CPNI
Centre for the Protection of National Infrastructure

National Cyber Security Centre

Data Centre Security

GUIDANCE FOR USERS

CONTENTS

Introduction 04
Risk management 06
Resilience 08
Key types of data centre 10
7 security risks 12
- Geography and ownership risks 12
- Risks to data centres' physical perimeter and buildings 14
- Risks to the data hall 16
- Risks to the meet-me rooms 20
- People risks 22
- Risks to the supply chain 24
- Cyber security risks 26

INTRODUCTION

Data centres and the data they hold are attractive targets

One of the UK's most valuable assets is its data. Together with the data centres that hold and process it, it underpins almost all facets of modern life. This makes data centres an attractive target for threat actors, due to the large and diverse amount of information they hold that supports our national infrastructure and businesses.

The opportunities for attack are diverse. Threat actors will target vulnerabilities in data centres' ownership, geography, physical perimeter, data halls, meet-me rooms (MMRs), supply chains, staff and cyber security in a concerted effort to breach data centres' defences and acquire or tamper with sensitive information or disrupt critical services.

The security and resilience of your data and infrastructure are critical.

High-profile data breaches and disruption to services are frequently reported with each incident causing operators and data owners potentially huge financial losses in regulatory fines, loss of sensitive IP, downtime, post-incident recovery, security improvements, and perhaps most valuably of all, reputation.

Cyber intrusion methodology evolves constantly, and sophisticated attackers have a strong incentive to defeat the defences you put in place. It should be assumed that at some point your defences will be breached and therefore it is also important to be able respond proactively by detecting attacks and having measures in place to minimise the impact of any cyber security incidents.

To combat these diversified threats, we need to approach data centre security holistically. By bringing together the physical, personnel and cyber security of data centres into a single strategy you can better withstand the diversified methods state threat actors, cyber criminals and others may use to attack them.

There is no one-size-fits-all approach to holistic data centre security. Every data centre user will need to consider this guidance based on their own risk assessments. This guidance contains the security considerations you need to be aware of to make sure your data stays protected.

This guidance is laid out by key areas of risk

Each of these areas should be considered when developing a risk management strategy that encourages a holistic security approach in data centres – moving from where the data centre is located, and who manages and operates it, to protecting against cyber threats. You should use this guidance to inform your own risk management strategy that is unique to your organisation's needs.

Yellow call out boxes indicate that further guidance can be found on a specific topic. A full list of URLs for all the CPNI and NCSC guidance referenced within this document is available at page 32.

CASE STUDIES

1

T-Mobile

In July 2021, a Turkey-based individual claimed to have gained unauthorised access to over 100 servers based in the United States belonging to telecommunications provider T-Mobile. This access was reportedly initially gained by remotely exploiting a misconfigured router on the company's network.

T-Mobile subsequently confirmed in a statement that its systems had been accessed in an unauthorised manner and information belonging to several million customers were exposed. This information is reported to have included the names, dates of birth and telephone numbers of customers.

https://www.zdnet.com/article/t-mobile-hack-everything-you-need-to-know/

2

United States Office of Personnel Management (OPM)

In June 2015, the United States Office of Personnel Management (OPM) revealed that sensitive information relating to millions of US federal employees had been exfiltrated via an intrusion on its networks.

This information included classified details of federal employees, including their level of security clearances, personal and family information and their biometric details.

The breach is reported to have been facilitated by a combination of poor cyber security measures, including a lack of two-factor authentication and sub-standard malware protection.

State-sponsored Chinese hacking groups are reported to have conducted this attack in order to increase its intelligence collection on American citizens.

https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

3

Meta

In October 2021, a misconfigured piece of networking equipment involved in ensuring interconnectivity between US company Meta's data centres caused a global outage of its services for over six hours. This outage affected billions of Meta's users and businesses who were unable to access the company's platforms Facebook, Instagram, WhatsApp and Messenger.

The outage was prolonged because Meta managed its own data centres, so the issue could not be resolved remotely. Instead, a team of engineers had to visit the affected data centres in person to reconfigure the affected equipment.

This incident compounded reputational issues that Meta was facing at the time, and shortly after the outage, Meta's share price was reported to have dropped by 4.9%

https://www.theguardian.com/technology/2021/oct/05/facebook-outage-what-went-wrong-and-why-did-it-take-so-long-to-fix

https://www.nytimes.com/2021/10/04/technology/facebook-down.html

RISK MANAGEMENT

Implementing a risk management strategy

Data centre operators and their customers should have individual risk management strategies designed to protect their critical assets and systems.

CPNI's risk management framework encourages any organisation to follow these steps to manage risk:

- **Identify your assets.**
- **Categorise and classify your assets in relation to their level of criticality in supporting your business.**
- **Identify threats (based on intent and capability).**
- **Assess the risks, based on the likelihood of the threat happening and the impact should the threat transpire.**
- **Build a risk register to allow senior decision-makers to make informed judgements on risk appetite and resource allocation.**
- **Develop a protective security strategy for mitigating the risks identified and review the adequacy of existing countermeasures.**
- **Implementation: propose new proportionate measures using a process, such as the CPNI Operational Requirement (OR) process.**
- **Review the process periodically and when there is a change in threat or change in operational environment.**
- **Recognise that risk management strategies between data centre operators and their customers are interdependent.**

Is your data centre robust?

As a data centre customer, you will want to seek assurances that a data centre is robust enough to hold your sensitive data, whether that is financial, communications, medical, travel or other kinds of personal data belonging to your customers or staff, or your own sensitive commercial data. Doing so securely also ensures your reputation and commercial advantage.

To be most effective, risk management strategies will be driven by senior leaders who understand the risks and protective security options available to help mitigate these risks.

The areas of security risk relevant to both data centres, and the data they hold, are detailed throughout this guidance.

This information should be used to inform your organisation's risk-based assessments and wider risk management strategy, regardless of whether you are a data centre owner, or a data centre customer.

Should you judge these threats to pose sufficient risk to your own assets and systems, we provide further information on the mitigations you might consider to better manage these risks, and where appropriate, we will direct you to CPNI or the National Cyber Security Centre (NCSC) comprehensive guidance on each topic.

