Data Center Security

Major Risks

and

Recommended Solutions

www.icdsecurity.com
**OVERVIEW**

Are you familiar with the main security risks that threaten data centers? This paper provides an overview of the most common and major risks that data center security teams. To help you combat each of these risks, we introduce the most effective solutions available in today’s market and explain how they can benefit daily operations at your data center.

Any one of the risks to your data center can have a considerable impact on any business. It is estimated by the USA Federal Communications Commission (FCC) that the cost of downtime at a large data center facility is greater than $2 million an hour.

Many security solutions available in today’s market not only deal with these risks but also help companies to improve the efficiency of security and business operations significantly.

The major risks are as follows:

1. Server failure
2. Undetected smoke that can lead to fire incidents
3. Ineffective monitoring of behavior of onsite individuals
4. Endangerment of high level management staff
5. Ineffective employee notification systems during emergencies
6. Inefficient management of data center keys
7. Equipment malfunctions in individual machine cabinets due to microenvironment conditions
8. Network connection failures
9. External hackers
10. Ineffective inventory management procedures

Read on to learn more about the latest solutions that will help you to secure your data center!
**RISK 1:**

**SECURITY SERVER FAILURE**

When data center servers fail, this creates significant disruptions to daily security operations. Security personnel are unable to manage card access, change authorization levels or verify card holder identity and they can not use any web-based applications. Access control doors and video cameras may lose their connection to the system during a server failure.

If the server stays down for too long, incident data from onsite system controllers cannot be uploaded in time, which may result in significant data losses.

**SOLUTION:**

**“CLUSTER” SOFTWARE INSTALLED ON MULTIPLE SERVERS**

“Cluster” software allows multiple servers to operate in coordination with one another by mirroring data from one server on another. In this way, data is protected and can be recovered immediately in the event of one server failure.

This solution helps security teams to mitigate losses caused by natural or man-made disasters. Cluster software also allows continuous operation by switching seamlessly between servers, which allows security teams to minimize system down time while server maintenance is performed.
**RISK 2:**

**UNDETECTED SMOKE**

Fire incidents in data centers are often caused by power surges in the electric apparatus. In the early stages of a fire incident the resulting smoke may be detectable by smell but is often too fine and in too small a quantity to be detected by standard smoke alarms, let alone the human eye.

Circulation through air conditioning systems may also cause the smoke in the room to become even more dispersed, which reduces the effectiveness of smoke detectors even further. By the time a fire incident is critical enough to activate the fire safety system, disruptions to operations and damage to equipment are often unavoidable.

**SOLUTION:**

**VERY EARLY SMOKE DETECTION SYSTEM**

“Very early smoke detection systems” or aspirating smoke detector (ASD) systems detect smoke in a facility at a very early stage by installing a “sampling pipe” that follows the path that smoke would be carried by an air conditioning system.

Capillary tubes on this pipe capture air samples and transport them to a central testing chamber. In this chamber, dust and other large particles are filtered out of the air and the level of smoke particles in the air is tested using a sophisticated laser detection mechanism. This data is then transmitted to a notification system that alerts users when smoke particle levels indicate an imminent fire incident.

ASP systems are therefore able to detect smoke in a matter of seconds, allowing end users to prevent fires and related damages to equipment much more easily. What is more, unlike traditional smoke detectors, ASP systems also feature a self-monitoring function which allows the system to notify users if it is incapable of performing smoke detection operations.
RISK 3:

INEFFECTIVE MONITORING OF INDIVIDUALS IN DATA CENTER AREA

A single computer room in a data center typically covers a fairly large area, with most pieces of apparatus arranged next to each other. It is common for each of these pieces of apparatus to be managed by separate personnel. For this reason, it is difficult to perform detailed tracking and management of personnel once they have been granted access to the area.

SOLUTION:

REAL TIME LOCATION SYSTEM

With real time location systems (RTLS), each employee is required to carry a wireless location marker device. Sentry devices are installed at major paths of entry and within the computer rooms of the data center. When the employee enters a sensitive area, the marker sends identification data to an electronic monitoring station, which enables location tracking software to record ID number of the employee as well as the time that they entered the sensitive area.

