ISACA Journal

Volume 4, 2014

Fire Protection of Computer Rooms—Legal Obligations and Best Practices

Features

Fire Protection of Computer Rooms—Legal Obligations and Best Practices

Haris Hamidovic, Ph.D., CIA, ISMS IA

Considering that the issue of fire protection in computer rooms is not specifically addressed in many national regulations, the US National Fire Protection Association (NFPA) Standard for the Fire Protection of Information Technology Equipment (NFPA 75) can be used as a recognized fire protection technical standard for these environments. This standard is also recommended by the Telecommunications Industry Association (TIA).[1]

In addition to complying with fire safety regulatory requirements, the recommendations of the NFPA 75 standard can also help organizations address the following concerns:

- Fire threat of the installation to occupants or exposed property
- Economic loss from loss of function or loss of records
- Economic loss from value of equipment
- Business interruption

Although the probability of occurrence of fire originating in digital equipment (servers, storage units) is very low because there is little energy available to any fault and little combustible material within the equipment,[2] risk may be significant considering IT equipment has become a vital and commonplace tool for business, industry, government and research groups.

Technical and Organizational Measures

For computer rooms, there are recommended measures (technical and organizational) to prevent the spread of fire and ensure sufficient fire alerts and effective fire extinguishing. The following measures are, therefore, recommended:[3]

1. Construction measures:
    - The IT equipment room shall be separated from other occupancies in the IT equipment area by fire-resistant rated construction (not less than 1 hour).
    - Every opening in the fire-resistant rated construction shall be protected to limit the spread of fire and to restrict the movement of smoke from one side of the fire-resistant rated construction to the other.
    - Noncombustible material shall be used.
2. Installation of automatic fire detection and fire alarm systems:
    - Automatic detection equipment shall be installed to provide early fire warning. The equipment used shall be a listed smoke-detection- type system.
    - The alarms and trouble signals of automatic detection or extinguishing systems shall be arranged to annunciate in a constantly occupied location.
3. Installation of automatic fire protection systems:
    - Where there is a critical need to protect data in process, reduce equipment damage and facilitate return to service, consideration should be given to the use of a gaseous clean agent[4] inside units or total flooding systems in sprinklered or nonsprinklered IT equipment areas.
    - The ideal system would incorporate a clean gas system and a pre-action water sprinkler system in the ambient space. Gas suppression systems are friendlier to the hardware in the event of a discharge. There is some concern regarding the use of water on sensitive electronic equipment, whereas the hardware in a room subjected to a gas discharge can often be brought back online soon after the room is purged.[5] Gas systems are, however, one-shot designs. If the fire is not put out in the initial discharge, there is no second chance. The gas system cannot be reused until it is recharged or connected to a backup source. Water systems can continue to address the fire until it

has been brought under control. While a water system is more likely to damage the hardware, it is also a better means of protecting the building structure. Water-suppression systems are often preferred or mandated by building owners or insurance companies. Water systems are also highly recommended in areas containing a high level of combustible material use or storage. The decision of what means of fire suppression to utilize must incorporate numerous factors, including the mission and criticality of the data center operations.[6]

- Effective room sealing is required to contain the clean agent so that effective concentrations are achieved and maintained long enough to extinguish the fire.
- NFPA recommends that the electronic and heating, ventilation, and air conditioning (HVAC) equipment be automatically shut down in the event of any suppression system discharge, although the reasoning behind this is different for water-based and clean-agent systems. Electronic equipment can often be salvaged after contact with water so long as it has been de-energized prior to contact. With water-suppression systems, the automatic shutdown is recommended primarily to save the equipment. With clean-agent systems, the concern is that an arcing fault could reignite a fire after the clean agent has dissipated. In either case, however, the decision to provide for automatic shutdown is ultimately the owner's, who may determine that continuity of operations outweighs either of these concerns.[7]

4. Additional organizational and other measures:
    - Designated IT equipment area personnel shall be continually and thoroughly trained in the functioning of the alarm system, desired response to alarm conditions, location of all emergency equipment and tools, and use of all available extinguishing equipment. This training shall encompass the capabilities and the limitations of each available type of extinguisher and the proper operating procedures of the extinguishing systems.
    - Listed portable fire extinguishers of the carbon dioxide type or a halogenated agent type shall be provided for the protection of electronic equipment. A sign shall be located adjacent to each portable extinguisher and shall plainly indicate the type of fire for which it is intended.
    - There shall be a management-approved written, dated and annually tested fire plan, damage control plan, and recovery procedures for continued operations.
    - Whenever electronic equipment or any type of record is wet, smoke damaged or otherwise affected as a result of a fire or other emergency, it is vital that immediate action be taken to clean and dry the electronic equipment. If water, smoke or other contamination is permitted to remain in the equipment longer than absolutely necessary, the damage can be grossly increased.
    - Seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Potential Damage to Electronic Equipment

The primary damage to electronic equipment is caused by smoke that contains corrosive chloride and sulfur combustion by-products. Smoke exposure during a fire for a relatively short period of time does little immediate damage. However, the particulate residue left after the smoke has dissipated contains an active by-product that will corrode metal surfaces in the presence of moisture and oxygen.[8]

