CPNI
Centre for the Protection of National Infrastructure

CPNI VIEWPOINT 02/2010

PROTECTION OF DATA CENTRES

APRIL 2010

CPNI in conjunction with the Sister Banks would like to acknowledge and thank ECA Ltd for their help in the preparation of this report. The findings presented here have been subjected to an extensive peer review process involving technical advisers from CPNI, Sister Banks and wider industry.

Executive summary

Scope of this guide

Data Centres have become critical to modern organisations: the processing and storage of information underpins the modern economy, which is characterised by a consistent increase in the volume of data and applications, and dependence upon the internet and IT services. The guide treats the protection of Data Centres holistically, covering the protection principles from initial site selection through to design, build, and operation. It covers all the elements required without proscription as individual requirements will vary. Where CPNI provides authoritative subject guidance in other documents or references with Protective Marking these are referenced back to their source i.e. the CPNI extranet.

The protection approach

Data Centre protection should start with a Risk and Threat Assessment, which combines threats, hazards, vulnerability and weaknesses and sets controls proportionate to identified risks. From this an Operational Requirement is developed that is agreed by the business and from which protection is justified.

The Data Centre Guide treats people, processes and technologies as factors combining to deliver the physical security, personnel security and information security controls that will protect the Data Centre and the services it delivers.

Once in place, protection controls should be continually tested and revised to ensure that they remain relevant and responsive to the agreed Risk assessment.

The Data Centre site

The Data Centre requires a reliable, stable electrical power supply (backed up by generators and uninterruptable power supplies), a location that is as free from risk and hazard as possible, and the availability of diverse communications.

The site should provide a layered approach to security with consideration given to security of the external environment and providing a secure perimeter. The facility should be further separated into appropriate security zones to protect the most critical and sensitive assets. These layers and zones will incorporate appropriate physical protection, detection and monitoring systems to deter, detect and delay any attacker.

Managing the Data Centre

Effective management of the Data Centre will depend upon a Risk Assessment and Protection Plan that is owned by executive management, appropriately managed and followed by all members of staff. Protection goes hand in hand with operational delivery that may also require a business resilience strategy incorporating business continuity and disaster recovery plans to ensure that an individual Data Centre does not become a single point of Corporate business failure.

Background

As the UK's economy becomes increasingly dependent upon information for delivery of online services and governance of major organisations, commercial Data Centres are recognised as forming part of the Critical National Infrastructure (CNI) –those assets deemed essential to the overall running of the country.

The loss or compromise of a major Corporate Data Centre could have a disastrous economic impact or cause significant reputational damage across the economy as customers and trading partners are affected by the failure of the organisation.

The Data Centre environment

Corporate Data Centres vary widely in nature; from massive reinforced bunkers through to simple cabinets of equipment. A dedicated Data Centre facility will typically comprise a number of key features that include:

- ***External Perimeter:*** a fence, wall or other barrier to prevent unauthorised access to the site, but incorporating an ***Entrance*** for authorised staff and visitors, and allowing the supply of **Goods, Power** and **Communications**;
- within the external perimeter are the ***External Areas*** which may include ***Car Parking*** and ***Fuel Storage*** facilities to power standby generators;
- ***Internal Areas:*** the Data Centre building itself;
- a ***Data Centre Control Room*** for management of the equipment, computers, networks;
- ***Electrical Power Supply:*** including the High Voltage (HV) Substation, Standby Generators, and Uninterruptable Power Supply (UPS) systems;
- ***Heating, Ventilation, Air Conditioning (HVAC):*** systems to maintain the environment within the Data Centre;
- ***Data Hall:*** the operational area of the centre where the computer equipment is housed.

