Cyberfort

WHITE PAPER

Data Centre strategies are at a tipping point

Why organisations need to consider outsourcing their Data Centre requirements to a specialist provider so they can achieve their data storage, management and security goals

Introduction

In the rapidly evolving world of technology, IT teams face increasing pressure to deliver robust, scalable, and cost-efficient IT infrastructure while managing security risks, compliance requirements, and a growing demand for innovation. For many organisations, in-house data centre management is no longer a sustainable model.

In a recent BBC article (1) it was reported that data centres in the UK are to be classified as critical national infrastructure, joining the emergency services, finance and healthcare systems, and energy and water suppliers. The article also highlighted how many organisations are planning to build new data centres across the UK. But many of the new data centres which are being planned are facing criticism over their potential energy and water use.

Building, managing and maintaining a data centre is not an easy task. In fact, building a large data centre at scale can take 1.5 – 3 years and has to factor in a number of environmental factors as well as the day to day running. At Cyberfort we have built 2 x UK based data centres in ex MOD nuclear bunkers to help our customers store, manage and maintain their data in secure operating environments and overcome the hurdles of having to build new on premises data centres themselves.

A specialist data centre provider with readily available space, security, power and infrastructure should be explored early as a strategic solution, as it will likely provider greater value, easier management and lower TCO than building and managing internal infrastructure with cost and complexity. In this article Cyberfort Data Centre and Cloud specialists discuss areas organisations should be thinking about when considering outsourcing data centre provision to a specialist provider instead of managing physical networks and infrastructure themselves.

Why organisations need to consider outsourcing their Data Centre requirements

As identified in the previous section of this article, IT teams face increasing pressure to deliver robust, scalable, and cost-efficient IT infrastructure while managing security risks, compliance requirements, and a growing demand for innovation. This article covers 5 key areas for why organisations should be considering data centre outsourcing as part of their infrastructure strategy.

01 Rising Infrastructure Demands

Managing a modern data centre is becoming an increasingly complex task for IT Directors, driven by exponential growth in technology demands and the pressures of an evolving digital landscape. This complexity is creating significant challenges for organisations, making traditional in-house management approaches both expensive and unsustainable.

The explosion of technologies such as artificial intelligence (AI), the Internet of Things (IoT), and big data has led to a dramatic increase in the need for high-performance computing and vast storage capacities. It is no secret organisations are generating, processing, and analysing unprecedented volumes of data to remain competitive. Unfortunately, many legacy systems are ill-equipped to handle this surge. Adapting these systems to meet modern requirements often involves costly upgrades or redesigns that demand significant time and expertise. This can hinder an organisation's ability to scale quickly and remain agile in dynamic markets.

Running an in-house data centre comes with considerable operational expenses that extend far beyond initial investments in hardware and facilities. Power and cooling costs are major contributors, especially as servers generate more heat and require increasingly sophisticated cooling systems. Staffing also represents a significant financial burden, as IT teams must possess a diverse range of skills to manage hardware, software, network infrastructure, and security protocols. These operational costs often increase as businesses grow, creating ongoing financial strain.

The modern regulatory environment adds another layer of complexity to data centre management. Organisations must comply with stringent standards such as the General Data Protection Regulation (GDPR), and various industry-specific requirements such as PCI-DSS in retail for example. Compliance demands resources, specialised knowledge, and continuous monitoring to avoid penalties.

Simultaneously, cyber threats are growing in scale and sophistication. IT teams must combat ransomware attacks, phishing schemes, and insider threats while maintaining robust disaster recovery plans to ensure business continuity. The cost of addressing these challenges in-house is high, often requiring investment in advanced tools and 24/7 monitoring capabilities that can be difficult for many businesses to sustain.

In summary, the growing complexity of data centre management driven by infrastructure demands, operational costs, and regulatory pressures is highlighting the need for businesses to explore alternative models, such as outsourcing, to maintain efficiency and competitiveness.

02 Addressing Common Concerns around Data Centre Outsourcing

While the advantages of outsourcing data centre operations are compelling, IT Directors often encounter concerns and misconceptions that can create hesitation in adopting this model. Addressing these apprehensions is essential to making a confident, informed decision that aligns with organisational goals. Based on our 20+ years' experience of providing outsourced data centre services at Cyberfort, the table below details the most common concerns we encounter when discussing this approach with our customers and how we provide practical solutions.

