Spring has sprung early!

By Simon Campbell-Whyte, DCA Executive Director

THE BIG NEWS THIS SPRING is the start of the EURECA project. For those that missed updates on the DCA website and the presentation at Data Centre World 2015, I will explain what this is all about and why this is probably the most important data centre industry project yet. First of all some background, it is the 2nd EU funded project the DCA have participated on, this time it is a Horizon2020 project of 30 months duration and it has a total budget of €1.5M. There are eight project beneficiaries who are University of East London, DCA, Green IT Amsterdam, Cerios Green, Carbon3IT, Maki Consulting, Norland and Telecity GmbH.

The project is our response to the EU Commission's funding call which laid down specific challenges to stimulate market transformation towards more sustainable energy products, buildings and services within the Public Sector. This included the EU Energy Efficiency Directive which requires that central governments purchase only products, services and buildings with high energy-efficiency performance. The call asked for proposals to overcome the operational barriers related to sustainable energy public spending such as the lack of knowledge, practical training and tailored guidelines, and also the lack of willingness to change procurement habits or perceived legal uncertainties.

So in our world of data centres this is a real challenge, but also a great opportunity to influence a market many would say needs to be opened up. On top of all that consider all that is happing in our sector: data centre KPI's, best practices and maturity models coming at us from all directions, ISO/IEC, ITU, EU Code of Conduct, CENELEC and ETSI to name some. This is becoming an increasingly complex landscape, even the excellent EU Code of Conduct now comprises of over 150 best practices.

So in very simple terms, the projects goal is to make all of this accessible to the non-expert both in language terms and to signpost the self-improvement roadmap of data centres, server rooms and computer rooms across the European Public Sector.

The methodology we proposed is to develop a tool that a public sector procurement officer or representative can use to input information about their data centre. This will range from the very basic such as energy consumption & temperature data and simple best practices such as "group involvement" through to more advanced information such as server utilisation data.

The output of the tool will provide maturity level scoring, along with recommended actions, relevant market navigation signposting and business case construction for improving the energy efficiency of their data centre. This could result in the purchase of products and services from all our members be it technology, data centre services or training.

As I write (March) we are initialising the project. Having presented the project to the industry at DCW15 we officially launch to the Public Sector at the Public Sector Show at London's EXCEL on June 23rd. We would like all members to help with the project by referring public sector contacts who are both already energy efficiency "champions" to help with knowledge sharing and also those who are looking to improve the energy efficiency of their data centre. Updates and opportunities to comment or contribute to the development of EURECA will also be made freely available at dedicated website to be launched soon and announced over the twittersphere and airwaves.

From bland to grand:

Why today's data centre should be a dynamo for business innovation and growth

By Huw Owen, CEO of Ark Data Centres

It's all too easy to ignore the data centre. Long perceived as the less glamorous end of IT, the data centre is often overlooked – or forgotten – by boardrooms and strategic operations managers.

Back in the day when data centres were simply operation rooms for back-office tasks, this neglect was understandable. But today's hyper nimble world of commerce cries out for fast, efficient data centres capable of supporting high-end process automation, e-commerce, modern supply chains, big data, cloud computing, a multitude of apps – and more.

Fact is today the data centre represents the heartbeat of an enterprise, and its performance is becoming a critical business differentiator. Response times, latency and uptime are all highly visible indicators of business efficiency, and organisations that

ignore and neglect their data centres risk falling behind competitors simply because their IT infrastructure isn't engineered for growth or innovation.

Data centres have evolved

Companies are waking up to the fact their legacy data centre no longer offers the scalability and flexibility they need to respond fast to new opportunities. But by turning to specialist providers they're gaining the ability to adapt business models instantly, accessing all the capacity and performance they need, the moment they need it – for example, whenever they introduce a new application – with no costly build-out, capital expenditure or delay.

