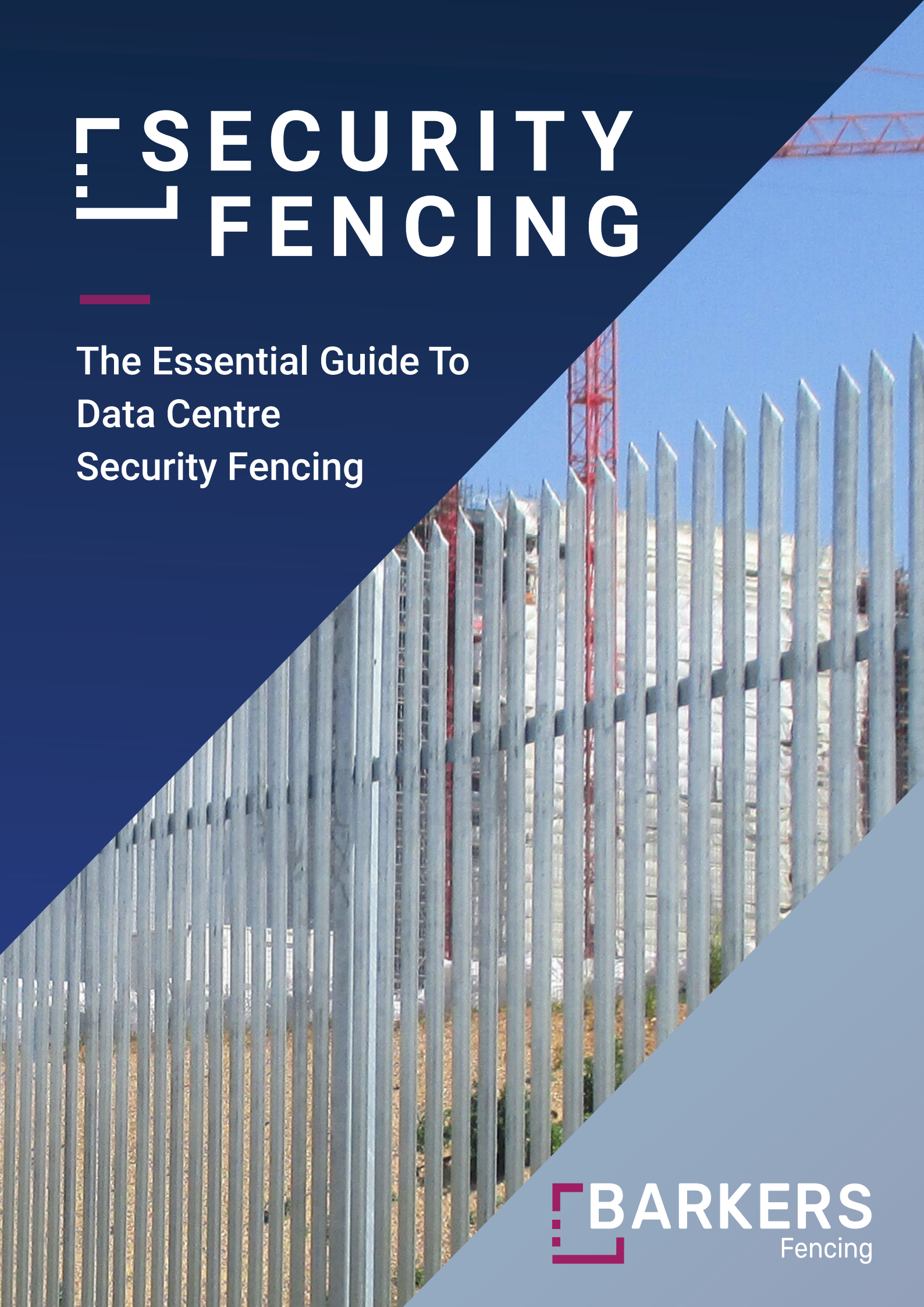




SECURITY FENCING

The Essential Guide To
Data Centre
Security Fencing

 **BARKERS**
Fencing

Introduction

The physical security of data centres is not something that first comes to mind when you think of 'data centre security'. In fact, by modern standards, there is certainly a trend heading towards the attack on servers or networks remotely in order to steal and access data.

Despite this trend, the physical security of a data centre is not something that should be overlooked. Globally, there are 7.2 million data centres currently in use, with this figure expected to rise by 2025.

