Taking a planned approach to data centre fire prevention

As denser, hotter data centres become the norm, a structured fire prevention plan will save time and money, reports Amelia Kwok

FIRE PREVENTION IS ONE OF the most neglected areas of data centre planning, but attitudes may be changing as more IT professionals become aware of the enormous risks posed to the business by fire.

"Seventy-two per cent of mission-critical applications experience nine hours of downtime per year," says George Gan, Marketing Director for Asia Pacific at fire prevention and security firm Xtralis.

An estimated cost per hour of downtime for a financial brokerage house is US$6.5 million. "Of the companies that experience a disaster but have no tested business recovery plans in place, only one in 10 are still in business two years later," says Gan.

All damage still depends on the extent of the fire, says Tim Hawthorne, fire protection specialist at the National Fire Protection Association (NFPA), an international non-profit organisation. "It could range from interruption of service provided by the data centre, to costly network shutdown and replacement of all components."

"Although there have never been any fire breaking out in our bank's data centre for the past 30 years, such an occurrence would have catastrophic effects on the Bank's day-to-day operations," says Clarito Magsino, CEO of the Development Bank of the Philippines (DBP) Data Centre Inc (DCI). All online systems would be down and would take at least a few hours to restore. In the meantime all branches will operate on manual mode, he elaborates.

A study done by the NFPA has shown that the majority of fires originating within data centres are Class C fires involving electrical distribution equipment. The typical fire types found within data centres are termed Class A and C fires, says the NFPA. Class A fires involve ordinary combustibles, such as wood, paper and cloth, while Class C fires involve energised electrical equipment.

Electricity is the main ignition source causing fires within data centres. Even electrical equipment installed in accordance with all applicable standards can still experience failure modes that potentially result in ignition, says the NFPA.

Other factors that have fuelled fires in data centres include the accumulation of under-floor combustible materials such as unused wiring insulation and connections, paper storage and supplies within data centre space, improper storage and maintenance of fuel for emergency generators, failure of personnel to adhere to stated guidelines and a lack of training, and fuel system pipes that leak.

INCREASED FIRE RISK

"A notable trend within the IT industry is a decrease in floor space and an increase in more compact and powerful computer systems," says Hawthorne at the NFPA. More heat is generated and it increases the number of potential ignition sources, which also heightens the possibility of a fire development.

This poses some difficulties in protecting data centres against fire and its products of combustion, since equipment and electrical cabling are more densely grouped together, says Hawthorne.

The fire risk within today's data centre has been largely amplified due to the heat density that is growing at an unprecedented rate.

High-density data centres present three special challenges. Firstly, in-rack cooling requires more cooling infrastructure, which may conflict with other equipment; Secondly, higher power calls for more wiring, resulting in a more constricted underfloor space. Lastly, the combination of higher power, more cooling equipment and more equipment per square foot means more opportunities for failure. Under certain conditions, overheating may result, increasing the fire risk. John Eager, senior associate in the critical facilities group of Syska Hennessy Group in the US points out that it is important to use an integrated design approach to the mechanical, electrical, plumbing and fire protection systems in data centres.

Clarito Magsino, CEO of the Development Bank of the Philippines (DBP) Data Centre Inc (DCI)

Finally, it is important to invest in staff training. Some facilities have 24/7 technical personnel on site, who must be properly trained to respond to a fire event, especially when employing a high sensitivity smoke detection system that allows for discretionary intervention.

THE PLANNED APPROACH

"When assessing and evaluating the damage and interruption potential of the loss of information technology equipment room operations, attention shall be given to the impact of the loss of data and communications lines," says Hawthorne. The steps include:

Setting the uptime

In planning and designing a fire protection system, the facility owner must first determine the level of uptime or data availability required, says Eager. The reliability level, be it 99.99 or 99.9 per cent will be a major determinant in the design and costs of the fire protection system.

Allocating space

Another important consideration is space planning. "Ideally, the data centre will be a maximum of two stories high. Support areas, including those that will be staffed, should be physically separated from the data centre itself by fire-rated walls and ceilings to allow for installation of the most reliable fire protection system. Effective space planning also allows for future expansion with the least disruption to ongoing operations," says Eager.

"Within a data centre, the type of smoke generated and the dynamics of the airflow create a challenge for the fire engineer to design an effective fire detection system," says Gan at Xtralis.

In fact, according to the USA Federal Commission of Communications, 95 per cent of all damage caused by fire in a data centre is non-thermal. The by-products of smoke from PVC and digital circuit boards produce gases that will cause corrosion of IT equipment.

Using the right technology

Critical facilities require a highly sensitive smoke detection system that captures air from various points in the space and sends it through to the sensor. It is the detection of smoke that is the most critical part of the fire protection system. This notifies building operators before the suppression system goes off, giving them time to locate the source of the smoke and determine the event warrants release of the fire suppression system and notification of the fire department, or whether it can be handled simply by powering off a piece of equipment or using a hand-held fire extinguisher. Thus, early detection can effectively reduce down-time, damage and the cost of re-arming the suppression system.

Smoke detectors are either ionisation or photoelectric. Ionisation smoke detectors respond quicker to flaming fires or flammable liquid as they are reactive to relatively smaller particles. Photoelectric smoke detectors, on the other hand, can sense large particles and react to fires which produce little smoke or no flame.

In addition to these two operating principles, there are also two categories of smoke detectors which differentiate in terms of response time, namely the early-warning smoke detectors (EWSD) and very-early warning smoke detectors (VEWSD). The EWSDs belong to the traditional ceiling-mounted, spot-type detectors of an ionisation or photoelectric type while the VEWSDs function by air-sampling. In these two instances, the air-sampling system is recommended by the NFPA as the system constantly evaluates the air from multiple points throughout the environment.

According to Edward Fixen at Schirmer Engineering Corporation, "Air-sampling systems provide very early warning by detecting smoke particles in the incipient stage of a fire. The system can be provided with multiple alarm points ranging from 0.0015 per cent to 6 per cent per feet, allowing it to be used within clean, dusty, dirty or smoky environments. VESDA is one of the more commonly used air-sampling smoke detection systems today. Due to its sensitivity, VESDA can reliably detect invisible levels of smoke and tolerate dilution from high airflows in the data centre. The detectors provide multiple levels of alarm which can be used to scale a response appropriate to the reported risk and so reduce the cost of nuisance alarms."

COPING WITH THE AFTERMATH

Magsino cautions that there are no sure-fire ways to evading the consequences of fire in a data centre. "What I foresee is that any occurrence of a fire within the data centre itself would trigger the fire suppression systems which in turn would put out the fire but damage the machines. So it would cause a minor inconvenience by disrupting operations for the few hours it takes for the systems to be up and running at the secondary off-site data centre. It would also cause a major disruption because of the time it would take to replace the damaged equipment inside the data centre and restore normal operations," he says.

While there are no fool-proof methods, it is still vital to incorporate fire protection methods. Magsino lists the three fire prevention and protection methods that the DCI uses. They are the FM-200 Fire Suppression System, Dry Chemical Fire Extinguisher Type DC and Halotron Fire Extinguisher Type HCFC.

The FM-200 Fire Suppression System curbs fire by discharging as a gas onto the surface of combusting materials; large amounts of heat energy are absorbed from the surface of the burning material, lowering its temperature below the ignition point. The Dry Chemical Fire Extinguisher is powder-based and the Halotron Fire Extinguisher discharges rapidly evaporating liquid.