NOTICEBORED

Technical briefing

Securing physical access and environmental services for datacenters

Important note

The control requirements identified in this briefing are generic, do not necessarily apply to any given datacenter and may not be sufficient for your specific requirements. They reflect published best practice standards such as ISO17799, combined with the author's practical experience of designing, operating and reviewing datacenters. Since every datacenter is unique, however, it is advisable to assess the risks in your specific situation to determine the appropriate security requirements. Furthermore, the risks vary over time, meaning that security should be reviewed periodically to make sure that it remains sufficient to the need.

The length of this paper reflects the large number of risks and the controls necessary to ensure safe and reliable datacenter facilities. On the other hand it is still only a briefing, in other words **professional advice should be obtained** for aspects such as datacenter architecture, power, air conditioning and health and safety, supplementing the standards, common sense and practical experience outlined here.

Introduction

Datacenters in many organizations house the "crown jewels" in IT terms - mainframes and other computer servers, disk farms, tape silos, networking equipment *etc*. and, of course, enormous quantities of data. This briefing identifies physical security controls typically used to protect valuable datacenter assets against risks such as physical damage, theft, fire and flood. It also describes typical environmental services required to maintain suitable operating conditions for the datacenter systems and workers.

This paper is specific to datacenters. It does not directly address physical security for distributed computing and networking facilities, office-based departmental servers and desktop systems, mobile or home working setups. The requirements for power, physical access controls *etc*. may be broadly similar but the impacts of security failures are generally much less, therefore lesser controls are usually appropriate.

Datacenter security requirements

Datacenter architecture

Control objective: *the datacenter structure should be designed and built to support the organization's requirements for information security and IT service reliability*

Typical controls:

- The datacenter should be appropriately positioned geographically *e.g*. above the water table or flood level; away from fire, electromagnetic and physical hazards; and in a location that can be physically secured against unauthorized access
- Datacenters should be designed by competent architects familiar with the specific needs of IT systems, including the associated information security requirements
- Plans, design drawings, diagrams, specifications *etc*. should be maintained up-to-date, showing wiring routes, environmental equipment, power demands *etc*.
- Facilities in earthquake-prone areas should follow relevant planning standards for seismic protection
- Facilities should be fortified against severe weather such as hurricanes *e.g*. roof anchored to walls, double-skin walls to reduce penetration by flying debris, window shutters, sump pumps
- Non-purpose-built datacenter buildings must be risk assessed and upgraded where necessary to provide sufficient protection

Physical access controls

Control objective*: prevent physical access to datacenter assets by unauthorized people.*

- Physical access controls suitable for the organization's datacenter security requirements should be professionally specified, designed, installed and maintained
- Access controls should reflect local practice and laws (*e.g*. guards may or may not be armed)
- The classic design uses concentric control boundaries, starting with the whole site (*e.g*. perimeter security fence and guards), then the data center building (*e.g*. single access point controlled by a receptionist/guard; 'moat' no-go area around) and finally the internal sensitive areas (*e.g*. separate card access controlled zones for tape operators, print operators, network managers and systems managers)
- Controls should be applied over *who* can access the facility (implies authentication of individuals), *when* they can access it (*e.g*. visitors may be specifically authorized for particular days using coded passes; special procedures for out-of-hours access) and *where* they can go (zones)
- Exterior walls, doors and windows should be strong enough to resist deliberate or accidental damage, including vehicle impacts and bombs if necessary
- Internal partition walls may be required to cater for differing equipment requirements, limit the spread of fires and provide separate physical access zones
- Walls should generally be 'slab-to-slab' to prevent unauthorized access under raised floors or above false ceilings
- Doors should be strong and solid, possibly metal-cored fire-resistant doors with concealed hinges fixed and locked into strong frames, themselves securely fixed to the walls, floor and ceiling, with anti-burst locking pins and strong locks

- Rooms housing especially sensitive equipment should ideally have no external walls, doors, windows or skylights to (*i.e.* internal rooms built like 'panic rooms')
- Secure cages and racks should protect sensitive equipment – these should be locked routinely and keys carefully controlled
- Structured visitor procedures should be in place *e.g.* all visitors must be pre-booked and authenticated; they may have to be accompanied by staff and/or security guards; they may have to be searched for camera phones, bugging devices, network sniffers *etc*.
- Datacenter location signs, if any, should be discreet (it is not considered good practice to broadcast the precise location and nature of your datacenter!)
- The issue and recall of keys and passes, especially master keys, should be carefully controlled with frequent reviews and reconciliation
- Motion detectors, microswitches, pressure pads and so on may be used to indicate when doors or racks are opened, rooms are entered *etc*.
- Closed Circuit Television monitoring should be professionally designed with suitably located day/night cameras covering all entry points (including the delivery yard and fire escapes), video recording, and proactive review by security guards; cameras should ideally move unpredictably to deter intruders trying to slip in/out when the camera is turned away
- Routine security guard inspections should include all facility entry/exit points and internal secure areas, 24x7; guard tour monitoring systems may be useful to ensure all points are visited regularly; all incidents should be logged; selection, training and motivation of security guards are important issues but beyond the scope of this briefing