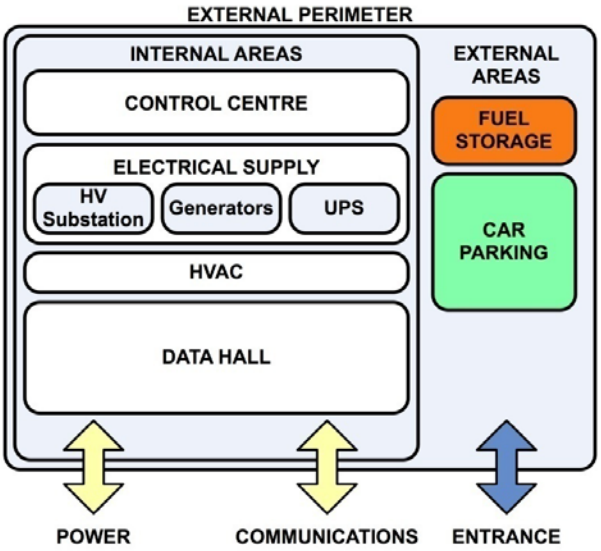

Figure 1 Schematic of a typical Data Centre facility

Where organisations cannot justify the need for an exclusive Data Centre facility, they may choose to share Data Centre services through managed hosting (where a third-party provides the server on their behalf) or by a co-location service (where their equipment is operated in a third-party Data Centre).

Achieving resilience and availability

The general approach to Data Centre protection is one of ‘defence in depth’ by creating successive layers of security measures - such that the facility is protected by numerous security controls, designed so that the failure of a single group of protective controls does not necessarily compromise the entire Data Centre.

The protection approach should start with a Threat and Risk Assessment, linked to an Operational Requirement the purpose of which is to ensure that the business needs are correctly understood. These in turn allow a layered defence model to be derived from a rigorous analysis of security requirements driven by a formal Risk and Threat Assessment model.

The protection strategy should take into account other key factors throughout its lifecycle from construction through to operational delivery of the business requirement and be reviewed regularly.

Understanding the business requirement

The Data Centre Protection Plan must be driven by the business’ overall strategy for security and resilience, and take into account the relation of the Data Centre to other critical business assets. In particular it will need to address the broader business impact if the Data Centre becomes unusable and the role of the Data Centre within the organisation’s Business Continuity and Disaster Recovery strategy.

The Data Centre may be a single, stand-alone operation which could be a single point of failure for the business operation it underpins, or part of a more comprehensive network of Data Centres with primary, secondary or even tertiary Data Centres. Equipment, networks and software applications should be planned carefully if multiple Data Centre sites are used to support business operations.

Protecting the Data Centre

Successful protection and operation of a Data Centre rests on understanding and managing the complex relationship between people, processes, technology and the physical environment in which they operate. Effective protection and service delivery cannot be achieved without a balance between these critical components:

- ***People*** are at the same time both the strongest and the weakest link. They are invariably the reservoir of corporate intellectual property; they know how the 'system' works, the flaws, loopholes and workarounds at every stage. They either make the facility work or not depending on a complex mixture of morale, motivation, training, experience, good management and effective leadership.
- ***Process*** is the arrangement of events; the methodology by which technology is applied to good effect by people; or by which the technology itself is arranged to deliver a desired effect. People and process together enable the facility to function smoothly as designed and be more or less resilient in the manner in which it is operated.
- ***Technology*** components are the vital core of the Data Centre facility and create a hugely complex series of interdependencies. Technology without people and process working together in harmony will never be truly resilient and capable of delivering sustained, consistent levels of high availability service.
- The Data Centre must have sufficient ***backup generators*** and ***uninterrupted power supply*** (UPS), protected ***fuel*** tanks for generators and domestic systems, a ***resilient infrastructure*** with no 'single points of failure', reliable and diverse ***communications***, and be housed in ***premises*** that are designed and operated with appropriate resilience levels in mind.

The Protection Plan

The Data Centre requires a Protection Plan to assess the facility for weaknesses, raise the profile of security, provide security in depth, and to ensure that security procedures and controls are subject to continual testing. The protection plan will contain the Threat, Risk and Vulnerability Assessment combining the results of the Operational Requirement analysis and develop the mitigation plan to identify key risks and manage, mitigate or present a plan to accept residual risk to the business.

Security zoning

Physical environments can be designed and managed in order to reduce the risk of unwanted events. Zoning is one component of physical security designed to reduce such risk to allow access to specific areas for those who have authorised business need for access whilst grouping key functions to appropriate controls. These layers and zones will incorporate appropriate physical protection, detection and monitoring systems, each contributing to the overall protection of the site by deterring, detecting and delaying an attack.

Zoning should promote a sense of ownership or territorial reinforcement, provide opportunities for natural surveillance and establish a clearly defined sequence of boundaries through which a visitor or departmental employee may or may not pass. Access from one zone to another is defined by the operations and security team.