Customer Concern Area	How Cyberfort helps customers overcome this concern
Data Sovereignty One of the most significant worries an organisation faces is whether outsourcing data centre operations will compromise their security. Sensitive data hosted off-premises may feel less secure, and organisations might fear breaches or unauthorised access.	At Cyberfort we have heavily invested in state-of-the-art security measures that are often beyond the budget or expertise of in-house teams. We have 130+ accredited and certified cyber security professionals available 24/7 to make sure the highest levels of security are implemented and maintained for any data stored in our UK based datacentres. The measures we have implemented include encryption for data at rest and in transit, AI-driven threat detection, 24/7 monitoring, and physical security such as biometric access controls. We also adhere to stringent security certifications like ISO 27001 and regularly undergo audits to maintain compliance. Additionally, organisations can mitigate concerns by opting for hybrid models, retaining sensitive workloads on-premises while outsourcing less critical functions to Cyberfort if they want a phased approach to moving data across to a third-party data centre.
Control and Accessibility IT leaders may worry that outsourcing will result in a loss of control over their data and systems. The thought of depending on an external provider for critical infrastructure can feel risky.	At Cyberfort we have designed our outsourcing agreements to maintain transparency and flexibility. We offer customised service level agreements (SLAs) that clearly define performance metrics, uptime guarantees, and escalation procedures. Advanced dashboards and management tools enable real-time monitoring of outsourced systems, giving organisations full visibility and control over their infrastructure. Moreover, hybrid and multi-cloud strategies can allow businesses to balance outsourced resources with in-house systems. These models ensure that businesses retain control over specific workloads or data sets while benefiting from the scalability and expertise of Cyberfort.

Customer Concern Area	How Cyberfort helps customers overcome this concern
 **Vendor Lock-In** Organisations may fear becoming overly reliant on a single provider, creating vendor lock-in that makes it difficult to switch or scale with evolving needs.	At Cyberfort we use open standards and interoperable technologies to significantly reduce the risk of vendor lock-in. We support multi-cloud environments and offer easy data migration options. All our contracts contain flexibility clauses, such as clear exit strategies and data portability guarantees.
 **Cost Transparency** Senior IT leaders may worry about hidden costs or unexpected charges in outsourcing agreements with suppliers.	Cyberfort offers transparent pricing models, including detailed breakdowns of costs and regular financial reporting. All our fees are clear from data transfers to storage scaling. We also offer fixed pricing or consumption-based models depending on the requirements from the organisation this can help IT leaders to better predict and manage expenses.
 **Business Continuity During Transition** The process of migrating to an outsourced data centre can seem risky, with fears of service interruptions or data loss.	At Cyberfort we have successfully migrated 100's of customers across to our data centres over the past 20+ years. We have well-established migration processes designed to minimise disruption. We help IT Directors to mitigate risks by planning a phased migration strategy, starting with non-critical systems to test processes and identify potential issues. We also emphasise regular communication during the transition and thorough testing after migration ensure smooth continuity.
 **Cultural and Operational alignment** IT leaders may question whether an external provider can align with their organisational values, culture, and operational goals.	Cyberfort has a strong understanding of many industries and maintain open communication channels. We schedule regular review meetings, performance reporting, and collaborative SLAs to help ensure alignment. Additionally, we offer dedicated account managers to act as liaisons between teams, further bridging any gaps.

By addressing these common concerns with clear solutions, IT Directors can build confidence in the decision to outsource. The key lies in partnering with a reputable, experienced provider like Cyberfort and maintaining proactive communication to align outsourced services with business goals. Far from losing control or compromising security, outsourcing can empower IT teams to focus on innovation while benefiting from expert support and modern infrastructure.

03 Why Outsourcing Is a Strategic Move

Outsourcing data centre operations is no longer just a tactical decision for reducing costs, it has become a strategic move for businesses aiming to stay competitive, agile, and innovative. So why is outsourcing data centre provision to a third-party provider a strategic move? From our experience at Cyberfort there are 3 key reasons why organisations should look to outsource their data centres instead of building from new.

Access to Expertise

Specialist data centre providers like Cyberfort bring a wealth of knowledge and experience to the table, often surpassing what many internal teams can offer. At Cyberfort we employ certified professionals who specialise in areas such as cloud architecture, cyber security, and compliance. This expertise ensures that organisations have access to cutting-edge technologies and best practices without the need to invest in continuous staff training or recruitment. Additionally, through our Governance, Risk and Compliance team organisations can stay abreast of evolving regulations, ensuring that customers remain compliant with standards like GDPR, HIPAA, and PCI DSS. Outsourcing also enables IT Directors to fill skill gaps quickly, particularly in areas requiring niche expertise, which can be difficult and expensive to maintain in-house.

Enhanced Security Measures

In today's digital landscape, security is a top priority. Cyberfort is one of only 24 NCSC assured consultancy providers in the UK and we can call upon our consultant's expertise to ensure any data centre solution built is based on NCSC's 14 guiding cloud principles. Additionally, our data centres are equipped with advanced tools and technologies that offer superior protection against cyber threats. Features include AI-driven threat detection, intrusion prevention systems, and 24/7 monitoring ensure a robust defence against attacks. Additionally, physical security measures such as access controls, 24/7 surveillance systems, and redundant power supplies further safeguard critical assets. Cyberfort also offers disaster recovery and business continuity solutions, ensuring that systems can quickly recover from unexpected outages or cyber incidents. These measures not only enhance security but also reduce the burden on in-house teams to maintain such safeguards.