Fire protection

Control objective*: minimize the risk of damage caused by fire and smoke.*

- Fire prevention is preferable to fire fighting! A strictly-enforced no smoking policy should be in place throughout the facility. Overloaded power cables and outlets must be avoided. Flammable materials (paper, cardboard, plastics and solvents) should be excluded from the datacenter as much as possible - don't let printouts pile up and clear out packaging materials and trash promptly
- Fire protection systems (fire alarms, heat and smoke detectors, automated fire suppression, extinguishers, emergency exit routes *etc*.) should be professionally specified, designed, installed and maintained – this is not a do-it-yourself job
- Certification of the fire protection may be necessary for legal or insurance reasons, and is considered general good practice
- High-sensitivity aspirating smoke detectors may be necessary because smoke dispersion by high-flow computer room air conditioners often desensitizes standard ceiling-mounted smoke detectors; aspirating tubes should be placed in voids as well as the main room space, and possibly within individual cabinets/racks
- Non-flammable or low-smoke/self-extinguishing furniture, carpets, wall coverings, fixtures and fittings should be used wherever possible
- Most datacenter doors should be fire doors rated for at least one or two hours to help contain any fires. They must seat snugly within proper door frames, especially if extinguishant gas is used for fire suppression. They should self-close and must not be propped open, except perhaps for non-access-controlled doors using magnetic door holdbacks linked to the fire alarm system.
- All wall, floor and ceiling penetrations such as cable conduits should be properly sealed with special firestop sealant/mastic, not left open nor blocked with rags or cavity wall insulation *etc*.

- The fire alarm should be interlocked with the fresh air supply, air conditioning and possibly other equipment supplies to avoid ‘fanning the flames’ in a fire
- A slight positive air pressure will help exclude smoke and dust ingress from surrounding areas
- Designated fire points with handheld fire extinguishers suitable for use on electrical fires should be located at or near exit points, not deep inside the rooms
- Magnetic media should be stored in locked fire safes certified to internationally recognized standards for media use (*e.g.* the German standard VDMA 24991), and should ideally be moved off-site on a regular basis
- An on-site tape library/store, if required, should be located in a dedicated fire-proof and access-controlled room, not in the main computer room (the main room should only contain tapes currently in use); sand may be the most effective extinguishant for magtapes which burn fiercely once ignited
- High-volume printers should be located in a separate room also with access limited to essential personnel
- Procedures for dealing with fires should be clearly displayed, understood by all workers who routinely use the facility and regularly practiced
- All fire equipment should be professionally checked and serviced regularly

Flood protection

***Control objective**: minimize the damaging effects of water on datacenter equipment.*

- The facility should ideally be located well above the water table, flood level and sea level, or at least protected by physical barriers from the main threats
- Roofs, windows, doors, walls and cable ducts should all be sealed against rainfall and flood water, and properly maintained. Flat roofs frequently cause problems – even a slight slope down to a drain can help, and great care must be taken to avoid penetrating the roof seal.
- Water pipes and tanks should either be removed or diverted around instead of running through or across critical areas. Emergency stop valves should be accessible and their positions and functions understood by essential personnel.
- Water leakage detector loops and sump pumps may be useful at low points under raised floors
- Drip trays under air conditioner units, pipes *etc*. with proper drains and possibly water detection will reduce the risk of problems from condensate or leaks
- Procedures should be in place to identify and deal promptly with early signs of leaks or floods
- Regular facilities inspections should be alert to any signs of water leaks, especially under any flat roofs, windows and water/drainage pipes, and in the underfloor voids
- There should be ready access to mops, buckets and plastic sheeting for emergency use (including out of hours for the security guards or night shift)
- It may be worth finding and possibly contracting with specialist firms having the capacity to recover, clean and restore flooded electronics professionally, perhaps as part of the contingency/IT disaster recovery plans

