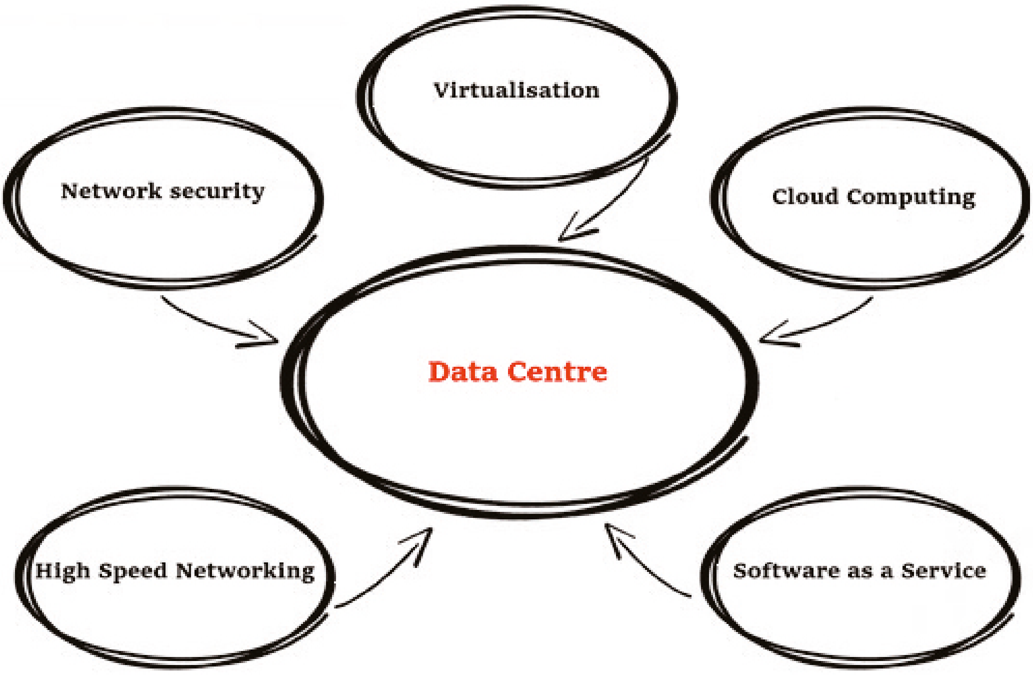
White Paper

THE CHANGING FACE OF 21st CENTURY DATA CENTRE SECURITY

On paper, physical perimeter security, just like cyber security looks pretty straightforward, but as we all know, by factoring in all the primary requirements, it becomes a complex task for security providers.

Jacksons Fencing

With over 23 billion IoT connected devices worldwide, UK data centre capacity is forecast to store data worth over £104bn annually by 2025 to cope with the ever growing reliance on secure electronic data transfer and storage, cloud based services and critical M2M connectivity. With land at a premium, data centre operators no longer have the luxury of cherry picking their sites and are increasingly forced to consider more densely populated locations, including residential areas.



This rise in demand for capacity has placed the architects, designers and construction firms responsible for their creation increasingly under the spotlight, not only to deliver projects quickly and efficiently, but also to reassure planners that the development for a business that operates 24 hours a day, 365 days a year, will not have a negative impact on local services and communities.

Noise, traffic and security

Would I want a data centre as a neighbour?

On the face of it, no.

