techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

Data storage and processing infrastructure security and resilience - call for views

techUK's submission to the Department for Culture, Media, and Sport's call for views

About techUK

techUK is a membership organisation launched in 2013 to champion the technology sector and prepare and empower the UK for what comes next, delivering a better future for people, society, the economy and the planet

It is the UK's leading technology membership organisation, with more than 850 members spread across the UK. We are a network that enables our members to learn from each other and grow in a way which contributes to the country both socially and economically.

By working collaboratively with government and others, we provide expert guidance and insight for our members and stakeholders about how to prepare for the future, anticipate change and realise the positive potential of technology in a fast-moving world.

Part 1: Risks to UK data storage and processing infrastructure

1. Are these risks to data storage and processing infrastructure the most appropriate risks for the government to address? If not, why not? [OPEN QUESTION]

techUK response

techUK welcomes the opportunity to respond to the Government's request for views on the topic of security and resilience in the digital and data infrastructure space. We would also like to thank DCMS for the significant engagement throughout the Call for Views (CfV), including our direct queries, attending an industry roundtable, and granting an extension to facilitate a more detailed response from the sector. TechUK's response to the CfV has been development in consultation with our members in our data centres, cyber and cloud programmes.

A glossary of terms can be found at the end of the document.

Scope

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org

techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

Before responding in detail to the specific questions outlined below, we would like to highlight some concerns techUK members have with the scope of this CfV. This Call for Views covers a wide array of complex issues in a fast growing and diverse ecosystem. The issues covered range from commercial relationships between data centres and their customers to supply chain security and the interdependency of cyber and physical risks, amongst many others. Many of these issues have been the subject of policy activity by DCMS and more widely across government, and there is significant concern amongst industry that this CfV has not been appropriately joined up or coordinated. Many security and supply chain risks associated with the colocation data centre sector under examination are already managed (if not always formally regulated) across the system. We strongly encourage DCMS to ensure greater policy coordination so that any future proposals it advances do not evolve in a vacuum.

A further issue of significant concern is the potential overlap between this early-stage work and the recent work undertaken by DCMS around supply chain security, strengthening resilience and updating the UK NIS Regulations. Some members have suggested that policy activity focusing on data centres should be incorporated into the NIS review, or at least begun once the review has been completed. This would allow industry a better understanding of the scope of both policies and a clearer idea of how their products and services might be covered. Plus, it would avoid any potential for policy conflict or duplication.

techUK understands that this CfV focusses on co-location data centres, and the wider ecosystem of CSPs (Cloud Service Providers) and MSPs (Managed Service Providers), some areas of which are NIS regulated. However, specific the extent to which NIS might be developed in future remains unclear. Further, as DCMS notes, there are other sector specific regulations which overlap in this area such as the Telecommunications (Security) Act 2021. Duplication and complexity of compliance is a key concern for techUK members.

techUK members would caution against any additional regulatory burden that might result from overlap between the NIS changes and recommendations brought forward from this CfV, particularly as some of our members provide data processing services across multiple sectors and already fall under the remit of multiple regulatory regimes. There is sometimes no clear separation in practice between CSPs, MSPs, and other technology services. For example, reflecting the shared responsibility model, CSPs are not wholly dependent on colocation data centres for their operation, nor the security of data within the system (which is managed and controlled by customers).

techUK would also like to highlight that this is a hugely diverse ecosystem of companies, all with different commercial models, risk profiles and strategies. Whilst techUK members understand and support the need to strengthen resilience per the fourth mission of the National Data Strategy and the second pillar of the National Cyber Strategy 2022, we judge that more industry engagement work would be beneficial to understand the significant effort and investment already underway across industry to do so, whether that be within Colo Data Centres, CSPs or hyper-scalers. In particular, we recommend direct ongoing consultation with owners/operators within the colocation data centre sector - of the type pursued on security issues by the Government with other non-CNI (Critical National Infrastructure) sectors (e.g., as CPNI (Centre for the Protection of National Infrastructure)/NCSC (National Cyber Security

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org

techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

Centre) advances with the retail and major events sectors) - as they are the best placed interlocutors on the detail of the physical and personnel security measures associated with specific sites.

techUK members questioned why the government identified MSPs as a sector they want to hear from with regards to their use of data centres and engagement with data centre operators. The Government could have sought views from a range of different users of data centres, including Government departments, and it would be useful to provide a rationale for why only MSPs were chosen. On the specific request for information, MSPs will have different relationships with data centre operators – they are a provider of services to data centre operators and users of data centre services. However, both these scenarios are a commercial relationship and governed by contractual service level agreements and it is unlikely MSPs would be willing to share this information.

techUK members encourage the Government to explore international best practice on data storage and digital infrastructure resilience and security to ensure that the UK remains competitive and does not create the conditions for companies to offshore their operations to jurisdictions with lower standards. This will ensure the best conditions for international trade in digital services.