Assessing risks, threats, hazards and vulnerabilities

A Risk Assessment is an essential part of achieving and justifying the cost of an overall Protection Plan for a Data Centre. It formalises the identification and control of threats, risks, hazards and vulnerabilities that may arise during site selection, construction, preparation and operation.

Data Centre controls

Data Centre location criteria

Any Data Centre needs a location free from natural or man-made hazards such as flooding and not close to hazardous operations, pollution or contamination. A reliable and stable power supply and the provision of utilities with genuinely diverse communications are essential. The site should be accessible for staff and not be in a high crime area where effective security measures are challenging.

Physical security of the site

Any Data Centre site should provide a layered approach to security which is planned as a single entity, for example with fences, gates, lighting and CCTV linked with access control measures. The perimeter should be demarcated and secured with a fence or other physical measures supported by appropriate surveillance and monitoring systems.

Site intrusion prevention and detection

A perimeter with effective fencing will complement internal control zoning to protect critical areas. The external perimeter fence should be monitor or patrolled. All entrances and doors to core buildings must be protected, alarmed and an appropriate access control mechanism provided. Active and passive electronic security can be used to supplement alarms and security physical measures. Threats from hostile vehicles should be considered. Car parking and goods delivery require separation and carefully planning. Intrusion Detection Systems (IDS) can be perimeter, barrier, ground based or free standing complemented by CCTV monitoring cameras and a lighting plan.

Communications routes and diversity

Communication route diversity into the facility is essential to give resilience. Standby power can be provided by generators and UPS, communications cannot. If two providers are used ensure routing is physically separate and that all access points are locked. Communications routing to the site should not be obvious but this is difficult to achieve. It is important that accidental damage cannot sever all services to and from the site and that communications services are monitored at all times.

External areas

Keep vehicle parking away from the key areas and protect from ram-raiding. Access for deliveries should be segregated from normal car parking access. External areas should be monitored by CCTV and patrolled at irregular intervals. Fuel tanks and other essential environmental control equipment should be protected from accidental or malicious damage. Access to roof or external gantry mounted equipment should be controlled and positioning considered for both ease of maintenance and security.

Internal areas

In designing or operating a Data Centre consider the building structure and building materials. Care must be taken when designing and operating reception. High value assets should ideally be held in an inner sanctum (the Data Hall). Security monitoring should be extensive and layered in zones. Building structure protection must be re-evaluated as part of the annual Data Centre security review; the Building Management System, Control Rooms, Network Operations Centres, internal CCTV and environment/fire control systems are important parts of the overall protection/integrity plan and should be controlled appropriately.

Electrical power

Electrical protection schemes must be in place to ensure the resilience of all vital services and utilities with no single points of failure by design. There should ideally be two sources of mains power supply. Uninterrupted Power Supplies (UPS) must be available to ensure critical business can continue for at least 30 minutes. The UPS is supported by standby generators which should be able to operate for 48 hours without extra fuel. These should be tested properly under load regularly to ensure they can deliver effectively.

Ventilation and cooling systems must be regularly monitored and maintained at an optimum temperature and humidity. Water supplies should be positioned to minimise the risk of potential damage and regular maintenance of all utilities is of paramount importance.

The Data hall

The Data Hall contains all sensitive and essential systems holding customer data and should be protected as a ‘building within a building’. It often has a ‘raised floor’ under which essential power and other cabling services, including forced cooling air, is housed or delivered. Access should be limited to those personnel working in the data hall. CCTV coverage should be used to scan the aisles and key racks for security and health and safety. All networks, systems and Information Assets should be protected from electronic threats.

It is imperative that the Data Hall is to be kept scrupulously clean at all times as dirt contamination can increase the mean time between failure of computer and other electronic equipment dramatically. Data Centre assets must be valued and recorded in an asset register. All power, communications and other cabling infrastructure should be laid neatly in cable baskets or trays, tied in and labelled with records kept and updated.

Management responsibilities

Good management delivers effective services. A security policy is essential that is owned by senior management, managed by the security working group, and reviewed annually. All senior management, business leaders and security staff must have a clear understanding of their roles and responsibilities.