Power supplies

***Control objective**: secure a clean, reliable power supply for critical datacenter systems.*

- Electrical power design, installation and maintenance for datacenters is another specialist job best left to the professionals.
- Power capacity is a significant design issue: inadequate capacity can lead to fires and sudden supply failures as a result of overloading. Someone should be held specifically responsible for monitoring power capacity and for confirming that capacity is adequate to support new equipment. This includes UPS capacity – individual UPS units for each rack allow more flexibility but they all then need to be maintained.
- Ideally, multiple/redundant power sources should be used *e.g.* power feeds from separate substations and diesel/gas-fuelled generators (diesel is safer than gas but the use of alternate fuels increases overall resilience; gasoline should be avoided if at all possible)
- Power quality is another issue for electronic equipment. So-called "computer-grade" (on-line no-drop sinusoidal output with frequency and voltage control) uninterruptible power supplies should ideally be used, especially for critical equipment such as servers and disk arrays. Mains regulators and filters offer some protection against power line noise, spikes, frequency or voltage fluctuation (brownouts) *etc*. but do not protect against power supply interruptions.
- Standby generators must deliver sufficient capacity to run all essential equipment and should preferably auto-start. The inductive load presented by equipment containing conventional transformers and the peaky impedance characteristics of switched-mode power supplies can create difficult conditions for generators without 'soft-start' capabilities.
- Fuel tanks for on-site generators must be adequate to cope with predicted use, possibly allowing for re-supply interruptions due to fuel shortages, strikes or bad weather (it may also be possible to identify priority access to other fuel tanks on site)
- Emergency power off buttons may be advisable in access-controlled computer and comms rooms but should be shrouded to avoid accidental use and tested at least annually
- Battery care and maintenance is very important for UPS systems. Wet lead-acid batteries should be kept in a containment basin in case of leakage, and the room should be vented of excess hydrogen. Cell condition should be checked regularly, and the overall battery capacity should be confirmed regularly by run-down testing.
- Switching panels should allow for alternate power feeds to be routed to essential equipment without interruption and for isolation of power segments for safe maintenance of power equipment, installation of additional power outlets *etc*.
- Batteries, generators and other heavy electrical gear should be in separate rooms or compounds with access limited to designated maintenance personnel.
- Regular preventive maintenance and testing should include full on-load tests of generators, UPS systems, switchgear *etc*. The power systems should be designed and maintained to instill sufficient confidence such that interrupting the incoming supply for testing is of no concern. As well as proving the systems operation, on-load tests are especially important for diesel generators since off-load testing can lead to blocked fuel injectors.
- The quality (*e.g*. voltage, amperage, frequency, spikes, noise) of the 'clean' electrical supply to equipment should be monitored continuously and compared against the 'dirty' incoming supply to confirm correct operation of UPS, filters *etc*.

Air conditioning

***Control objective**: maintain temperature and humidity within acceptable operating limits.*

- 'Computer grade' highly reliable air conditioner units (chiller/fan cabinets located in or near the computer room plus condenser/fan units in a secure outside position, connected by secure cabling and pipework)
- Excess capacity including additional redundant units to cope with equipment failures or planned outages for maintenance, as well as fluctuations in ambient conditions and heat load within the facilities
- Equipment sensibly located to avoid hot spots
- Temperature monitors including overall room sensors and perhaps others within critical racks *etc*., with local indicators and connected to a remote monitoring console, with suitable set-point alarms (checked regularly)
- Routine preventive maintenance *e.g*. cleaning, checking mechanical and electrical operation, coolant levels, condensers, changing filters *etc*.
- Contracted on-demand emergency maintenance/support cover in case of equipment failure
- Standby emergency air conditioners to cope with air conditioner failure, outage due to maintenance or inadequate capacity for peak demand (clearly implying the need to increase routine capacity)
- Monitoring and operating procedures, including suitable planned response if temperature alarms are triggered or

Cabling

***Control objective**: provide reliable power and data feeds to the datacenter equipment.*

- Cables should preferably be laid neatly in conduit or else in cable trays, and should be properly but discreetly labeled to match the corresponding wiring diagrams. Cabling diagrams must be maintained and should be checked periodically, especially before undertaking any maintenance work.
- Incoming cables should ideally be routed underground in sealed, secure conduits encased in concrete. Ordinary cable ducts are more liable to accidental damage, flooding *etc*. and overhead cables are probably the least secure of all.
- Multiple communications routes and suppliers offer greater resilience, with diverse physical routing to avoid common-mode failure (*e.g*. a cable duct fire may take out copper and fiber-optic connections but may not affect a point-to-point microwave link or satellite connection on the roof).
- Power and data cables should be routed to avoid high traffic routes *etc*. Power and copper data cables should however be physically separated wherever possible.
- Electrical cables must have more than adequate capacity for the predicted power usage (see power section above).
- Safety- or business-critical cables (such as those used by the fire alarm and suppression systems, and essential communications cables) should be routed through metal conduit/tubing or be armored for additional physical protection.
- Only 'low smoke' cable jackets should be permitted within the datacenter – this applies to all forms of cabling.