Finally, several techUK members questioned the lack of clarity around the drivers behind this consultation, with some assessing that the broader scope beyond Co-Lo issues was unhelpful and other questioning if some security arrangements across the wider ecosystem should be considered. techUK members would be grateful for clarifications from DCMS to ensure Government receives the most appropriate evidence.

Our Response

techUK believes individual members would be best placed to input on Part 2 & 3 on the security and resilience of specific data centres and have encouraged our members to do so.

The outcomes identified under Part 1, risks to data centres, of the CfV are aligned with the goals of techUK and our members. Our members providing cloud services, cyber security and data centre services agree that the threats to sensitive data continue to evolve, are partially the result of the increasing abundance of data, the digitisation of public sector data and the wider geopolitical context. In this context, the tech sector takes seriously its responsibilities to address security risks directly.

Business continuity and safeguarding the delivery of large-scale data storage is a core commitment of the sector, where competitive advantage relies on an uninterrupted service provision and agility to meet demand and novel challenges. Resilience and security measures are necessary and commonplace, and the sector is keen to share insights which could improve wider system resilience and better inform policymakers. The sector is also best placed to provide insights into the types and frequencies of identified risks, helping direct resources and attention where they are needed most.

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

As the wider economy is increasingly reliant on digital tech, novel economic and national security risks are bound to evolve. The sector is keen to work with government to ensure that existing and novel risks to digital infrastructure and data are mapped and continue to be appropriately mitigated. The risks that DCMS have included in the CfV are comprehensive and relevant to the sector.

In most cases, as we will demonstrate, they are already identified by the sector through a combination of standards, regulation, and competitive foresight. However, some horizon scanning will be required going forward, particularly in relation to the evolution of climate change related risks (the July 2022 heatwaves being one example). In this case, techUK is working with the GCSA (Government Chief Scientific Advisor) to develop a guidance document on the impacts of heatwaves on data centres and telecoms infrastructure. As with many areas of industry, there exists a heterogeneity in adoption and application of standards. In the data centre context this relates to the level and type of service offered.

For the sake of clarity, we have divided risks into Continuity of Service risks and Data Access risks for the sake of our response. Continuity of service risks are those which threaten continuity of service and data access risks are those which threaten the integrity/availability/privacy of data. Resilience in the former risk category is categorical in nature, with clearly identified risks and tiered mitigation strategies. Security in the latter is far more dynamic with emergent risks and novel threats dependent on developments in adjacent sectors. We will explore these two categories in our response.

Context

Colocation (colo) data centres, a market segment which is well represented in the techUK data centre group and council, are responsible for the housing, bandwidth, server cooling, power, and physical security of their customers servers and server operations. Space inside a colo data centre is leased out on a commercial basis, with providers competing over quality of service, and increasingly security and resilience provisioning. In this respect, it is fair to say that the market-based approach is successful in improving service continuity, security, and resilience of data over time.

Colocation data centre activities can range from simply housing server stacks for third parties, to so called “smart hands” functions, this describes a range of technical support offered to customers who store their data in a data centre. This includes asset tagging; asset buy backs and data destruction. The rise of smart hands services does somewhat blur the boundaries between traditional colocation services (housing, power provision etc), and IT service provision. We cover the drivers and benefits of smart hands below.

Cloud platform providers are common customers of colo data centres, purchasing space and thereby digital capacity to run their services. While physical security and resilience of the data centre is the responsibility of the colo, cyber security and resilience is usually the responsibility of the customer, CSPs, and in turn their own customers in line with the shared responsibility model. CSPs ensure that cloud consumers are equipped to ensure the security and resilience

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

of data in several ways including, for example, through providing advice on cloud design choices and by offering training on security solutions.

