CPNI
Centre for the Protection of National Infrastructure

National Cyber Security Centre

Data Centre Security

GUIDANCE FOR OWNERS

CONTENTS

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 operator 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.**

Risk management strategies between data centre operators and their customers are therefore interdependent.

As a data centre operator, you will want to ensure your risk management is robust to attract clients, maintain your reputation, and comply with relevant regulatory compliance regimes.

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

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 threats pose risk to your assets and systems, we provide further information on the mitigation you might consider to better manage them. 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 provides 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.

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.

Reuters, 'Millions of websites offline after fire at French cloud services firm', 10/02/2021.

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 available. We provide some of these standards in the additional resources section.

As there is extensive guidance available on data centre resilience, we will not cover it in detail here.

As a data centre owner, are you able to demonstrate that:

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

1

GEOGRAPHY AND OWNERSHIP RISKS

Where your data is stored?

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 outside your commercial engagements in Russia or with Russian individuals and companies.

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.

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.

The ICO has up to date guidance on GDPR

Foreign direct investment

If a data centre 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.

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. In other facilities, the level of security should meet customer expectations and be designed to attract newcomers.

How to implement security

The process for implementing security at a data centre is no different from implementing security at any other sensitive or critical site. CPNI recommends a risk-based approach to security mitigation and advises that one of two models for implementing security measures are followed. Both models involve a layered approach, integrating physical, personnel and cyber security.

The models against attack

To successfully mitigate the risk of an attack it is important to understand how threats to your site, workforce or assets – including from states and terrorism – will manifest themselves. Understanding these threats will help shape your security strategy and ensure it is effective and proportionate. CPNI recommends the use of two differing philosophies dependent on the threat.

To counter the threat from forcible attack such as theft or terrorism, the 3Ds philosophy should be used. The 3Ds principles 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 of time, enabling response and intervention prior to any loss.
To counter the threat from a surreptitious attack such as espionage, the BAD philosophy should be used. The BAD principles implement effective Barriers, control Access, and Detect attacks. In a reverse approach to that used for 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 risk from insiders who exploit or have the intention to exploit an organisation's assets for unauthorised purposes.

The BAD philosophy is part of the Surreptitious Threat Mitigation Process (STaMP), which should be used by those responsible for classified government data 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.

New build data centres

Security during the design and build phase of a new data centre is important as mistakes made at this stage can impact on the security of the facility when it is built. We recommend viewing the Build It Secure pages on the CPNI website, which outline the approach to implementing security during the build.

We recommend viewing the Build It Secure guidance on the CPNI website, which outlines the approach to implementing security during the build.

CPNI's guidance on Security-Minded approach to Digital Engineering provides further details on managing information security to ensure sensitive information about the design is only shared with those who need it is of particular importance.

During the planning application process, arrangements should be made to ensure sensitive information is not released on public planning portals or put into the public domain during consultations. Early engagement with planning officials is the best way to ensure this.

The gov.uk website provides guidance on managing sensitive information in planning applications.

There may be additional physical security risks that need to be considered and mitigated due to the unique design of data centres. With complex and widespread heating and cooling systems, it is likely that grills and cages will be required on any venting, ducting or wastewater systems – which are large enough for a person to use to gain access.

Consideration should also be given as to whether smaller ducting systems could be used to pass material from secure areas to non-secure areas as a way of circumventing security checks. The mitigation for this is likely to be a mesh over any ducting that could be exploited in this way.

Hostile reconnaissance

Data centres should consider the risk from people external to the organisation who wish to conduct harm. Recognising they may not get a second chance to achieve their aims, hostile threat actors will typically plan carefully through reconnaissance of a site.

Understanding hostile reconnaissance and the attack-planning process gives security managers and staff a crucial opportunity to disrupt the hostile in two main ways:

» **Denying them the ability to obtain the information they need from their research because they simply cannot obtain it, or the risk of detection to achieve this is too high.**

» **Promoting failure: both of their ability to conduct hostile reconnaissance (they will not be able to get the information, they will be detected), and of the attack itself.**

Deterrent measures can be cheap, relatively easy to deploy, or may involve more targeted deployment of existing assets. They will involve the security practitioner working with colleagues from across the organisation, most notably in communications. Their ultimate effect should be to deter the hostile yet have a neutral or even positive effect on employees and visitors.

Hostile reconnaissance training and awareness

CPNI's Check and Notify (SCaN) training aims to help businesses and organisations maximise safety and security using their existing resources.