Extending the reach of an enterprise's information delivery platform is just the start, because data centres have changed. Thanks to major technology and infrastructure innovations, they've become powerhouses for generating competitive advantage through greater agility, lower costs and reduced risk.

Greater efficiency fuels greater business innovation

Data centre operators like Ark have pioneered innovations in efficiency that generate dramatic savings for customers both on carbon – and therefore on tax – and energy costs (often to the tune of very significant numbers every year). These savings allow enterprises to spend more of their IT budget on new projects that make their organisations even more successful. In other words, the cost benefits gained from partnering with a specialist data centre releases budget that can be invested in new technologies, apps and customer-facing infrastructures that deliver added value, support fast market entry and optimise operational performance.

What's more, the highly sophisticated monitoring capabilities of today's world-class data centre facilities means enterprises gain the guaranteed resilience they need to cope with any demand with no danger of disruptions. No more worrying about technology refresh cycles or having to wring more from existing capital investments. And no more concerns about business risk, potential exposure or liability resulting from security and compliance issues.

But to reap these rewards, businesses need to take a deeper dive into the detail. Data centres are no longer a commodity item, and it pays to find a partner that looks beyond typical REIT (real estate investment trust)

style accounting rules to deliver full cost transparency and a commitment to a long term professional relationship of integrity and complete trust. A provider that is not distracted by the need to balance quarterly capital expenditure against the long term needs of its customers.

Ingredients for success

Ensuring you benefit from the efficiency gains that fuel greater business innovation means finding a provider that can deliver the savings you need. So, alongside obtaining a fixed PUE (power usage effectiveness) you'll need to dig deeper to check if that PUE accounts for all overhead costs – and not those related to a specific data centre room. You'll also need to check the investment profile of the provider you select. What's their long-term stance on technology innovation, for example – are they committed to embracing new technologies that deliver TCO savings directly back to customers.

Are they network and vendor agnostic – eliminating expensive or unexpected 'technology lock ins' on the horizon. How do they maintain security accreditations, and are security standards embedded within the organisation itself? Check if a provider can work at 'above SECRET' levels, in case your needs change in the future. And this is a condition today, then you'll need to be assured from Day One of any go live. Because elevating your security requirement later may have a significant impact on the end price you pay.

Finally, are they able to offer dedicated service teams that live and breathe your business and will collaborate with your IT teams to enable your business application and infrastructure evolutionary path?

Preparing for better business

Many organisations are finding their legacy data centre infrastructure is no longer equipped to meet the demands generated by today's technology environment.

Virtualisation, cloud computing and the deployment of new applications that require high-density and high-performance computing are mismatched with yesterday's enterprise storage, server and networking data centre infrastructure. Shifting the legacy data centre from being high maintenance to enabling high performance can prove an expensive – and onerous – task.

Making the move to a specialist data centre provider that's focused on the future, can prove significantly less expensive and much easier than upgrading a legacy site. What's more, you can be up and running in just 12 weeks – compared to the industry standard of a year. Making it possible to start benefiting from energy efficiencies and all the capacity you need to keep your business competitive and agile.

Evaporative FreeCooling

The big daddy of data centre cooling?

By Roy Griffiths, Technical Director of Workspace Technology

AS DATA CENTRE COOLING is responsible for the majority of 'non compute' energy consumption in the data centre, getting the right solution to ensure ultimate efficiency is the goal of most data centre professionals. Fortunately there are multiple energy efficient cooling systems available to satisfy most requirements all providing their own unique benefits, ultimately choice will be made on a range of metrics, but key will be the level of energy efficiency.

There are many explanations or descriptions for the term 'Efficiency' – 'One of the best analogies for describing efficiency in data centres has to be 'The good use of natural energy in a way that does not waste any' in terms of DC cooling systems available on the market today this terminology is probably best suited to describe Evaporative Cooling Systems.

Evaporative cooling is nature's method to cool, it is the system your body uses to cool down and certainly the most sustainable, and environmentally friendly system by far.