Cost Optimisation

Outsourcing transforms capital expenditures (CapEx) into manageable operational expenditures (OpEx). Organisations can avoid the significant upfront costs associated with building and upgrading their own data centres, including investments in hardware, cooling systems, and physical facilities. Instead, with Cyberfort organisations pay predictable fees based on usage or flat-rate models. By outsourcing to a specialist provider, organisations can achieve economies of scale as we serve multiple customers, which enables the delivery of cost-efficient solutions that would be prohibitively expensive for individual businesses to replicate. This cost optimisation allows IT leaders to allocate budgets to strategic initiatives rather than infrastructure maintenance.

04 Key Benefits of Outsourcing Data Centres

Outsourcing data centre operations to specialist providers is a transformative strategy that delivers significant advantages across scalability, security, cost efficiency, and innovation. This section explores the key benefits that make outsourcing an attractive option for businesses aiming to modernise their IT infrastructure while maintaining focus on strategic goals.

Scalability and Flexibility

Most organisations operate in dynamic environments where IT demands fluctuate due to factors such as market trends, seasonal activities, or unexpected growth. In-house data centres often struggle to adapt quickly, requiring costly infrastructure upgrades or over-provisioning.

Outsourcing solves this challenge by providing on-demand scalability. At Cyberfort we offer flexible, scalable solutions that can quickly and seamlessly adjust for changes in capacity ensuring optimal performance without the financial and operational burdens of overhauling in-house systems. For instance, if a business needs additional storage or computing power during a peak period, an outsourced provider can deliver these resources seamlessly and scale them down when demand subsides.

This flexibility is invaluable for supporting growth. As businesses expand into new markets or launch digital transformation initiatives, providers can accommodate increased workloads without requiring additional investments from the customer.

Business Continuity

Downtime can have catastrophic effects on a business, including financial losses, reputational damage, and customer attrition. Specialist data centre providers prioritise business continuity with robust disaster recovery (DR) plans and guaranteed service levels.

Cyberfort has 2 UK based data centre facilities with failover mechanisms, ensuring resilience against localised disruptions such as natural disasters, power outages, or cyber attacks. These redundancies are coupled with stringent recovery time objectives (RTOs) and recovery point objectives (RPOs) outlined in service level agreements (SLAs).

By outsourcing, businesses gain access to cutting-edge DR tools and expertise, reducing the risk of critical data loss and ensuring uninterrupted operations.

Enhanced Security

Outsourcing to a specialist provider like Cyberfort significantly strengthens security. As mentioned earlier in the article Cyberfort has invested heavily in physical and digital security measures that many businesses cannot afford to replicate in-house. These include:

- Advanced encryption for data in transit and at rest.
- AI-driven threat detection and mitigation systems.
- Continuous monitoring and real-time alerts.
- Access controls and round-the-clock surveillance.

Additionally, through our GRC team organisations can stay current with the latest regulatory requirements, reducing the risk of compliance breaches. We also undergo third-party audits to maintain certifications such as ISO 27001 and SOC 2.

Focus on Core Competencies

By outsourcing data centre management, businesses can redirect internal IT resources toward value-added initiatives like application development, customer experience enhancement, and strategic planning. IT teams no longer need to focus on routine tasks like hardware maintenance, software updates, or capacity planning. This focus on core competencies improves overall organisational productivity, fosters innovation, and positions businesses for long-term success in a competitive landscape.

Sustainability

Specialist providers are at the forefront of green IT practices, making sustainability a significant benefit of outsourcing. At Cyberfort we have adopted energy-efficient technologies, renewable energy sources, and innovative cooling solutions to minimise environmental impact. By outsourcing, businesses can align with corporate sustainability goals while reducing their carbon footprint.

In conclusion, the benefits of outsourcing data centre operations extend far beyond cost savings. It offers scalability, business continuity, enhanced security, and sustainability, while empowering IT teams to focus on innovation. For businesses aiming to thrive in a rapidly evolving digital landscape, outsourcing is a strategic investment that drives operational excellence and competitive advantage.

05 Building the Business Case

For IT leaders, the decision to outsource data centre operations instead of building/maintaining a data centre hinges on presenting a well-reasoned business case. This case must not only outline the financial implications but also demonstrate how outsourcing aligns with organisational goals, mitigates risks, and unlocks strategic value. Below, we explore the key components of building a compelling business case for outsourcing to a third-party provider instead of building a data centre.