You can also learn more about how to approach protective security risk management in more depth on CPNI's website.

The NCSC also provide guidance on approaching risk management from a cyber security perspective.

RESILIENCE

A wide range of attacks

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.

OVHCloud

As demonstrated by the October 2021 Facebook outage incident, the cascading effects of a loss of service can be huge.

In March 2021, a fire broke out at French cloud services provider OVHCloud destroying one of its four data centres and damaging another at its Strasbourg campus in France. This resulted in the company directing its clients, which include the French government, to activate their disaster recovery plans and reportedly denied access to a large number of domains and services.

Ensuring that a data centre is resilient is key

For data centres, worst case risk scenarios tend to focus on availability issues such as service disruption due to natural hazards, power outages, hardware failures or denial-of-service attacks.

Data centres need to ensure they are resilient against a range of threats and hazards. They are typically already designed to be resilient to these types of availability issues, with numerous standards and guidance widely available. We provide some of these standards in the additional resources section at the end of this guidance.

As there is extensive guidance available on data centre resilience, we will not cover it in detail here. However, there are some questions about resilience that we would advise a data owner to ask of a data centre operator to ensure they are less vulnerable to deliberate acts to disrupt services:

- **Can the data centre demonstrate that it has physically separate communications routes into the data centre?**
- **Can the data centre demonstrate it has diverse power supply and backup power options?**
- **Are the building service rooms critical to the functioning of the data centre (e.g. electrical, battery and mechanical rooms, backup generators etc.) protected from physical attack and sabotage?**
- **Can data centre operators demonstrate that in the event of a physical or cyber incident, they have sufficient people power, e.g. adequate numbers of security personnel, engineers, and other incident management staff, who can provide a sustained response?**
- **Can the data centre demonstrate a resilient and diversified supply chain, including services, hardware, and software, which can withstand disruption and minimise bottleneck effects?**

Lastly, you should consider using multiple data centres or storage locations to increase resilience and reduce the associated risk of having a single point of failure.

KEY TYPES OF DATA CENTRE

Data centres: The options

There are several options for the type of data centre you may choose as a data owner. They offer different levels of service which can impact the control you have over security arrangements.

It is important to remember that as a data owner, whichever option you choose to go with, the responsibility for managing the risks to your information remains with you.

You should therefore understand the benefits and disadvantages of each option and use this to inform your risk management strategy.

Enterprise or 'wholly-owned' data centres

These are data centres that an organisation solely owns and operates for their own use, giving complete oversight of your security and operational arrangements, but often incurring higher costs.

Co-located data centres

These are centres where your organisation's data system is housed within a shared facility, along with other organisations' data. This is often more cost-effective due to the lack of upfront costs of building and running a data centre. While this option allows flexibility and the ability to scale at speed, you don't have sole access to the data centre and may have fewer (or no) customisable security options.

Managed hosting data centres

The hybrid model – a customised data-hosting package provided by a third-party in a data centre. The servers you use can be dedicated or shared with other customers. This option removes the need to hire staff and places responsibility for security on the third-party. While attractive from a convenience point of view, you have less oversight or control of your security arrangements.

Cloud-hosting data centres

Your data is stored in a network of servers across different data centres, in different locations, which increases your flexibility to scale at speed and may also improve your resilience in the case of an outage due to the distributed nature of your data. However, you will need to be clear on how your data is stored and managed; where and how your data will be moved, stored, or split while in the cloud, for example. Cloud service administration systems are often also highly privileged: if they are compromised, they could have a significant impact on your data.

The NCSC provides comprehensive guidance on the use of cloud services and their security.

The table below summarises the degree of control you may have over areas of risk for data centres, depending on the option you choose:

Control of aspects of a data centre	Enterprise	Co-located	Managed hosting	Cloud
Ownership	High	Medium	Medium	No
Location	High	High	Medium	Low
Data hall occupancy	High	No	No	No
Data hall operations	High	Medium	No	No
Building services operation	High	No	No	No
Facilities management	High	No	No	No
Security requirements	High	Medium	Low	Medium
Access to data centre	High	Medium	No	No
Access to your equipment	High	Medium	No	No
Staffing	High	Low	No	No
Supply chain	High	Medium	No	No
Security procedures (physical/personnel)	High	Low	No	No
Cyber security	High	Medium	Low	Low

1

GEOGRAPHY AND OWNERSHIP RISKS

Where is your data stored?

Managed hosting or cloud hosting providers may sometimes seek to store your data or manage your service in multiple locations, including outside of the UK. When this happens, it is important you know where your data is stored and from where it may be accessed.

Some governments mandate easy access to privately held information in data centres within their countries. Here are two examples:

Russia's System of Operative Search Measures (SORM) allows Russia's domestic intelligence agency, the Federal Security Service (FSB), to covertly monitor communications to, within, and out of Russia.

The FSB can also compel companies and individuals to share data stored in Russia with them and could prevent the data holder from disclosing this to the data owner.

All communication service providers (CSPs) operating in Russia are obliged to install equipment to enable the FSB to monitor communications. The FSB is not obliged to provide CSPs or commercial companies with any details of their monitoring by SORM.

This may mean that you are unaware of how your sensitive communications and information may be used in Russia or with Russian individuals and companies.

Once you are confident that where your data is stored is consistent with your risk appetite, you need to apply the same principles to where your data is accessed

China's National Intelligence Law (NIL) allows Chinese intelligence agencies to compel Chinese organisations and individuals to carry out work on their behalf and provide support, assistance and co-operation on request. This law may affect the level of control you have over your information and assets as you engage with Chinese individuals and organisations, especially if you work in an area that is of interest to the Chinese state, even if your data is hosted outside mainland China.

Where your data is accessed

Once you are confident that where your data is stored is consistent with your risk appetite, you need to apply the same principles to where your data is accessed. For example, if you use a follow-the-sun business model – whereby services or administration of your systems take place remotely by employees or contractors based overseas – local laws will still apply and may introduce further risks.