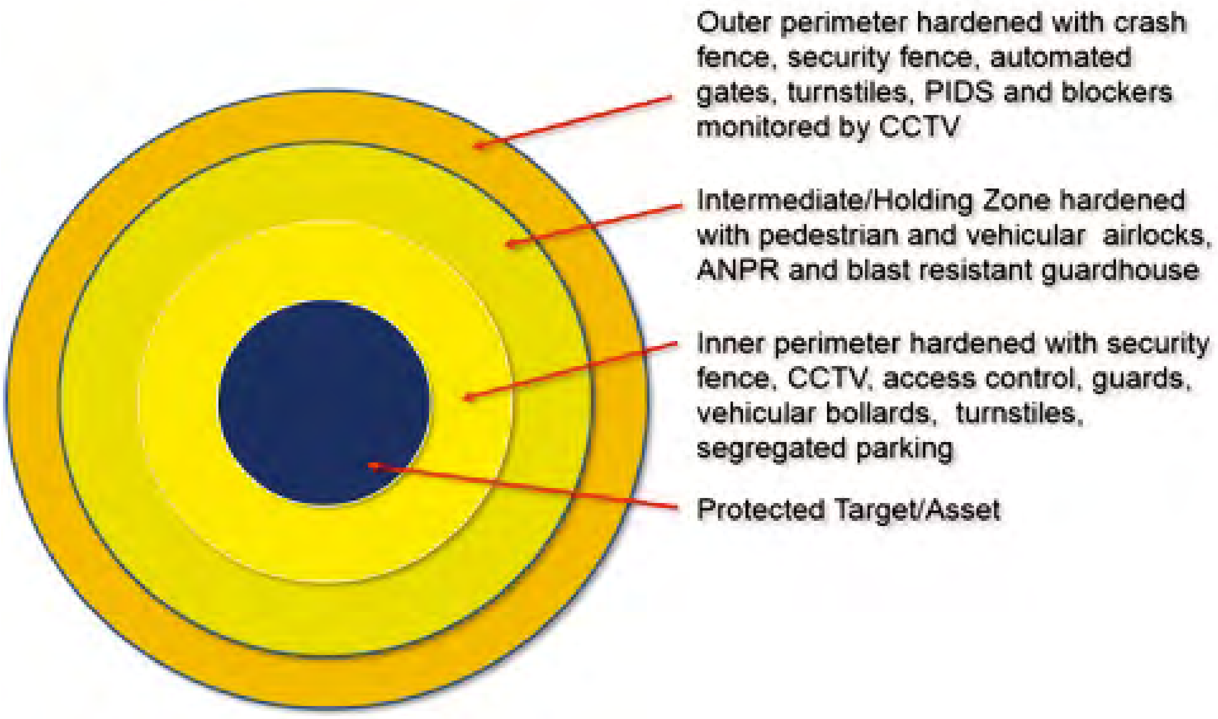
While it is relatively easy to contain noise migration from data halls, it's no secret that external noise created within a data centre site can be considerable, it is after all a business that never sleeps.

HVAC systems, event triggered security and fire alarms, HV Sub Stations, back-up generators and vehicle traffic don't usually make for good neighborly relations in built-up areas; neither do 4m high security fences with coils of razor wire topping and post mounted CCTV cameras and floodlighting blend easily into the landscape.

If you do get to the point where outline planning is granted, then the Risk and Threat Assessment stages which follow will ultimately bring you to a site design that works for your operation and is able to offer appropriate security against unauthorised access. It is at this point that a different set of challenges emerge; but it's also where new solutions can be brought to bear which would make a data centre a much more attractive neighbour.

Same security principles, different methods

The good news is that the principles and considerations we apply around the design of physical perimeter and key assets protection in and around a data centre through layered security levels and strategic target hardening is in many ways similar to those you already employ to the protection of your network, data, equipment and devices and many terms you use will have direct equivalents in the world of physical perimeter security - so, we're on familiar ground.


