Snow - what snow?! ...

Even the weather can't stop the DCA, writes Steve Hone, DCA Operations Director.

THE 22ND JANUARY saw the Data Centre Alliance members only AGM which this year was held at QinetiQ's conference centre at Cody Technical Park in Farnborough. Despite the freezing temperatures and severe weather warnings of more snow to come the event was amazingly well attended with 90 members attending the AGM and a further 35 who joined them for the networking event which followed; so a personal thank you goes out to all those members who battled their way through the ice and snow on the day.

Given that not two years have yet passed since the DCA launched in May 2011 it was amazing to see so many members coming together; with over 300 members now actively involved in the DCA from all corners of the industry, one thing is clear next year a larger auditorium will be needed.

The AGM itself was split into two sessions Simon Campbell-Whyte DCA Executive Director chaired the session and introduced DCA President Steven Norris who gave a rousing conference address. Steven highlighted the importance of having an Industry Association such as the DCA to represent the Data Centre Sector, especially for helping those who do not understand data centres and the essential role they play. He also praised DCA members in building the collaboration platforms so essential for tackling the R&D, standards, skills, government and policy issues which face our ever growing industry.

The next presentation was from DCA Vice Chairman and CEO of Aimes Grid Services Professor Dennis Kehoe who covered the three DCA research and development projects currently underway and the work which the DCA is doing in supporting members in working with bodies such as the European Commission to put forward the industry's need for collaborative R&D projects and initiatives.

The final presentation before the break was given by Dr Ian Bitterlin; a key leader within the DCA Technical Council, Ian announced the DCA Certification programme for independent, industry led data centre standards. The scheme, under development for nearly 3 years, is currently going through final DCA member approval and Ian concluded by highlighting some of the key features the new DCA certification will address.

PEDCA

- Pan European Data Centre Academy
- Framework 7 Bid
- DCA lead with Partners from across UK, NL, DE
- Problem Identification and Solution Development proposal
- Submitted Early 2012

The second session of the afternoon got underway with an update from Dr Chris Francis of IBM and Chairman (Nominee) of the BSI UK mirror for ISO data centre standards. Chris provided an update on the role the DCA is providing to the development of new emerging standards on behalf of its members at both EU and ISO International levels.

This is essential and very important work as these emerging standards will affect us all and the DCA is providing its members with

> Given that not two years have yet passed since the DCA launched in May 2011 it was amazing to see so many members coming together; with over 300 members now actively involved in the DCA from all corners of the industry, one thing is clear next year a larger auditorium will be needed

regular updates and opportunities to comment via its collaborative member's online portal www.data-central.org

Skills and training was the subject of the next session led by Stephen Dennis, Head of Skills Development. This provided an update of the work the DCA is doing to ensure the industry is maximising the effectiveness of education and training, especially within academia, but also working with members who deliver training to ensure optimum returns on member's investments.

Stephen also outlined the output of several workshops with industry leaders and academia over the past 12 months where the needs to address a growing skills gaps, affecting many sectors of the Data Centre industry, were identified.

The final presentation of the AGM was provided by DCA Chairman Guy Willner. Guy has vast experience as the founder of IX Europe and former CEO of Equinix which together with his current work as CEO of International Data Centre Group, provides him with a unique perspective on the importance of international collaboration. Guy outlined the DCA's plans to widen participation and membership of the association which will result in DCA Chapters being formed in many regions around the world building on the DCA's existing network of members who currently span 18 countries.

Simon Campbell-Whyte drew the AGM to a close and handed over to Dominic Philips from Datum and Mike West from Keysource who kindly co-sponsored the networking evening as part of the official opening of Datums new Data Centre on the QinetiQ campus. A special thank you goes to Karl Bowling and the staffs at QinetiQ who were perfect hosts and really looked after everyone who attended. Many thanks again to all those that attended both the AGM and networking event and we look forward to working with you all in the year ahead and seeing you again at the next AGM in Jan 2014, hopefully without the snow!

Data centre security – Let's get physical

By Richard Jackson, CEO Jacksons Security.

In a society which is becoming increasingly dependent upon the processing and storage of information to oil the cogs of commerce, data centres - which provide the all-essential lifeline to ensure the continued efficiency of this information exchange - are vital to our modern economy. The consequences of a loss or compromise to the efficacy of a data centre can be potentially disastrous in terms of the chaos caused and the significant financial implications of a break in service. However, possibly even more detrimental in the long run is the loss of reputation which would inevitably occur following a major disruption in productivity.

When security is referred to in the context of a data centre, all too often thoughts focus on the security of confidential information and the steps that need to be taken to ensure that critical intelligence is stored safety and effectively.

However, there is little point in investing heavily in systems and protocols which contribute to an enhanced standard in the storage of data, if the physical security of sites housing such data fails to replicate the same commitment to protection excellence.