So how does it work? Evaporative free air cooling technology makes use of the external air to cool the DC environment, unlike simple air economizers which require supplemental or chilled water when external temperatures reach 21°C, Evaporative systems engage the cooling mechanism by simply passing the airflow through wet filter pads.

So what is so good about it? The primary benefit is the drastically reduced power consumption in comparison to more traditional systems, in fact the well known FreeCool® Evaporative DC cooling system delivers typical power consumption reduction of 90% compared to some traditional mechanical systems, delivering typical PUE3 of 1.15 or lower, other primary benefits include:-

- Reduced CO2 emissions
- Significantly reduced energy consumption and operating costs
- Supports existing cooling technologies
- Improved DCiE / PUE Efficiency Ratings
- Improved company 'Green Credentials'
- Improved resilience with practical support by UPS systems.
- Flexible airflow configuration options
- Modular, Scalable Architecture
- Can be deployed as a new scheme or retro-fitted to existing data centres

In practical terms the benefits above not only allow for robust operational advantages but also provide sound commercial and financial benefits allowing users to take advantage of significantly reduced cost overheads, and where available take advantage of government grants that are available to support the installation of such systems

Nothing is perfect so what are the drawbacks?

In the past Evaporative cooling solutions have been dismissed for server room and data centre environments due to historical issues with air quality and humidity control. Specialist Data Centre centric direct air Evaporative cooling systems such as Freecool® challenge the barriers to air economizer cooling as a suitable technology for server room and data centre environments.

The obstacles to air exchange have been removed as modern computing equipment is much more robust with regard to both temperature and humidity.

Typical computer manufacturer environmental operating specifications are 10°C to 35°C and 10% to 95% relative humidity. ASHRAE have acknowledged the advances of modern computers and the need to balance energy efficiency against system reliability. ASHRAE make recommendations for a server room temperature range of 18°C to 27°C, it is recommended that humidity levels are replaced with dew point.

Another observation on a sustainable note is the requirement of the system to use water during the cooling process, however not only is the use of water in evaporative systems around 25% less than traditional water cooled chiller plant, the water that is used then simply evaporates into the air, so that nature can re-use.

It is of course true that poor air quality can cause detrimental issues where direct air is used, the designers of the direct air Freecool® system have recognised this and have a two fold solution, firstly all external and internal Freecool® systems are fitted

with a combination of G3 / G4 filters. The optional 'Coolwall' system is designed to deliver instant backup in the event of a range of programmable conditions including external air quality, internal environmental conditions, fire suppression activation or primary cooling failure. The 'Coolwall' consists of chilled water cooling coils which are designed to support full cooling capacity at 20°C external ambient. The 'Coolwall' installation is designed to restore 100% of cooling capacity within 30 seconds of activation and is controlled by the Schneider Crouzet controller which will ensure appropriate dampers are closed to support closed loop cooling.

So how about some real life examples of where this technology has been used?

Evaporative cooling technology is deployed throughout the data centre market from Telco operators, to Co-Location providers, standalone privately owned data centres to the Public Sector. Two of the most outstanding recent examples include the multi award winning Leicester City Council and University of Aberdeen data centres. Both projects utilised Freecool® and was a significant element of the complete Design and Build Services provided by Workspace Technology Ltd.

University of Aberdeen

The NESS partnership (North East Shared Services) is a joint venture between the University of Aberdeen, Aberdeen College, Robert Gordon University and Banff and Buchan College. It was agreed to create a 'Shared Services' data centre facility.

The existing data centre located at the Edward Wright Building on the University of Aberdeen's campus was the preferred location. This data centre was approximately 23 years old supporting the University's core ICT services. This facility had enough space for the combined rack count but was out dated and lacked the required power, cooling capacity, defined installation standards, and suffered from a PUE of 2.6.

The innovative solution provided, included Design, Civil and Construction works, Freecool® Technology, aisle containment, electrical design including Schneider switchgear, back up power generation, structured cabling and Schneider APC rack and PDUs, StruxureWare DCIM and post contract ongoing 24/7 support and maintenance back up – all services are delivered by Workspace Technology's highly experienced in house teams.