Outer perimeter hardened with crash fence, security fence, automated gates, turnstiles, PIDS and blockers monitored by CCTV
Intermediate/Holding Zone hardened with pedestrian and vehicular airlocks, ANPR and blast resistant guardhouse
Inner perimeter hardened with security fence, CCTV, access control, guards, vehicular bollards, turnstiles, segregated parking
Protected Target/Asset

Apply the 5 Ds of target hardening:

Data & Systems Protection	Perimeter Security & Access Control
System Perimeter	Site Perimeter
System Architecture	Site Plan
Ports	Pedestrian and Vehicle Access Points
Firewall	Perimeter fence
Virus	Unauthorised Visitor
Hacker	Intruder
Quarantine	Man/Vehicle Trap
Client Authentication	Verify identity at access and egress points
Monitoring & Reporting	CCTV
Intrusion Detection & Prevention	PIDS (Perimeter Intrusion Detection System)
Network Segmentation	Strategic zoned security hardening
Local Computer Policy	Hardened protection of individual assets
Security for DS systerms, Tier 1-4, Senior Cyber and Risk Assurance Board, ISO27001	LPS 1175 Certified Security Ratings, Secured by Design Pre-ferred Specification, NPSA (CPNI) Approved
Blocked Port	Static PAS 68 Bollards
Switch	Rising PAS 68 Road Blockers and Bollards
DMZ (Demilitarised Zone)	Stand off area between perimeter and assets
Security Protocol	5 Ds of perimeter security
Security Configuration	5D Security architecture
Administrative Tools	Security Control Centre
Scheduled Vulnerability Scan	Regular inspection of the fence line and access
Scheduled Updates/Patches	Maintenance of security fencing, gates, barriers and access control
Security Patches	Repairs to security fencing, gates, barriers and access control
Traffic Redirection/Port Forwarding	Temporary security measures while security fencing, gates, barriers and access control are being maintained or repaired
Core Protection	Target Hardening

On paper, physical perimeter security, just like cyber security looks pretty straightforward, but as we all know, by factoring in all the primary requirements including:

- The protection of the external perimeter against scaling over, burrowing under or cutting through
- Securing and controlling entrances for authorised staff, visitors, supply of goods, power, services and communications
- Prevention of vehicle borne attack
- Securing car parking and protecting the exterior of the data hall
- Protecting fuel storage, the HV substation, standby generators and HVAC systems
- Securing and controlling access to buildings
- Integrating lighting, surveillance and intrusion detection
- Localising security devices to operate independent of data centre system infrastructure

In practice, things become a little more complex; more so if you then need to overlay fencing and gates of a style which will provide the appropriate level of security and control without either:

- Advertising that they are protecting a valuable data centre
- Looking out of place in their surrounding environment
- Can offer some effect in mitigating the spread of noise and light from the site.

Smart solutions to complex challenges

Recognising that there would be continued increase in demand for land as the population rises and the services and infrastructure grows to serve them, we decided over 10 years ago to invest heavily in the R&D, testing, manufacture and certification of a variety of novel and effective perimeter fencing and gate systems which offer a 'smarter' solution than the generic mesh or palisade security systems widely available.

Our objective wasn't to underline how clever and capable the company is, but to change the physical security landscape and arrive at effective and sustainable solutions to 21st Century challenges, where people, transport networks, commerce and industry will need to coexist in ever closer proximity.

Since then, we have proven through LPS1175 certification and NPSA (CPNI) approval, that it is possible to combine high security performance and up to 32 db noise reduction capabilities within one fencing system. We have proven that it is possible to employ timber and steel to great effect in a high security fence design with a reduced carbon footprint and we have proven that a high security fence can be aesthetically pleasing and disguise its performance capabilities.

Tested, approved, certified and preferred

The resulting products from our high security portfolio have LPS 1175 certified ratings from A1 through to E10, NPSA (CPNI) approval up to the highest level and Hostile Vehicle Mitigation protection to PAS 68 – all of which additionally meet with 'Police Preferred Specification' through Secured by Design. These products have already been employed in some of the highest security applications in the UK and export markets including the protection of embassies, laboratories, communication monitoring sites, MoD facilities, secure detention sites, power stations, other sensitive sites and of course an increasing number of data centres.

However, specifying and installing appropriate security products won't guarantee 24/7, 365 days a year protection of your site.

