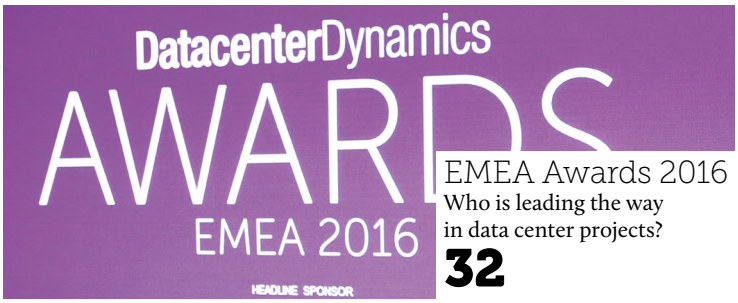
November 2016 • datacenterdynamics.com

DatacenterDynamics

The Business of Data Centers

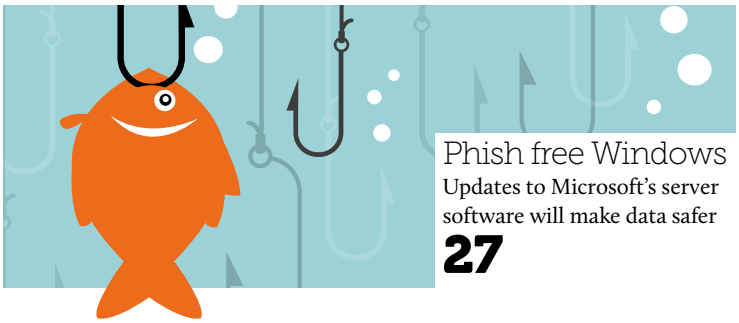
Cover Story
The attack of the IoT
Millions of new devices put the Internet at risk
24



EMEA Awards 2016
Who is leading the way in data center projects?
32

Many clouds
Users want multiple clouds: data centers must provide
16

Saving forest data
Japan helps share scientific data for environment work
18



Phish free Windows
Updates to Microsoft's server software will make data safer
27

Contents

November 2016

VOL 04 // ISSUE 18

Our tracks guide you through the DCD magazine, website and events

- **Colo + Cloud**
- **Power + Cooling**
- **Design + Build**
- **Security + Risk**
- **Core>Edge**
- **Servers + Storage**
- **Software-Defined**
- **Open-Source**

Meet the team

Peter Judge
Global Editor
@Judgecorp

Green Guru (Critical Environment). Also, open source, networks, telecoms, international news.

Max Smolaks
News Editor
@MaxSmolax

Captain Storage (IT & Networks). Also, international incidents, data sovereignty.

Sebastian Moss
Reporter
@SebMoss

Gets excited about open source software, security and high performance computing.

David Chernicoff
US Correspondent
@DavidChernicoff

Former CIO, test lab leader and developer. Our man in Philadelphia gets his hands dirty.

Virginia Toledo
Editor LATAM
@DCDNoticias

Editor LATAM edition DatacenterDynamics. Breaking the molds. Based in Madrid, Spain.

Celia Villarrubia
Assistant Editor LATAM
@DCDNoticias

Assistant editor LATAM DatacenterDynamics. News and pithy opinions in international edition.

Paul Mah
SEA Correspondent
@PaulMah

IT writer, also teaches tech in Singapore. Deep interest in how technology can make a difference.

Tatiane Aquim
Brazil Correspondent
@DCDFocuspt

Our Portuguese-speaking correspondent with an in-depth knowledge of Brazilian public sector IT.

UNITED KINGDOM
102–108
Clifton Street
London
EC2A 4HW
+44 (0) 207 377 1907

USA
28, West 44th Street,
16th floor
New York,
NY 10036
+1 (212) 404 2378

SPAIN
C/Bravo Murillo
178 – 2ª Planta
28020 Madrid
España
+34 911331762

SHANGHAI
Crystal Century Tower, 5/F,
Suite 5B
567 Weihai Road
Shanghai, 200041
+86 21 6170 3777

SINGAPORE
7 Temasek Blvd
#09-02A,
Suntec Tower One
Singapore 038987
+65 3157 1395

ADVERTISING
APAC
Vincent Liew
EMEA
Yash Puwar
LATAM
Daniel Clavero
Santiago Franco
USA
Kurtis Friesen

DESIGN
Head of Design
Chris Perrins
Designers
Fay Marney
Holly Tillier

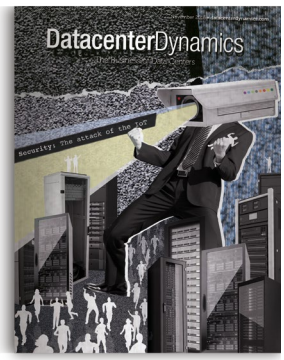
ASSOCIATE PUBLISHER
Ewelina Freeman

CIRCULATION
Manager
Laura Akinsanmi

FIND US ONLINE
datacenterdynamics.com
datacenterdynamics.es
datacenterdynamics.com.br
twitter.com/DCDnews
Join DatacenterDynamics Global Discussion group at *linkedin.com*

SUBSCRIPTIONS
datacenterdynamics.com/magazine

TO EMAIL ONE OF OUR TEAM
firstname.surname@datacenterdynamics.com



Safe operation

thanks to hygiene-certified

dry cooling

- Up to 80 % less water consumption than a cooling tower
- Plume-free throughout the year
- Verified aerosol-free operation
- 100 % dry operation for majority of the year

HYGIENE
VDI 2047-2
CERTIFIED

JÆGGI

www.jaeggi-hybrid.eu

When it needs to be safe:
Hybrid Dry Cooler HTK

We place economic efficiency and environmental protection on an equal footing. Our products and services make an active contribution to lowering your operating costs and conserving resources. Our coolers carry hygiene certificates and are verified for aerosol-free operation. In a concern for the highest possible safety from the manufacturer side, JAEGGI had the sophisticated design of its units officially inspected by an independent body.

We naturally take the requirements of the relevant laws and standards of other countries into consideration when constructing our units. In particular, we have engaged with independent advice from one of the co-authors of ACOP L8 to ensure that our hybrid dry coolers are fully compliant with all current UK guidelines. It has been confirmed, both in the laboratory and in measurements in the field, that JAEGGI units do not generate any measurable aerosols when used as specified, and are thus tested for safety.

Member of Güntner Group GÜNTNER

When the IoT struck back!

We have had warnings that connecting a lot of devices to the Internet might cause problems. In October we saw what those problems might be.

A host of consumer devices, including IP security cameras and video players, were subverted with malware, and took part in a colossal botnet attack on the Internet's infrastructure. Netflix, Amazon, Spotify and several other consumer sites became unavailable for many people. The Mirai botnet had previously hit the Krebs Security site, and had been open sourced, meaning that it is available to anyone.

This illustrates how much the risks to digital infrastructure have changed.

We've got the hang of securing business IT equipment, with PCs and servers locked down by default. It looks as if Internet of Things (IoT) manufacturers are having to learn that lesson over again - and they are putting out an order of magnitude more devices.

Our security coverage looks at this and other novel risks to our online infrastructure (p20). We also take a look at how traditional Windows server software is adapting to traditional phishing attacks (p27).

We have just held our London Zettastructure event, full of illuminating content there on this issue and many others. Some of it has made it into this magazine - the rest will be developed in future issues, and on the web.

DCD's EMEA awards are now in their tenth year, and just as exciting as ever. The shortlist is now out (p32), so you can see who are a contender for this year's anniversary prizes, to be awarded in London in December.

Air gaps are a big con as a security strategy according to Ed Ansett (p31). Industrial equipment is often insecure by design; if you believe you can simply keep it disconnected from the Internet, you may be mistaken, because there are all sorts of ways connections can be added without any consideration.

•

Peter Judge – Global Editor
@Judgecorp

IoT is a problem. The vendors haven't learnt, and the impact of their failure is an order of magnitude bigger

650 Gbps

Size of Mirai-based botnet attack (Krebs on Security)

THE GAME-CHANGING DATA CENTER.