Within the wider ecosystem, managed service providers (MSPs) are employed to help their customers to meet certain business functions via an outsourced service. This means that they can be or are sometimes exposed to the data housed in data centres and are therefore part of the equation when considering the security and resilience of said data, sensitive or not.

Continuity of Service Risk (resilience)
Sensitive access risk (physical access), Concentration risks (all), Multi-impact risks, Future risks.

Data centres ensure resilience in their operations through redundancy measures, application of industry standards and performance metrics, and internal and external drivers. This section will highlight the risks as the sector sees them through demonstration of its resilience measures.

Recognisable facilities are those with >240KW power supply, floor area >200M2, environmental controls and backup generation. Of the 500 recognised facilities in the UK, around 200 could be considered colo data centres. These data centres require a lot of power to not only run server stacks for their customers, but also to maintain the SLAs (power, and environmental controls) that are required to keep the IT equipment running effectively. Some estimates suggest that collectively data centres in UK use up to 3.6TWh/year or 1% of the national power supply, however smaller unconsolidated server rooms are not included in this figure. They also require uninterrupted connectivity to the telecoms network and staff access for daily functioning. The staff access factor became an issue during the COVID-19 pandemic, but one which techUK members were able to traverse with the support of DCMS, whilst also dealing with a surge in demand from video conferencing platforms, for example.

It is recognised within the industry that the ability to mitigate certain risks is not consistent across the board. Newer data centre facilities are built to higher resilience standards, and often when services outages occur, it is the older/legacy data centres with patched retrofit improvements that do not provide the same standard of robust performance. This is reflective of the lessons learned over the past decade about cyber and future physical risks (climatic and others), and the advancement in design planning and technology that have occurred over the same time frame. Certain redundancy measures are standard across the board however, which ensures that a minimum standard of service continuity can be expected under most scenarios. Built in redundancy measures are outlined below.

Built in redundancy

It is crucial that a risk-based approach towards security and resilience is maintained across the sector, we observe that built-in redundancy helps to ensure continuity of service in the face of identified risks:

External power supply

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org

techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

- A majority of operator facilities will have separate, independent electricity feeds from the grid. This does however depend on age, location, availability of grid supply to the locations and the topography of the data centre electrical distribution.

Emergency generation

- Onsite energy generation capacity will be predicated on the maximum theoretical power draw that the facility could impose, plus additional redundancy, denoted by configurations like 2N or N+2. Where N is the maximum theoretical power demand of the site. Sites usually have priority arrangements for gasoil replenishment with fuel providers to accommodate longer outages.
- We note that at present, other organisations/sectors may take priority in terms of gasoil fuel replenishment (e.g., hospitals, emergency services) acknowledging that human life needs to be a priority. The importance of data centres and digital infrastructure to these services in a crisis is not well explored

Communications

- Resilient sites will have dual or multiple independent connections.

Cooling:

- Cooling will be configured to the maximum possible required, plus headroom, with additional redundancy denoted in a similar way (2N, N+2, 2N+1, etc) to ensure compliance with contractual obligations / SLAs (Service Level Agreements).

Software and Technology

- Software and technology supplier failure can be mitigated through cloud, software and technology escrow solutions. This approach is increasingly adopted in the financial services sector (see Prudential Regulatory Authority SS2/21)

Built-in redundancy in data centre design successfully accommodates the most important interdependency risks, primarily those from interruptions in power supply and communications which are often out of a data centres control. Power and cooling (operational controls) are largely accounted for in redundancy measures.

Interdependency risk mitigation

Beyond this, the fact that digital infrastructure comprises multiple interoperating systems confers a significant degree of natural redundancy. There is generally more scope to re-route data traffic compared to other utilities, even at scale. The way that cloud service providers build Availability Zones (AZs) is an example. An AZ is generally one or more discrete data centres within an overarching region with redundant independent power, cooling, networking, and connectivity, which customers can use to achieve greater fault tolerance. The clustering of multiple AZs by region means that if one site is compromised by a power outage or other stochastic event, it will not affect the other zones. Traffic can also be rerouted to adjacent, functioning zones in the event of service outage. AZs are limited at present due to the Regulations on General Data Protection (GDPR).