The importance of maintenance and repair

Just like keeping your software and hardware updated to provide the best protection of client data and the integrity of your network, a well maintained perimeter ensures that the physical security of your data centre is equally performing to its designed specification:

1.Inspecting the fence line

Here's the easy and obvious bit, but it does need to be a scheduled event and from our experience, that's rarely the case.

- The perimeter fence line needs to be 'walked' and access gates 'checked' both from within the site and more important along the attack face –look for attempted breaches, note if foliage, weather conditions, natural or man-made topography changes have effected security integrity.
- Check that all fixings and fittings are secure, look for damage and corrosion.
- Clear away any litter, debris and dirt, take a note of everything requiring attention in a condition report then if necessary, prioritise repairs and remedies.

2.Inspect and test gates, turnstiles, barriers and blockers

For data centres, the consequences of a gate, turnstile, barrier or other secure access control equipment failing could be extremely serious; far in excess of an irritation or inconvenience.
Gates, vehicle and pedestrian barriers - especially those with automated operators and control boxes - require special attention, not only to maintain security and operational efficiency but also to meet your duty of care to everyone on your site – and in these litigious times, that includes user error and intruders.
HSE Regulation 18 classes automatic gates and barriers as machinery and as the occupier of the facility you are required under Regulation 5 of the Workplace (Health, Safety and Welfare) Regulations 1992 and European Directive EN 13241-1 to ensure that they are always in safe working order.

Vehicle access control barriers in particular will typically be subject to heavy use and abuse...so committing to a formal Maintenance and Repair schedule in addition to checking for general wear and tear and carrying out essential repairs are key requirements.

3. The application of common sense

Of course, the operational processes you adopt to ensure the security performance of your perimeter which will need to form a part of your security SOPs.

But, much of it boils down to common sense – the problem with common sense though is that it's not uncommon to forget to apply it until after an event.

When planning the physical perimeter security for a new 'urban' data centre, here are some of the key steps:

1. Ensure the risk assessment is both thorough and provides both for redundancy and resilience
2. Know your site, it's specific conditions and the areas around it and within it
3. Specify and select the appropriate products for their intended purpose and suitability for site conditions
4. Check that the product installed meets with the specification ordered
5. Ensure that no shortcuts are taken in the installation
6. Accept that in general, security products installed won't improve over time - their performance will degrade
7. Have a workable recovery plan which takes account of maintenance and repair
8. Once installed, don't assume security products are working just because they haven't failed –inspect, check, test, maintain and repair are the watchwords to robust security performance and integrity

Long-term, future-proof solutions

As a business, we understand that data centre management and their operations teams have a lot to contend with in running and future-proofing their enterprise in a high growth, capital and skills intensive business. Within an increasingly competitive landscape where security, availability and resilience play a key role in the core proposition. This is why our tested and certified high security perimeter fences and gates, noise reduction barriers, access controls, PIDS and PAS 68 solutions are all designed to work reliably and require the minimum of maintenance over a long service life.

Our timber fencing, gates and barriers are covered by a 25 year service life guarantee and able to withstand '1 in 50 year' weather conditions.

They are additionally supported by a family business with a reputation for quality and innovation stretching back to 1947 and a team of expert installers and maintenance and repair engineers covering the country; all committed to doing their part in keeping intruders out so that you can concentrate on delivering the best possible 24/7, 365 days a year service.

Copy provided by Peter Jackson, CEO Jacksons Fencing, Group Vice Chairman, Site Security & Access Control Group, Data Centre Alliance.

Contact Us

For further information, advice or to arrange for a site visit or CPD, please contact us on 0800 41 43 43 or email highsecurity@jacksons-fencing.co.uk.

Head Office Security and Export Enquiries

Stowting Common, Ashford, TN25 6BN
T: +44 (0) 1233 750 393 or 0800 41 43 43
E: security@jacksons-fencing.co.uk
W: www.jacksons-security.co.uk