RIMS the risk management society

RISK PERSPECTIVE

Sponsored Content by:

TÜV SÜD Global Risk Consultants®

Protecting Critical Electronic Equipment from Fire

Almost every aspect of business today is powered by electronic equipment, from data center servers to telephone equipment/network rooms to process control systems. Although this equipment often works behind the scenes and is out of sight from the everyday consumer, businesses recognize that protecting such technology is a critical part of operations and key to business continuity and loss control efforts.

Reasons compelling organizations to adeptly manage fire exposures to electronic equipment continue to grow, and include:

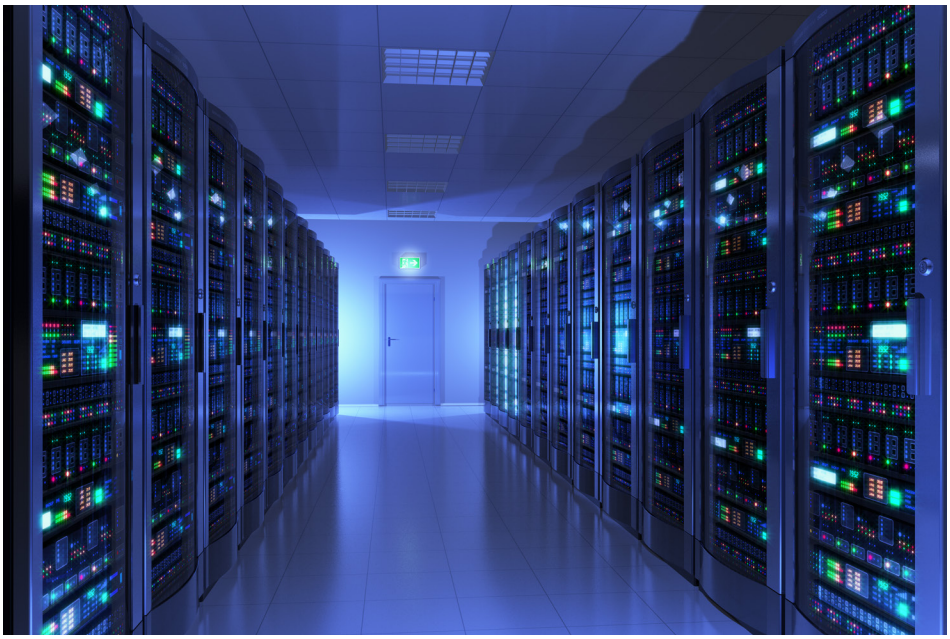
- Increased regulatory activity
- Higher levels of public scrutiny
- Greater demands for aggressive environmental liability management
- Stricter insurance requirements
- New technological advances for processing and warehousing

For over 60 years, engineers at TÜV SÜD Global Risk Consultants have been helping pioneer advances in fire protection by developing new methods to address today's escalating concerns and ensure the health and welfare of businesses around the world.

Electronic data processing equipment is ubiquitous; all industries are dependent on it and, therefore, have exposure to its loss. With so much of an organization's operational capabilities dependent upon interconnected electronic devices, a fire involving electronic data processing equipment can result in significant property damage and an even larger business interruption loss. As such, it is vital that businesses understand how to cost-effectively protect critical electronic equipment to prevent a disaster.

Understanding the Risks

Before we can even discuss how to protect an organization's electrical equipment, we must first analyze some of the risks the modern business environment poses to such equipment. Advances in technology and the emergence and popularity of cloud-based systems have transformed the traditional data center at most facilities. In many cases, on-site data centers and electrical equipment rooms consist solely of small "communication closets" that connect the site to the cloud or a corporate data center.



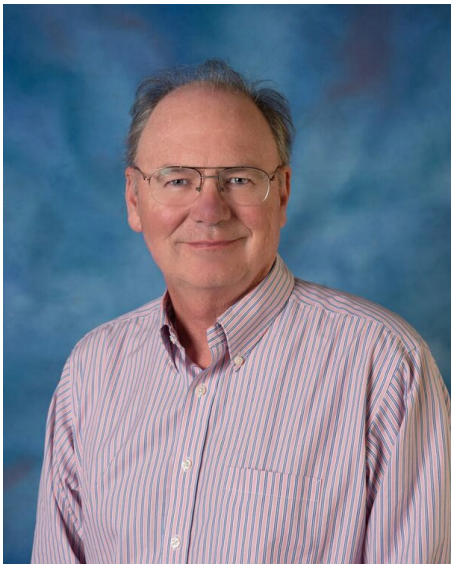
In other cases, the rooms themselves are the same size, but the footprint of the equipment required has been greatly reduced. Where server rooms were once filled with critical equipment, now many have become metaphorical "junk drawers" containing all types of items, including some that may be combustible. Essentially, while the amount of equipment in these "communication closets" has shrunk, the risks associated with them have not.

"We have large amounts of extra space in those rooms now," said Charles Macaulay, Chief Engineer for TÜV SÜD Global Risk Consultants. "Whenever we see extra space, we like to use it. We put desks in there and store supplies in there. But, we also have equipment necessary to operations in there. This equipment is critical, and where before we protected it, now there's exposure. So, there's a higher probability of loss for the business because of that."