UK GDPR considerations

The UK General Data Protection Regulation (GDPR) sets out key principles which data controllers and data processors must comply with when processing personal data, including restrictions on personal data being transferred out of the UK unless the jurisdiction has adequate levels of data protection or there are appropriate safeguards in place. Failure to comply with the principles of the UK GDPR can result in substantial fines – up to 4% of your company's total worldwide annual turnover, or up to £17.5 million (whichever is higher) in the most serious cases, as well as potentially damaging your reputation.

If you think you may need to transfer personal data internationally, or that personal data may be transferred between UK and non-UK data centres, make sure to check the latest ICO guidelines on how to do so legally and securely before you do.

Depending on the sensitivity of your data, or your obligations under UK GDPR, you may wish to ensure that at a contractual level with your provider, your data is only ever stored within an agreed jurisdiction (for example, countries that form part of the data adequacy whitelist) to mitigate any risk.

The ICO has up to date guidance on GDPR

Ownership security considerations

The ownership of the data centre, or who the centre could potentially be owned by, can put your sensitive or business-critical information at risk.

Foreign direct investment

If a data centre you use is open to foreign direct investment (FDI), shareholders from a country hostile to the UK may be able to gain greater influence over operational decisions, including security-related ones. This may increase the risk posed to your infrastructure and/or data should shareholders be linked to or pressured by their domestic government, which may be hostile to UK interests.

To prevent this you can take a number of steps:

» **Conduct your own due diligence**
Be sure to conduct appropriate due diligence on who is invested in the data centres you use and consider their geography and ownership.

» **Create contractual agreements**
You should consider contractual clauses that could ensure that your data will remain in the UK, regardless of who takes ownership of the data centre, and that you are forewarned of any FDI or ownership changes that happen after you sign your contract. You may also want to consider adding a clause that allows contracts to be cancelled early in the event of any change in ownership.

» **Contractual clauses can used to ensure you are notified, and possibly required to approve, any changes to IT or Operation Technology (OT) networks or security systems. These clauses can not only be applied to changes in hardware, but also changes to security policies and procedures, as well as use of subcontractors. This helps ensure that transfers of ownership do not result in changes to the data centre that has a detrimentally impact on your equities.**

CPNI, the NCSC and the Department for Business, Energy and Industrial Strategy (BEIS), have produced joint guidance on making informed decisions with regards to foreign investment and how this will work under the new National Security and Investments Act compliance regime.

2

RISKS TO DATA CENTRES' PHYSICAL PERIMETER AND BUILDINGS

Securing the perimeter and site

In most data centre operating models, security of the perimeter, the site, and the building will be the responsibility of the operator. In an enterprise-owned facility, site security is defined by the enterprise based on its own risk assessment.

Data centre operators should be able to demonstrate they have used a risk-based layered approach to security. The process for implementing security at a data centre is no different from implementing security at any other sensitive or critical site.

To counter the threat from forcible attack such as theft or terrorism the 3Ds philosophy should be used. The 3Ds ask you to Deter, Detect and Delay attackers. The goal is to Deter the attacker from targeting your site or assets by creating a strong security appearance or messaging. Detect attacks at the earliest opportunity, and use security products that Delay the attacker for a period that enables response and intervention prior to any loss.

Data centre operators should be able to demonstrate they have used a risk-based layered approach to security.

To counter the threat from surreptitious attack such as espionage the BAD philosophy should be used: implement effective Barriers, control Access, and Detect attacks. In a reverse approach to forcible attack protection, layers that form Barriers, control Access and Detect attacks should be created as close to the asset as possible. This philosophy focuses on detection and not delay of attacks, due to differing measures of success for the attacker. Taking this approach allows you to focus security measures on the asset, which in turn can also help mitigate the risk from insiders.

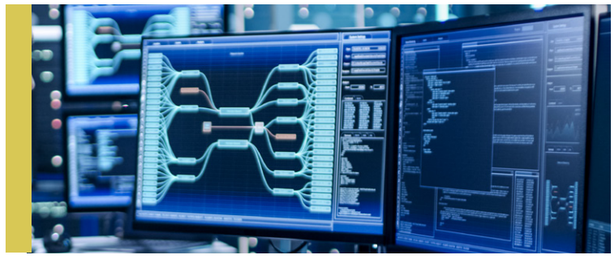
The BAD philosophy is part of the Surreptitious Threat Mitigation Process (STaMP) which should be used by those responsible for Government-classified data that is deemed to be under threat from espionage. More information about STaMP, the CPNI Surreptitious Attack Protective Security Philosophy and its principles is available through a CPNI adviser or via our restricted access extranet.

What should I be thinking about?

Although most data owners will not be responsible for the external security of the perimeter, site or building, there is a number of questions you should ask the operator to understand the level of security. You should consider:

- **Are there layered physical security measures to prevent unauthorised access to critical parts of the site?**
- **What types of threats have the security measures been designed to mitigate? You will need to ensure these cover the threat methodologies identified in your own risk assessment.**
- **What assurance can the data centre provider give you about ensuring those accessing the data centre are legitimate? Is a pass-wearing policy in place? Is a stringent visitor management system in place? What checks are in place for facilities (e.g. cleaners)?**
- **How does the data centre ensure and demonstrate good security culture amongst its staff?**
- **How many security staff operate on site? What are their roles and how is the security control room staffed and operated?**
- **Have you discussed with the data centre the option of implementing your own detection layers to maximise your opportunities for detection, at rack, room or hall level?**
- **If you require multiple racks, have you asked your data centre provider to locate them together to better control access – and limit the number of cables running across the data centre? What level of protection is there on cable runs?**

You should be provided with security details under a non-disclosure agreement at contract tendering stage. Physically visiting a prospective provider is the best way to ensure the correct levels of protection are used.



Meet-me rooms also form part of your perimeter

Meet-me rooms act as the physical interface between your services and the internet, allowing two separate networks to peer and transfer data.

Where data is transferred between networks, depending on the scenario, encryption may be shared, or may not be used. This provides a particularly vulnerable point and is therefore attractive to an attacker.