In terms of connectivity, there is capacity in the network, provided by the cloud to accommodate even quite a sudden increase in demand – the wholesale move to online activity during the pandemic was accommodated in this way relatively seamlessly. Backups, duplication, and site replication allows the tech sector functions to minimise data loss and

techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

speed up recovery from stochastic events which may occur at site level. Compared with other sectors, digital infrastructure providers and carriers carry substantial social responsibility in situations of crisis, such as widespread power shortage or outages, heat stress or other forms of grid disruption. In such scenarios, we encourage the Government to consider whether priority access to power be given to those providing digital services as a further redundancy measure.

Life cycles and tech advancement

The relatively short lifecycle of technology assets in the data centre sector presents benefits for resilience. For a colo facility, remaining fit for purpose and competitive is a market driver of regular asset upgrades. A standard colo warehouse can expect to run for around 30 years before it would have to undergo a period of significant upgrade and refurbishment. CRAC (Computer Room Air Conditioning) units (which provide cooling) last ~10 years, and CRAH (Computer Room Air Handling) units, between 10 and 30 year. ICT hardware (servers for example) have significantly shorter lifecycles (3-5 years). Fast replenishment cycles for ICT hardware add to the resilience of data centres in relation to long-term market or environmental challenges.

Somewhat alluded to in the previous paragraph is the pace of technological advancement in the DC sector. New cooling solutions, more efficient servers or chip advancements are being created continuously. To remain competitive, operators can be encouraged to consider adopting the latest servers regularly; in colos this responsibility will typically rest with the customer. Liquid/immersive cooling solutions are currently being trialled to replace air cooling systems. Adopting best practice solutions in a data centre can help to mitigate climate risk, security threats and the potential for service outages.

Competitive resilience

This culture of improvement and application has implications for the resilience of data centre sites and the ICT equipment they house. Availability and continuity of service are business imperatives for operators. The level of resilience is dictated by the type of activity hosted within the facility and will be reflected contractually in service level agreements. Greater redundancy means greater cost, as well as greater embedded energy associated with redundancy. The resilience needs of clients contribute to a widespread culture of competitive resilience in colo operators.

We should reiterate here that there are tiers of resilience and security provision in the commercial data centre market, and customers may choose to pay a lower price for a less robust contract. Conversely, customers with highly sensitive data or a critical reliance on guaranteed service uptime will choose operators with higher standards for security and resilience.

Comparisons with other infrastructure sectors

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org

techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

The unconsolidated nature of the UK data centre sector at present means that there is a competitive market for all service offerings. This reduces the risk of complacency that may occur in mature, consolidated markets. The lack of price controls, characteristic of other infrastructure sectors, has allowed operators to think longer term when it comes to investment in resilience. This is an advantage of the data centre sector, which can be agile and take into consideration long-term trends in sustainability, security, and other customer demands.

Small, collaborative community

The data centre community in the UK is relatively small. News travels fasts and significant events cannot occur without the sector taking note and learning lessons. Increased focus on climate change and climate resilience in the UK sector can be attributed to flood and wildfire incidents in the US (2019-2021). The sector also horizon scans in conjunction with the Telecoms sector through fora at techUK to be aware of issues which could affect both sectors. Power supply provisioning issues are one such topic of mutual interest in recent months.

Industry standards and design specifications

As is the case in many industries, collective standards are commonplace for the building design and operation of colo data centres. These are what inform consumers on the type, level of security and resilience, and service they can expect from specific operators when "shopping around" for a data host. The sector has developed an impressive range of peer reviewed, International Technical Standards, KPIs, metrics and toolkits covering resilient design and operation.

The EN50600 series developed by CEN/CENELEC address resilience, relating to the data centre facility's "availability classes", where availability is synonymous with resilience (available to provide services). These standards, though uncertifiable, are gradually being harmonised internationally (with ISO and ITU) to improve consistency. Heterogeneity of standards is not an issue unique to the data centre sector, and most are clear enough to categorise an element of design or operational capabilities for an installation.

Data centres also work to a range of generic risk standards such as ISO 31000 and ISO 22301. The Information Security Management System (ISMS) via the ISO/IEC 27001 standard is being implemented by operators to improve the overall security posture of their operations. This often leads to a more streamlined approach to compliance, alongside other frameworks such as the PCI-DSS and SSAE/ISAE SOC 2 controls. These standards improve the security of physical and information assets.