Whether you are a designer, architect or construction firm, this surge in demand for data protection means that there is a need to deliver projects quickly, to a high standard, taking into consideration the individual environment in which your data centre is located.

Whatever the size, purpose or location of your data centre, its physical security cannot be understated, with the consequences of a security breach being catastrophic to businesses, government agencies and even you and me.

This guide was born out of a need to help aid safe specification of security fencing within Data Centre settings, to ensure you select a long-term solution that is both resilient and effective.





Contents

What To Consider When Specifying Data Centre Security Fencing	4
What Security Fencing Do You Need For Your Data Centre?	6
How Are 1175 Products Tested?	8
Added Features To Your Security Fence	9
Additional Security Measures	10
Data Centre Case Study	11

What To Consider When Specifying Data Centre Security Fencing

When specifying data centre security fencing, the importance of getting it right can't be downplayed. Perimeter security is the first line of defence to stop unauthorised people from gaining access to the assets. Security weaknesses could lead to data getting into the wrong hands, or downtime in service - both of which could massively affect your reputation.

There are a range of considerations that should be taken that can reduce the likelihood of an attack, and, taking your time over the specification of your security fence could be the difference between secure data, and vulnerable data.

What Data Is Being Protected?

Every data centre is different, and as such, there is no 'one-size-fits-all' approach. A risk assessment needs to be conducted. Here are some things that need to be considered:

- *What data is being protected?*
- *What are the threats and risks?*
- *What would the cost of a successful attack be?*

Governmental or privilege data will require a high investment in its security, for example.

In a physical sense, threats are often from forced entry or vehicle borne.



Mitigating Threats

The first step to mitigating threats to your data centre is through perimeter fencing.

This will allow you to funnel all traffic into your data centre from a single point, enabling you to keep a record of who is accessing your site.

Certain high security fences can also provide protection from hostile vehicles.

The additional use of surveillance such as CCTV cameras and guards will also add another control measure, if necessary.



Site Requirements

Each site is unique so you should closely consider your surroundings, ground considerations, wind loading, weather conditions and build constraints.

These factors will determine the type of fencing, gates and other security products which will lend themselves well to your site.



Entrance Security

The entrance of your data centre needs to be protected as well as your perimeter.

It is important that your site entrance is at least to the same rating as your perimeter fence, in order to eliminate weak points.

You may need to consider vehicle entry, pedestrian entry, or both.

Vehicle entrances and the surrounding area are typically at the biggest threat from vehicle impact.



What Security Fencing Do You Need For Your Data Centre?

As discussed earlier, data is valuable and appropriate measures should be put in place to ensure it is secure. The threats identified through the risk assessment need to be mitigated. These could range from vandalism, targeted intrusion, accidental vehicle impact from a nearby road, protests, or state sponsored attack.

For peace of mind that your security fencing will perform as promoted we advise choosing a third party accredited fence. For a relatively small increase in costs, using tested and approved security systems will offer a greater degree of confidence to the clients.

Government Property

If protecting UK Government property, you will need to consider CPNI rated security fencing. CPNI, which stands for Centre of Protection of National Infrastructure, is the government authority for protective security advice to the UK national infrastructure. Their role is to protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.

CPNI rated fencing is independently tested to a strict set of guidelines, which are deliberately kept ambiguous. Further information can, however, be gained by contacting CPNI directly.

A fence – or any other solution that proves resistance to a forcible attack – can be awarded a CPNI PROTECTION Level. This is calculated based on the attacker's anticipated and assumed skill level and how long a product can remain resistant under attack.

CPNI grading is as follows: CLASS1, CLASS 2, CLASS 3, CLASS 4, with CLASS 4 PROTECTION offering the highest level of protection, which is established by the CPNI organisation.

LPS1175 Fencing

The Loss Prevention Standard (LPS) has become popular amongst the fencing industry, as it is easy to interpret and use, with the latest version becoming more universal. Now with a matrix style performance classification system rather than a number of specific set ratings.

Testing of the LPS1175 is tough, and BRE proudly report that 95% of products submitted fail to achieve the security ratings initially sought by manufacturers.



How Does The LPS 1175 Certification Work?