NOW IN MONTREAL & QUEBEC CITY, CANADA

ECO-FRIENDLY

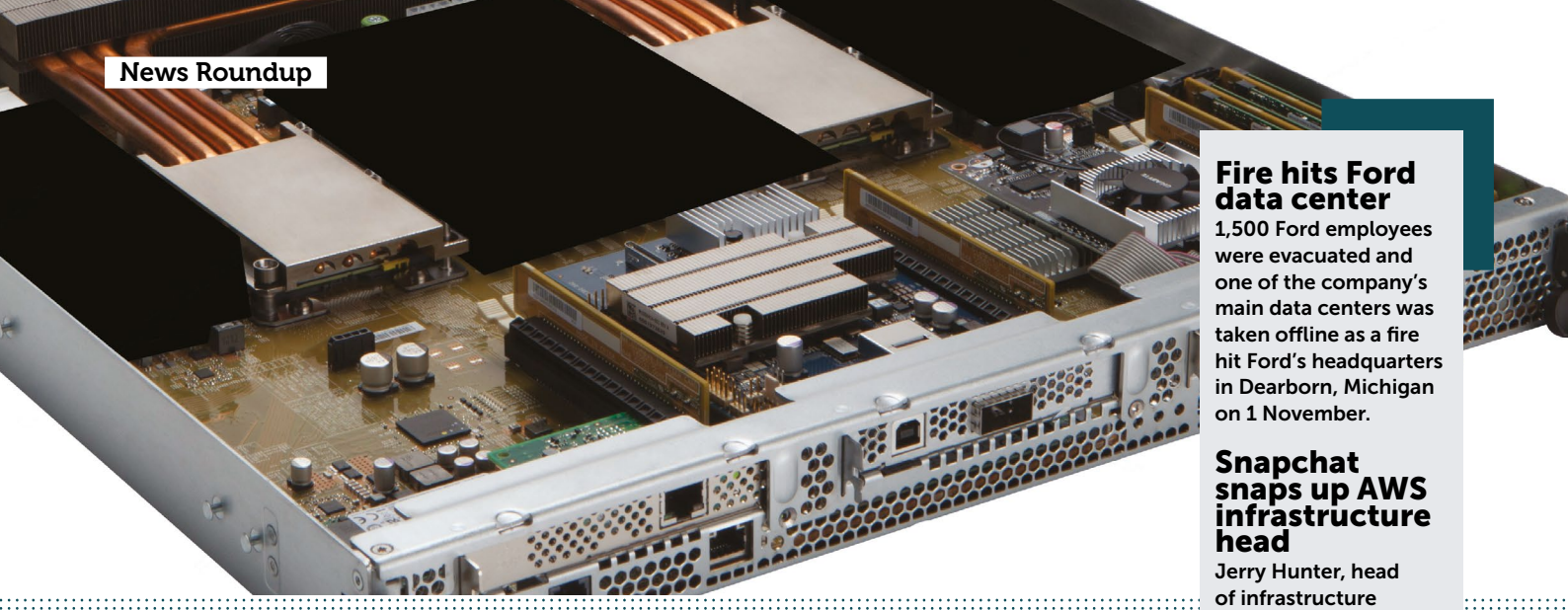
Clean energy and a smart cooling system for impressive efficiency.

FLEXIBLE COLOCATION

High-density cabinets with adaptable space in a carrier-neutral data center.

4DEGREES-COLO.COM

4° DATA CENTERS



Fire hits Ford data center

1,500 Ford employees were evacuated and one of the company's main data centers was taken offline as a fire hit Ford's headquarters in Dearborn, Michigan on 1 November.

Snapchat snaps up AWS infrastructure head

Jerry Hunter, head of infrastructure at Amazon Web Services, has become VP of engineering at Snapchat - which currently has no data centers at all.

STT seals Tata deal

Singapore's ST Telemedia has completed a deal to buy Tata's data centers in Singapore and India, giving it a majority of Tata's data center business

ACI opens in Limerick

Electronic payment and banking company ACI Worldwide has opened its European data center in Limerick, Ireland. The redundant facility will add 50 jobs to the region.

Microsoft shares raw Olympus servers

At DCD's Zettastructure event in London, Microsoft open-sourced another set of blueprints for hyperscale servers - but this time, they are only halfway finished.

Project Olympus was designed in collaboration with the Open Compute Project (OCP). It is not just a server ecosystem, but a new hardware development model that encourages wider community participation in the early design stages, heavily inspired by development methods used in open source software. It is just 50 percent complete, with the rest of the work due to take place over the next eight months, with yet-to-be-announced partners.

Microsoft has been steadily increasing its participation in open source initiatives, having joined OCP in 2014. Through the non-profit, the company has been sharing designs of servers used in the data centers that power Azure, as well as some more unusual ideas, like the notion that lead-acid UPS battery banks could be replaced by small Li-Ion cells distributed throughout the racks.

Microsoft is also a huge buyer of OCP hardware, with more than 90 percent of the servers it procures today being based on OCP-contributed specifications.

According to Microsoft, the current open hardware development model lacks agility, since it requires designs that are production-ready. With Project Olympus, Microsoft proposes an alternative: open hardware designs are donated earlier in the cycle than any previous OCP project.

Project Olympus itself consists of a universal server board, high-availability power supply with included batteries, 1U/2U server chassis, high-density storage shelf, a new universal rack PDU and a standards compliant rack management card.

Surprisingly, Project Olympus uses three-phase AC power, instead of the DC bus bar seen in OCP's Open Rack. Kushagra Vaid, Microsoft's Azure hardware manager, explains why below.

http://bit.ly/2fvxkP3

VOX BOX / DCD VIDEO

Kushagra Vaid
Azure hardware general manager
Microsoft

Why does Project Olympus use AC?
There are two reasons to use three-phase AC. The first is efficiency: a DC bus bar has I^2R losses, while three-phase distribution has only one conversion and is 97 percent efficient. The second is phase balancing. A cloud data center can lose seven percent of its capacity because of phase imbalance caused by uneven distribution of workloads. Olympus is phase balanced by design, because every phase goes to every server.

http://bit.ly/2fvC8UX

Peter Feldman
CEO
DataGryd Data Centers

What's happening at your iconic Manhattan building?
In 60 Hudson Street, we need high power and high cooling - but in a space which is almost 100 years old. The building is the main network hub for the US East Coast, and connectivity continues to grow. We're a space and power provider that takes care of the challenges that New York presents where cloud providers can make money on their core services.

http://bit.ly/2exZCKa

VMware puts cloud data center service on AWS

Virtualization giant VMware has signed a much-anticipated deal with the public cloud service leader Amazon Web Services, which gives both a more credible hybrid cloud strategy - by offering VMware's software defined data center (SDDC) on Amazon's cloud, as VMware Cloud on AWS.

The new service will be VMware's major public cloud offering, and it will eliminate the binary choice between the VMware environment and the AWS public cloud, the two companies' CEOs said at a San Francisco press conference. It will be the first VMware-supported implementation of VMware's software on Amazon's cloud, and will be sold by VMware and not by AWS. Meanwhile, VMware will continue to support its VMware public cloud, and has deals with other cloud providers including IBM.

Most hybrid implementations are built on AWS and enterprise data centers overwhelmingly built on VMware, admitted AWS CEO Andy Jassy: "People want to leverage the investment they've made to manage their software on-prem," he said. "You want to use the same software in the public cloud."

That's quite a change in sentiment from Amazon, which has previously wanted to simply replace enterprise data centers. That's still the long-term goal, but the two CEOs agreed that on-premises IT would be around for "decades."

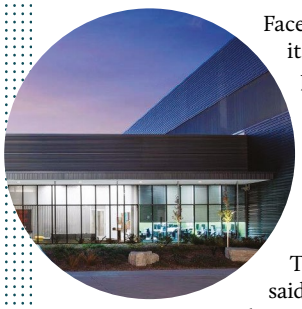
Meanwhile, VMware is changing tack since its acquisition by Dell as part of a merger with EMC. VMware CEO Pat Gelsinger said the vCloud Air public cloud offering will continue, but VMware has handed over a jointly-developed public sector cloud initiative to its partner QTS.