Moreover, real time location systems are capable of interfacing with video surveillance systems and access control systems. This allows security staff to monitor all activity within the data center with greater efficiency by collecting and integrating data from all three systems.
RTLTS systems offer the following functions:

- Effective and continuous monitoring of each employee’s location; notifications when an employee enters a restricted zone

- Security staff in separate locations can conduct remote site management effectively by tracking and monitoring all employees entering and exiting the data center.

- A variety of checking mechanisms and ways to monitor employee activity, including employee real time location, employee data by area, record checks by name, position, gender and other key search terms, and record checks according to a set time frame.

- Monitoring of employee movement trajectories using a virtual site map
- Interfacing capabilities with video monitoring systems that allow staff to retrieve a visual image of the tracked individual at any time

- 3D electronic maps with switch, zoom and roaming functions
- Role-based authorization management mechanisms, displaying different information to different employees according to their level.
**RISK 4:**

**ENDANGERMENT OF HIGH LEVEL MANAGEMENT STAFF**

If data center personnel with high authorization levels are endangered any way, this can put the safety of all assets at the data center at risk. One of the most important security objectives for a data center is to monitor the safety of high level personnel and respond immediately if their safety is compromised.

**SOLUTION:**

**EMERGENCY ALARM SYSTEM**

With emergency alarm systems, high level management personnel are equipped with wireless emergency alarm apparatus that send an emergency alarm signal that can notify security guard staff to enact any necessary measures.
RISK 5:

INEFFECTIVE ALERT NOTIFICATION PROCEDURES DURING SECURITY INCIDENTS

During an emergency, it is often necessary to send out a variety of warnings to different individuals according to their role, location or risk level.

In these scenarios it is crucial to deliver relevant information to the target group of people using the fastest, most efficient method necessary. If this work is left to individual employees, the scope for error makes it difficult to avoid losses to assets and even of lives.

SOLUTION:

MASS NOTIFICATION SYSTEM

Mass notification systems (also known as life safety systems) are an effective way to notify and protect individuals.

In the event of a security incident, mass notification systems can send real time information to occupants of office towers, or specific areas within the building premises via an audio or video message, SMS or email to encourage the correct incident response by all those affected.
**RISK 6:**

**DATA CENTER KEY LOSS**

The number of doors and lock-controlled machines in a data center necessitates a large number of keys. If management of these keys is conducted by individual employees, it is difficult to do so systematically and effectively. Even with dedicated personnel, it is difficult to keep track of which individuals are authorized to use what keys, or what the intended use of each key is.

What is more, in many data centers, it is still typical to keep records using pen and paper, which makes it difficult for security staff to maintain clear records. In the event of a security incident, it is necessary to go over these records line by line, which is a highly inefficient use of time. Using paper records, it is also difficult for managers to monitor key usage and whereabouts in real time. In this situation, it is easy to lose keys due to human error.

**SOLUTION:**

**KEY MANAGEMENT SYSTEM**

Using key management systems, data center keys are stored in dedicated key cabinets that are resistant to break-ins. Access to keys is granted automatically using a keypad, swipe card or biometric scanner, eliminating the need for dedicated personnel. The system also keeps detailed records of all retrieved keys (including time and date used, key number, user photo etc.)

This system also includes a complete security alarm mechanism that instantly sends an alarm notification to the relevant personnel or department in the event of a malfunction, incorrect operation, authorization violation, or forced breach.

The system completely eliminates the risk of loss due to human error or flawed management and allows management personnel to track key locations and usage in real time via an RFID tag on each key. Key use authorization can also be adjusted by the security team at any time. In the event of a security incident, the system can generate a highly detailed and accurate report of key usage during the time of the incident and reduce the scope of a security investigation considerably.

Lastly and most importantly, integrating a key management system with the access control system prevents individuals from taking keys and making illegal copies.
RISK 7:

MACHINE CABINET MICROENVIRONMENT DETERIORATION

In a data center computer room, equipment malfunctions are often due to conditions in the physical microenvironment surrounding individual machines, such as sub-optimal temperature, humidity levels and other factors.