Building management systems

Building management systems (BMS), also known as building automation systems, are a type of control system used to control and monitor the mechanical and electrical equipment in most modern buildings – such as ventilation, lighting, power, fire, and facilities management functions.

In a data centre, the BMS system usually controls the heating, ventilation, and air conditioning (and humidity). Though BMS tend to be controlled by the data centre provider, a disruption to any one of these systems could cause an outage, potentially impacting your network. It is worth finding out what measures the data centre has put in place to manage BMS issues.

With this in mind, key considerations relevant to your risk assessment as a customer within a shared data centre include:

- **Whether you are connected to the data centre provider's BMS.**
- **What assurances the data centre provider can give you regarding access to these systems, so only essential personnel have access with rights limited to what is needed to undertake their role efficiently and safely.**
- **Confirmation from the data centre provider that the BMS itself is protected as a secure system, and operated from a secure area (i.e. not the building's reception or guest areas).**
- **Whether a cyber-vulnerability assessment of the BMS has been undertaken with recommendations acted upon.**

CPNI has guidance on protecting assets which contains information on how owners can protect their perimeter and building.

CPNI's guidance on building and infrastructure provides advice on physical security measures for protecting sites.

3

RISKS TO THE DATA HALL

Data halls: The heart of the data centre

At a data centre's heart, you will find data halls. They contain the data servers customers rely on.

Data centre customers renting entire suites and halls are usually responsible for their own security – effectively creating a second perimeter which must be secured.

Whether you are using network equipment racks within a shared hall, suite, or your own floor/hall, you should consider measures to detect and verify unauthorised access to your rack and rigorous procedures for access control and intrusion detection, including controls over doors and service corridors. Consider access arrangements in case of emergency.

Remember: Control of access is especially important when using shared data centres. The shared environment means people unknown to you could have access to the same data hall and proximity to your networking equipment. No matter how secure the data centre may be, as a data centre customer, it is your responsibility to ensure sufficient controls are in place to limit who might be able to access your networking equipment.

Securing the data hall

If you have your own suite or hall, you need to conduct your own risk assessment and identify the security measures you need. The limit of the area you control should be considered your perimeter. This is the first line at which you would be able to detect an intruder targeting your data.

To secure your area in the data hall:

- **Decide who will have legitimate access to your suite/hall/racks.**
- **Consider the most appropriate method of controlling access. It could include an automated access control system (which may be independent from that used by the data centre to give you maximum control) or locks with an audit function (which can provide the same function without the need for supporting infrastructure).**
- **Enhance security of the automated access control system by using two-factor authentication and anti-pass-back technology.**
- **Decide how access control will be managed (e.g. will your own security team monitor access control logs and check against permit to work for maximum security?)**
- **CCTV should cover all access points you control (consider both visible CCTV and CCTV embedded in racks).**
- **Remember that your CCTV system could have a network, wi-fi or internet-facing presence and could be compromised by an attacker (see our advice on how to protect physical security systems against cyber-attack)**
- **If you have an intrusion detection system used with CCTV, consider what level of monitoring, verification and response is required.**
- **Consider the most appropriate locking systems, ensure you understand the standards that they have been tested to, and any operational limitations.**
- **Cages can be used as an additional layer of protection around your racks in shared data halls. You may want to introduce a search and screening process for the area you control.**
- **A tamper-evident seal should be used on secure racks, cables, etc. to deter (or show evidence of) an attack.**
- **Have you factored in anonymity considerations such as the locations of your racks, references to your organisation's name in other areas of the data centre, the staff you employ and the uniforms they wear?**

Control of access is especially important when using shared data centres.

To agree with the DC owner:

- **Have you agreed the actions your data centre would take in the event of a fire, power outage or when maintenance work is required (e.g. involving the building management system), as well as records of any outages and notification of planned work? Do you know if fault and maintenance records are kept by the data centre?**
- **Can grills on egress/ingress of heating ventilation and air conditioning equipment and cable runs be installed to make it more difficult to gain access to your rack(s)?**

- **Is building services equipment situated outside the data hall to reduce the need for plant and equipment technicians to enter it?**

- **Are you satisfied with post-incident investigation policies and procedures in place for unplanned outages? Will you be provided with sufficient detail to allow you to identify any suspicious patterns to these?**

Additional measures for protection include:

- **‘Anonymity’: avoiding labelling racks, rooms, uniforms and buildings.**

- **Regular inspection for signs of damage and tampering.**

- **Minimal cable runs and requesting that your data racks are located together if sharing a corridor with other customers.**

- **Encoded labelling designed to frustrate any attacker’s understanding.**

- **Keys and code protection to stop unauthorised disclosure.**

CPNI guidance on protecting your assets contains guidance on technology used for access control.

CPNI also has guidance on secure destruction.

CPNI also has guidance on the use of CCTV.

External devices

Any equipment brought into a data centre which can store, record, and/or transmit text, images/video, or audio data presents a security risk.
Mobile phone and personal electronic devices with cameras, apps and network connectivity are a particularly high risk. It is worth considering whether mobile phones should be handed in when entering sensitive areas. The data centre operator may have a policy on this. If they do not, you could introduce restrictions on devices in the area you control.

This may include introducing an electronic device booking management process, which keeps a register of authorised devices and implements controls on their entry and exit to sensitive areas.

If health and safety is an issue, dedicated phones without additional functionality may help. Signage and phone lockers at entrances to sensitive areas can increase compliance, along with CCTV monitoring.

CPNI has further guidance on screening people and their belongings to identify prohibited items.

Technical vulnerabilities

UK NACE is the National Technical Authority for technical security. It protects organisations from technical espionage, keeping information and premises safe from technical attack.

Technical security is the practice of detecting the compromise of protective security systems, analysis and prevention of technical attack, mitigation of technology vulnerabilities, and the deployment of countermeasures.

The following technical vulnerabilities should be considered:

Radio transmitters are present within a broad range of technology products – from building system sense and control (e.g. fire alarms, door locks), to IT network data transfer (such as wi-fi). These technologies are vulnerable to manipulation, interception, and denial of service through a range of techniques, or can be used to obfuscate technical attacks by operating within heavily populated spectrum bands (e.g. wi-fi and Bluetooth).