The service runs directly on AWS' physical hardware, so VMware can run vSphere, Virtual SAN (vSAN), and network virtualization platform without having to use nested virtualization. VMware can be accessed hourly on-demand or in subscription form.

The plan is to allow VMware users to build on AWS without new training.

http://bit.ly/2exHqyz

Facebook adds cold storage in Altoona



Facebook will extend one of the buildings in its Altoona data center cluster, after three previous expansions at the Iowa location.

The latest addition will be a 100,000 sq ft (9,290 sq m) cold storage facility to store photos users access rarely.

This fourth expansion is the latest from Facebook's "construction teams who have worked onsite since 2013," Brice Towns, Altoona data center site manager said in a Facebook post. The first phase of the Altoona data center was a 476,000 sq ft (44,221 sq m), $300 million construction, the second was a 468,000 sq ft (43,478 sq m) building, and the third a 496,000 sq ft (46,079 sq m) facility.

The new cold storage facility comes after Facebook's Prineville and Forest City data centers also had cold storage sites added.

In May 2015, Facebook software and infrastructure engineers Krish Bandaru and Kestutis Patiejunas described the company's cold storage tech.

They said: "The data centers are equipped with less than one-sixth of the power available to our traditional data centers, and, when fully loaded, can support up to one exabyte (1,000 PB) per data hall.

"Since these facilities would not be serving live production data, we also removed all redundant electrical systems — including all uninterruptible power supplies (DCUPS) and power generators, increasing the efficiency even further."

http://bit.ly/2enVBs2

Huawei to build Tier III modular campus in Dubai

Chinese infrastructure giant Huawei has been contracted to build a large modular data center campus for Dubai International Airport, in the United Arab Emirates (UAE).

The collection of facilities codenamed DXB will offer advanced reliability features and will be used to host the airport's private cloud.

According to a report by Xinhua, this will become the first modular campus in the world to be fully certified as Tier III – concurrently maintainable - by the Uptime Institute.

Dubai International Airport is the biggest civil aviation hub in the Middle East. It served 78 million passengers in 2015, and hoped to increase this number to 90 million by the end of next year.

The company required a new data center to support its operations, and chose Huawei to provide modular data centers within the DXB, which is planned to consist of two facilities, that will mirror each other to achieve high availability.

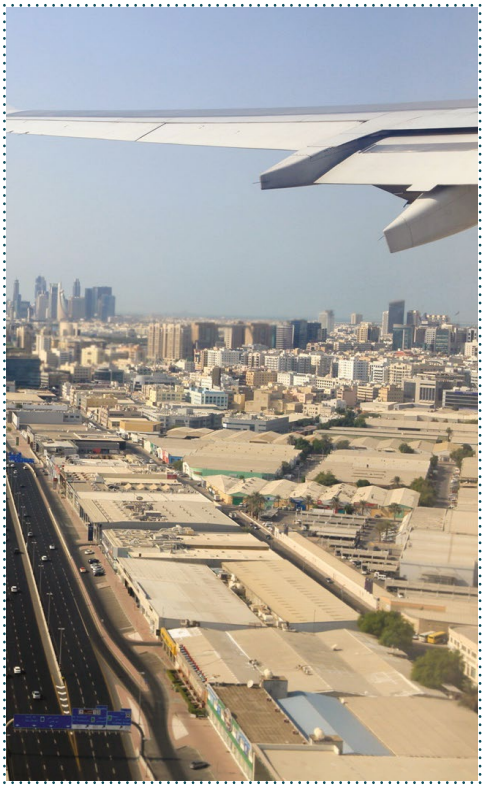
The first CXD data center is scheduled to come into operation sometime in 2017. The deadline for the second phase is yet to be confirmed.

Modular data centers can be constructed in a fraction of the time it takes to erect a traditional facility, and can be easily shipped to areas where building a permanent data center is impractical.

"Technology is key to enhancing our ability to grow, innovate and ultimately enhance the customer experience," said Abdel Rahman Alhosani, vice president in charge of business technology infrastructure and operations of Dubai Airports. "At the same time we will improve system reliability across both airports and cut operational costs."

Dubai has attracted cloud operators, including Chinese giant Alibaba.

http://bit.ly/2enXJA1



AWS opens Ohio region, with three data centers

The US East (Ohio) Region of Amazon Web Services is now online, consisting of three separate Availability Zones - geographically distinct data centers within the Ohio area.

Ohio Governor John Kasich previously endorsed Amazon's $1.1 billion plans for the state, and again hailed the news as good for the region: "Ohio is not just embracing the new knowledge economy, we're also advancing the technologies on which that economy will thrive. Technologies like the cloud computing, artificial intelligence, drones, and self driving vehicles."

Amazon is also funding the 100 megawatt Amazon Wind Farm US Central in Ohio that is expected to produce 320,000 megawatt hours of wind energy annually when it is fully operation from May 2017.

In addition, AWS will team up with the Ohio Academic Resources Network (OARnet) that works with member organizations to provide intrastate networking and other IT services.

The two groups will 'explore' AWS Direct Connect access to Ohio's 100-gigabit research backbone network, allowing colleges, schools, medical research hospitals, and state government to take advantage of a state-funded high-speed network connection straight to AWS.

AWS now has five regions in the US, made up of 16 Availability Zones. Nine more Availability Zones and four regions in Canada, the UK, France, and China are planned to come online in the coming months.

http://bit.ly/1C7SxDT

UK cryogenics to power Malaysian test site

A UK and Malaysian consortium will build a test data center that makes use of liquid nitrogen for power and cooling.

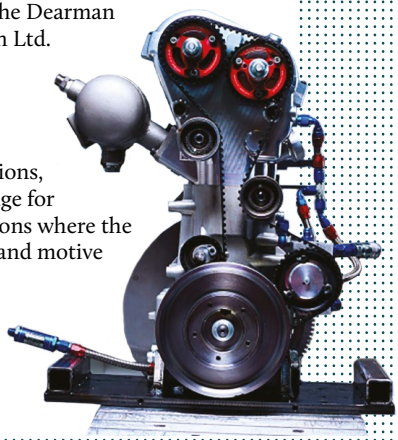
Dearman from the UK and Green Data Center LLP of Malaysia will investigate how data centers might harness a Dearman engine - a system which uses the expansion of liquid nitrogen to simultaneously provide power and cooling. The project will start with a 220kW demonstration facility and decide on the eventual role of the Dearman engine based on its performance. Two universities, Heriot-Watt in the UK and Universiti Teknologi Malaysia, are also involved.

Cryogenic energy storage uses liquefied gases to store energy. They can be kept in insulated containers and then drive a turbine when they are allowed to expand and evaporate. The expansion also provides cooling (due to Boyle's Law).

Self-taught engineer Peter Dearman wanted a car powered by liquid nitrogen and invented the Dearman engine, now marketd by Dearman Ltd.

"It is very clear that Dearman engines are an alternative to diesel engines," Dearman's head of communications Ben Heatley told DCD. "Both in fixed applications, providing supermarket cold storage for instance,, and in mobile applications where the engine can provide refrigeration and motive power for a delivery truck."

Green Data Center LLP is a startup working on immersion cooled data centers.,



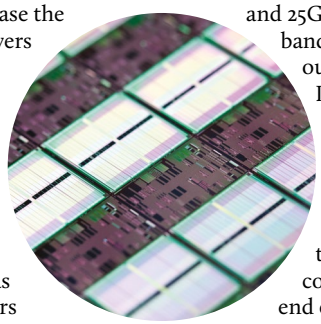
http://bit.ly/2eBiC9y

Vendors use OpenCAPI to gang up on Intel

Some of the world's largest manufacturers of silicon chips have released the specification for a server expansion technology that promises to be much faster than PCIe.

OpenCAPI is a hardware standard originally developed by IBM that puts compute power closer to the data and can be used to connect components like new types of memory, GPU accelerators, and networking and storage controllers.

The OpenCAPI Consortium claims that in specific use cases, it could increase the performance of servers tenfold.



The technology is supported by chip vendors including AMD, IBM, Mellanox Technologies, Micron, Nvidia and Xilinx, as well as server manufacturers like Dell EMC and Hewlett Packard Enterprise. However it does not feature Intel – the world's largest maker of CPUs.