The most important asset to be preserved following the loss is corporate media (company database). Severe damage to disk read/write heads and tape transport mechanisms is probable if an attempt is made to operate with media that are not clean. A "head-crash," caused by particulate on the surface of a disk, will not only damage the drive, but result in a loss of data. Dirty tapes will stick and break, causing loss of data.[9]

IT equipment and materials for data recording and storage can incur damage when exposed to sustained elevated ambient temperatures. The degree of such damage will vary depending upon the exposure, equipment design and composition of materials for data recording and storage. The following are NFPA guidelines concerning sustained high ambient temperatures:[10]

- Damage to functioning information technology equipment can begin at a sustained ambient temperature of 79.4°C (175°F), with the degree of damage increasing with further elevations of the ambient temperature and exposure time.
- Damage to magnetic tapes, flexible discs and similar media can begin at sustained ambient temperatures above 37.8°C (100°F). Damage occurring between 37.8°C (100°F) and 48.9°C (120°F) can generally be reconditioned successfully, whereas the chance of successful reconditioning lessens rapidly with elevations of sustained ambient temperatures above 48.9°C (120°F).
- Damage to disc media can begin at sustained ambient temperatures above 65.6°C (150°F), with the degree of damage increasing rapidly with further elevations of sustained ambient temperatures.
- Damage to paper products, including punch cards, can begin at a sustained ambient temperature of 176.7°C (350°F). Paper products that have not become brittle are generally salvageable.
- Damage to microfilm can begin at a sustained ambient temperature of 107.2°C (225°F) in the presence of steam or at 260°C (500°F) in the absence of steam.

NFPA 75 also states that it is a popular misconception that electronic equipment exposed to water and moisture is permanently damaged. Water that is sprayed, splashed or dripped onto electronic equipment can be easily removed. Even equipment that has been totally submerged can be restored. However, in every case of water damage, immediate countermeasures are imperative. It is most important to turn off all electrical power to the equipment.

Automatic fire suppression systems provided in computer rooms should be selected with due consideration of the hazards being protected and the impact of the agent on energized information and communications technology (ICT) equipment or on unprotected emergency responders performing depowering functions. Detection and actuation systems should be periodically reviewed to avoid unwanted discharges of the automatic fire suppression systems. Accidental discharge of extinguishing agents can cause damage to equipment or danger to personnel. Fire suppression agents should not cause severe damage to the ICT equipment. Suppression agents such as those containing dry chemical agents or corrosive wet agents in fixed systems should not be used in any area containing ICT equipment.[11]

Conclusion

The formal implementation of protective measures will not be effective if these measures are not functional. For example, installation of the most expensive automatic fire extinguishing system will not produce results if the unit is defective.

Personnel responsible for fire protection have to stay informed on the building’s changes, such as upgrades and renovations, to maintain projected technical characteristics of buildings with regard to fire protection.

In addition, it is necessary to maintain the good working condition of all installed equipment that allows the functioning of the designed fire-protection system.

Also, provision should be made for loss of critical equipment through fire, particularly where interruption to operations is not tolerable or where replacement times for equipment are beyond an acceptable period of interruption to operations. The fire protection strategy for computer rooms should be formulated after determination of, or in conjunction with, the choice of a disaster recovery plan. Small oversights might turn into economic disaster.

Endnotes

[1] Telecommunications Industry Association (TIA), TIA-942, "Telecommunications Infrastructure Standard for Data Centers," 2005
[2] Mangs, Johan; Olavi Keski- Rahkonen; "Full-scale Fire Experiments on Electronic Cabinets," VTT Building Technology, Publication 269, Finland, 1996, www.vtt.fi/inf/pdf/publications/1996/p269.pdf
[3] National Fire Protection Association (NFPA), NFPA 75, Standard for the Fire Protection of Information Technology Equipment, USA, 2013, www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=75
[4] A "clean agent" is an electrically nonconducting, volatile or gaseous fire extinguishant that does not leave a residue upon evaporation. National Fire Protection Association (NFPA), *Standard on Clean Agent Fire Extinguishing Systems*, USA, 2012, www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=2001
[5] British Standards Institution (BSI), BS 6266:2011, *Fire protection for electronic equipment installations—Code of practice*, UK, 2011
[6] Sun Microsystems Inc., *Sun Microsystems Data Center Site Planning Guide. Data Centers' Best Practices*, 2003
[7] *Op cit*, TIA
[8] *Op cit*, NFPA, 2013
[9] *Ibid*.
[10] *Ibid*.
[11] National Fire Protection Association (NFPA), NFPA 76, *Standard for the Fire Protection of Telecommunications Facilities*, USA, 2012, www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=76

Haris Hamidovic, Ph.D., CIA, ISMS IA, is chief information security officer at Microcredit Foundation EKI Sarajevo, Bosnia and Herzegovina. Prior to his current assignment, Hamidovic served as IT specialist in the North Atlantic Treaty Organization (NATO)-led Stabilization Force in Bosnia and Herzegovina. He is the author of five books and more than 70 articles for business and IT-related publications. Hamidovic is a certified IT expert appointed by the Federal Ministry of Justice of Bosnia and Herzegovina and the Federal Ministry of Physical Planning of Bosnia and Herzegovina.