An annualised PUE3 of less than 1.15 has been achieved. The financial benefit is a reduction in the power bill for the data centre by £94,000 per year whilst improving the environment by reducing the data centre carbon foot print by 612 tonnes per year. Across all the NESS partners the refurbished data centre will produce an annual financial saving of £256,000 with the total carbon foot print being reduced by 1450 tonnes.

This innovative data centre has been awarded multiple accreditations and awards including the prestigious British Computer Society – Data Centre Project of the Year 2013, & Computer Weekly – European Public Sector Data Centre of The Year 2013, and Green Gown – Effectiveness and Efficiency in the Estate.

Leicester City Council

Workspace Technology Ltd delivered 'Carbon Neutral' Cooling, as an integral element to a complete design and build project. The solution utilised the Freecool® Direct Evaporative Cooling System combined with

contemporary renewable Photovoltaic (PV) Technology, with back up resilience provided by Workspace Technology's Coolwall system. The PV power contribution exceeds that of the Freecool® power consumption.

Freecool® installations are designed and built from scalable standardised modules that can be interconnected in a bespoke arrangement supporting 'real world' customer applications. The Leicester City Council project was no exception with the solution designed to support a maximum critical load of 250kW N+1 with a deployment of nine 30kW Freecool® units. Workspace Technology provided a complete turnkey installation including full design of all construction, mechanical and electrical systems, completed by our own in house construction, engineering and installation teams.

The data centre whilst only recently commissioned has won 3 awards including:-
Public Data Centre of the Year 2014 – DataCenterDynamics EMEA Awards
Innovation in the Medium Data Centre 2014 - DataCenterDynamics EMEA Awards
Best IT/Ecommerce Project 2014 – Public Sector Sustainability Awards

So is Evaporative FreeCooling 'The Big Daddy' of Data Centre Cooling?

There are of course other cooling systems that provide some really great innovations, and of course Evaporative Cooling is not a solution that will suit all applications or preferences so is Evaporative Cooling 'The Big Daddy' of Data Centre Cooling?- maybe not, but it certainly can be described as The Greenest Cooling Daddy!

Knock, Knock!! Who's There???

Cordant Services have recently joined the DCA, here Lee Ennis discusses just how safe our datacentres are.

JUST HOW VALUABLE is your data? That is a question that organisations up and down the country need to ask themselves when it comes to truly safeguarding data centres, for their own and perhaps even more importantly their external customers' benefit.

Reputational damage is only the start of your worries, who can forget Zurich Insurance being fined £2.3 million by the FSA for losing customer data (which would have been considerably more if they hadn't admitted liability early on). I could name another four or five household names that had received hefty fines for similar breaches of customer data.

Additionally a customer that doesn't feel confident that you are using every measure available to protect the facilities that house their data will seek one that can. The key factor is being able to provide the broadest range of security in order to protect these valuable assets which sit at the core of a customer's business. With business drivers from confidentiality issues to simply being able to manage transactions in confidence, customers have to put an increasing emphasis on 'belt and braces' security of their data centres.

While data centres will typically have several layers of technology protecting them from break-ins, from gate security to access control systems, down to the individual door controls and CCTV, these are only part of a truly comprehensive solution. Physical security is sometimes undervalued for its part in ensuring that a data centre is seamlessly protected.

Technology plays a major part, but it is boots on the ground that ultimately provide a physical deterrent and also an immediate response in the event that someone bypasses the security systems and enters the facility. And the responsiveness of technology used remotely causes problems which can only be avoided by having a physical presence on site. I've yet to encounter a remote system that doesn't drive a control room operator to the point of switching it off due to continual alarming of non-identified threats. The 'boy who cried wolf' scenario kicks in and ultimately leads to lethargy in responding, or the operator just going into auto mode and just moving to their next task.