Consideration should be given to the coverage of these systems and how they are managed and monitored for adversarial behaviour such as spoofing of SSID of network, or use of internet broadcast access points as an egress route for a covert implant in conventional equipment.

Avoidance of use of smart or connected systems (such as wireless fire detection) would be advised to mitigate the risk of an actor triggering such a system in order to facilitate a secondary attack.

Watch out for crosstalk

Crosstalk is a phenomenon where data travelling down a wire can be detected by another wire running close to it. This can allow unintentional ‘bleed’ of secure data into insecure networks.

As additional networks are installed for protective security measures, such as CCTV or access control, there is an increased chance of crosstalk causing a problem.

How do data centre owners demonstrate they have measures in place to reduce the risk of crosstalk?

- **Physically segregating secure and insecure cabling.**

- **Using shielded twist pair and fibre-optic cabling.**

- **Segregating and filtering power between secure and insecure systems.**

The UK NACE website has more information on dealing with crosstalk.

4

RISKS TO THE MEET-ME ROOM

What are meet-me rooms?

A meet-me room (MMR) is the area in a co-located data centre where communications service providers (CSPs) like telecoms companies physically connect one another's data servers and exchange traffic. This happens each time mobile phone operators transfer calls/messages between different networks, for example.

Data centre operators should strictly limit access to an MMR. It is important however that MMR security details and assurances are provided by data centres during tendering under an NDA.

Data centre operators should strictly limit access to a meet-me-room.

Remember: This guidance also applies to points of presence (PoP) and internet exchange points.

Given the higher level of risk that MMRs introduce, here are **8 key considerations** to discuss with your data centre:

» **Access control**
Are CSPs, their contractors and data centre operator contractors escorted? Are passes worn and authorised and access lists kept and reconciled with permit-to-work logs? How is work conducted within the MMR verified to ensure it matches any work-orders?

» **Screening processes**
The criteria the data centre operator uses for approving or rejecting MMR access.

» **Intrusion detection, including CCTV**
Are these monitored live by the data centre operators or is it the responsibility of the tenants themselves?

» **Entry and exit searches**
Are items such as mobile phones and other personal electronic devices prohibited or subject to a movement management policy? Are staff searched on entry and exit? Is equipment taken into the MMR consistent with the stated purpose of their entry?

» **Types of rack**
What assurances can providers give you regarding the security of racks they use?

» **Rack locking**
How does the data centre ensure that racks are always locked? Are the racks regularly inspected by the data centre provider? Are they vulnerable to master keys kept by your data centre?

» **Anonymisation**
Are racks sufficiently anonymised to prevent those with hostile intent from being able to identify where data is sent?

» **Asset destruction**
Is there a secure asset destruction process? Is it regularly audited to complement the searches conducted on exit? Does it help to reduce numerous risks including accidental loss, espionage, insider attack and theft?

5

PEOPLE RISKS

Consider risks related to people

It's important to mitigate any security risks related to people. People and personnel security comprises an integrated ecosystem of policies, procedures, interventions and effects which seek to enhance an organisation or site's protective security by:

- Mitigating the risk of workers exploiting their legitimate access to an organisation's assets for unauthorised purposes; this is known as 'insider risk'.
- Optimising the use of people (both workforce and, where appropriate, the public) to be a force multiplier in helping to prevent, detect and deter security threats.
- Detecting, deterring and disrupting external hostile actors during the reconnaissance phase of attack planning.

Insider risk

People are an organisation's biggest asset. However, they can also pose an insider risk. The recruitment of insiders is an attractive option for hostile actors attempting to gain access to data centres and the data they hold.

CPNI defines an insider as a person who exploits, or intends to exploit, their legitimate access to an organisation's assets for unauthorised purposes. Remember, an insider could be a full-time or part-time employee, a contractor, a supply chain business partner, or customer. In fact, it could be anyone who has been given rightful access to a data centre asset.

An insider could seek to join your organisation to conduct an insider act. They may be triggered to act at some point during their employment, or after their employment officially ends.

Certain factors may increase an organisation's vulnerability to insider activity, including:

- **Ineffective leadership and governance structures to run an insider threat programme.**
- **Lack of role-based risk assessment to identify specific high-risk roles.**
- **Inadequate personnel security measures during pre-employment screening.**
- **Inadequate ongoing personnel security policies and procedures, limiting the organisation's ability to monitor and investigate insider activity.**
- **Poor leadership and management practices, which may reduce organisational trust and erode employee loyalty and commitment.**
- **Ineffective security awareness and training, both at induction, throughout employment and exit.**
- **Lack of a strong security culture, resulting in the workforce not taking individual responsibility for security and reduced compliance with security procedures.**

CPNI provides comprehensive guidance and frameworks on managing insider risk.

Security culture

Data centre operators will often have a relatively small number of their own staff onsite but will be joined by staff from other organisations. These may include staff from the data centre's client organisations employed to provide security and engineering support to their own infrastructure – and other third-party contractors who provide services such as general site security, cleaning, and maintenance.

The benefits of an effective security culture include:

- **A workforce that is likely to be engaged with, and take responsibility for, security issues.**
- **Increased compliance with protective security measures.**
- **Reduced risk of insider incidents.**
- **Awareness of the most relevant security threats.**
- **Employees are more likely to think and act in a security-conscious manner.**

CPNI provides a variety of materials on security culture to help organisation assess, direct and shape their own security culture initiatives.

Data centre operators should be able to demonstrate that they promote a good security culture by conducting:

- **Pre-employment screening processes**
  You should seek assurance that data centre operators screen prospective employees who may gain access to your critical assets. Employment screening is the process by which you check whether a potential candidate is suitable for your business.
- **Staff monitoring**
  While pre-employment screening helps ensure that an organisation recruits trustworthy individuals, people and their circumstances and attitudes change, either gradually or in response to events. Therefore continued staff monitoring throughout the duration of their employment is required.
- **Security training for staff**
  Dedicated, motivated and professional security staff are an essential component of any protective security regime to mitigate against the insider and external people threat.