Often, the go-to solution to prevent disasters is fire sprinklers or gaseous fire suppression systems. These systems are typically required by building codes and insurers and, while they are certainly important, they can pose their own set of risks. The key point to remember is that these are fire *suppression,* not fire *prevention,* systems—once sprinklers are activated, a business already has a very serious situation on its hands, and the damage to critical equipment is going to be severe. "If the sprinklers are activated, it's already too late," Macaulay explained. "We need to look at things *before* the sprinklers are activated."

Sprinklers can also give an organization a false sense of security that they have effectively addressed the risk. "Just because a smoke detection device sensed that a fire and gas was discharged, your problems aren't over yet," he said. "There are still many things to do. And if you're not careful, the situation will end up being worse than when it first started."

One of the most important decisions is whether to leave critical equipment powered



Charles Macaulay
Chief Engineer
TÜV SÜD Global Risk Consultants

up when a fire is detected. Critical data centers or electronic equipment rooms are typically set up to run at all times, but if this equipment is not depowered when smoke or fire is detected and fire suppression systems are discharged, additional problems can arise. Macaulay explained that when the extinguishing gas is eventually removed from the room, the fire is very likely to reignite and may be even hotter and more aggressive than before as arcing continues with the energized equipment. Response plans for such scenarios need to take this possibility into account and provide the necessary resources for personnel to locate the problem before the gas concentration is reduced and the fire restarts.

On the other hand, if the equipment is powered down when gas is discharged, it will have already cooled before personnel can enter, and even an infrared camera may not be able to help locate the problematic equipment. Essentially, according to Macaulay, you have taken care of the fire and minimized the damage, but still have no idea what went wrong. Although it may lengthen downtime, businesses in these situations will need to have protocols and procedures in place to start up equipment slowly to determine the source of the fire and ensure safety of personnel and the facility.

Three Keys to Protection

There are three main keys to protecting critical electronic equipment from fire: 1) good housekeeping, 2) effective detection and 3) well-trained response. Following these three tenets will help protect an organization against potentially devastating physical losses.

Good housekeeping: Furniture, paper and plastics will burn hotter and produce more smoke than a fire within electronic equipment. Allowing such extraneous, combustible materials in an organization's server or electrical equipment rooms is often the main culprit behind catastrophic losses from fire, smoke and soot damage. According to Macaulay, good housekeeping in the form of keeping rooms "scrupulously clean" and removing as many combustibles as practical is the primary way to limit the potential for fire damage in electronic equipment areas.

"If you look at third-party data centers, such as those owned by large e-commerce operations or IT organizations, their facilities are immaculate," Macaulay said. "It's good practice for all to do the same—and that includes your network closets."

Effective detection: Since fires within electronic equipment typically grow slowly, starting with component overheating, which leads to arcing and eventually an open flame, the use of highly sensitive smoke detection (HSSD) is imperative.

Smoke detection alerts an organization of a problem with electronic equipment long before there are open flames. It gives a business time to respond before there are hazards. While a business can find the piece of equipment that is sparking, smoking and flaring before it becomes a disaster, simply having a detection system in place with no protocol is not going to solve the problem.

"The goal of the people responding to the alarm is to locate the power supply, the overheated component, whatever is causing the detection system to go off, and then communicate with the IT people at the office and decide if they should pull the plug on the equipment or shut it down remotely," Macaulay explained. "All appropriate steps can be taken once you identify the piece of equipment. You can shut down one piece of equipment in one department instead of shutting down the entire operation."

Well-trained response: Good housekeeping, fire detection and even automatic extinguishing do not substitute for effective emergency response. A well-trained and well-equipped response team will be able to assess the scene, notify appropriate parties, investigate the source of the smoke or fire and isolate the equipment in question.

"It's all about personnel," Macaulay said. "The people responding to the alarm need to be equipped properly. When responding to an issue in a small room, it's easy to find the source of the issue. If there's only one rack, we can find it easily. But, in a larger network room, that could be much more difficult."

Macaulay pointed to the fact that most equipment within an electrical room looks alike—usually all black racks—so even if there is soot on a rack or other piece of equipment, it will not be detected easily. Spaces that house electrical equipment also usually have good ventilation and strong air flow, which makes it difficult to smell smoke.

"It's important that the people who respond to the alarm can take the information the alarm is giving them and then use additional equipment like an infrared camera or portable smoke sniffer to identify the equipment that is causing the problem," he added.

Given how much is at stake from an operational standpoint, plans for protecting important electronic equipment and data centers from fire hazards should incorporate more than just a few basic techniques. There should be a multi-step process in place to help ensure that the business can continue to run as smoothly as possible. "I think the biggest issue is that a lot of people have a false sense of security, especially at the local IT level," Macaulay concluded. "You have to protect IT equipment, but protection involves a lot more than extinguishing systems that will put out the fire for a short amount of time."

For more information, visit
www.tuvsud.com/grc