Your people are your biggest advantage in preventing and tackling a range of threats, including criminal activity, unlawful protest, and terrorism.

SCaN training empowers your staff to correctly identify suspicious activity and know what to do when they encounter it. In addition to this, the skills your staff learn will help them to provide an enhanced customer experience. The training helps ensure that individuals or groups seeking to cause your organisation harm are unable to get the information they need to plan their actions.

CPNI provides in-depth guidance on the principles of, and mitigations against, hostile reconnaissance.

Consider cable pit security

Cable access and draw pit chambers will have covers (sometimes called 'manhole covers' or 'maintenance covers') that are an important and often overlooked part of data centre infrastructure. Some examples of how security could be enhanced include making sure that these are:

- **Positioned out of the way where they are not vulnerable to damage.**
- **Locked to prevent unauthorised access.**
- **Monitored to detect unauthorised access or tampering.**

When thinking about cable chambers, consider threats, what the likely attack methods may be, and the potential impact of a successful attack.

Meet-me rooms also form part of your perimeter

Meet-me rooms act as the physical interface between services and the internet, allowing two separate networks to peer and transfer data (e.g. two telecommunications networks – see 'Risks to the meet-me room' for more detail) – and are directly linked to racks.

That means they form part of the boundary. 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.

As a data centre owner, what measures have you put in place to manage BMS issues?

- **Is your BMS connected to client networks?**
- **What assurances can you give customers regarding access to these systems?**
- **Is your BMS itself protected as a secure system and operated from a secure area (i.e. not your building's reception or guest areas)?**
- **Has a cyber vulnerability assessment of the BMS been undertaken and its recommendations acted on?**

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

3

RISKS TO THE DATA HALL

Data centre operators are responsible

Data centre operators are responsible for data hall security. Data owners may have additional security layers in place.

Remember: Control of access is especially important when operating shared data centres. The shared environment means people unknown to the data centre customer could have access to the same data hall and in proximity to their networking equipment.

Demonstrate to your customers that you are prepared:

- **Have you agreed the actions you 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 have post-incident investigation policies and procedures for unplanned outages? Will you provide customers with sufficient detail to allow them identify any suspicious patterns to these?**
- **Can grills on egress/ingress of heating ventilation and air conditioning equipment and cable runs be installed to make it difficult to gain access to your racks?**
- **Is building services equipment situated outside the data hall to reduce the need for technicians to enter it?**

Additional measures for protection include:

- **'Anonymity': avoiding labelling racks, rooms, uniforms and buildings.**
- **Regular inspection for signs of damage and tampering.**
- **Minimal cable runs.**
- **Encoded labelling designed to frustrate any attacker's understanding.**
- **Keys and code protection to stop unauthorised disclosure.**

CPNI has 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 is a security risk.

Mobile phones and personal electronic devices with cameras, apps and network connectivity are a particularly high security risk. It is worth considering whether mobile phones should be handed in when entering sensitive areas.

This may include introducing electronic device booking management, 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 provides further information on this topic on its "Screening People and Their Belongings" page.

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 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 in 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. How are they managed and monitored for adversarial behaviour such as spoofing of SSID of the 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

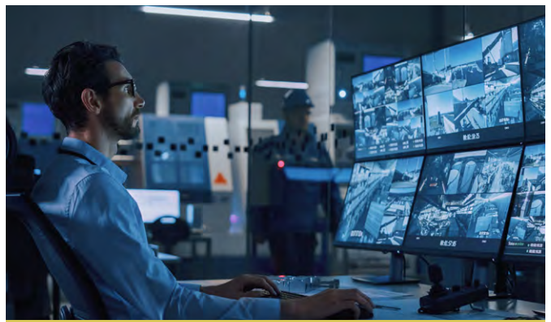
Crosstalk is a phenomenon where data travelling down a wire can be detected by another wire running close to it. This can allow unintentional 'bleed' of secure data into insecure networks.

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.

To reduce the chances of crosstalk:

- **Physically segregate secure and insecure cabling.**
- **Use shielded twist pair and fibre-optic cabling.**
- **Segregate and filter 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. You may decide not to allow customers access to view security arrangements. It's important however that MMR security details and assurances are provided to your customers 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 MMRs introduce, here are **8 key considerations** to demonstrate to your data centre customer:

» **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 you use for approving or rejecting MMR access.