6

RISKS TO THE SUPPLY CHAIN

Supply chains can be vulnerable to attack

Most organisations rely upon suppliers to deliver products, systems and services. But supply chains can be large and complex. Effectively securing the supply chain can be hard because vulnerabilities are inherent, or introduced and exploited at any point in the supply chain. A vulnerable supply chain can cause damage and disruption.

Attackers have both the intent and ability to exploit vulnerabilities in supply chain security. This trend is growing. Physical, personnel and cyber security risks needs to be considered within any risk assessment.

As part of the supply chain, data centre services you procure may be outsourced by your provider (if you are using a managed hosting data centre option, for example). If so, it is important to:

» **Understand the impact outsourcing can have on your data centre requirements.**

» **Undertake a risk assessment identifying critical assets (i.e. your servers, racks and any associated security arrangements that you directly manage) andarticulate what risks a supplier poses to those assets.**

Understand the impact outsourcing can have on your data centre requirements.

Data centre software and systems

Software and software updates downloaded from suppliers' websites provide opportunities for malware to be installed alongside legitimate products. The malware can include additional remote access functionality that could be used to take control of systems on which it is installed.

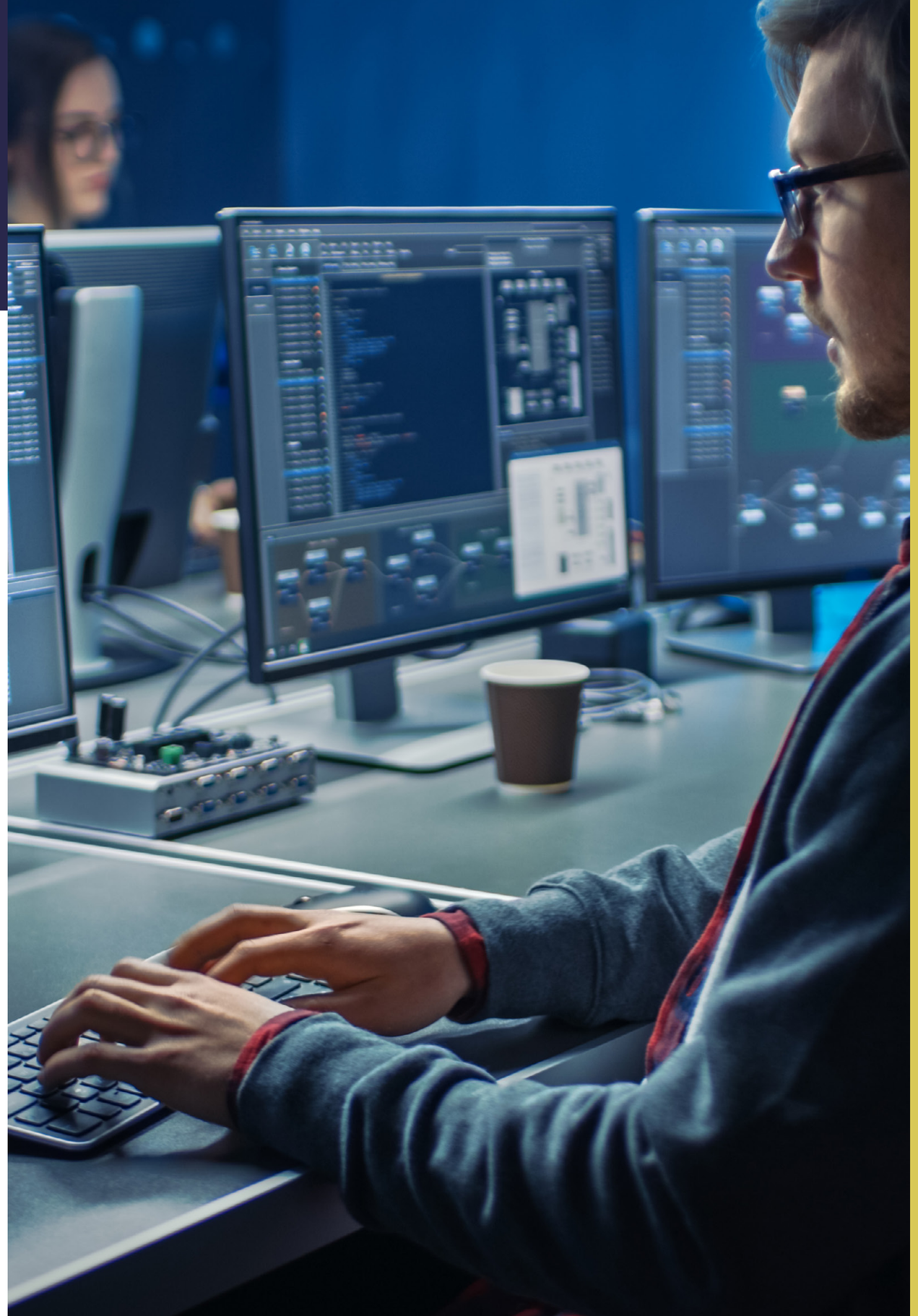
Compromised software is very difficult to detect if it has been altered at the source, since there is no reason for the target company to suspect it was not legitimate. This places great reliance on suppliers, as it is not feasible to inspect every piece of hardware or software in the depth required to discover this type of attack.

All software and systems supplied throughout a data centre (such as servers, networking systems, building management/automation systems, CCTV networks, enterprise IT, and so on) should be updated throughout their lifecycle with the latest firmware versions and security patches to minimise the risk of cyber-attack.

The NCSC's 10 steps to Cyber Security contains guidance on patching and vulnerability management provides more detail.

The NCSC and CPNI have developed 12 principles to help you establish effective control and oversight of your supply chain. Our guidance covers cyber, physical and people security.

An infographic of the 12 principles is also available.



7

CYBER SECURITY RISKS

Data centres and cyber security

Data centres' infrastructure and systems are required to store, process, and transfer data at scale, and are complex.

