www.mayflex.com

White Paper

How IP Security is used within a data centre

Infrastructure.
Networking.
Electronic Security.

All together.

MAYFLEX
A Sonepar Company

+ Introduction.

In this article we introduce the concepts and technologies to consider when deploying physical security in a data centre. The latest IP based security devices coming onto the market have enabled security practitioners to deploy both IT and physical security onto converged IP platforms. This article looks at the considerations when designing a physical security system, and how IP technologies can be deployed to remove threats and improve site operational management of staff, visitors and contractors.

+ Communication.

In the modern world data centre administrators and security professionals face significant challenges. This is because they need to design a secure facility, which negates all possible risks whilst also ensuring the design does not compromise the functionality of the data centre.

Traditional security approaches and technologies are limited in a data centre environment as they are typically installed as standalone systems and focus primarily on perimeter threat detection.

Data centre security is different. To truly protect the modern data centre an organisation must deploy both the latest technologies alongside an integrated security system that provide control and integration with other systems through software based video and access control management systems.

+ Designing a security strategy using the latest IP technologies.

There is a need for a more comprehensive and integrated security approach with data centres than other sites and the new security technologies enable a high level of convergence when designing a physical security system. The overall security strategy will typically include the following components:

1. Consideration of security and compliance objectives.
2. Developing Security controls for each component of the data centre security system.
3. Design of standard operating procedures across all the systems such as security, HR, payroll.
4. Full site auditing and visitor management.
5. Security systems that are not standalone but are fully integrated with other systems.
6. Security technologies that provide the benefits of convergence such as virtualization, scalability and redundancy.
7. An integrated site command control philosophy through the use of Video management software and enterprise level Access control systems.

+ Physical Considerations.

An integrated security approach can be achieved when based on the latest security technologies which integrate with the other systems to provide protection at the site command control level.

Some of these applications of new technologies include:

+ Fencing around the site which has IP addressable sensors placed on it to alert attacks.
+ Video analytics overlaid on perimeter and entrance cameras.
+ IP based Access control and badge readers at each access point which enable automatic authentication over the network for employees.
+ IP-CCTV cameras to monitor parking, perimeter areas and neighbouring properties.
+ Key entrances should have a mantrap, security kiosk, and physical barriers with all access monitored on an IP based ACS which provides audit information
+ CCTV to monitor each person entering a facility linked via the network to biometric parameters.
+ Security kiosks equipped with network access to the badge database to verify badge identification with pictures of each user and their badge.
+ Computer Rooms must be monitored by CCTV and have redundant access to Power, cooling, and networks.
+ IP cameras powered using PoE to ensure increased up time
+ Offsite Backup - there must be regular automatic

+ IP Security Applications

In addition to the core security elements described above there are a number of other effective applications of IP security technologies such as:

Video Analytics

The introduction of IP based CCTV cameras has provided security system designers with a host of new features on these digital devices. One such application is video analytics.

Video analytics can be used to detect a number of security threats and automatically alert on events such as: bag unattended, trip wires, and unusual behaviour, tail-gating and perimeter breaches.

In addition to these alerts there are also a number of useful applications for business and operations such as: people counting, heat mapping, energy control and virtual zones.

Lone worker safety

Data centres present areas of greater risk to staff and visitors, such as server and communication rooms which typically have high voltages, trip hazards, confined spaces and by nature are isolated areas where a staff member is working alone, often at unsociable hours.

IP cameras should cover all areas to help management avoid incidents and to comply with duty of care responsibilities such as the use of video analytics to identify a man down situation.

Rogue workers

The issues of ex-employees and rogue contractors presents problems. Solutions include the use of IP CCTV integrated with networked access control to combat bad practices such as password sharing and theft.

When considering ex-employees, vendors or contractors, the broader message should be that insider threats are not limited to your current employees. Internal security has to be secure and should apply across the organisation and to those who have left the business.

Auditing - Time line traceability

The use of technology to help security staff manage a site, control access and provide audit trails is an imperative for compliance.

IP centric products lend themselves to enabling security teams to cross check on employees and visitors regarding badge and site access. All entrances, exits and sensitive areas must be monitored so that security can keep track of who was where and when. Which also helps with building evacuation if there's an incident.

Rack and aisle security

Consideration of camera viewing angles and positioning to ensure you achieve full coverage is an imperative in computer rooms. Using technologies such as 360 degree cameras will provide no blind spots and ensures total situational awareness. Networkable IP cameras can be used from the control desk to the rack to help facilitate access to a given location, once a visual check has been performed when an associate or contractor physically reaches a hall location.

Following an incident footage can be correlated with the access control database to provide the security team with history that allows for easy retrospective reviewing of events.

+ Conclusion

A company's Data Centre is one of the most important assets to a business as it often at the heart of the organisations operations. This means that a security director or CIO cannot afford to have the data centre compromised. A security policy must be developed and implemented that is embedded and holistic – built across IP networks, virtualization, mobility and the cloud.

When building a new facility, IP based physical security should be considered as part of an end to end security strategy. The security team should be involved from day one and the latest IP based technologies should be deployed to ensure a fully integrated security solution that includes redundancy and resilience on converged networks which ensure the site is safe and secure for employees and visitors alike.

www.mayflex.com

Mayflex UK
Excel House
Junction Six Industrial Park
Electric Avenue
Birmingham B6 7JJ
United Kingdom

Tel +44 (0)121 326 7557
Email sales@mayflex.com
Website www.mayflex.com

Mayflex MEA DMCC
PO Box 293695
Office 11A, Gold Tower
Jumeirah Lakes Towers
Dubai
United Arab Emirates
Tel +971 4 421 4352
Email mesales@mayflex.com
Website www.mayflex.com

Certificate No. FS 547274 Certificate No. EMS 542863

All together.

Printed on paper made from 75% recycled fibres.

MF1079_09/18

MAYFLEX
A Sonepar Company