RISK INSIGHTS Technology

Packetts

Common Data Centre Hazards

Data centres are the heart of most businesses—they are the central channel for any data moving in or out. Any organisation that creates or uses digital data has a need for a data centre. Despite the widespread need for data centres, there are several common data centre hazards that repeatedly ruin businesses. By protecting your business against these common hazards, you can help ensure your business' future success.

The Common Hazards

Although security incidents may be infrequent in a data centre, the consequences are huge. The infrequent nature of the incidents can make employees adopt a lax approach to common, easily preventable risks. Keep your data centre safe by defending against the following hazards:

- **Failure of the Security Server** – If your security server fails, you will lose card access management, the ability to change authorisation levels, access to Web-based applications, control of doors and video camera connection and the ability to verify card holder identity. To prevent security server failure, install cluster software on multiple servers—cluster software allows multiple servers to run simultaneously by mimicking the data on the other servers. It lets you protect and recover data in the event of a security server failure.

- **Undetected Smoke** – Data centre fires can be caused by power surges in the electrical system. Smoke can only be detected by smell in the early stages of a fire. By the time the smoke becomes noticeable, damage has already occurred. Early detection is therefore crucial to minimising fire damage. By installing an aspirating smoke detector (ASD), you can catch a fire in the early stages, before the smoke is noticeable. An ASD is comprised of tubes that follow the same path that smoke would take through the air conditioning system. The tubes collect air samples and deposit them in a central testing chamber. Once there, the samples are tested for smoke levels.

Although security incidents may be infrequent in a data centre, the consequences are huge. The infrequent nature of the incidents can make employees adopt a lax approach to common, easily preventable risks.

- **Ineffective Personnel Monitoring** – Due to the size of data centres, it can be difficult to effectively track personnel. You can solve this problem by providing each employee with a real-time location system device (RTLS) to track his or her location at all times. The RTLS sends identification data to a monitoring station if an employee enters a high-security area. The system has the capabilities to interact with the surveillance system and the access control system to provide further security.

- **Threat to High-authorisation Personnel** – When personnel with high-authorisation levels are at risk, the data centre assets may be placed at risk as well. However, if personnel are provided with wireless emergency alarm systems, they can send alarms to the security department in an emergency.

Common Data Centre Hazards

- **Ineffective Alert System** – There is potential for human error when multiple alerts are sent out, depending on the risk, location and personnel. By using mass notification systems, also known as Life Safety Systems, it is possible to send out mass notifications in real time. The messages can be issued through audio, video or email and can provide the correct response to the incident.

- **Lost Key Cards** – Losing key cards is surprisingly easy—and monitoring key card use can be deceptively difficult. By storing key cards in cabinets that allow designated employees access via keypad, card swipe or biometric scanning, you can eliminate human error and unauthorised key card use. Equipping key cards with a real-time identification tag helps record card usage and curb illegal card use.

- **Unfavourable Microenvironments** – Equipment failure may occur if environmental conditions surrounding the machinery are subpar. It can become difficult to monitor the environment surrounding each machine due to the large size of the data centre. However, it is possible to take real-time tests of temperature, humidity, voltage and power sources by installing machine cabinet monitoring systems. The system sounds an alarm if the environment drops to an unfavourable state.

- **Failed Network Connection** – Modification to system networks is responsible for 80 per cent of network connection failures, according to industry reports. Of the total amount of time spent attempting a recovery, 90 per cent of the time is spent on diagnostics, while 10 per cent is spent on the resolution. By installing a smart patch panel system, users can control all of the links used in a network. They can mark certain links as confidential and sound an alarm in the event of an illegal connection or broken connection.

- **Hackers** – Hackers are an external security threat. By combining a physical access management system with a digital log-in system, only individuals with access will be able to log in to the server.

- **Faulty Inventory Management** – When employees perform data inventory, they may accidentally lose some data. By providing employees with a Radio Frequency Identification Asset Management system, the equipment is immediately identified.

The Warning Signs

There are several warning signs that can alert you to the likelihood of a hazard occurring in your data centre. Watch for the following signs to determine your risk:

- Outdated diagrams of equipment configuration
- Outdated diagrams of physical wiring
- Neglected charging of uninterrupted power supply batteries
- Neglected testing of fuel levels and the generator
- Inadequate testing of the backup generator
- Neglected testing of the annunciator system
- Failure to recharge the fire suppression system
- Failure to test the emergency power-off system
- Failure to document the emergency power-off system
- Inadequate routine air conditioning system maintenance
- Improper anchoring of equipment
- Inadequate documentation of evacuation procedures
- Failure to follow physical security procedures
- Inadequate training for personnel

Preventive maintenance and risk awareness can protect the heart of your business—your data centre. Implement proactive measures and routine testing to stay protected.