A physical presence from a guard used to the facility is highly beneficial as they can use their intelligence to identify what is activating the alarm and take immediate action if possible. This includes action to prevent further reoccurrence if it is a false alarm. A physical security presence on site is also vital in controlling passes, ensuring that all engineer and contractor passes are disabled after each visit and only activated once they arrive on site and have been verified. This is a vital role as unless biometrics are used, which is not common, a pass is open to abuse by almost anyone.

Access control testing and auditing of the systems on a regular basis is paramount and should never be overlooked. It may be embarrassing to those caught out and could ultimately lead to a customer having to involve their HR Department, but it allows for any weaknesses to be kept in house and put right immediately to prevent any possible reoccurrence. In my experience it is mostly the human and not the tech element that fails these tests, and that's precisely where the physical security presence is required to drive and monitor those humans and their failings!

Another more serious human threat from within the organisation itself is the potential danger of theft or misuse of data by employees, with documented examples existing of staff payroll and personal information having been stolen. To combat this risk, searching of staff entering and exiting a data centre is a necessary task and well-trained security staff can do this in a professional and unthreatening way.

The security risk at a data centre needs to be continually assessed, and a manned presence is best placed to do this. The best advice is, don't wait for a risk to have presented itself before acting; manned security can identify risk on a daily basis. Lastly, don't forget to ensure that your security supplier also has a copy of your Business Continuity Plan as they will be on the front line, putting it into action out of working hours.

Data safe-keeping starts with the data centre

Data centre security at some level is a given with most facilities – but not all data centres are created equal. By Lexie Gower, Marketing Manager at Datum Data Centres.

AS OUR WORLD becomes digitalised, and businesses transmit more of their critical data in digital format, the potential impact of data loss is untenable. This has increased the importance for data centres to provide the highest levels of security for organisational data.

So what makes one data centre more secure than its neighbour? At Datum we believe it is an interplay of physical attributes, processes and people.

From the base up

To protect business critical data, at the most basic level the physical location is key. As a starting point, the data centre should be built in a secure position safe from both intentional and accidental incursion. This means being well away from the main road, out of a flood or other high risk zone, and behind a secure perimeter. But sometimes unintended damage can be caused by simple things such as neighbouring road works, building developments or passing traffic. A controlled external environment has the advantage that it helps to mediate against such risks, something that is unlikely to be true of an industrial estate or a city street.

The additional security of a fully controlled secure park location is compelling for clients with sensitive data for whom security is a non-negotiable requirement.
Construction and design of the build are also important. To withstand aggressive attacks or forces of nature, a data centre needs to be solidly built, windowless, with redundant power and cooling built-in and power supplier securely underground. And to protect against malicious or opportunist incidents, the design should incorporate full multi-level access systems utilising, at the very least, surveillance cameras, fire detection, biometrics, automatic door locks and access pods.

Whilst the physical attributes are the foundation stones of security, Alcatraz would have been an open prison had the guards left doors unlocked and a fully fuelled boat moored to the dock. Strong processes need to be in place, adhered to and evidenced covering client-authorised access lists, proof of identity, and multi-level visitor checking without exception. Security training and a strong client-focus are vital components of the whole approach in order to ensure that more than lip service is paid to the safe housing of your vital infrastructure. In addition, relevant accreditations can demonstrate that the processes more than just documentation, offering real assurance to your infrastructure.

Telling the whole story

Because not all clients have the same needs and not all data centres are the same, the provision of security can vary from data centre to data centre. Datum's experience with clients has shown us that our story resonates very strongly with organisations for whom security and high availability are paramount. A well-equipped, well run data centre in the right location is the most essential security evaluation that all organisations should develop to be properly equipped for their digital future.

Biometric physical access control in data centres: Ensuring regulatory compliance, with indisputable audit trails

By Andy Billingham, Managing Director – EMKA (UK) Ltd – Corporate Partner, DCA. Adapted from an original report by Digitus Biometrics.

