

Understanding Fire Hazards in Computer Rooms and Data Centres

By Kai Foo Chan
Chief Engineering Technical Specialist
FM Global – Global Services, Asia

Picture courtesy of Firepix International

COMPUTER SYSTEMS ARE NOW the backbone of almost all industrial and commercial operations. The high values inherent in this complex equipment, combined with a company's dependence on computers for continuity of operations, make loss prevention a high priority. Almost without exception, companies cannot afford to lose the use of their computer systems for any length of time.

Based on the loss experience at locations insured by FM Global, there are various active and passive measures that can be taken to ensure adequate, cost-effective protection for electronic data processing (EDP) facilities. The focus here is on the protection of mainframe computer systems, high-value minicomputer systems and major industrial process control systems from fire and other major sources of loss.

The recommendations are based on the application of an overall risk analysis. It's a flexible approach that considers the values at risk (i.e., the total potential loss from physical damage and interruption of operations) then examines the traditional concerns of construction, occupancy, protection, and the human element. All of these factors have an interrelated effect on the possible effects of a fire or other incident.

FIRE HAZARDS

Fuel inside a computer area – this is one of the first areas to consider when looking at fire hazards. The aim is



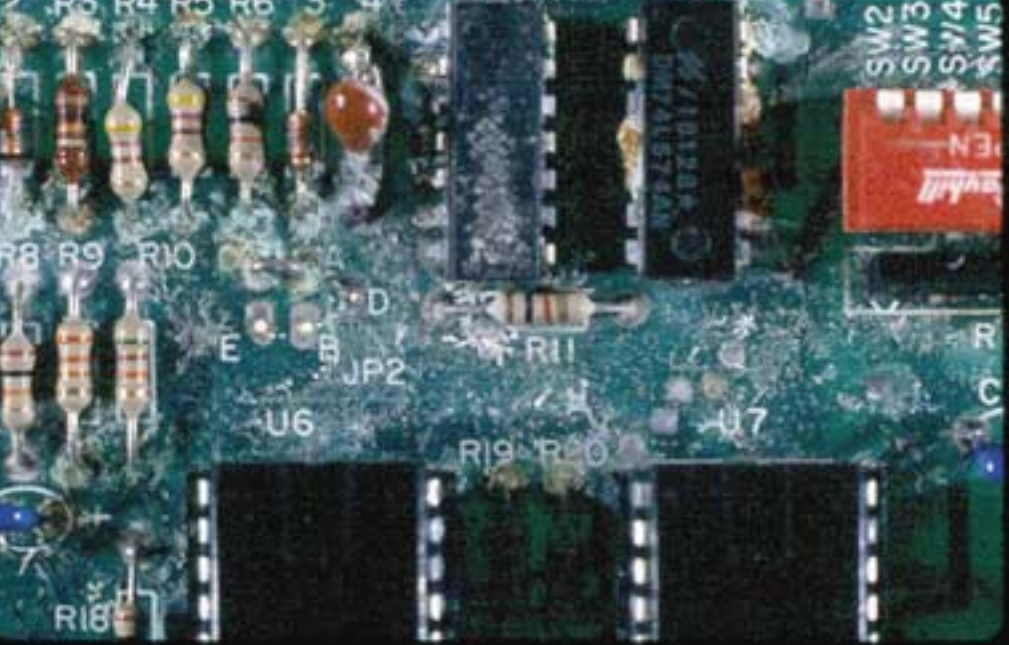
© 2005 Factory Mutual Insurance Company. Reprinted with permission. All rights reserved.

to reduce the amount of combustible material to a bare minimum. That involves using non-combustible housings for computer systems, reducing the amount of flammable media storage within the computer room – such as magnetic tapes and disks – or storing it in protective storage and minimising the use of combustible construction materials such as ductwork or insulation. Also, reducing the amount of flammable furnishings and stationery kept in the computer room is recommended. This will help reduce ignition sources and, if a fire does break out, reduce the fuel load available to that fire.