Health and safety

***Control objective**: provide a healthy and safe working environment for datacenter staff and visitors.*

- Health and safety aspects should be covered in the design and in practice *e.g*. access paths kept clear of obstructions; regular safety testing of electrical equipment; false floors properly fitted and level; fire escapes marked and kept clear of obstructions; evacuation procedures well rehearsed; special procedures in place for working in areas fitted with automatic fire suppression. Building regulations normally cover most of these issues and competent architects familiar with datacenter designs should be well aware of the local requirements.
- Facilities should be regularly inspected by competent health-and-safety trained people. All necessary corrective actions should be logged and promptly resolved. A small budget allocation may help speed up remedial works. Unannounced *ad hoc* inspections by management may also be worthwhile if issues are not being resolved effectively.
- An 'owner' (custodian) should be designated and held responsible for all aspects of each major area of the facility.
- Power extension cables, multiway adapters, unfused spurs and similar temporary power wiring should be banned from the datacenter. They create unnecessary fire and tripping hazards and are unreliable compared to permanent wiring. Sufficient power sockets should be provided in the first place or professionally installed within the constraints of the available supply.
- Emergency services response times should be evaluated. It may be worth employing firemen, armed guards, first-aiders *etc*. or at least training local staff to provide a prompt initial response, subject to securing their own personal safety.

Miscellaneous other issues

***Control objective**: minimize other risks to the datacenter assets and IT services.*

- Consider having a direct exchange phone in the computer room and possibly a fax machine attached or readily available, in case the PBX fails. Cellphones are another backup but remember that they may fail in a serious emergency situation such as 911.
- All valuable hardware assets (IT equipment, air conditioners, UPS *etc*.) should be labeled, recorded on an asset inventory and maintained.
- IT Disaster Recovery Planning should prepare to restore IT services as an integral part of the overall facility emergency plan. Functions such as Facilities, IT, Physical Security *etc*. should cooperate on planning and hold joint emergency exercises.
- Dust and dirt should be excluded from the data center as far as practicable *e.g*. using a filtered fresh air supply and filtered air conditioners, with filters changed regularly, and 'TakMats' at entrances to reduce shoe-borne dirt. Rooms should be cleaned regularly by appropriate staff using microfiltered vacuum cleaners who have been cleared to enter the relevant secure areas (standard office cleaners are unlikely to be suitable without additional training and awareness in issues such as using designated cleaning sockets and not knocking buttons or cables). Full deep-cleaning by specialist suppliers may be worthwhile once dusty building works have completed.
- All equipment and exposed metal surfaces should be securely connected to a common low impedance earth point, mat or bus. This is primarily a safety issue but also helps minimize the effects of electrical interference, static electricity and lightening.

- A security culture should be encouraged, not just in the datacenter but in the organization as a whole. Security-aware, alert and truly on-the-button employees, maintenance staff, security guards *etc*., are a tremendous asset to the organization. It should be accepted common practice for people to notice potential [information] security concerns, notify the relevant managers and get issues resolved quickly. Management can help by explicitly encouraging this kind of behavior.
- The principles of separation of duties and least privilege should be applied where applicable to datacenter operations and security. Proactive management oversight, routine job rotation and mandatory vacations for people in sensitive positions add to the general security culture.
- Faraday shielding, filtering of power and data cables *etc*. may be necessary to minimize electromagnetic interference (inbound) and emanations (outbound), potentially including EMP/HEMP protection and Tempest in military situations.
- Lightning protection may be needed, especially in tall or 'spiky' buildings in lightening-prone areas. Even in areas with low lightening risk, surge arrestors may still be advisable on all incoming copper data, telephone and power lines for critical datacenters, coupled with effective low-impedance earthing. Fiber-optic lines are practically immune to this problem and should be used to replace copper cables wherever possible.

Conclusion

The fact that this 'briefing' is eight pages long is telling. Securing physical access and environmental services for a datacenter is not a simple task with many pitfalls for the unwary, hence the reason that there are several references to calling on professional architects and other experts to assist.

For more information

For general advice on information security controls or this topic in particular, contact the Information Security Manager (x1234), visit the information security website on the intranet or follow the hyperlinks to useful Internet resources from www.noticebored.com/html/physical.html.