The first OpenCAPI-enabled products are expected in second half of 2017.

OpenCAPI is capable of delivering low latency and 25Gbps of bandwidth, easily outperforming PCIe, which maxes out at 16Gbps. The open standard will be available to the public at no cost before the end of the year.

IBM plans to introduce Power9-based servers that use the OpenCAPI specification in the second half of 2017. Meanwhile Google and Rackspace are collaborating on a Power9 server codenamed Zaius, which will also feature OpenCAPI. Mellanox plans to enable the new specification capabilities in its future products, and Xilinx plans to support OpenCAPI enabled FPGAs.

Interested parties can register and download the specification directly online. Companies with plans to develop products based on OpenCAPI may do so by either joining the Consortium – which has an open membership structure - or obtaining a relevant license. The organization will also provide reference designs.

http://bit.ly/2dPlyoi

$25bn

Price paid by CenturyLink for network firm Level 3

US tax breaks pay $2 million per data center job

Local and state governments in the US are being too generous with subsidies for data center projects, considering the amount of jobs they actually create - according to research by Good Jobs First, a policy thinktank that promotes accountability in economic development.

The numbers suggest that government officials are losing sight of the big picture when offering tax exemptions to win data center investment, and end up paying approximately $2 million for every new job. Data centers get tax breaks in 27 states.

Good Jobs First recommends a cap on subsidies, at $50,000 per job, and added that government agencies should be ready to walk away from bidding wars that lose taxpayers' money.

In a study entitled Money Lost to the Cloud, the non-profit identified 11 major data center projects by the likes of Apple, Amazon, Facebook and Google, and found that the average cost per job in all incentives stood at $1.95 million.

Good Jobs First said the real figure is likely even higher, since some state and local governments fail to disclose the total subsidy program costs.

http://bit.ly/2e038qL

Facebook Wedge 100G switch available

A new 100Gbps version of Wedge, Facebook's top-of rack data center switch, has been accepted by the Open Compute Project (OCP) and delivered to the wider world as a product from Edgecore Networks.

The Wedge 100 is a 32 port 100GBE switch, built by Accton Technology to Facebook's design, for use within Facebook's data centers. The design has been shared, and accepted by the Open Compute Project, and meanwhile Accton is making a commercial version of the switch, the Wedge 100-32X, which is being sold through Accton's subsidiary Edgecore.

The switch joins a growing range of Open Compute compliant switches, designed to simplify data center networking and allow large data centers to specify efficient low-cost open source hardware. Since OCP was set up by Facebook in 2011, it has been joined by large web-scale cloud companies including Apple in 2015 and Google in 2016, while delivering specifications for racks, servers and switches.

The Wedge 100 uses much of the same hardware as its predecessor, the Wedge 40, and runs the same FBOSS software, extended to support the the 100G ASIC chips and optics in the new model. It includes a compact microserver built to the industry standard in the standard 95mm x 95mm computer-on-module COM-Express Type 6 form factor, but also supports larger standard 95mm x 125mm size modules for more advanced CPUs.

To make life easier for Facebook's busy technicians, the switch is more serviceable: its top can be popped off without tools, and hot-pluggable fan trays can likewise be removed without tools, using a clip instead of a thumb screw. There's now a status LED for fan trays.

http://bit.ly/2egFOaV

Node Pole bought by power companies

The Node Pole, a major data center development in the industrial north of Sweden which is home to Facebook, has been acquired by local energy companies Vattenfall and Skellefteå Kraft.

As well as Facebook's facility in Luleå and Hydro66 colocation site in Boden, the site hosts other facilities, and has ample space and power available for future projects.

The new owners will continue developing the Node Pole as a data center hub. Financial terms of the deal were not disclosed.

"Today's news is the ultimate proof that our vision has been right all along," the Node Pole chairman Peter Ericson said. "We now see the largest benefactors from these types of investments gearing up and also wanting to be proactive in building a long term investment climate and development cluster upon our supreme basic conditions."

The news comes ahead of the long-expected changes to the pricing of electricity for data centers, expected to be announced by the Swedish parliament in December.

The Node Pole is just 50 miles away from the Arctic Circle. It benefits from cheap, 100 percent renewable electricity derived from hydroelectric dams on the Lule River, where the grid hasn't had a blackout since 1979.

The entire development is being acquired by Vattenfall and Skellefteå Kraft – the former is Sweden's largest utility company that's already providing electricity to both Hydro66 and Facebook.

According to the Node Pole, the partners will continue developing the data center campus, but will make it a part of an even larger plan – establishing Sweden as the first choice in Europe for all kinds of industries in need of stable, long-term access to cheap and sustainable energy.

The company says that Sweden currently has around 1,400MW of spare power capacity.

http://bit.ly/2eDF4MO

Equinix to use space laser WAN links

A new satellite laser network will connect to Equinix data centers and provide a backup to fiber connections.

Laser Light's high articulation laser optics (HALO) network uses space-based laser communication technology, and aims to provide Optical Satellite as a Service (OSaaS) networks for carriers, enterprises and government customers at Equinix facilities. It will be able to connect to points around the globe with 100Gbps links.

The satellite company will establish its first Point of Presence (PoP) at Equinix's DC11 International Business Exchange data center in Washington, DC. Once there, it will test and demonstrate its technology, ahead of a planned further expansion to Equinix facilities including those in the UK, Japan, Brazil, Australia, the Middle East, and across Europe.

The service capacity of the HALO constellation of 8-12 medium Earth orbit satellites is planned to be 7.2 Tbps, made up of 48 satellite-to-satellite 200Gbps optical crosslinks and 72 satellite-to-ground 100Gbps optical up/down links.

Ihab Tarazi, Equinix CTO, told DatacenterDynamics that "SpaceCable" would be an option alongside conventional fibre,

"These satellites put in now can use new coherent advanced optics – the same ones they use underwater – and with that you're going to be able to squeeze a lot more capacity into satellites, so we see satellite distribution as a second option for places that you cannot get to so easily with cable," said Tarazi. "But fiber will always be number one in its capacity, and satellites will be filling in the gaps in places that are hard to get to."

http://bit.ly/2eo8PVy

Facebook triples size in Fort Worth

Facebook is expanding its data center complex in Fort Worth before the site opens. The announcement came just as the first racks started to arrive, ready for the first building to open early in 2017.

The project at 4500 Like Way, will now include five buildings providing up to 2.5 million square feet (230,000 sq m). When Facebook started work on the site in July 2015, three buildings were planned, totaling 750,000 sq ft (70,000 sq m). The expansion will use 39 acres of land bought for the purpose in 2015, according to a report in the Star-Telegram. The expansion follows continued growth in Facebook's data center estate, and underlines the explosive growth of the industry in the Dallas Fort Worth area.

"We plan to expand our Fort Worth data center to five full buildings over the course of the next few years, and invest in the necessary supporting infrastructure," said KC Timmons, site manager.

With an average of 950 workers on site every day, the project has taken more than 1.7 million hours of work so far.The site has a power purchase agreement which will fund 200MW of new wind power for the Texas grid.

The site has a 20-year $146.7 million tax incentive package from Forth Worth City Council, along with a 10-year deal which gives up to 60 percent abatement on taxes for property value.

Facebook has also begun work on a $250 million site won by Los Lunas, New Mexico, after a bidding war with Utah.

http://bit.ly/2eW4zqu

Chanel puts data centers in Paris show

Chanel head designer Karl Lagerfeld used data centers as the theme for an event at the Paris Fashion Week.

Guests saw models parading in front of a Grand Palais backdrop decked out to look somewhat like a data center. Ethernet cables in various colors were wound round and plugged into some kind of fascias. The actual kit looked obscure, although it was installed in racks and had some sort of overhead cabling. One strange detail is that close ups seem to show activity lights on by empty sockets.

DCD was not on the guest list, so we turned to the experts. The Guardian's fashion editor Jess Cartner-Morley wrote that it was a mix of both future and retro:

"The retro mood was overt in the styling. Models in skewed baseball caps and side ponytails wore medallions around their necks in the style of the Beastie Boys' Licensed to Ill era. (That the medallions could be reconfigured as modern office-pass lanyards added a layer of modern, e-surveillance paranoia.) Handbags were modelled on robots of a Star Wars vintage. But the clothes were classic Chanel: bouclé tweed suits worn shoulder-robed with flat boots, and silk tea dresses slit to the hip for this season's on-trend flying panels, in circuit board prints."