Fuel outside the computer area

– Shielding computer operations from a fire outside the computer area is critical. In fact, loss history has shown that computer rooms have been damaged more often by fires originating outside the rooms than by fires originating within them. Computer equipment can be damaged from heat or smoke that travels from the original fire area.

The causes of fire – FM Global loss experience reveals that electricity accounts for the highest number of fires and the greatest financial loss. A



© 2005 Factory Mutual Insurance Company. Reprinted with permission. All rights reserved.

computer facility includes a maze of power and signal wiring, and cables associated with both the equipment and building services. In addition, within the immediate surrounds of the computer area you will often find various other electrical equipment that may present a hazard. An ignition in that equipment could create an exposure fire. Even when the design and construction of a facility is to modern codes and standards, failures involving electrical components that lead to faults and ignition do still occur. Research has shown that enough heat may be generated by faults in low-voltage wiring, such as signal wires, to generate damaging concentrations of combustion products and ignition of adjacent combustible material.

Non-thermal fire damage – FM Global loss data has also revealed a less obvious side-effect of fire. Exposure of electronic equipment and wiring to even a small, smoldering fire may result in extensive non-thermal damage, i.e., damage caused by factors other than heat. The most significant agents of damage are the products of combustion, especially of burning plastics.

When many plastics burn – especially polyvinyl chloride (PVC), which is commonly used to insulate wiring – acidic vapors are given off. When these combine with moisture and oxygen, metal surfaces and electronic circuitry will corrode. In addition, particulate matter, such as soot, will coat components, causing them to fail.

Water allowed to dry on electronic circuitry leaves residue that is likely to cause malfunction if the equipment is operated (energized) without first wiping it clean. Water falling on energized circuits will cause short-circuiting and

irreparable damage to those circuits that get wet. Another undesirable aspect of leaving equipment energized during a fire is that internal ventilating fans will continue to operate and spread contaminants further within the equipment.

On the other hand, magnetic tapes and disks exposed to products of combustion and water are usually not permanently damaged. Data is usually salvageable by prompt cleaning and drying.

USING AN OVERALL RISK ANALYSIS APPROACH

The choices facing risk managers and facility planners considering the adequate protection of their data processing operations are complex. Whereas, in the past, one would opt for either automatic sprinkler protection or a gaseous extinguishing system, regardless of the equipment or building construction and design, today's approach is one of overall risk analysis. This is an integrated approach considering all relevant site-specific factors, including the values at risk (how much equipment and how

much of the building is expected to be damaged in a fire), construction, exposure from other areas or buildings, fire detection, smoke control, emergency response, equipment maintenance, and disaster recovery.

Duplication of records is a vital safeguard for data that is critical to the continuation of operations. Duplicate records may be stored at another properly protected location on your property or off premises. Alternative computer facilities may also be desirable for many operations. Such facilities may have compatible data processing systems in place; or they may simply provide a basic properly ventilated and wired building into which data processing equipment can be moved.

Once the risk analysis has been done, protection should consist of a combination of various safeguards, a discussion of which follows.

Construction – It is best to locate the computer center and associated media storage in a separate building of non-combustible construction, with adequate protection from any exposure from another nearby building, and adequate security measures to discourage unauthorized entry. If the computer room shares a building with other operations, it should be separated by a wall that has at least one-hour fire resistance and is smoke-tight.

Ventilation – Computer areas and records storage areas that share a building with other operations should have their own ventilation systems. Computer rooms should be at an air pressure slightly higher than adjacent areas in order to keep out damaging smoke and fumes. At existing locations, smoke detectors and smoke dampers should be arranged to keep smoke out of the computer room.

Research has shown that enough heat may be generated by faults in low-voltage wiring, such as signal wires, to generate damaging concentrations of combustion products and ignition of adjacent combustible material.