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org

techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

Source[vi]: CEN/CENELEC/ETSI	Availability of overall set of facilities and infrastructures			
	Low	Medium	High	Very high
	AVAILABILITY CLASS			
Infrastructure	**1**	**2**	**3**	**4**
Power supply/ distribution EN 50600-2-2	Single-path (no redundancy of components)	Multi-path (resilience provided by redundancy of systems)	Multi-path (resilience provided by redundancy of systems)	Multi-path (fault tolerant even during maintenance)
Environmental control EN 50600-2-3	No specific requirements	Single-path (no redundancy of components)	Single-path (resilience provided by redundancy of components)	Multi-path (resilience provided by redundancy of systems), allows maintenance during operation
Telecommunications cabling EN 50600-2-4	Single-path using direct connections	Single-path using fixed infrastructure	Multi-path using fixed infrastructure	Multi-path using fixed infrastructure with diverse pathways

Climate resilience

Climate risks are mitigated in the design specifications of data centres using granular, location-specific weather data. Common sources of these data are ASHRAE and CIBSE. CIBSE is a key reference for building design guidance, produced in collaboration with UK Climate Impacts Programme, Arup and the University of Exeter. These include the latest climate change projection to ensure future proofing of sites. ASHRAE publishes external ambient weather data for every country and major city in the world to inform design specifications for new data centre builds as well as upgrades to existing sites. The relationship between these data sets is unclear at present. Most in the sector agree that ASHRAE data provides the appropriate headroom for operators.

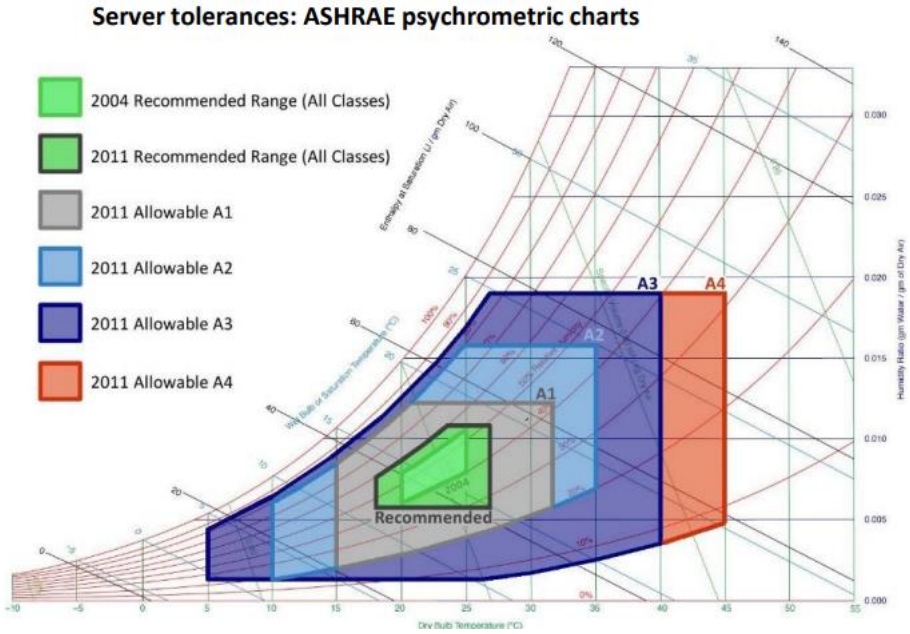
Work is ongoing to expand the temperature and humidity ranges within which computing equipment will work reliably, admittedly in a bid for operational efficiency but with positive benefits for climate resilience. ASHRAE has defined operating envelopes for servers in terms of temperature and humidity boundaries, which extend informal license to the facilities which will house said computing equipment (colos). These envelopes have become expanded as servers have modernised. This constitutes operational resilience at the IT hardware level. Legacy servers, however, are unlikely to be warrantied to the same limits as modern servers. It follows that data centres housing legacy equipment will be less able to cope with heatwaves, especially if high temperatures are sustained. The envelopes are illustrated below.

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org

techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK



It should be noted that these envelopes should be applied with care, with additional factors such as air pollutants present and server density affecting their application.