MAINTAINING COMPLIANCE with various data privacy rules and regulations – PCI DSS, HIPAA, FISMA, and more – is often seen as primarily a matter of securing data networks against unauthorised access. However, data privacy directives invariably focus on physical security as well as network security, and consider the protection of physical assets to be as important as protecting the data stored or processed in those assets.

Physically securing private information in data centre's has proven challenging, however, as the necessary technology has lagged far behind network security technology. The network security industry is a steady stream of innovative response to high-tech threats. For most data centres, physical security rests with technology from the last millennium.

This article explores an advanced security methodology by which enterprises can best secure physical assets within their data centres, with greatly enhanced security against the growing trend of insider threats and a 100% indisputable audit trail of physical access. The result is a more thoroughly secured operation that follows best practices for asset protection, reduces the risk of physical security breaches, and demonstrates the highest effort for regulatory compliance.

Commonality among data privacy directives

When boiled down to their essence, data privacy rules and regulations all seek to accomplish the same thing. Government regulations and non-government standards invariably ask four basic questions regarding access to sensitive information:

- Do you have safeguards in place to control access to sensitive data?
- Are you able to continuously monitor who is accessing sensitive data?
- Are you alerted in real-time when information is being accessed without authorization?
- Can you produce an audit trail showing who has accessed sensitive data and when they accessed it?

It's important to remember that "access" within the context of these questions means physical access as well as network access, and that specific requirements for controlling physical access exist in all rules and regulations concerning the protection of private or sensitive information. Following are examples that span multiple industries:

- **PCI DSS Requirements 9 and 9.1:** "Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data."

- **HIPAA Title II, Physical Safeguards:** "Access to equipment containing health information should be carefully controlled and monitored. Access to hardware and software must be limited to properly authorised individuals."

- **FISMA (FIPS 200 Section 3):** "Organizations must limit physical access to information systems, equipment, and the respective operating environments to authorised individuals."

Biometric security at a data centre

These regulations also share a commonality in the requirement for alerts and audit logs of physical access opportunities, though all are notably lacking in specifics regarding implementation. In each regulation, a covered entity must consider its risks and determine for itself reasonable and appropriate physical access alerting and auditing methods for information systems that contain or process the data being protected.

In practice, even those enterprises that are highly concerned about addressing risks related to physical access have been unable to elevate alerts and audits to the level they can for network security. This is primarily a matter of deficient technology, as 100% accurate alerting and auditing solutions for physical access have typically extended no further than a data centre's front door.

Shortcomings in common physical security practice

Data centres are usually physically secured with a mixture of unconnected platforms that may include palm readers, proximity card readers, and keyed locks.

Because of their size, palm readers, the most secure platform in this group, are found only on doors. Servers that handle especially sensitive data are typically protected from data and device theft by locking server cabinets that are accessed with keys or key cards. The use of mixed access-control devices can raise serious issues as regards both sound security practice and the ability to demonstrate regulatory compliance.

The problem begins with the fact that keys and key cards can become separated from their authorised users. Any key or key card that is forgotten, lost, stolen, or otherwise separated from an authorised user represents a potential, undetected security breach. The greater the number of keys and key cards in a given environment, the greater the possibility of unauthorised access to physical assets in a server cabinet.

As a result, there is no effective means to issue an alert when unauthorised access occurs, and audit trails are incomplete. When an unauthorised user opens a cabinet with a working key card, there is a log entry but no alert. The audit log from a palm reader at a data centre's front door provides solid evidence of who was in the data centre at any given time, but beyond that, all that's known is which key cards, and not which users, opened which server cabinets. If the server cabinets are secured with keys – or

Biometric swinghandle with fingerprint sensor and emergency opening

are not locked – there is no audit trail at the server cabinet level at all.