» **Intrusion detection, including CCTV**
Are these monitored live by you or is this the responsibility of the tenants?

» **Entry and exit searches**
Are items such as mobile phones or 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 you give regarding the security of racks you use?

» **Rack locking**
How do you ensure that racks are always locked? Are the racks regularly inspected and are you able to demonstrate effective key control?

» **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, 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 has become 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 who intends to exploit, 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 deliberately seek to join your organisation to conduct an insider act or 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 on their website.

Security culture

As a data centre operator, you will often have a relatively small number of staff onsite. However, it is likely you will be joined by staff from other organisations, including staff from the data centre's clients who provide security and engineering support to their own infrastructure, and third-party contractors providing 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.

Contract staff

Many staff onsite at a data centre are contracted by third parties, rather than directly employed by you as the operator.

CPNI recommends that organisations use the same personnel security measures with contractors as they would with their directly employed staff, and where impossible, a risk assessment is made as to if they need to downgrade personnel security standards and what alternative measures can be used.

Some factors to consider within your risk assessment for contractors should include that:

- **Timescales for recruiting contractors are often tight. This can result in pressure to overlook pre-employment screening measures, especially if it is anticipated they will be employed for a short time.**
- **Income from contract work can be irregular, which can be a motive for unauthorised activity for financial gain.**
- **A contractor's primary loyalty may not necessarily be to the employing organisation and their commitment to security may be diminished.**
- **A contractor may feel they are not part of the team in which they are working.**
- **A contractor may be working in competitor organisations consecutively or simultaneously.**
- **Contracts may be renewed or extended to the point where a contractor works in an organisation for many years, often with little or no re-screening.**
- **A contractor may move between departments with the department not being aware of security constraints applying to them.**
- **A contractor may be poorly supported by the organisation that contracted them; it may not provide assistance, welfare support or monitoring to non-permanent staff.**

CPNI provides comprehensive guidance on personnel security and contract staff.

Pre-employment screening processes

You should screen prospective employees who may have access to your critical assets. Employment screening is the process by which you check whether a potential candidate is suitable for your business.

All individuals should be subject to a suitable level of screening, informed by a role-based risk assessment. This includes permanent, temporary and contract workers. Screening should not be limited to new starters, but also individuals who are moving internally between jobs, as different roles may require different levels of screening.

Security checks as a part of your employment screening should include confirmation of identity and right to work.

CPNI provides further guidance on pre-employment screening, including when hiring from overseas.

Staff monitoring

While pre-employment screening helps ensure that an organisation recruits trustworthy individuals, people, circumstances and attitudes change.

It is important that employee risks are not just reviewed at the pre-employment stage. A programme of monitoring and review should be in place. It should enable potential security issues or personal issues that may impact on an employee's work to be recognised and dealt with.

There are different mechanisms to enable this, for example:

- **Line management – ensuring line managers are well-equipped to endorse best practice security and engage with their staff to help them understand security behaviours. They play a key role in helping the organisation develop a good security culture.**
- **Staff vetting reviews – ensuring employees are regularly reviewed for security clearance helps to keep sight of any significant changes that individuals may go through and how this may impact on their organisational engagement.**
- **Protective monitoring – using the organisation's IT audit logs to understand employee activity and behaviour. Spotting and investigating IT security breaches is the traditional remit of protective monitoring. In addition, it may be that subtler IT behaviour change is seen that points to a potential issue when combined with information from insider threat practitioners and stakeholders.**
- **Effective reporting/assessment mechanisms – providing confidential mechanisms for individuals to report concerns about any employee (whether permanent, contractor, management, visitors, or anyone else with access to an organisation's assets) allows everyone to play a part in reviewing the risk of other personnel.**

Further CPNI guidance is available on staff monitoring within the Insider Risk Mitigation Framework.

Security training for staff

Dedicated, motivated and professional security staff are an essential component of your protective security regime and mitigate against insider and external people threats.

During both online and physical reconnaissance of a site, hostiles may look for a means to physically enter your organisation.

They may look for information online, such as employees talking about lax security practices or previous process failures. If they are confident enough, they may try to gain access to your organisation, try to bypass security, or use fraudulent ID.

Employees tasked with document verification, whether during pre-employment screening and/or during visitor entry, will be vigilant to the threat of fraudulent documentation.

Motivated, attentive and observant security personnel will also form a highly effective deterrent and final line of defence where other interventions have failed.