Data Centre assets must be valued and recorded in an asset register as part of the Data Centre Protection Regime. Data Centre security managers should be involved in recruitment of new staff. Business Continuity Plans must accommodate every possible instance of disruption. These plans should form part of the organisation's broader resilience strategy and to be effective must be kept up to date and rehearsed regularly.

Network Operations Centre (NOC)

Sometimes called the Operations Bridge, the NOC is the nerve centre that controls hosting operations. It must be manned and controlled with appropriately skilled and security cleared staff in a room with strict access control. The NOC must be supported by UPS power.
The NOC should be co-located with the Data Centre within the inner security area and afforded the same levels of resilience as the systems it supports and controls. If the NOC is not co-located the communications to the systems it controls become significantly more important to guard against failure.

Personnel Security

People are key assets, the strongest and potentially the weakest link and the most likely source of risk and mistakes in any Data Centre operation. All staff should be recruited by pre employment screening, security terms and conditions in their conditions of service and subject to a personnel security review process. Security and technical awareness and training are essential. Remember the 'insider' may present the greatest single threat to Data Centre operations.

Typical Data Centre threats, vulnerabilities and controls

Control area	Objectives	Threats and Vulnerabilities	Controls
Location	Select a hazard-free location for the Data Centre with reliable power supply, diverse communications, and available utilities, infrastructure and transport.	• Site subject to restrictive covenants and planning limitations • Flooding • Flight paths and airfields • Proximity to Critical National Infrastructure sites • Pollution and contamination • Extreme weather	• Create a 'buffer zone' around the site • Ensure diversity of supply for power, utilities, transport • Survey site and surrounding area
Physical security of the site	Develop a 'layered' security approach that minimises risk to life and damage to asserts, and maintains business continuity.	• Site presents a target for attack, theft, vandalism	• Consider appropriate use of signage • Perimeter fence and other barriers
Site intrusion prevention and detection	Establish a secure site perimeter and security zones within the site.	• Unauthorised access within the security perimeter • Accidental damage to assets by people, vehicles	• Landscape and plant to deter approach • Use security fencing and protect all entrances • Use CCTV, lighting, perimeter intrusion detection systems to supplement passive measures • Monitor or patrol the external perimeter • Control movement of vehicles • Gather intelligence about area threat
Communication route and diversity	Establish resilient diverse communications.	• Disruption to communications by accidental or deliberate physical damage, or supplier failure	• Use multiple communications suppliers • Physically separate supply routes • Mark and regularly inspect supply routes • Lock and inspect access points
External area	Protect the external areas (within the perimeter) of the Data Centre.	• Accidental or deliberate damage or disruption to critical services housed within the external perimeter	• Site fuel tanks away from threats • Keep vehicles away from critical assets • Shield equipment from damage/attack • Protect emergency cut-off switches

Control area	Objectives	Threats and Vulnerabilities	Controls
Internal areas	Protect the internal areas of the Data Centre.	• Accidental or deliberate damage or disruption to facilities and equipment within the Data Centre	• Construct to security standards • Use reception area to manage access • Keep control room away from reception • Protect building management system, environmental controls, loading bay • Site data hall at centre of security zones with access controls between zones • Us internal CCTV, fire detection/protection
Electrical power	Maintain continuity of power supply.	• Accidental or deliberate damage to power supply • Loss of power from National Electrical Power Supply • Failure of internal electrical systems	• Use diverse providers and physically separate supply routes • Test and maintain Uninterruptable Power Supplies (UPS), onsite emergency generators
Data hall	Protect operation of computer assets within the data hall.	• Accidental or deliberate tampering with computer equipment • Server, system or cabling failure	• Implement and manage stringent access controls • Monitor data hall aisles and racks with CCTV • Protect systems against electronic threats in accordance with information security best practice • Manage cabling infrastructure and environmental controls • Keep data hall spotlessly clean
Management responsibilities	Deter attackers, protect assets, detect incidents, react to incidents, recover to normal operations.	• Procedural errors leading to service failures • Attackers subvert or fool staff • Staff unable to identify or manage incidents	• Prepare and maintain a security policy and make staff aware of roles and responsibilities • Conduct background checks on staff • Maintain an asset register • Plan and test business continuity and recovery procedures • Integrate security approach into broader resilience strategy