© 2005 Factory Mutual Insurance Company. Reprinted with permission. All rights reserved.

Power Supplies – Electrical power to computers and peripheral equipment should be designed with emergency shut off switches located next to the exit doors of the equipment room. Control, signal and power circuits should be installed in a manner to minimize the possibility of damage from fire, impact, abrasion, released liquids and other potential hazards. Backup power and emergency standby power should also be provided.

Occupancy – Occupancy conditions should not present a hazardous environment to computer systems. Preferably, keep paper supplies and records outside the rooms housing the computers and peripheral equipment. Also, limit the amount of furnishings in the computer room and ensure that any necessary furniture is non-combustible.

FIRE DETECTION

Smoke detection systems are a basic requirement for all computer and record storage areas. Where values are very high, high-sensitivity systems are recommended. Detection systems may serve multiple functions: activate alarms at an attended location; shut off the computers and peripheral equipment; activate a smoke removal system; and activate a fire suppression system (gaseous or sprinkler).

Detectors are spaced more closely in computer facilities than in other occupancies. One reason is that ventilation is normally quite strong in computer areas and tends to dilute the smoke quickly. Also, because of the damaging effects of even small quantities of products of combustion from burning or even

heated plastics, it is important that the detectors sense the faintest trace of smoke in the earliest stages of generation.

FIRE PROTECTION

For the computer room – A total flooding gaseous extinguishing system is recommended for computer rooms where other fire damage mitigation, such as subdividing equipment into different rooms, or providing smoke control systems, cannot be used to prevent a potentially costly loss. In some cases, discharging the agent directly in the equipment's enclosure is desirable. As with any gaseous agent, room construction should be tight to prevent any agent leakage out of the room. A smoke-activated gaseous extinguishing system is preferred over a heat-activated automatic sprinkler system because the latter is slow to activate.

Automatic sprinkler protection is desirable for all computer rooms. Gaseous extinguishing agents protect the high-value electronic equipment from damage, whereas sprinklers are needed to extinguish fires in ordinary combustible material or combustible construction materials in a computer room. Computer system equipment should be de-energized by a smoke detection system before sprinklers operate to avoid electrical damage.

For cable spaces – Fire protection for noncombustible spaces containing grouped cables should be provided. In particular, where loss potential from a fire involving combustible cables is high, a gaseous extinguishing system is recommended. The extent of the hazard presented by grouped cables is

best discussed with loss prevention consultants.

Manual protection – Portable extinguishers should be provided at clearly marked locations in computer rooms and related service areas. Select carbon dioxide extinguishers when purchasing new units. Water-type extinguishers will also be needed, as well as fire hose lines where there are quantities of ordinary combustible material.

Human Element – Your emergency organization is a key component in the overall protection scheme. Personnel should be trained to take the correct steps without delay at times of emergency, such as shutting off power; using portable extinguishers on incipient fires; ensuring extinguishing and detection systems are operating; and notifying the fire department and designated facility personnel of the location and scale of the incident.

Having a salvage plan in place for immediately after an incident has occurred is also a very important concern. After a fire, employees should take appropriate action to minimize exposure of data processing systems to smoke and water. Cover equipment; remove portable equipment; install fans and dehumidifiers; and de-energize equipment. Where a gaseous extinguishing system is operating, personnel should be sure the protected area remains closed to confine the agent.

A disaster recovery plan is vital where computer operations are critical to an organization's survival. A major component of such a plan would be arrangements made with a restoration specialist who should be on the scene within hours to take appropriate damage-limiting action. Prompt cleaning and decontamination can restore equipment in a cost-effective manner and help return data processing equipment to normal operation.

Implementing Overall Risk Analysis

As the dependency on computer systems for business continuity grows, it's to your advantage to have a keen understanding of the particular risks that are specific to a computer room and the practical steps you can take to mitigate these risks. By taking these steps, you can significantly reduce the chances of a serious fire and the consequential costly interruption to your business operations.