Vogue's Suzy Menkes asked: "If the models were supposed to be a futuristic tech group, shouldn't these smart women have been wearing techno fabrics and the kind of clothes that suit hot desking and 20 hour work shifts? Instead they had on boring old baseball caps."

There were, however, robot handbags that flashed.

http://bit.ly/2d8S5OM

CoreSite opens 230,000 sq ft Santa Clara site

US-based CoreSite Realty has opened its latest data center - its fifth on the Santa Clara campus, and seventh in Silicon Valley. 62 percent of a possible 230,000 sq ft (21,000 sq m) of turn-key capacity has already been leased.

The new data center is the largest on the Santa Clara campus, and was built to meet what the company calls a strong demand for multi-tenant data center space in the Silicon Valley market.

Paul Szurek, CoreSite CEO, said: "Santa Clara remains one of the top markets in the US, with strong data center demand, and we believe that our SV7 development provides a differentiated colocation solution to this robust market.

SV7 will provide native connectivity to AWS, along the with company's suite of interconnection services, such as the CoreSite Open Cloud Exchange, and the Any2 Internet Peering exchange. The location also enjoys direct access to submarine cables between North America and Asia-Pacific.

http://bit.ly/2eyjJrt

Snowden reveals NSA built a Tier III data center in the UK in 2011

Newly released documents from Edward Snowden have revealed that the NSA built a Tier III data center at the Royal Air Force Menwith Hill base in North Yorkshire, England in 2011, to support intelligence work.

The 10,000 sq ft (923 sq m) data center was the NSA's first Tier III facility - although it is not believed the site was certified by by the Uptime Institute.

Menwith Hill specialized in monitoring communications sent between foreign satellites and wireless communications on the ground, such as cellphone calls and WiFi traffic.

A 2006 NSA document states: "The commercial satellite communication business is alive and well and bursting at the seams with increasingly sophisticated bulk (Digital Network Intelligence) traffic that is largely unencrypted. This data source alone provides more data for Menwith Hill analysts to sift through than our entire enterprise had to deal with in the not-so-distant past."

Targets included the People's Republic of China, Latin America and North Africa, but a particular focus was on Afghanistan and Pakistan.

How much data was recorded is unknown, but a May 2011 example cites 335,663,981 metadata records stored in the span of 12 hours.

To store all of this, more than $40 million was spent at the Menwith Hill Station (MHS) between 2009 and 2012 on a new 95,000 sq ft operations building that included the 10,000 sq ft data center, codenamed Phoenix.

http://bit.ly/2dPrSoE

GEIST
Future Thinking • Solutions Today

Superfast!

Rack PDUs from order to delivery in as few as 3 days

Waiting months for your rack PDU order to arrive from the other side of the world must be incredibly frustrating. Geist manufactures PDUs locally - built to your specification - so they arrive when you need them.

With Geist you can power up your servers within days.

GEIST POWER | Upgradeable

Head to **go.geistglobal.com/DCD-SuperfastNov** for more information

DCD > Enterprise | New York

Free qualified end-user passes available

+ THE EAST COAST'S MOST ANTICIPATED DATA CENTER TRANSFORMATION EVENT

March 14-15 2017 // **Marriott Marquis**, Times Square

For more information visit www.**dcdconverged**.com

#DCDEnterprise

One cloud provider is never enough

Enterprises never consolidate to just one cloud. They need help with hybrid, says *Paul Mah*

If you expected the cloud to suddenly simplify IT, the reality may be something of a disappointment. Enterprises are not buying into one cloud over another, but are rolling out multi-cloud deployments.

Enterprises are finding that they are running applications which are committed to different cloud providers, according to Omer Wilson, the APAC marketing director at Digital Realty. And he should know, as Digital has a large number of cloud providers operating from within its data centers.

Customers are demanding access to a number of providers, because one provider is not enough, Wilson told us: "Customers don't change their view in terms of the providers. They just need access to the cloud, they need access securely. They don't need access to just one large provider; a lot of them are using a number of different cloud providers."

So they might have one cloud instance for customer relationship management (CRM), and a completely different architecture for their financial systems and payment gateway.

Inevitably, this means that enterprises need a hybrid architecture to facilitate their consumption of multiple clouds, be it a private cloud deployment or secured, high-speed access to the relevant public cloud providers.

"They need secure multiple access points to give customers access, and they need to be able to move workloads intelligently between the different deployments," said Wilson, who noted that such requirements are seen not just within the enterprise sector, but also with his customers in the financial services, telecommunications and system integrator sectors.

Paul Mah
SEA Correspondent
@PaulMah

Customers have one cloud instance for customer relationship management (CRM), and a completely different architecture for their financial systems.

Location is another factor when it comes to picking the right data center that enterprises look at. He said: "Depending on the type of customers they are, there may be geographical requirements, where they have to be in certain geography with their data – their customers are demanding that."

Of course, a lot also hinges on the needs of individual enterprises. Factors include how far along an organization is in their cloud journey, the remaining applications that needs to be put into the cloud, or even the location of their worldwide or regional headquarters, noted Wilson. Moreover, some may be looking at developing large hubs for serving the region, while others may be looking at provisioning an edge presence, he said.

Unsurprisingly, the multi-cloud requirements of modern enterprises and the networked nature of cloud services makes the network even more crucial today.

"[The] network has always been important, but in the last few years it has become even more so," said Wilson. "When enterprises are trying to deliver cloud services to the customer, there's when it becomes important. When they are accessing it in the background, it is important that they can access it securely."

According to Wilson, part of what makes connectivity important is how even the largest cloud and data center providers cannot be physically present in every geographical location.

This brings to mind the goal of cloud juggernaut Amazon Web Services (AWS), which has said it aims to have data centers in "virtually every major country." At the moment however, its only data centers in Southeast Asia are located in Singapore.

"[Providers] are never going to be in [every country], or everywhere the customers need to be. The important thing now is we need to break down the barriers. The customers just need to access their cloud and their content," he said.

This would explain Digital Realty's launch last month of its Service Exchange platform in partnership with Megaport, a global interconnection services provider. The idea behind Service Exchange entails leveraging the capability of SDN (Software Defined Networking) to deliver private dedicated network access directly to cloud providers such as AWS, Google Cloud and Microsoft Azure.

"Even though we don't have a physical footprint in various markets, [we are] now enabling access though Service Exchange to enable customers to get out to where they need to be." he said. While some predicted that the rise of cloud computing would reduce demand for data centers, the reality is that cloud providers actually increased demand for data center space, said Wilson. And he says the fundamental requirements that undergird modern data centers have stayed the same.

"There is always going to be cooling, backup power, and physical security. These are the basics, along with considerations such as whether there is raised floor for cooling," Wilson told us.

Other demands from customers such as financial institutions include Uptime Tier certification, physical security, and the availability of the building. However, he did concede that server technology is changing quickly, and that the structure of the data center suite is evolving as data centers become more software-defined.

"Data center providers and operators need to be ahead of the curve, our job is to be flexible enough in the locations we can serve them, to match the technology that customers are developing," he said.

Wilson says the traditional focus on achieving 2N redundancy is changing: "Historically, we built data centers with everything backed up and fully redundant. Now we can be very flexible. If the customer doesn't need that much redundancy, we can build it up in terms of the suite structure. If they need more, we build up," he said.

> *Customers have one cloud architecture for CRM, and another for their finance and payment gateway*

"We leave the flexibility to have the space available to the customer. However, we don't assume from day one that they need the structures that we built for (other) customers. It is a flexible, modular design."

So what's next for Digital Realty in the region? According to Wilson, the company could be making Service Exchange available here as soon as early next year, along with catering to customers in Singapore that require a smaller footprint in terms of space. The latter is not only to serve customers within the market, but to cater to multinational companies from the US and Europe markets looking to begin with a smaller deployment.