ASHRAE data has been used to produce cooling maps to indicate parts of the world where free cooling (non-mechanical) is feasible. These Green Grid free cooling maps have been reviewed since first publication (2009) but techUK advocates for them to be regularly updated in line with climatic changes, as well as for more granular approaches to be implemented in some locations.

Supply Chain Resilience

Supply chain disruptions, like those experience in the past two years due to the COVID-19 pandemic, are mitigated in several ways by operators. Spare parts and equipment are stocked up to be on hand in the event of supply chain delays. Operators are acutely aware of the international shortages in chips and semi-conductors. The Government is urged to act more quickly to ensure supply is resilient. Without action, the availability of ICT hardware may become a limit to growth and technological advancement resilience in the data centre/cloud sectors. techUK has published a position on semi-conductors recently which can be found here.

techUK members have highlighted the importance of coordination and alignment with the Network and Information Systems regulations to avoid weaknesses in the upstream supply chain of data centres and thereby cloud providers. However, as stated in our response to the NIS consultation earlier this year, we do not advocate for an all-encompassing regulation for companies providing managed services due to the risk of a strictly tiered monopoly on highly resilient premium services.

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org

techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

The data centre supply chain also includes human capital in the form of operational staff, managers and technicians in the case of smart hands. The rise of in-house provision of smart hands services mitigates the risks of unvetted access to sensitive data. There remains a risk of contracted engineers, cleaning staff and security officers at sites potentially having access to sensitive data. This is managed at the discretion of individual operators who will have measures to vet staff and restrict access to the necessities. It is our understanding that site visits occasionally take place to appreciate the physical security measures in place to protect the integrity of a typical data hall.

As techUK has consistently highlighted, there is a critical shortage of skilled workers across the technology sector, including security professionals, network technicians and cloud engineers. Addressing this broader skills shortage and ensuring data processors and cloud providers have access to the best talent will further reinforce the security and resilience of services hosted in data centres. This also applies to data centre smart hands operators.

Industry and government need to look at an extended pipeline of skilled talent, which would also require attention to be paid to the visa arrangements which risk preventing talented individuals moving to the UK for these types of work.

External Policy Drivers

International best practice for the data centre sphere includes the Climate Neutral Data Centre Pact, the Infrastructure Masons and the Coalition for Disaster Resilience Infrastructure (CDRI). techUK and its members work actively with CDRI on sharing best practice on infrastructure resilience. Policy drivers such as the mandatory TCFD, Banking Supply Chain Resilience guidance, and the Downstream Oil Draft Resilience Bill promote transparency in risk management, active management of risks, and supply chain resilience in digital infrastructure.

Smart Hands Services

Smart hands services are offered by certain colocation operators. This is a form of data centre contracted technical support, removing the need of customers to hire their own technical support. This overcomes issues of unauthorised access and saves money for customers. Smart hands services include asset tagging, waste disposal, unpacking and installing servers, recycling servers, asset buy backs, and data destruction.

This practice keeps the management of third-party assets in-house, mitigating the risks of unauthorised access. As well as having cost, security and sustainability benefits, operators who offer smart hands services add an additional layer of personnel security to their operations. Physical access risks are an increasing concern for colocation operators housing sensitive data.

Data Access Risks (security)
Sensitive access risks (cyber access), Aggregation of illicitly accessed data, State threats, Multi-impact risks, Future risks.

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org

techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

Sensitive Access Risks (cyber access)

Supply Chain Resilience (Cyber Security) – techUK members have engaged extensively with DCMS on the need to improve the cyber resilience of supply-chains across all sectors of the UK economy, including in last year's DCMS Call for Views on Supply Chain Security. We will provide our response to that alongside this document.
Broadly, techUK members recognise key common barriers facing all organisations from effectively managing their supplier risk. These range from:

- Commercial
    - Not wishing to adversely impact project schedules or client relationships;
    - Less mature suppliers not having the procedures in place to suitably manage their cyber security risks; and
    - That customers/end users often find it difficult to manage supply chain risk because what they are asking from suppliers is not fit for purpose.
    - Constraints of existing contracts and an apparent hesitancy to ask 'intrusive questions' at the risk of impacting the business relationship can further enforce barriers that prevent organisations from effectively managing their supplier risk, especially as the nature of Services means that it can be difficult to flow down requirements and expectations.
- Cost and efficiency
    - Some members highlight challenges around cost and efficiency in effective supply chain risk management. While there have been positive moves made, such as the introduction of the Defence Cyber Protection Partnership in the Defence industry, these schemes have struggled on take-up, reducing their effectiveness.
- Capability and Skills
    - Some organisations struggle more with shortfalls in skilled cyber security focused employees, whether through cost implications or lack of understanding. Companies within the supply chain all have different risk appetites, internal processes and client bases which means no two companies' approaches are identical.