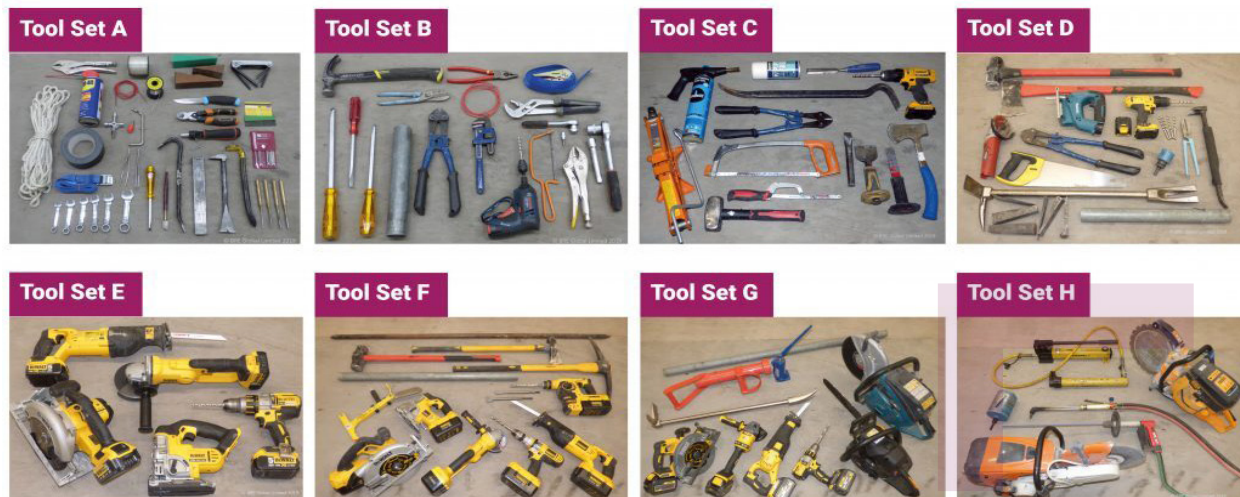
You might be thinking, how does the classification work and what makes a security fence LPS1175 certified?

The LPS in LPS 1175 certification stands for 'Loss Prevention Standard'. LPS 1175 has been developed to be a universal classification system for intruder resistance and can be applied to a vast range of applications. The classifications range from an opportunist attacker with bodily force and basic tools to multiple experienced attackers using chainsaws and petrol grinders.

DELAY	20 minutes	A20	B20	C20	D20	E20	F20	G20	H20 (SR8)
	15 minutes	A15	B15	C15	D15	E15	F15	G15	H15
	10 minutes	A10	B10	C10	D10 (SR4)	E10 (SR5)	F10 (SR6)	G10 (SR7)	H10
	5 minutes	A5	B5	C5 (SR3)	D5	E5	F5	G5	H5
	3 minutes	A3	B3 (SR2)	C3	D3	E3	F3	G3	H3
	1 minute	A1 (SR1)	B1	C1	D1	E1	F1	G1	H1
TOOL KIT	LPS 1175 Issue8	A	B	C	D	E	F	G	H
	LPS 1175 Issue 7	A	B	C	D	D+	E	F	G

The table shows a matrix of how products are classified. Those classifications indicate the tool kit resisted and the delay achieved in minutes.

Tool sets were updated in issue 8, in line with tools becoming more easily accessible, the new tool sets are shown below.



How Are 1175 Products Tested?

During testing, each assault continues after either:

The objective
is achieved

Maximum
working time
has passed

Maximum test
duration has
ended

Testing team
decides the
attack is
ineffective

Additional tests are then conducted to demonstrate all areas of the fencing can resist the damage inflicted from the intruder's side.

However, if the tester notes a small weakness once the time has been exceeded, the product will not pass. If they spot a weakness, these highly trained professionals will try again and again to see if they can gain access within the timeframe. It's safe to say it's a rigorous regime they run!

And once the product has passed the test. The company and these products are subjected to thorough audits of product and documentation to ensure the certified product is upheld.

Hostile Vehicle Mitigation

Impact from a rogue vehicle could do considerable damage to a data centre and potentially take out vital assets such as generators and servers.

During your risk assessment you may have identified vehicle borne threats around part of your perimeter. If this is over an extended area of your perimeter, you have limited space or you want your HVM measures to be subtle, it may be worth looking into a impact tested fencing. If you look for an impact tested fence which is also forced entry tested, you are mitigating two threats in a single solution.

This combined solution will be ideal for applications where space is at a premium or where you don't want to draw attention to the security measures.

