size and Share Source: https://www.mordorintelligence.com/industry-reports/united-kingdom-hyperscale-data-center-market

businesses to deploy and control their systems while relying on specialist data centre operators to deliver resilient facilities at scale.

7. Crucially, data centre operators do not have routine access to, or visibility of, customer systems or data. We do not monitor customer networks, inspect customer traffic, or manage customer security tooling. This is a deliberate design feature, reflecting customer expectations, contractual confidentiality obligations and data protection requirements.

8. Recognising the distinct role of data centre operators within the wider digital infrastructure ecosystem is therefore essential to ensuring that the regulatory framework introduced by the Bill is both effective and workable in practice.

Cyber security incidents and our customers

9. VIRTUS recognises that many of its customers operate systems and services that are critical to the UK economy and the day-to-day functioning of society. Customers include operators of essential services, digital service providers and managed service providers, all of whom are subject to their own cyber security and incident reporting obligations under the NIS framework.

10. In a colocation environment, customers retain full control over their IT systems, networks, software and data. Cyber security incidents affecting customer systems typically occur within customer-managed environments and are detected, investigated and addressed by the customer or their appointed service providers. **Data centre operators are not immediately notified of many such incidents, and where they are, this is often on a limited and confidential basis after the cyber security disruption has occurred**.

11. VIRTUS does not have technical visibility of customer networks or applications and does not monitor customer traffic or security events. As a result, VIRTUS cannot reliably identify whether a cyber incident has occurred within a customer environment, assess its severity, or determine whether it meets regulatory reporting thresholds.

12. Even where a customer voluntarily discloses the existence of a cyber incident, VIRTUS is constrained by contractual confidentiality and non-disclosure obligations. These agreements typically prevent the disclosure of customer identity, system details or incident information to third parties, including Government, without explicit customer consent.

13. For these reasons, it is simply impractical for data centre operators to be responsible for reporting cyber security incidents that occur solely within customer-managed systems and do not affect the operation or continuity of the data centre service itself.

14. A clear and proportionate allocation of responsibilities in this area is essential to avoid duplication, reduce regulatory burden, and ensure that incident reporting under the Bill delivers meaningful improvements to UK cyber resilience.

Barriers to reporting

15. The Bill already places direct incident reporting obligations on operators of essential services, relevant digital service providers and relevant managed service providers.

16. These entities have direct operational control over their systems and are best placed to assess, classify and report cyber incidents under regulations 11, 12A and 14E.

17. Requiring data centre operators to report incidents affecting customer systems risks duplication. In practice, the same incident could be reported multiple times by different parties, or potentially, reported inaccurately by an operator without full technical context.

18. In this context, extending equivalent reporting obligations to data centre operators for customer-managed incidents adds regulatory complexity without improving resilience outcomes.

Current cybersecurity standards

19. VIRTUS operates to a comprehensive set of independently certified quality, security and resilience frameworks that demonstrate our commitment to structured, risk-based cyber security and operational excellence. These standards are designed to maintain high levels of service integrity, protect customer environments and align with internationally recognised best practice.

20. VIRTUS' current quality and security credentials include certification to key ISO management standards such as ISO/IEC 27001 for information security management, ISO 9001 for quality management, ISO 20000-1 for IT service management, ISO 22301 for business continuity, ISO 45001 for health and safety, ISO 14001 for environmental management and ISO 50001 for energy management.[2] These standards provide a structured governance, risk and control framework, supported by risk assessment, documented procedures, continuous monitoring and regular external audits.

21. VIRTUS also adheres to industry-specific compliance frameworks such as ISAE 3000 (SOC 2 Trust Services Criteria) and PCI DSS for payment card security, reinforcing discipline in areas such as confidentiality, integrity, availability and customer data protection.[3]

22. Collectively, these standards demonstrate that VIRTUS already operates within a rigorous risk management regime that promotes continual improvement, threat awareness, incident response preparedness and resilience. Any cyber security reporting regime emerging from the Bill should recognise and align with these established frameworks, using them as evidence of good practice rather than layering additional, duplicative obligations that do not work with data centre operational realities.

Recommendations and conclusion

[2] VIRTUS Accreditation: https://virtusdatacentres.com/why-virtus/quality-credentials
[3] Ibid.

23. It is critical that the Bill and guidance are amended to reflect these clear barriers and complications with the proposed regulatory regime. Specifically making explicit that data centre operators are not responsible for reporting cyber incidents occurring solely within customer-managed systems, networks or applications, where there is no impact on the data centre service.

24. Such an approach would preserve the intent of the Bill, avoid imposing unworkable obligations, and ensure that incident reporting responsibilities sit with the organisations that have visibility, control and legal authority to act.

25. VIRTUS is very supportive of the Government's efforts to ensure a high standard of cyber security reporting and recognises the importance of effective, proportionate incident reporting for genuinely systemic risks. However, as drafted, the Cyber Security and Resilience (Network and Information Systems) Bill risks imposing cyber incident reporting obligations on data centre operators that are not aligned with the colocation operating model.

About VIRTUS

VIRTUS Data Centres, the UK's leading and largest data centre company, is investing billions of pounds in the UK to power the critical infrastructure required for emerging technologies like AI and other industries of the future. We operate 11 live data centres in the UK and are developing a further 6, serving customers from the world's major tech companies, alongside leading UK banks, research and education facilities, and Government. Backed by Macquarie, we have ambitions to invest up to £18bn in new UK data centres, dependent on the right regulatory and policy support being in place.