Assessing the Total Cost of Ownership (TCO)

To make a strong case, IT Directors must first quantify the total cost of ownership (TCO) for their current in-house data centre operations. This includes both direct and indirect costs, such as:

- **Capital Expenditures (CapEx):** Initial investments in hardware, software, real estate, and facilities.
- **Operational Expenditures (OpEx):** Ongoing costs for power, cooling, staffing, maintenance, and security.
- **Upgrades and Scaling:** Costs associated with hardware refreshes, capacity expansion, and technology obsolescence.
- **Downtime Costs:** Financial losses due to system outages or service disruptions.

Once these costs are calculated, they can be compared to the predictable, scalable pricing models offered by outsourcing providers. This often reveals significant cost savings and highlights the financial predictability of transitioning to an operational expenditure (OpEx) model.

Demonstrating ROI

Beyond cost comparisons, the business case should emphasise the return on investment (ROI) of outsourcing. Key areas to highlight include:

- **Cost Savings:** Quantify reductions in power consumption, staffing, and maintenance.
- **Efficiency Gains:** Showcase how outsourcing improves system uptime, disaster recovery times, and workload scalability.
- **Strategic Focus:** Explain how outsourcing frees internal IT teams to focus on innovation and high-value projects.

Cyberfort can help IT teams to present data-driven scenarios that estimate savings and operational improvements over time, underscoring the long-term financial and strategic benefits.

Risk Mitigation

A robust business case addresses how outsourcing mitigates operational and security risks. For example Cyberfort can deliver:

- **Enhanced Security:** Advanced measures like AI-driven threat detection, 24/7 monitoring, and compliance with regulatory standards.
- **Business Continuity:** Redundant systems, disaster recovery plans, and SLAs with guaranteed uptime.
- **Regulatory Compliance:** Expertise in navigating complex regulations like GDPR, HIPAA, and PCI DSS.

This helps IT Directors to illustrate how outsourcing shifts risk management responsibilities to experienced providers, reducing exposure to downtime, data breaches, and compliance penalties.

Aligning with Strategic Goals

A critical part of the business case is aligning outsourcing with broader business objectives, such as:

- **Agility:** Outsourcing enables businesses to scale IT infrastructure rapidly to meet market demands or expand into new regions.
- **Innovation:** With routine infrastructure tasks managed externally, IT teams can focus on strategic initiatives like digital transformation or AI adoption.
- **Sustainability:** Highlight how outsourcing to providers with green IT practices supports corporate social responsibility goals and reduces environmental impact.

By showing how outsourcing supports the organisation's growth, innovation, and sustainability targets, IT professionals can position it as a strategic enabler rather than just a cost-cutting measure.

Addressing Stakeholder Concerns

Stakeholders often have concerns about outsourcing, such as loss of control, security risks, or cultural alignment. Addressing these proactively strengthens the business case:

- **Control:** Emphasise hybrid or multi-cloud models that allow the organisation to retain control over critical workloads.
- **Security:** Showcase provider certifications, compliance expertise, and SLAs that guarantee protection.
- **Cost Transparency:** Present detailed cost breakdowns and highlight predictable pricing structures.

Encouraging stakeholder buy-in through clear communication and addressing potential objections ensures smoother decision-making.

Building a business case for outsourcing data centres requires a comprehensive assessment of costs, benefits, risks, and alignment with strategic objectives. By demonstrating financial advantages, operational efficiency, and risk mitigation, senior technology leaders can position outsourcing as a forward-thinking decision that drives both immediate and long-term value. Ultimately, a well-crafted business case transforms outsourcing into a strategic enabler that supports growth, innovation, and resilience.

Final thoughts

Outsourcing data centres to specialist providers is no longer just an operational decision; it's a strategic move that positions businesses for long-term success. For IT Directors, the case for outsourcing lies in its ability to enhance security, drive cost efficiency, and enable business agility. By leveraging the expertise and resources of a specialist provider, organisations can future-proof their IT infrastructure, reduce risks, and focus on driving innovation.

Outsourcing is not merely about cutting costs; it's about unlocking the potential to do more with less. IT teams who embrace this shift will find themselves better equipped to meet the challenges of tomorrow.

1. https://www.bbc.co.uk/news/articles/c23ljy4z05mo

Discover more about Cyberfort's all-encompassing Data Centre and Cyber Security Services

At Cyberfort we provide a range of customers with all-encompassing Cyber Security Services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks, proactive Detection and Response to security incidents through our security operations centre and a Secure and Recover set of Cloud solutions which keeps data safely stored, managed and available 24/7/365.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.

For more information on our Data Centre and Cyber Security services please contact us at the details below:

+44 (0)1304 814800 | info@cyberfortgroup.com | https://cyberfortgroup.com

We look forward to working with you