The perceived threat is the threat of accidental and/or hostile vehicles, and not having HVM in place could leave a site vulnerable to a vehicle damaging generators, servers and other vital assets. HVM fencing is an ideal solution for high-security data centres, as it provides maximal security and safety in a single fence line, whilst not drawing attention to the centre itself.

Added Features To Your Security Fence

Once you have specified your security fence after having been advised on your security rating, additional features and toppings should be decided upon.

For example, do you need HVM additions, curved pales on your palisade fencing to deter intruders, or even barbed wire?

All of this is essential when maximising your site security, as you need to try to make your fencing look as formidable as possible when housing sensitive data.

The range of additional extras you can add to your data centre security fence to improve security are endless, they include:

Barbed/ Razor Wire

Barbed wire is a type of steel fencing wire constructed with sharp edges or points.

When touched it's painful and is likely to puncture skin.



Curved Pale Top

A curved pale top is a cost-effective solution for those wanting to enhance the fence's intimidating appearance further, without added installation costs of cranked posts and barbed or razor wire.



Electric Pulse Fencing

Electric pulse fencing provides a high-security solution for premises by creating an electrical circuit when touched by a person or animal.



Sometimes, a security fence alone isn't enough when it comes to data centre security, and other elements need to be added.

Additional Security Measures

It is important that if you have used accredited fencing on your perimeter, that your entrances achieves the same security rating.

For pedestrian entry, you can choose between gates and turnstiles. Turnstiles are ideal for heavy use areas or where a higher degree on control of entry is required - particularly if the area is unmanned, turnstiles ensure only those authorised can enter.

For vehicle entry, high security data centres often use a sally port configuration. A sally port (also known as a tiger trap or air lock) is two barriers, where the vehicle moves through the first barrier to the compound in which the vehicle can be vetted and searched.

Once approved the second barrier opens letting the vehicle pass through. A sally port can be achieved in a number of configurations, using a combination of cantilever or bifolding gates, bollards, road blockers or rising arm barriers.

With vehicles present, it's also worth considering impact tested fencing around vehicle entrances. If an attack were to take place, the attacker may decide the fence looks weaker than the gate and change the line of attack.

Access control can be configured to work with card readers, pin codes, ANPR cameras and even facial recognition technology.

Security measures can seem costly, and the right security measures for the site will depend on what is being stored and the perceived threat.

When considering the value of security it's worth taking into consideration the potential cost of damage, security breach, reputation damage, lost data and downtime.





Data Centre Case Study

Barkers Fencing were originally approached by an architect looking for a highly secure, third party tested fencing system, to protect their client's high value data centres across the EMEA. We were able to demonstrate our engineering expertise and experience in high security fencing, which were proven to protect critical, high value assets. After strong discussions we were introduced to the end client.

The Challenges:

The sensitivity of the data and the impact a security breach would have meant that the client required heavy duty security fencing.

For that reason, CPNI accredited palisade security fencing and gates were permitted and approved for government use.

Over time the threats developed, and the client also required a solution which would provide hostile vehicle mitigation (HVM).

Data Centre Case Study

The Solution

Working with the client's in-house security team, we developed a standard layout for the perimeter of their sensitive sites. The specification includes two products to mitigate the threats:

StronGuard™ palisade security fence, which has been tested independently and certified by CPNI to delay forced entry attack.

StronGuard™ RCS, which is a derivative of StronGuard™ intruder resistant security fence and certified to PAS68 standards to provide HVM of a 7.5tonne vehicle traveling at 30mph.

To achieve its security fence accreditation, StronGuard™ utilises a high load anchor with no visible fixings, stopping perpetrators from attacking the front face of the fence.

A combination of the high load anchor and the fact the design has no foot holes makes both systems difficult for intruders to breach.

StronGuard™ RCS was selected as the client wanted a HVM solution, that wouldn't draw attention to the fact they have something to protect, in areas where a vehicle was a perceived threat.

Another benefit of StronGuard™ RCS is that although it is an impact tested solution, the clever engineering of the system means that it doesn't require large, excavated foundations – It is often installed in near standard palisade footings.

Since this project, we have established a strong relationship with the client and are now working with the client's consultants/contractors across the EMEA region, delivering resilient security fencing and gates.



Etna Works
Duke St
Stoke-on-Trent
ST4 3NS



+44 (0) 1782 319264



sales@barkersfencing.com



www.barkersfencing.com

 **BARKERS**
Fencing