Are there plans for more data centers in Southeast Asia? "We still feel there is enough significant demand in terms of our existing and new customer base to enable growth. Loyang [data center] is building up nicely and still available," said Wilson.

Digital Realty in Asia

- **Singapore Loyang Way, 13.2MW**
- **Singapore Jurong, 30MW**
- **Hong Kong, 8.6MW**
- **Melbourne, 12MW planned**
- **Sydney, 6MW**
- **Osaka, up to 76MW**

Brazil and Japan share rainforest data

Brazil and Japan have built a shared data center for biodiversity data. *Tatiane Aquim* investigates

Amazon rainforest

- 5.5 million sq km of green space
- 60 percent of this is in Brazil
- 16,000 tree species
- 2.5 million insect species
- Highest biodiversity on Earth

Tatiane Aquim
Brazil Correspondent
@DCDFocuspt

Brazil's Federal Government has promised that scientific data generated within the nation must be stored in Brazil. A collaboration with Japan is helping to make this happen.

The National Research Network (RNP) of Brazil has partnered with the National Institute of Amazonian Research (INPA) to create a shared data center in Manaus, which will store scientific data collected by the Forest Museum project, safely within the confines of Brazil.

The initiative is being put together with Kyoto University, using finance from the Japan International Cooperation Agency (JICA-Brazil). The shared data center will be run by the RNP, which expects an average demand of 1Tbyte per month.

With this in place, Brazil now has a dedicated network infrastructure, along with data processing and storage, for the academic community.

It will disseminate knowledge and help develop collaborative research, providing a large database for researchers in Brazil and abroad.

The partnership with the University of Kyoto will allow Brazil's national research network to demonstrate the importance of secure storage for international projects, and the feasibility of sharing data from any region.

> *The data center will share and preserve scientific data*

"The shared data center is an essential component in the Brazilian academic community's IT infrastructure, increasing the interaction between research institutions, promoting the exchange of knowledge, facilitating the analysis of documents, and speeding up information processing and tool development," said José Luiz Ribeiro Filho, director of solutions and services at the National Education and Research Network.

The shared data center (CDC) is the first initiative of the Interministerial Program RNP, formed by several ministries including Science, Technology, Innovation and Communications, Education, Health, Culture and Defense, to invest in a computing cloud service for the education and research community in the country.

Hosted by INPA, this is the largest data center in the North of Brazil, and the fifth largest in the country.

For its implementation in 2015, the RNP used IDS1000 containers, from Huawei.

The data center will give visibility to the scientific project and ensure the integrity of data collected.

The results of the data center project will contribute to the definition of public policies and the establishment of goals and guidelines for future provision of cloud computing services for the education and research community.

The infrastructure consists of a power container (UPS and generator) and another container with 10 IT racks. Each of them is 40 feet (12m) long. The direct expansion (DX) cooling system is pre-defined by Huawei for containers.

The precision cooling, UPS, generators, fire detection and prevention are all monitored locally and remotely.

As well as monitoring all supporting infrastructure, the system monitors the status of doors, motion sensors, video cameras, and especially the use of IT equipment.

The center is connected by optical fiber with two links to the metropolitan ring network Manaus, built by RNP in partnership with the Amazonas State Government and operated by the data processing company Prodam.

Internally, the center uses both fiber optic and Cat 6A copper cabling.

RNP expects the center to give international visibility to the scientific project and ensure the integrity of data collected.

RNP has several partnerships with international institutions. The Telemedicine University Network (Ruth) links teaching hospitals and health units throughout the country with a high-performance infrastructure.

The organization also coordinates projects with the European Union to strengthen collaboration between the two tech research communities.

RNP, along with the MCTIC and the European Commission, has managed projects involving national and international academic institutions in cloud computing, including security aspects, high-performance processing and experimental platforms. Middleware also figures in a project for collaborative applications and the virtual global community.

The whole project should contribute to environmental research and help efforts to preserve this important natural resource. ●

• This feature appeared on DatcenterDynamics.es. Translation by Peter Judge

DatacenterDynamics

Guide to

Security + Risk

Inside

It's not the cloud, it's you

Stop pretending public cloud is less secure than your data center, says *Max Smolaks*

Max Smolaks
News Editor
@MaxSmolaks

For as long as public cloud services have existed, we've been hearing about security concerns as one of the main barriers to wider adoption. There's a long-standing perception in the industry that things start going terribly wrong as soon as corporate data moves outside the corporate firewall.

We've seen this before in the enterprise computing world, with the BYOD-induced panic just a few years ago, when IT managers balked at the idea of storing corporate data on personal smartphones.

The perceived risk of cloud is not based on fact, but on anecdotal evidence and news headlines.

But are services like AWS or Azure really any less secure than their on-premises counterparts? And what about OpenStack-based cloud deployments, with the entire code of the platform available to any member of the open source community?

In a recent study commissioned by Verizon and conducted by Harvard Business Review, cloud security remained the most commonly cited barrier to increased adoption, with 35 percent of respondents having doubts about the safety of their data when using public infrastructure.

At the same time Verizon itself, in its latest Enterprise Cloud Report, highlighted that in the past two years, fewer than five percent of companies had experienced a significant data breach that was directly attributable to a cloud-based service — and that included SaaS applications.

The fear somehow ignores a whole generation of security tools and practices, which have been developed specifically for cloud environments and see public infrastructure as an essential part of the foundation for corporate IT.

Is public cloud really posing a danger to enterprise networks? To settle the matter, *DatacenterDynamics* engaged two of the world's largest managed hosting providers: Rackspace and Datapipe. You could argue that public infrastructure is slowly eating their business, but instead of organizing the resistance, both companies now offer managed public cloud services.

With their reputation on the line, the two are also increasingly interested in cloud security, and here they seem to agree: while there's no such thing as a completely secure public cloud, today public infrastructure is no more dangerous than your own data center.

Joel Friedman, who successfully combines the roles of CTO and chief security officer at Datapipe, told *DatacenterDynamics* that the weakest link of the information security chain is people – and that doesn't change if you rent your infrastructure from public cloud providers. ▶

Industry view:

Jason Steer, Solutions Architect, Melno Security EMEA

"As cloud outpaces legacy architecture, you stick with what you're familiar with. As you get older, it's hard to find the time to learn. We still get a lot of the same questions, so customers clearly don't know the right questions to ask. They ask extremely high levels of security of us, but would never be able to match that level of security themselves.

"I've worked at multiple security vendors during my career, and I feel like the security industry has kind of underdelivered. Shame on the vendors in developing products that continue to be behind attackers' methodology, because they put profits ahead of innovation. How do you find the technology to innovate at the speed attackers innovate? You have to have tools, people and intelligence.

"It seems simple and obvious that you should know what an incident looks like, but if you don't know who has access to your data, you can't tell. We've relied far too much on detection technologies that have let us down, and have let go of best practices because we've trusted the vendor to do the job properly, and they've let us down."

▶"I don't think there's really any doubt that instance security can be achieved – otherwise nobody would have computers on the Internet. I don't think there's really much of a doubt about physical security – I've never heard of any heist against a well-known public cloud provider.

"Governance is an issue, and there are toolsets, but it's not really indicative of a risk to a provider itself, just about technology. So then it comes down to the platform. If you were to look back at any of the breaches that have occurred in the public cloud, I would say that it's not due to lack of inherent security controls in the platform, but due to the way that the end-user or their organization has configured the platform.

"Someone published their encryption keys to GitHub. Someone didn't have multi-factor authentication enabled, and [their adversaries] were able to phish or keystroke-log their way in. The platform had capabilities to protect them, but the end-user never configured those properly. So therefore, it's about education, it's about implementation, but it's not about the underlying platform."

According to Friedman, adopting public cloud services could protect your data from the watchful eyes of various intelligence agencies, more effectively than some of the measures designed in-house.

"The tools are available. Both Microsoft and AWS offer key management functionality, which allows you to bring your own keys and encrypt [data] so the service provider doesn't have access to the underlying data set. It's encrypted, and the customer maintains the key," Friedman explained.

"Is it technically feasible that they could backdoor their code? I suppose, but I don't think anyone is legitimately concerned about that. I think a lot of this has to do with perceived risk, for those that don't understand the platform."