Technology to eliminate these shortcomings

In addition to providing extremely accurate identification for access control, db ServerRack offers several key advantages relative to the rack itself and, when paired with db Nexus, to the task of securing the entire data centre:

- **Simplified security administration**

With biometric access control, administration is greatly simplified compared to the mixed-solution environment found in most data centres. There are no keys or key cards to assign, track, retrieve, and reassign. Removing all access privileges is a matter of a few keystrokes within the Digitus Access Software, as is reassigning access to specific areas facility wide, or even among multiple geographies.

- **Reduced opportunities for breaches**

Because biometrics eliminates the user of access enablers that can become separated from their authorised users, there are far fewer opportunities for security breaches. The authorised user absolutely must be present for access to be granted at any biometrically controlled checkpoint.

- **Indisputable audit trail**

Especially of interest in demonstrating compliance with government regulations concerning data storage, biometric access control produces an indisputable audit trail. db ServerRack extends that indisputable audit trail to the server cabinet. When paired with db Nexus, that audit trail can cover the entire enterprise, recording and reporting each instance of each individual's access from door to door to cabinet, and the exact time of each access – indisputably.

Although no data privacy rule or regulation specifies biometrics as the specific means to secure physical access, the Digitus solution unquestionably provides the most secure methodology available for addressing the intention of those rules and regulations, and its implementation is sure to satisfy even the most thorough regulatory audit.

Conclusion: Ensure regulatory compliance for physical access across your entire data centre

The need to protect sensitive data has never been higher, from the perspective of both good business practice and regulatory compliance – and that applies to physical as well as to network access. Physical security does not guarantee compliance, and compliance does not guarantee physical security. But the availability of a single, networked platform that can deliver biometric access control to every access point within an enterprise, with an indisputable audit trail, is a strong step toward unifying compliance and security programs – from the front door to the server cabinets.

The DCA will be holding the Site Access Control & Security workshop at UEL on the 12th June, all details can be found in the DCA Event Calendar http://www.data-central.org/events/event_details.asp?id=592386&group=

Scanning fingers on a touch screen

The changing face of 21st century data centre security

By Peter Jackson, CEO Jacksons Fencing.

WITH THE UK INDUSTRY expecting a 22% expansion in capacity over the next four years, to cope with society's every growing reliance on IoT (Internet of Things); from secure electronic data transfer and storage, cloud based services to critical M2M connectivity and 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 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 the local community.

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 three 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, the Risk and Threat Assessment stages which bring you to at a site design that works, and is able to offer appropriate security against unauthorised access is where a different set of challenges begin; 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, here are just a few examples:

On paper, physical perimeter security just like IT 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 a) advertising that they are protecting a valuable data centre or b) looking out of place in their surrounding environment and c) can offer some effect in mitigating the spread of noise and light from the site. At this point, you'll probably be glad to stick to dealing with trojans, malware, viruses and hackers and leave the vandals, thieves, activists and terrorists to us.

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.

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 systems, Tier 1 – 4,		
Senior Cyber and Risk Assurance Board, ISO27001	→	LPS1175 Certified SR Ratings, Secured by Design Preferred
Specification, CPNI Approved		
Blocked Port	→	Static PAS 68 Bollards
Switch	→	Rising PAS Road blockers and Bollards
DMZ (Demilitarized zone)	→	Stand off area between perimeter and assets
Security protocol	→	Onion principle of layered security
Security configuration	→	5 D Security architecture
Administrative Tools		→ Security Control Centre
Scheduled Vulnerability scan	→	Regular inspection of fence line and access
Scheduled Updates/Patches	→	Maintenance of security fencing, barriers, gates and access control
Security Patches	→	Repairs to security fencing, barriers, gates and access control
Traffic Redirection / Port Forwarding	→	Temporary security measures while security fencing, barriers, gates and access control are being maintenance or repaired
Core Protection	→	Target Hardening

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 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 offer LPS1175 certified ratings from SR 1 through to SR6, CPNI approval up to the highest level and Hostile Vehicle Mitigation protection to PAS 68 Ð 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.

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.