CPNI Centre for the Protection of National Infrastructure

National Cyber Security Centre

Data Centre Security

KEY CONSIDERATIONS FOR DATA CENTRE USER SENIOR LEADERS

There is no one-size fits-all approach to holistic data centre security. Every data centre user needs to consider CPNI and NCSC's data centre security guidance based on their own risk assessments and risk management. This guidance contains the key security considerations you need to be aware of as a senior leader to make sure that the data of your organisations and your customers stays protected.

Risk management

The CPNI risk management framework encourages users 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.

Resilience

You should ask yourself if the data centre can demonstrate it has physically separate communications routes, diverse power supplies and back-up power, protected building services rooms, the human resources to cope with a physical or cyber incident, and a resilient supply chain.

It should be assumed that at some point your data defences will be breached. It is important to be able respond proactively by detecting attacks and having measures in place to minimise the impact of any cyber security incidents.

Geography and ownership

Managed hosting or cloud hosting providers sometimes store your data in multiple locations, not necessarily in the UK. It's important you know where your data is stored, since some countries such as China and Russia have laws that could put it at risk.

Physical perimeter and buildings

Security of the perimeter, the site, and the building is usually the responsibility of the operator, but data centre users should consider the physical security measures in place and whether threats and risks have been identified and mitigated. You may need to discuss the option of implementing your own detection layers to maximise opportunities for detection at rack, room or hall level.

The data hall

No matter how secure the data centre, as a customer, it is your responsibility to ensure sufficient controls are in place at the data hall to limit who might be able to access your networking equipment. If you have your own suite or hall, you need to conduct your own risk assessment and identify the security measures you need.

Meet-me rooms

Access should be strictly controlled to meet-me rooms. Meet-me room security details and assurances should be provided by data centres during tendering. As well as access control, data centre users should consider access screening processes, intrusion detection such as CCTV, rack security, and asset destruction.

People

People can become force multipliers to improve security. They can help detect, deter and disrupt hostile actors planning attacks and a good security culture can also reduce the risk of the insider threat. The data centre you select should be able to demonstrate the policies and procedures it has place to deliver good people and personnel security.

Supply chain

Securing the supply chain can be hard because vulnerabilities are inherent or introduced and exploited at any point in the chain. As a data centre user, it's important you understand the impact outsourcing can have on your data centre requirements and the risks a supplier poses to assets.

Cyber

Remember that data centres are valuable targets for threat actors seeking to conduct cyber attacks. The motivation for these attacks is usually stealing, destroying or compromising your data. Data centre customers should assume that a successful cyber attack will happen and take steps to ensure such attacks can be detected and the impact minimised.

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

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.

CPNI
Centre for the Protection
of National Infrastructure

National Cyber
Security Centre