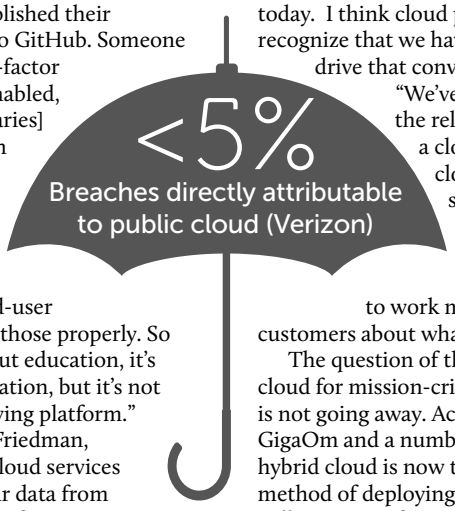
Brian Kelly, chief security officer at Rackspace, expressed similar views at a recent meeting with press and analysts in London. Kelly – who spent the past 30 years managing security for customers including the US government and the mayor of New York - admitted that today's cloud security architectures felt rooted in yesterday's technology.

"One of the real challenges that we have in the cloud industry is to really change the perception that you can be, and should expect to be, safer in the cloud," he said.

"Cloud providers need to take responsibility for giving consumers a greater understanding of what's available. We owe them much greater control and transparency. Some of this lack of trust in the cloud is due to the fact they don't really see what's going on.

"We give payment card clients reports on compliance. I want to know what's happening with my workload. The easiest thing for me to do would be to have a dashboard which displays the compliance state of my workload, and use that to make judgements about whether I need to worry about that today. I think cloud providers need to recognize that we have the obligation to drive that conversation.

"We've got to change the relationship from a cloud vendor to a cloud partner, and start to have deeper conversations, and take on things. I think we've got to work more closely with customers about what their options are."



The question of the validity of public cloud for mission-critical workloads is not going away. According to IBM, GigaOm and a number of analysts, hybrid cloud is now the dominant method of deploying infrastructure, and will remain so for years to come.

Support for AWS, recently announced by VMware, seemingly represented the final truce between internal IT (mostly running on vSphere) and the public cloud (dominated by Amazon). Both companies admitted that in order to sucesfully build hybrid architectures, two different industries would have to share their secrets and cooperate.

Hybrid deployments can be complex to build and maintain, but they will save money and resources - and if you pay attention, they will not make your data any less secure. You just have to have the right tools - remember BYOD issues that were solved by the advent of a new category of Enterprise Mobility Management software?

The mission of security professionals remains the same, as always: protect your 'crown jewels', invest in the best tools and staff you can find, and hope for the best. And maybe, just maybe, outsource the public cloud shenanigans to someone else. ●

Security breaches can be costly and damaging to your business. Prevent them with wired or wireless server cabinet locks from HES.

INTERGRATE PRODUCT WITH EASE
Single-card solution that works seamlessly with your new or existing access control system, simplifying installation and management.

ENSURE COMPLIANCE
Door and lock status monitoring for regulatory compliance and protection.

VERSATILE PROTECTION
The **KS100** is a PoE hardwired locking option with wireless Aperio® technology that supports low or high frequency cards. The **KS200** utilizes a multi-technology reader with hardwired Wiegand wiring.

hes
ASSA ABLOY

*Visit hes**innovations**.com to find the right cabinet lock for your project.*

ASSA ABLOY, the global leader in door opening solutions

Security: The attack of the IoT

Peter Judge
Global Editor
@Judgecorp

Security experts have been warning for years about the dangers of the Internet of Things (IoT). Now the predictions have come true, says *Peter Judge*

IT security just changed. Until now, it was tough, but people had a handle on it. The range of attacks was understood, and technology such as firewalls and threat detection were evolving to keep pace with them. PCs and servers were known technology, and even the arrival of the cloud and the consolidation of those servers in public, shared data centers wasn't going to make a huge difference.

Then along came the IoT. All sorts of new devices are being hooked up to the Internet, to gain the benefits of control and connection. CCTV cameras, video recorders, games consoles, and all sorts of industrial devices have been given access to web services, and are being managed and controlled remotely.

Some voices warned about this. "You can't lock a door and leave a window open, and you can't lock the window but leave the garage open," said Brian Witten, director of IOT at security firm Symantec back in 2015. "Sometimes attackers come in over the bridge from traditional IT systems into "operational" technology (OT) or IoT systems. Sometimes they dial up cellular modems on these IoT devices, and other times they attack them directly over the Internet."

Within the data center industry, there's a worrying tendency for industrial control systems (ICS) and mechanical system to contain unconsidered Internet connections, perhaps via Wi-Fi or embedded cellular systems for monitoring.

In 2015, there were 295 incidents of cyber attacks through ICS systems, according to the ICS CERT organization, but Ed Ansett of i3 Solutions warns that these are under-reported, leaving the public and the industry unaware of what it should be doing (see box).

But the biggest threat from the IoT could come from outside the data center, completely oustide the industry's control. Hundreds of millions of devices are being added to the Internet, including cameras, fitness devices and the proverbial toasters, with scant consideration for security.

These devices are out there with factory-set passwords, or no passwords at all, containing processors capable of running malware. It only takes a virus written to hit these devices, and they can be turned into an army of "bots," ready to launch a distributed denial of service (DDoS) attack on the Internet's key infrastructure.

And this is what happened in October. Malware called Mirai infected millions of IP cameras and video devices from China's Hangzhou Xiongmai Technology, which were then signalled to attack Dyn, a provider of the Internet's domain name service (DNS).

Dyn failed under the onslaught of millions of spurious requests, and as a result, services including Amazon, Netflix and Spotify could not access DNS and failed.

The irony is huge. Consumer devices hit the world's prime industrial network, the Internet, and the effect was felt through consumer services.

"In a relatively short time we've taken

a system built to resist destruction by nuclear weapons and made it vulnerable to toasters," tweeted Jeff Jarmoc, a Salesforce security engineer.

Or, as Steven Vaugh-Nichols said at ZDnet: "It doesn't take a nation to wreck the Internet. All it takes is the hundreds of millions of unsecured shoddy devices of the Internet of Things (IoT)."

The dangers on these systems aren't new. Their connections to the Internet have standard, factory-default passwords or, even worse, hard-coded Internet credentials. We know not to do this on our PCs and Wi-Fi routers, but for some reason other intelligent devices are being shipped with dumb security.

Security expert Brian Krebs spotted Mirai was involved. His site had been hit by an astonishing 620Gbps attack using Mirai-infected bots only a month before. He also pointed out that the Mirai source code has been put online. So essentially, anyone can mount such an attack.

Dealing with this is tricky, but there's a serious complication. The devices that are used, and their owners are essentially bystanders, who are not directly hit by the malware, and are probably completely unaware of it.

Thanks to the publicity around the Dyn attack, Hangzhou Xiongmai has issued a product recall, along with instructions to secure your IP cameras.

But how many users will hear about these moves, and be sufficiently motivated to do anything? Hangzhou Xiongmai supplies technology that is used in products with other vendors' badges - so how many people will even know they harbor a potential danger?

Some sort of body needs to enforce better security on IoT devices, through consumer regulations or other laws.

It is hard to see how this will happen but, until it does, the only thing for infrastructure players to do is to brace themselves for it, and build more DDoS defences. ●

Industrial attacks

Data centers are vulnerable to attacks on their their physical infrastructure, warns Ed Ansett of i3 Solutions. Industrial controls systems can be attacked through their control protocols, and insecure network connections.

In 2016, a German nuclear power plant was found to be infected with the W32. Ramnit Windows virus, and the Conficker malware, both thought to have spread via infected USBs.

"Practically every data center uses one or more for these protocols," says Ansett, in a presentation which lists flaws in Modbus, BACnet, and SNMP versions 1 to 3. Attacks on these protocols can hit the data center's cooling systems and power distribution, effectively disabling it.

Malaysia Increasingly Attractive Data Center Hub for Companies

Real Estate, Affordable Energy and Location make the country suitable for firms looking to build data centers in South East Asia

It's not uncommon for images of beaches, wildlife, densely-populated cities and Formula One racing to be conjured up when Malaysia is mentioned. Increasingly, data centers are mentioned in association with the South East Asian country given Malaysia's concerted effort to make itself a world-class data center hub by 2020.