CPNI has produced in depth **guidance on Robust Visitor Entry Processes.**

In addition to the technical requirements of a CCTV control room, CPNI has also produced **guidance on CCTV control rooms** and how to get the most effective performance from the CCTV operator team

The human factors approach looks at creating a CCTV control room designed to support activities of the control room staff in a particular environmental context.

The potential benefits of this approach include:

» **Identifying areas for control room improvement.**

» **Getting the best operator job performance.**

» **Optimising the potential detection of incidents/ crimes.**

With the above in place, there may be financial benefits in the longer term.

CPNI provides in-depth **guidance on professionalising security** and promoting security culture within an organisation.

6

RISKS TO THE SUPPLY CHAIN

Supply chains can be vulnerable to attack

Before you can do anything to secure your supply chain you need to understand the risks (and benefits) you are taking on by engaging suppliers.

Most organisations rely upon suppliers to deliver products, systems, and services. But supply chains can be large and complex, involving many suppliers doing many things. Effectively securing the supply chain can be hard because vulnerabilities can be 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 real and growing. So, the need to act is clear. Physical, personnel and cyber security risks need to be considered fully within any risk assessment.

It is important to:

- **Protect information you share with suppliers.**
- **Specify security requirements to a supplier delivering something to you.**
- **Gain confidence in your approach to establishing control over the supply chain.**
- **Continue improving and maintaining security.**

You should understand the sensitivity of contracts you are awarding, and the value of the information or assets suppliers hold, will hold, have access to, or handle, as part of the contract. Think about the level of protection you need suppliers to give your assets and information, as well as the products or services they will deliver to you as part of the contract.

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 functionalities that could be used to take control of the systems on which it was 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 the supplier, 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 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 also provides some indicators of good practice which can be used to provide operators and data centre customers with 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's 10 Steps to Cyber Security contains more detailed guidance on identity and access management.

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 with 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 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 guidance on secure design principles 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 10 Steps to Cyber Security guidance also provides information on approaches to securely building systems and services.

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 information can be found in the NCSC's guidance on logging for security purposes and separately, 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 for the business such as an information security management system (ISMS).

The NCSC has issued guidance on incident management to help ensure there are well-defined and tested 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.

In the event of a concern or potential security incident, implementing the NCSC's good logging guidance (see above also) will help you to retrospectively look at what has happened and understand the impact of the incident.

You may also 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*

Geography and ownerships 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 Build it Secure: *https://www.cpni.gov.uk/build-it-secure-0*
- CPNI security-minded approach to digital engineering: *https://www.cpni.gov.uk/security-minded-approach-digital-engineering*
- Crown Development Guidance from the Ministry of Housing: *https://www.gov.uk/guidance/crown-development#sensitive-information-in-planning-applications*
- CPNI see, check and notify pages: *https://www.cpni.gov.uk/Scan*
- CPNI's disrupting hostile reconnaissance: *https://www.cpni.gov.uk/disrupting-hostile-reconnaissance-0*
- 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*
- CPNI contract staff: *https://www.cpni.gov.uk/contract-staff*
- CPNI employment screening: *https://www.cpni.gov.uk/employment-screening*
- CPNI insider risk mitigation framework: *https://www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework*
- CPNI robust visitor entry processes: *https://www.cpni.gov.uk/robust-visitor-entry-processes*
- CPNI professionalising security: *https://www.cpni.gov.uk/professionalising-security*

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*
- Risk management
- The NCSC cyber assessment framework: *https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework/caf-objective-a-managing-security-risk*
- The NCSC CAF guidance *https://www.ncsc.gov.uk/collection/caf*
- The NCSC identity and access: *https://www.ncsc.gov.uk/collection/10-steps/identity-and-access-management*
- The NCSC privileged access management: privileged access management: *https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management*
- The NCSC network administration: *https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns#section_3*
- 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*
- The NCSC privileged access management: *https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management*
- 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 guidance on logging for security purposes: *https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes)* and the NCSC making compromise detection easier: *https://www.ncsc.gov.uk/collection/cyber-security-design-principles/making-compromise-detection-easier*
- The NCSC incident management: *https://www.ncsc.gov.uk/collection/incident-management*
- The NCSC logging practices: *https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes*
- The NCSC guidance on Security Operations Centres (SOC): *https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide*

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: *https://www.ncsc.gov.uk/cyberessentials/overview*
- 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.