They are a valuable target for threat actors seeking to conduct cyber-attacks. The motivation for these attacks may include:

» **To steal valuable or sensitive data.**

» **To deny access to, disrupt, degrade, or destroy data centre operations and services.**

» **To compromise data integrity.**

Managing cyber security risks to data centres is about protecting the data held there (data at rest) and the data that passes through them (data in transit). Data centre operators (and their customers) should assume that a successful cyber-attack will happen, and therefore take steps to ensure that attacks can be detected, and the impact minimised.

IT infrastructure and network connectivity

Data centres require operational technology (OT) networks for building management services. These services are vital to maintaining and protecting data centre operations. This includes services such as power and cooling. Physical data centre security is also dependent on network connected systems such as access control.

External network systems are provided by data centre operators to allow customers the means to access the services they run from there. Data centre operators can also use these external networks to remotely manage their data centre infrastructure. Since the management of the data centre infrastructure is often carried out by managed service providers (who will also access these communications networks to provide support services), there are implications for the supply chain.

External connections can provide pathways into the heart of data centre operations. Attackers will see these as a vector to try and exploit weak data centre cyber defences to target sensitive or valuable data or disrupt data centre operations.

Managing cyber security risk

A comprehensive cyber risk management regime is invaluable, should be embedded throughout your organisation, and should complement the way you manage other business risks.

The section on risk management above provides links to CPNI and the NCSC guidance to help manage your cyber risks. That guidance provides information on the tools, methods, and frameworks available to help you manage this important aspect of your business. The NCSC has also published the 10 Steps to Cyber Security guidance, which includes further information on why risk management is important for organisations to help protect themselves in cyberspace.

The NCSC Cyber Assessment Framework provides some indicators of good practice which can be used to provide operators and data centre customers a baseline for risk management.

Protect against cyber-attack

There is no guaranteed way to avoid cyber-attacks. However, the worst outcomes can be avoided if an organisation's services are designed and operated with security as a core consideration. This requires the following areas to be considered:

» **Policies and processes**
The production and implementation of policies and procedures that are owned and approved by the board is an important step in helping you manage the cyber risk to your business. These should be developed as part of the risk management process.

Policies and procedures need to be communicated in order that the organisation's approach to the security of its networks and information systems is clearly understood by all that use them. It is important that anyone accessing data centre systems understands their obligations in protecting those systems, which can include internal staff and contracted service providers.

» **Access management**
You should verify, authenticate and authorise any access to data or systems. Unauthorised access to data, systems and services could lead to loss of data or disruption of services. Good identity and access management on your networks should make it hard for attackers to pretend they are legitimate.

The NCSC has published guidance for identity and access management, as part of its 10 Steps to Cyber Security.

It is vital that remote access to data centre resources is managed properly. This is particularly important where there is a requirement for users to carry out activities that require privileged access.

If an attacker can compromise a person with privileged access rights or a device used for administration activities, they can inherit privileged accesses, which provides potential for more impactful attacks. This also means an attacker may have the potential to cover their tracks so that their attack is more difficult to detect or remediate.

The NCSC has specific guidance on privileged access management.

The NCSC also has advice on how to avoid repeating ineffective solutions when administering a network.

» **Data security**
Data used by business can take a variety of forms, and could include information that would be valuable to an attacker, including personal data related to customers or staff; design details of networks and information systems; or intellectual property (IP).

Even if there is no legal requirement to protect data, there is often a commercial or security reason for it to be protected from unauthorised access, modification, or deletion. Measures should be taken to protect data in transit, at rest, and at end of life – that is, effectively sanitising or destroying storage media after use.

In many cases your data will be outside your direct control, so it is important to consider the protections that you can apply, as well as the assurances you may need from third parties.

With the rise in increasingly tailored ransomware attacks preventing organisations from accessing their systems and data stored on them, other relevant security measures should include measures such as maintaining up-to-date, isolated, offline backup copies of all important data.

The NCSC's 10 Steps to Cyber Security provides further information to help you protect your data.

» **Architecture and configuration**
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 maintained and updated to adapt effectively to emerging threats and risks in the cyber security landscape.

The worst outcomes of cyber-attacks can be avoided if your services are designed and operated with security as a core consideration. The NCSC publishes guidance describing a set of secure design principles to help with this. This provides information on how you can:

- **Make compromise of and disruption to your systems more difficult.**
- **Make compromise detection easier.**
- **Reduce the impact of any compromise (see below for further information on detection and reduction of impact).**

This guidance can be used to help you build new systems but is also helpful in reviewing the cyber security of existing systems.

The NCSC's 10 Steps to Cyber Security provides information on approaches to securely building systems and services.

The NCSC's secure design principles guidance provides further information to help you secure your systems

Detecting cyber security events

There is no guarantee that the protective measures in place will mitigate an attack and organisations should prepare by assuming that cyber compromises will occur. These preparations should aim to ensure quick response times and support decision-making. In addition, exposing the root cause can help manage future attacks and resolve any ongoing issues.

The following factors can aid your organisation's response in the event of a cyber intrusion:

» **Audited and logged information** with access controls and isolated from other corporate trust domains can help identify suspicious user behaviour for either an attacker or insider.

» **Monitoring and analysis tools used to compare log and audit data against** 'indicators of compromise' (from threat intelligence sources – see below) can help identify and investigate events of interest.

» **Threat intelligence** can come from discussion forums, trusted relationships, paid-for contracts with threat intelligence companies, or even generated internally. It should be routinely collected from quality sources and kept up to date.

» **Governance, roles, and workflows** help operational monitoring teams establish roles and responsibilities that cover both security and performance-related monitoring. Monitoring teams should include members who:

- **Know the network, its hardware and software, and the types of data they process and produce.**
- **Can work with threat intelligence to identify, investigate and triage security events.**
- **Understand the organisation's business and assess the significance of security events in terms of their potential to cause harm, such as disrupting operations or leaking sensitive corporate or personal data.**

Security monitoring takes this further and involves the active analysis of logging information to look for signs of known attacks or unusual system behaviour, enabling organisations to detect events that could be deemed a security incident.

Your monitoring capability should work seamlessly with your incident management (see below for more information on incident management) and may even comprise some of the same staff in order to help you respond and minimise the impact.

