

Data Centre Security

KEY CONSIDERATIONS FOR DATA CENTRE OWNER SENIOR LEADERS

There is no one-size fits-all approach to holistic data centre security. Every data centre operator or owner needs to consider the NPSA and NCSC guidance based on their own risk assessments. The guidance contains the security considerations you need to be aware of as a senior leader to make sure you and your customers' data stays protected.



Risk management

The NPSA risk management framework encourages data centre owners to identify assets and threats, assess risks, develop a protective security strategy, implement measures, and review processes periodically. Remember that the risk management strategies of data centre customers and operators are interdependent.

As a data centre operator, you will want to ensure your risk management is robust to attract your clients, maintain your reputation, and comply with relevant regulatory compliance regimes. To be most effective, risk management strategies will be driven by senior leaders.

While less likely than attacks that focus on acquiring or degrading data, threat actors may also seek to disrupt services by targeting data centres through either a destructive cyber attack or a physical attack against a data centre. The cascading effects of a loss of service can be huge.



Resilience

Data centres need to ensure they are resilient against a range of threats and hazards, including natural hazards, power outages, hardware failures or denial-of-service attacks.

As a data centre owner, ask yourself if you have physically separate communications routes into the data centre, diverse power supply and back-up power options, and whether building service rooms are protected from physical attack or sabotage. Do you have the people power to deal with a security incident? Is your supply chain resilient?



Geography and ownership

In the UK, GDPR sets out principles data controllers must comply with. Understanding regulations on data security in the country where your data centre is located is also important. Some foreign governments – China and Russia are examples – may mandate access to data that limits your control and ability to provide assurances.



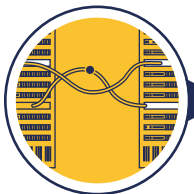
Physical perimeter and buildings

Security of the perimeter, site and data centre building is the responsibility of the operator. In an enterprise-owned facility, site security is defined by the enterprise based on its own risk assessment. In other facilities, the level of security should meet customer expectations and be designed to attract newcomers.



The data hall

Data centre operators are responsible for data hall security. Data customers may have additional security layers. Control of access is especially important when operating shared data centres. You must be able to demonstrate to your customers that you are prepared.



Meet-me rooms

Data centre operators should strictly limit access to meet-me rooms. You may decide not to allow customers access to view security arrangements. It's important however that meet-me room security assurances are provided during tendering. Measures to protect meet-me rooms include access control and screening, intrusion detection such as CCTV, entry and exit searches, rack protection, anonymisation, and asset destruction.



People

It's important to mitigate any security risks related to people, such as 'insider risk'. Data centre owners should optimise the use of people as force multipliers to prevent, detect and deter security threats. Having a good security culture means your workforce is likely to be engaged with, and take responsibility for, security issues.



Supply chain

Effectively securing your supply chain can be hard because vulnerabilities are inherent or introduced and exploited at any point. A vulnerable supply chain can cause damage and disruption. Data centre owners should consider physical, personnel and cyber security risks within any risk assessment.



Cyber

Data centre owners should assume that a cyber compromise is inevitable, take steps to detect intrusions and minimise their impact and take preventative cyber security measures. Organisations should ensure that good cyber security is built into their systems and services from the outset, and that those systems and services can be updated to adapt effectively to emerging threats.

For the full guidance, please visit: www.npsa.gov.uk/data-centre-security

Disclaimer: This guide has been prepared by NPSA 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 NPSA and NCSC have used all reasonable care in producing it, NPSA and NCSC provide no warranty as to its accuracy or completeness.

To the fullest extent permitted by law, NPSA 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 NPSA 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.