techUK members unanimously agreed that the key to useful supply chain resilience lies in the use of an effective risk-based approach. Any potential future intervention being considered by Government must seek to manage risk against the need for continual innovation, not just in the technologies used but also commercially.

Aggregation of illicitly accessed data

As this response has already touched upon, the eco-system in this space is large and complex. In many areas of the tech sector and the downstream value chain, organisations should share responsibility to understand and mitigate against ever-changing threats. Companies operating in data driven industries should (and often do) try to collaborate and more effectively share threat intelligence with their networks.

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org

techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

There are existing contractual elements which allow data centres and their customers to understand their roles and responsibilities in relation to both cyber and physical threats and we note that techUK members have real ambition and interest in strengthening resilience.

State threats

As we see geo-political shifts across the globe, specifically in light of the war in Ukraine, it is clear that the risk of state sponsored cyber-attacks is increasing. To date, the technical mitigations against such threats are identical to those employed against criminal activity, but techUK recognises the need for caution in understanding the commercial relationships at play in key sectors (not just traditional Critical National Infrastructure). To that end techUK has engaged extensively on the National Security and Investment Act 2021 which obviously applies across the technology sector. It is in the interest of industry to work with policymakers to develop best practice for resilience and recovery to mitigate the risk from malicious, potentially advanced, state threats. This should include stochastic cyber events (hacks) as well as market manoeuvres which may undermine the integrity of the data economy.

Future risks

The crossover between physical and cyber security continues to be a key trend across all sectors. Often, the insider threat is one of the main risks to any organisation and this is no different in the data centre market. Whether a breach is physical (in a hardware stack) or virtual (through inappropriate use of logical access controls) is often immaterial to the damage that can be felt by UK organisations and citizens. It is important to address these issues concurrently and remains the case that personnel can often be both the biggest risk and most effective mitigation, a trend unlikely to change. For this reason, we suggest the interdependency of physical and cyber access be explored more.

The rise of smart hands and data centre contracted/vetted technical/cyber literate staff is one way that personnel risks are mitigated. It is reasonable to say that periodic reviews are necessary in the industry to stay ahead of malicious threats and to keep policymakers informed. techUK endeavours to connect industry with the relevant government departments in a horizon scanning capacity.

The increasing convergence of cloud computing and edge computing, and the emergence of a broader distributed or hybrid cloud, should also be considered by DCMS. Companies like Gartner have predicted that 75% of all data will be processed at the edge by 2025, and colo edge servers in smaller regional data centres or other infrastructure is expected to be a growth market. The evolution of security and resilience measures in this emerging market is worthy of future research and consideration by DCMS.

Finally, it is worth noting that the pace of advancement in quantum computing also has long-term cybersecurity implications, such as the risk introduced by quantum systems that can break the encryption of data collected and stored today. Identifying technologies, such as Quantum Key Distribution (QKD) that can help with the long-term resilience of data centres and network infrastructure will be key to safeguarding data processing services.

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

Glossary

CSP – Cloud Service Provider
MSP – Managed Service Provider
NIS – Network Information and Security (Regulation)
CNI – Critical National Infrastructure (Designation)
CPNI – Centre for the Protection of National Infrastructure
NCSC – National Cyber Security Centre
SLA – Service Level Agreements
ICT – Information and Communication Technology

Hyperscaler – Advanced data centre facility that provides the space, power, cooling and the network infrastructure required to support the mass scale requirements of data and cloud computing.
Colo– Colocation data centre: A data centre operated by a third party with a commercial rental business model.
On-Premise – A data centre run out of an office or warehouse, usually for a single party and without the bespoke power and environmental conditions of a hyperscale or colo facility.

Contact: Adam Young Environment Programme Manager
T +44 7944 071 459 | E Adam.Young@techuk.org