Securing a data centre

Why a specialist security approach is a project imperative

data centres, security design, CPTED, security risk analysis

By Dr Maher Magrabi

Data centre security can be defined as the operational practices and technologies that are employed to safeguard the data centre from external threats and vulnerabilities. The growth of Cloud Computing, Software as a Service, and Platforms as a Service has driven the growth of physical data centres. Being a physical asset, on-shore data centres are also a critical component in national infrastructure. Data centres are the physical facility that houses Information Technology (IT) infrastructure comprising computing, storage, networking, and power resources. As these data centres store sensitive and/or proprietary information that may include customer data and valuable intellectual property, cyber and physical security is paramount to its operation. This article will focus on the physical elements of data centre security.

Risk context

The first step to good security design is to develop a definition of the risk context through a comprehensive security risk assessment. This process engages the stakeholders and creates a sound basis for the deployment of security measures to mitigate the risk and to understand any residual risks that will rely on operational procedures.

Designing out crime

Crime Prevention Through Environmental Design (CPTED) refers to a methodology that employs four principles.

- **Surveillance**: increasing surveillance through eliminating blind corners and strategic lighting,
- **Access Control**: managing vehicular and pedestrian access through architectural features, security barriers and electronic access control systems,
- **Territorial Reinforcement**: establishing territorial reinforcement through signage, lighting, and fencing, and
- **Maintenance**: introducing ongoing maintenance and operational regimes in order to reduce the incidence of crime or minimise the risk exposure if an incident does occur.

The early application of these principles provides valuable input to the architectural and services design team and often prevents having to apply expensive security measures at a later stage.

Beyond CCTV and EAC

Traditional approaches to building security rely on the electrical consultant to add CCTV cameras and electronic access control across the entire premises. Without appreciating the risk context or the design intent, the roll-out of these systems is often done more as an exercise in security theatre rather than to achieve real security outcomes.

Holistic security

Security is a trade off, whether this is in terms of the economic cost or in terms of the operational latitude of the business. Risk driven security decisions that are applied as a mix of operational, hardware and electronic security are critical for assets such as data centres. The operational security consists of the security management functions, the regular procedures and routines, as well as emergency and incident management planning. Hardware security refers to the barriers that deter and delay forcible entry into the site and building including gates, fences, walls, doors and windows. Electronic security comprises the systems that detect unauthorised access or forcible entry and capture evidentiary information that can be used to investigate breaches and prosecute offenders.

Monitoring and control

There are various factors that warrant consideration where it relates to monitoring and control including parking, fencing, electronic access control, security gatehouse, security control room, vehicle and pedestrian access gates, loading dock access and usage, video surveillance and lighting. Intelligent design also recognises that these disparate systems can work in concert when specified correctly and integrated into one system that achieves security outcomes. For example, an attempted perimeter intrusion is detected by the intrusion detection system, but also triggers the security lighting system and the relevant cameras to track the intruder and provide the security staff with remedial options through the electronic access control system and duress alarms.

From Perimeter Security to the Rack Level

Traditionally, emphasis has been placed on perimeter security, gaining access to the site, the building and the server room. Once inside, there is often minimal security to prevent unauthorised access to data halls and enclosures. Extending the electronic access control system to the rack level with sufficiently granular access permissions to allow segregation and access control between authorised users provides for rack level access control.

Conclusions

Data Centres represent high value and specialised assets that require robust security which begins with the design of the facility and runs through all aspects of the physical building, the systems utilised, and the operational execution. A specialist security consultant is able to deliver the depth of design to realise the security objectives of data centres while working within operational and budgetary constraints.

LOTECONSULTING
Fire Safety I Security
Making the world safe and secure

security@loteconsulting.com