Any review of physical security measures should start with a comprehensive Risk and Threat Assessment to identify and prioritise the potential threats to site security. Decision makers for such matters should always focus on a long-term solution which will deliver a security infrastructure which will stand the test of time and therefore represent a sound investment. This is definitely not an area where cost should be the over-riding factor – fit for purpose products that have undergone rigorous testing, have been proven to offer a consistent high standard of performance and which are guaranteed to deliver over a lengthy period of time, should prevail. Meticulous risk and threat assessments should also form part of the maintenance

programme supporting the data centre to ensure all the protection measures that have been put in place remain relevant and capable of withstanding the challenges that are detected.

The Onion Principle

Security surveys employ what is termed the Onion Principle to develop a layered wall of defence around a potential target. The aim is to work from the outside into the centre, treating each different boundary as a layer which needs to be hardened to delay the attacker, protect the site's assets and provide security staff with intelligence through surveillance.It is this methodology, i.e. reviewing a site from the outside in, which should be applied when determining the required perimeter and physical security solutions for a data centre. All too often decisions are based on a printed plan, a product catalogue, a specification sheet or from a desk in an office looking out – but an effective perimeter / physical security protocol must be evolved by looking from an intruder's perspective, from the outside, looking in.

Jacksons offers a unique consultative service which enables clients to plan their physical perimeter protection and access control into the overall security architecture of the data centre. A holistic approach to fencing, gates, lighting, CCTV and access control measures must be adopted to ensure a successful outcome. Thorough site audits will take into consideration existing security measures and identify any potential weaknesses, and will play an active role in the development of a fully integrated security system, fit to face the challenges of the various methods and forces of attack employed by the modern day intruder. The 'layered' approach operates by identifying the various perimeters within the site, and increasing the level of defence as you enter deeper into the heart of the facility and closer to the most critical and sensitive assets.

Location, Location, Location

The site itself needs to be, as far as possible, uninhibited by risks and hazards – and must be located to benefit from a diverse range of utilities, infrastructure and transport unhindered by geographical / physical factors. The current flooding throughout parts of England and Wales and the associated encumbrance to business' in flood affected regions underpins the importance of this point.

The design and layout of roads providing direct access to the data centre site is a further important issue influencing site security. Ideally a design should be introduced which makes it impossible for vehicles to pick up speed on any roads leading to the site – one vehicle wide routes and the inclusion of chicanes can help to reduce the travel speed of traffic.

Varying ground levels need to be carefully recorded to ensure that any perimeter gates which are installed are not rendered ineffective as a result of large gaps underneath the installation. A reliable and stable source of power needs to be available, supported by an equally reliable standby power solution which will kick in, in the event of a grid power outage. 24-hour access to power is critical but not just to maintain the smooth operation of the equipment housed within the data centre. A loss of power may also represent a loss in site security since it will automatically affect any automated gates / barriers which have been installed to ensure effective access control.

Overall perimeter site security

The outer edges of the data centre's property boundary line should be viewed as the exterior perimeter of the site and this clearly requires a robust and effective ring of security around it to deter any unwanted / unauthorized entry. Whilst aesthetics almost certainly over-ride functionality, it is possible to introduce a 'hardened' perimeter security boundary which boasts all the necessary strength and resistance to attack required, whilst also blending in with the local landscape.

In addition to this the data centre facility needs to be divided into appropriate security zones representing the site's most important resources. Each layer of security should include a physical barrier to entry as well as detection and monitoring systems to deter, detect and delay any attack.

There should always be a limited number of entry points which are controlled via automated gates or barriers to the site, thus ensuring that any visitors are always identified at the same access point. Direct access into the data centre site should be segregated offering two entrances that results in only one vehicle or person gaining entry at any given time. Vehicle parking should also be kept away from the main areas and protection against potential ram-raiding activity is advisable.

Area surrounding data centre

Fuel tanks / essential environmental control equipment such as heating, ventilation and air conditioning units can serve as an easy target for malicious damage so thought should go into securing these areas via the introduction of suitable bespoke protection e.g. inherently strong steel cages. Similarly, the siting of roof or gantry mounted equipment should be incorporated into the security review and access restricted to minimize the risk of tampering.

Emergency cut-off switches also represent an acutely sensitive area and these will also require a robust layer of protection to deter / prevent any external interference, which could cause a major threat to the overall site security. Loading bay activities are best controlled by the main reception and monitored by CCTV. It is also important to ensure that CCTV footage is stored off-site, thus removing the opportunity for unauthorized visitors to review coverage with the intent of identifying possible loopholes in the system.

Acute access control

Throughout the data centre itself, a vigilant approach to access control is essential. Certain zones within the premises will represent high-risk areas which should only be accessible to authorized personnel via strict access control measures. In order to avoid unauthorised persons gaining entry by following an authorised person, a modern integrated access control system should always feature an anti-tailgating (airlock control) initiative.

For further information please contact Jacksons Security at www.jacksons-security.co.uk or call 01233 750 393.