

Data Centre Security: Guidance for owners

Read the full guidance at www.cpni.gov.uk/data-centre-security

Geography and ownership security

Regulations in some countries mean the data you store could be accessed by a foreign government. Also, UK GDPR sets out principles data controllers must comply with, or risk being fined. It's important to be aware of all the geographical considerations that impact on the security of your data centre.

Data centres' physical perimeter and buildings

The security of the physical perimeter and site of your data centre is your responsibility and should meet customer expectations. Do you know how to deter, detect and delay attackers or discourage espionage or hostile reconnaissance?

The data hall

Data centre operators are responsible for data hall security. Are you sure that access to customers' equipment is controlled? Are you able to demonstrate you're prepared for a power outage or a fire? Your data hall must be thoroughly protected.

Meet-me room considerations

Access to MMRs should be strictly controlled. It's also important to consider security measures such as meet-me room screening, searches, intrusion detection, anonymisation and asset destruction.

People security considerations

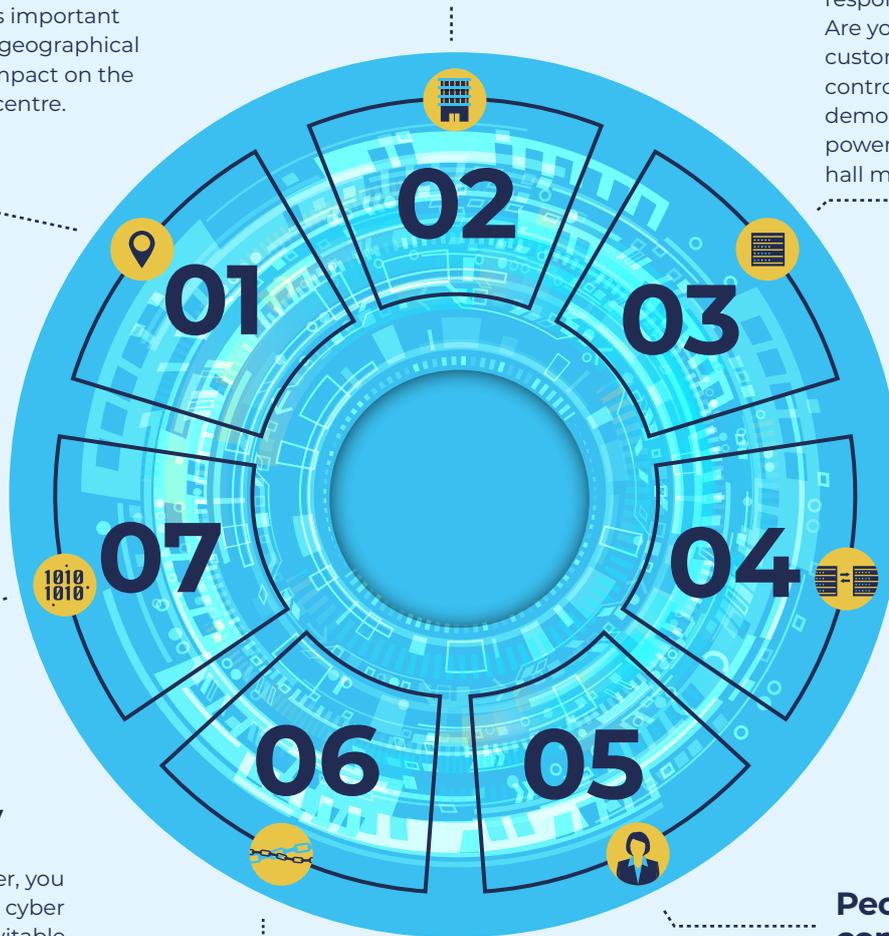
A data centres workforce can both enhance security as a force multiplier but could also introduce further risks. Ensure you develop a strong security culture that motivates and engages staff and mitigates 'insider' risks – recruitment of insiders is an attractive option for threat actors.

Supply chain considerations

It's important to consider the security of your entire supply chain. The companies you work with and buy products and services from present their own security risks and vulnerabilities. You need to understand all the security risks you face by introducing third parties.

Cyber security

As a data centre owner, you should assume that a cyber security breach is inevitable. Take steps to detect intrusions, minimise their impact, and prevent further incidents. A comprehensive cyber risk management regime should be embedded throughout your organisation.



Disclaimer: This guide has been prepared by CPNI and NCSC is intended to provide holistic protective security guidance regarding the use of data centres. This document is provided on an information basis only, and whilst CPNI and NCSC have used all reasonable care in producing it, CPNI and NCSC provide no warranty as to its accuracy or completeness. To the fullest extent permitted by law, CPNI and NCSC accept no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the guidance or arising from any person acting, refraining from acting, relying upon or otherwise using the guidance. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

© Crown Copyright 2022.

You may use or reuse this content without prior permission but must adhere to and accept the terms of the Open Government Licence for public sector information. You must acknowledge CPNI the source of the content and include a link to the Open Government Licence wherever possible. Authorisation to reproduce a third party's copyright material must be obtained from the copyright holders concerned.