Further advice can be found in the NCSC's guidance on logging for security purposes.

There is also further guidance on making compromise detection easier.

Minimising impact of cyber security incidents

Once a cyber intrusion has been detected, good incident management should help reduce the impact, and this includes:

- **Quickly responding to incidents after detection to help prevent further damage, as well as reducing the financial and operational impact.**
- **Managing the incident while in the media spotlight to reduce reputational impact.**
- **Applying what you have learned in the aftermath of an incident to make you better prepared for any future incidents.**

Businesses should therefore put in place measures to plan for this eventuality. This should include putting the appropriate governance in place such as an information security management system (ISMS).

Ensure there are well-defined and tested incident management responses in place that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain the impact of compromise should be in place.

The NCSC has issued guidance on cyber incident management best practice.

In the event of a concern or potential incident, good logging practices (see page 20) will allow you to retrospectively look at what has happened and understand the impact of the incident.

You may consider implementing the NCSC's guidance on Security Operations Centres (SOC) where the use of a security information and event management (SIEM) tool will allow real-time analysis of security alerts and give indication of abnormal behaviour.

ALL LINKS

Introduction
- ZDNET, 'T-Mobile hack: Everything you need to know', 28/08/2021: https://www.zdnet.com/article/t-mobile-hack-everything-you-need-to-know/
- CSO Online, 'The OPM hack explained: Bad security practices meet China's Captain America', 12/02/2020: https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Risk management
- CPNI operational requirements https://www.cpni.gov.uk/operational-requirements
- CPNI protective security risk management: https://www.cpni.gov.uk/rmm/protective-security-risk-management
- The NCSC risk management guidance from a cyber security perspective: https://www.ncsc.gov.uk/collection/risk-management-collection

Resilience
- Reuters, 'Millions of websites offline after fire at French cloud services firm', 10/02/2021: https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU

Key types of data centre
- The NCSC cloud security guidance: https://www.ncsc.gov.uk/collection/cloud-security

Geography and ownership risks
- ISO guidelines: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit
- CPNI, the NCSC, Department for Business, Energy and Industrial Strategy (BEIS) informed investment: https://www.cpni.gov.uk/informed-investment

Risks to data centres' physical perimeter and buildings
- CPNI protecting your perimeter and building: https://www.cpni.gov.uk/protecting-your-assets
- CPNI protecting your building and infrastructure: https://www.cpni.gov.uk/building-infrastructure

Risks to the data hall
- CPNI CAPSS guidance: https://www.cpni.gov.uk/cyber-assurance-physical-security-systems-capss
- CPNI technology used for access control: https://www.cpni.gov.uk/technology-control-rooms
- CPNI secure destruction: https://www.cpni.gov.uk/secure-destruction-0
- CPNI screening people and their belongings: https://www.cpni.gov.uk/screening-people-and-their-belongings-0
- UK National Authority for Counter-Eavesdropping: https://www.fcdoservices.gov.uk/uk-nace/
- CPNI CCTV: https://www.cpni.gov.uk/cctv

People risks
- CPNI insider risks: https://www.cpni.gov.uk/insider-risk
- CPNI security culture: https://www.cpni.gov.uk/security-culture

Risks to the supply chain
- The NCSC vulnerability management, 10 Steps to Cyber Security: https://www.ncsc.gov.uk/collection/10-steps/vulnerability-management
- CPNI 12 principles to help establish effective control and oversight of your supply chain: https://www.cpni.gov.uk/system/files/documents/2e/87/Supply_Chain_Security_Collection_Jan2018.pdf
- CPNI infographic of the 12 principles: https://www.cpni.gov.uk/system/files/documents/28/b3/supply_chain_ncsc_cpni_infographic.pdf

Cyber security risks
- CPNI supply chain security: https://www.cpni.gov.uk/system/files/documents/2e/87/Supply_Chain_Security_Collection_Jan2018.pdf
- The NCSC privileged access management: https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management
- The NCSC CAF guidance: https://www.ncsc.gov.uk/ collection/caf
- The NCSC secure system administration: https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns#section_3
- The NCSC 10 Steps to Cyber Security: https://www.ncsc.gov.uk/collection/10-steps/architecture-and-configuration
- Secure design principles: https://www.ncsc.gov.uk/collection/cyber-security-design-principles
- The NCSC introduction to logging for security purposes: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes
- The NCSC Guidance on Security Operations Centres: https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide
- The NCSC incident management: https://www.ncsc.gov.uk/collection/incident-management

FURTHER RESOURCES

- Cyber Essentials is an NCSC-backed self-assessment scheme ensuring that organisations are protected against a wide variety of the most common cyber-attacks.
- IT Service Management (ISO 20000): a global standard that describes the requirements for an information technology service management (ITSM) system.
- Information Security (ISO 27001): an information security standard, providing a set of standardised requirements for an information security management system (ISMS).
- International Standard for Assurance Engagements (ISAE 3402): an assurance standard for internal financial reporting controls. In SOC terms, an ISAE 3402 is a SOC1 (see below).
- SSAE 16: a US standard (mirroring ISAE 3402) consisting of two different reports (see below). Note that from May 1 2017, SSAE 16 was superseded by SSAE 18.
- A SOC 1 type 1 report: an independent snapshot of an organisation's internal financial reporting controls on a given day.
- A SOC 1 type 2 report: shows how controls have been managed over time.
- Quality management (ISO 9001): an international standard that specifies requirements for a quality management system.
- Business continuity management (ISO 22301): an international standard for business continuity management covering disruptive events such as natural disasters, environmental accidents, technology mishaps and manmade crises.
- The Telecommunications Industry Association standard TIA942: a US standard that specifies the minimum requirements for telecommunications infrastructure of data centres and computer rooms including single tenant enterprise data centres and multi-tenant internet hosting data centres.
- The uptime data centre tier standards are a standardised methodology used to determine availability in a facility. The standards are comprised of a four-tiered scale, with Tier 4 being the most robust.

CPNI
Centre for the Protection of National Infrastructure

National Cyber Security Centre

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

To the fullest extent permitted by law, CPNI and the 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.