Traditional environment monitoring systems tend to focus on an entire room and are unable to detect the environmental conditions that lead to the malfunction of individual piece of equipment.

SOLUTION:

MACHINE CABINET MONITORING SYSTEM

Machine cabinet monitoring systems perform real time tests of the temperature, humidity level, electric voltage, current and power source operational status in the environment immediately surrounding individual machine cabinets. These systems also feature sensors that monitor smoke levels, cabinet door status, nearby trespassers etc.

If conditions are below optimum levels, alarm notifications are sent to the relevant personnel in advance to help them make appropriate adjustments to the environment and prevent any potential damages or losses. Using a single IP address, the computer cabinet is also supported by a network of access monitoring systems, onsite LCD control systems, video image capture systems and anti-theft alarm systems.

All of this ensures that the critical pieces of apparatus in the computer room can operate continuously in optimum conditions in the safest possible environment.
RISK 8:

NETWORK CONNECTION FAILURES

Research indicates that 80% of system down time in data centers occurs during modifications to system networks. Moreover, in the event of a malfunction, 90% of the recovery process is spent on diagnostics and the remaining 10% is spent on recovery operations.

Information security relies to a large extent on the physical security of the system’s network links. It is therefore essential to protect the integrity of the system’s links and prevent illegal connections from external agents.

SOLUTION:

SMART PATCH PANEL SYSTEM

Smart patch panel systems allow users to control the structure of all links used in a network. Smart patch panels can monitor and control the functionality of a network and its individual components and ensure that links are properly maintained, networks are fully functional and all network connections are secure.

One of the biggest differences compared to traditional cabling systems is that smart patch systems are able easily to designate certain links as “confidential”, allowing the management software to assign network equipment to certain MAC addresses and ensure that only the designated equipment is permitted to interface with that connection.

If an illegal connection is made, or if a connection is broken, the system will issue an alarm notification. This function is far beyond the capability of traditional cabling systems and has a significant impact on the overall security of the system.

Smart patch systems are also able to integrate with other security systems, such as the surveillance system. For example, if a smart patch panel system registers a connection error, the surveillance system can supply a visual confirmation of the incident via a camera installed by the patch panel.
**RISK 9:**

**HACKERS**

In an age when companies are increasingly reliant on electronic data, security breaches due to external hackers a major source of vulnerability. While IT security has the biggest impact on protection from hackers, physical security systems can also play a role in defending organizations from external attacks.

**SOLUTION:**

**INTEGRATE PHYSICAL ACCESS MANAGEMENT AND LOGIN SYSTEMS**

Integrating the physical access management system with the login information system ensures that only those who have been granted entry to the computer room via the access control system are permitted to log in to the server.
RISK 10:

INEFFECTIVE INVENTORY MANAGEMENT

Keeping an inventory of data center hardware is typically done by employees, either by scanning equipment serial codes or other methods. In this situation, employee workload is increased and errors are common.

Employees are required to complete inspections of equipment throughout the data center and keep detailed records in a database. The workload and risk involved in managing movable IT assets is particularly high. Loss of data tapes for example, is one of the biggest headaches for data center managers.

SOLUTION:

RFID ASSET MANAGEMENT SYSTEM

With RFID technology, employees need only carry an RFID reader device as they conduct their inspection and they can immediately identify which equipment is situated in what location, and whether any equipment is missing. This technology can also improve the accuracy of inventory records.

Inventory accuracy is an especially sensitive issue for financial service sector companies and any other company that needs to conduct regular audits to ensure the safety of their IT infrastructure equipment. If a bank were unable to locate its server for example, the impact on their business would be critical.

IT managers of leased hardware enjoy significant benefits from RFID asset management systems, as they are able to determine which equipment items are in use, and which are idle in order to control costs more effectively.

Furthermore, RFID readers can be installed by data center entry points and can send notifications if any hardware is taken away from the data center.
OTHER SYSTEMS TO CONSIDER:

- Face recognition system
- Video analytics
- Anti terrorist apparatus
- Security inspection equipment

GOT ANY OTHER QUESTIONS?
CLICK HERE TO CONTACT US THROUGH OUR WEBSITE!

www.icdsecurity.com