RISK NOTE

Server Room/Data Centre

OVERVIEW OF ISSUE

Computer server systems and equipment are utilized by the government, corporations and industries, including the healthcare industry, for storing and processing information, data, files and records. Healthcare organizations normally install these systems in a room or cluster of adjacent rooms. In both scenarios, the electronic data and systems are exposed to potential physical damages resulting in loss of data and records, including patient health information, disruption of care, damage to equipment and building and legal proceedings against the healthcare organization.

A careful analysis, design and implementation of mitigation strategies are critical to managing the risks associated with server rooms and data centres.

KEY POINTS

- Provide adequate protection against fire and water damages
- Create adequate up-to-date backups of all electronic data and systems
- Create a disaster/business recovery plan for worst-case scenarios.

THINGS TO CONSIDER

Construction and Location

- Consider the following for new projects or renovations:
  - Design all server rooms/data centres in accordance with appropriate building/fire codes, provincial and local regulations and applicable codes, including national standards. Ensure authorities having jurisdiction (e.g. city engineers and fire departments) are involved as required in the project design and coordination. Property insurers may provide valuable insight into best practice designs.
  - Use noncombustible construction materials, including ceiling and floor tiles, insulation, cable raceways and routing assemblies.
  - Avoid plastic materials, including those with fire-retardant composition, as these produce large quantities of smoke in a fire.
  - Avoid locating the server room/data centre in below grade areas, in areas exposed to potential floods or areas with roof drains or domestic water lines. Avoid locating them in areas with ignitable liquids or gas.
  - Consider using communication and data cables that meet one of the following criteria: FM Approved Group 1-4910, FM Approved Group 1, plenum rated cable listed to Underwriters Laboratories (UL) Standard 910 or cables that have a maximum flame spread distance of 1.5 m/5 ft or less when tested in accordance with National Fire Protection Association 262.
- Refer to HIROC's Risk Reference Sheet - Property - Water Damage for server rooms/data centres with domestic water or liquid lines inside (including ceiling or raised floor areas).
- Consider enclosing the server room/data centre with fire rated walls, floors and doors of at least one hour fire-resistance rating. Seal duct and pipe penetrations with an approved sealant with a fire-resistance rating equivalent to the rating of the wall or floor. Consider fire separating the Uninterruptible Power Supply (UPS) System if located inside the server room/data centre.
- Minimize the use of interior windows and doors into the server room/data centre. Provide tempered or wired glass for windows.
- Provide fire dampers (fire rating equivalent to the rating of the wall or floor) inside ducts passing through fire rated walls and floors in accordance with appropriate codes.
- Consider removal or protect all exterior windows (of the server room/data centre) against strong winds and rains if these are located in a building exterior wall.

Server Room/Data Centre

Occupancy

- Remove abandoned or spare cables that are not in service and are not intended for future service. Remove any used packaging materials after every shift.
- Limit any storage of in-process computer equipment or parts for installation in the server room/data centre to one pallet load.
- Locate any storage or staging area for computer equipment, supplies (i.e. printing inks, printer papers) and parts to a fire-separated area or room.
- Consider providing an automatic and a manual power-down programs and procedures for de-energizing data processing equipment and HVAC (heating, ventilating, cooling, and air-conditioning) systems when a fire protection device in the server room/data centre activates. Power to the lighting system in the server room/data centre can remain energized to aid manual firefighting activities. A power-down program aims to address concerns with fire re-ignition, smoke migration, maintain clean agent concentration (for the fire extinguishing system, if utilized), and minimize damage to exposed electronic circuits.
- Perform backups of all digital records, software, system, information, files and data, and store the tapes or drives preferably in an offsite secure location or onsite vault, cabinet or safe adequately protected against theft, vandalism, fire, and water damage.
- Provide adequate HVAC system, UPS, and backup emergency power supply.

Fire Protection

- Implement an access control system/program to the server room/data centre (including ensuring all access doors are locked, utilizing a video recording system, and logging/escorting all visitors to the room).
- Provide fire protection (e.g. appropriate portable fire extinguishers, sprinklers, clean agent fire extinguishing system, and/or water mist system), fire detection and alarm systems throughout all building spaces (including above the ceiling and under any raised floors) in accordance with appropriate codes.
- Consider engaging the property insurer as they may provide valuable insight into best practice designs.
- Install smoke detectors in the fresh air intake and return ducts and consider interlocking them with the air handling system of the server room/data centre.

Maintenance and Emergency Response

- Maintain good housekeeping (i.e. remove unnecessary storage of combustibles like printing papers and used packaging materials) inside server rooms/data centres.
- Educate emergency response personnel with procedures for responding to incidents concerning the server room/data centre. Determine who is authorized to interrupt electrical power in the server room/data centre in case of fire. Identify staff responsible for notifying the fire service/department. Train emergency response personnel in regards to proper operation of fire extinguishing equipment/system.
- Provide the local fire service/department with a general description of the facilities, data processing equipment, and related equipment as part of the pre-emergency planning.
- Develop a detailed written disaster recovery plan for the server room/data centre based upon a complete loss of facility and services.
- Review, update and test the emergency response (or incident management system) and disaster/business recovery plans to ensure they are up-to-date and functional.
- Implement adequate maintenance program for the HVAC, UPS and backup emergency power systems.

REFERENCES

- FM Global. (2012). Data Centers and Related Facilities. [Property Loss Prevention Data Sheet 5-32].
- National Fire Protection Association. (2013). Standard for the fire protection of information technology equipment.
- Canadian Consulting Engineer. (2012). Fire protection: Mission critical – protecting data centres.

This is a resource for quality assurance and risk management purposes only, and is not intended to provide or replace legal or medical advice or reflect standards of care and/or standards of practice of a regulatory body. The information contained in this resource was deemed accurate at the time of publication, however, practices may change without notice.

Date last reviewed: October 2017