That's because the country is particularly well suited to handle the expected influx of data center investment when compared to regional neighbours Indonesia and Thailand. This is because of the country's service orientation of Malaysia's economy, close proximity to the Asia Pacific region's major hub city (Singapore) and a concerted policy of attracting ICT and data center business in specially zoned and provisioned areas in the Kuala Lumpur metropolitan area (Cyberjaya) as well as the Sedenak Iskandar Data Hub (SIDH), which is fast becoming known as a data centre park with abundant, readily accessible and top notch infrastructure and utilities. The Data Hub is a government initiative led by MDeC.

A depiction of Malaysia's Sedenak Iskander Data Hub which is known as a resource-rich data center park

Investment Advantages In Malaysia Apparent

Malaysia, which is already a major established investment hub for multinational companies in South East Asia, is also attractive to data center investors given that it is a mere 60 kilometres from Singapore which makes latency for those with operations in the city-state virtually a non-issue. Proximity to Singapore has been cited as an advantage by companies, such as NTT Communications, that have primary data centers in Singapore and recovery facilities in Malaysia.

Competitive real estate prices and the country's lower electricity tariff relative to Singapore and resource availability for potential data center operators compared with many other markets at a relatively similar level of development are also factors that make it attractive for investors considering larger data centers in Malaysia.

Fast-Growing Data Center Market

These advantages are not lost on data center operators and led DCD Intelligence to project double-digit growth on a year-over-year basis from 2016 to 2020 which will make it the fastest-growing South East Asian country when white space is considered.

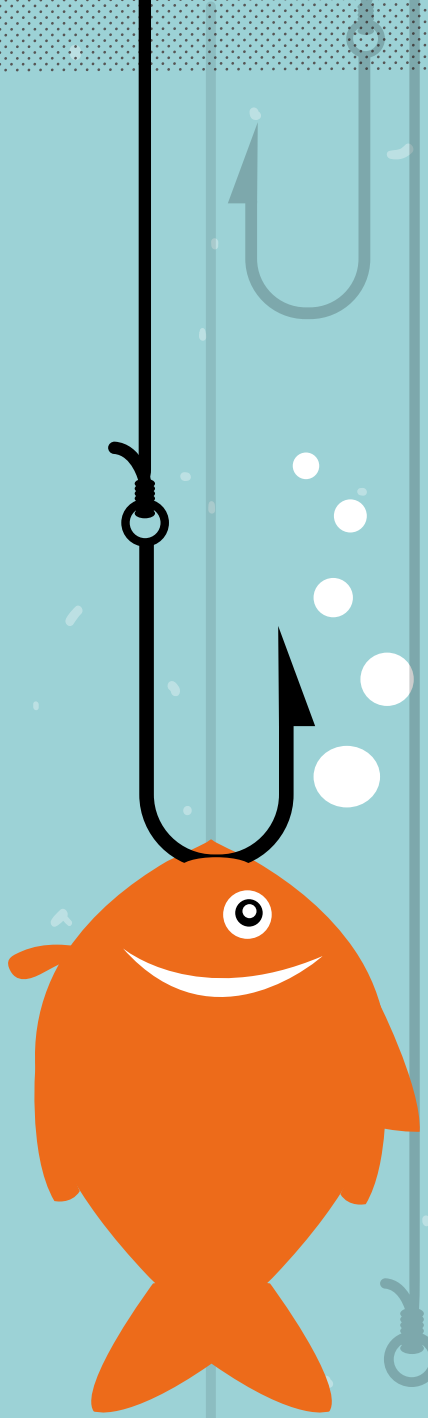
The type of data centers Malaysia offers matters to investors as well. The Malaysian data center sector is designed to meet the needs of both the IT needs of an emerging economy that typically grows at least 4% quarter-on-quarter, according to DCD Intelligence. That's in addition to the requirements of international clients using Malaysia to house their local or regional IT capacity. Malaysia's availability of suitable local outsourcing facilities and services, which has increased significantly over the years, is a core data center requirement and the country is better suited to meet those needs than ever. As such, DCD Intelligence expects colocation and outsourced space in Malaysia to grow 21% in 2016.

Investment dollars have flowed into the country as a result of the many cited advantages. Huawei is one example of a company that clearly sees the data center advantages of Malaysia. The Shenzhen, China-based company opened the Asia Pacific Digital Cloud Exchange data center, a 90,000 sq. ft. facility of office and warehouse space for data hosting and logistics in Iskandar, last June. Huawei is using the data center to service its regional customers.

The data center sector is already an integral part of the country's economic transformation and will soon be a well-known part of the Malaysian landscape.

MDEC Driving Transformation

Contact Details
Phone: *+603 8314 1854*
Mobile: *+6019 665 6588*
Email: *eric@mdec.com.my*



Phish-free Windows

People are the weakest link. *David Chernicoff* explains how the latest version of Windows helps prevent foolish admin errors and phishing

Despite the efforts of IT administrators, security vendors, and even the mainstream media, computer security's weakest link remains the person sitting in front of the console. The daily reports on malware and ransomware attacks all make it clear that there remains a major problem in securing your IT infrastructure: The end user.

Phishing attacks and spearphishing have become more sophisticated, with attackers focusing on targets that have elevated privileges on corporate networks, carefully preparing fake emails after studying their target business and determining the best way to get their targeted individual to allow them access. These are now the preferred attack vector for sophisticated attackers. Combining these social engineering attacks with common security flaws in devices, services, and unpatched servers gives the well prepared attacker plenty of avenues for their nefarious activities.

These attackers are nothing if not patient; research from Microsoft showed that the average network penetration lasted for more than 200 days before it was discovered by the victim, yet the timeline from the first host being compromised to a domain admin being compromised was no more than 48 hours.

Most commonly, the compromise is done using a Pass the Hash attack, a technique discovered in 1997 and which can be used against any system that uses Lan Manager (LM) or NT Lan Manager (NTLM) authentication, regardless of the operating system using them.

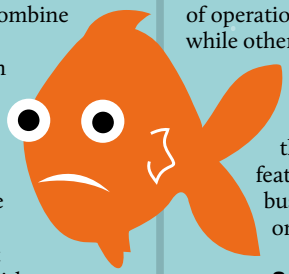
Attempts by system vendors to remove LM and NTLM authentication from their operating systems have failed because of the large number of applications and services that require its availability for proper operation. Pass-the-ticket attacks, discovered in 2014, allow similar types of compromises using a forged Kerebos key distribution center and work on Windows Server 2000 and newer. ▶

David Chernicoff
US Correspondent
@DavidChernicoff

▶ Once an attacker has gotten administrative credentials, they retain them for as long as that account exists, and since admin account routines have far more access than necessary for the user to do their job, attackers get elevated levels of access for as long as necessary to move up the chain or find valuable information to steal.

Windows Server 2016, recently delivered by Microsoft, represents a bid to gain more share from Linux in the data center, with improvements to security, including shielded virtual machines.

The new OS includes four technologies designed to prevent compromised credentials giving an attacker unlimited access. Credential Guard, Remote Credential Guard, Just Enough Administration and Just-in-time Administration (see box) combine to provide privilege access management (PAM), which limits the ability of as attacker to compromise a Windows Server environment. It makes use of capabilities added to the Active Directory Domain Services and the Microsoft Identity Manager. Along with protecting AD environments from attack it can also be used to regain control overt a compromised directory service.



Finally, and while it might seem a bit belated, Windows Server 2016 also adds the Windows Defender antivirus / anti-malware protection that has long been available in Windows client software. When directly asked why it took so long for Defender to make its way to the server platform Microsoft's response was a simple - "customers weren't asking for it."

Most enterprises have made major investments in enterprise-wide anti-virus/ malware solutions, so the absence of a built in feature to provide this protection was rarely missed. However, it is now available by default and provides instant protection against potential threats, limiting yet another potential window of vulnerability.

Windows Defender generally runs headless, and should the administrator choose to use and administer the software it requires management via Windows PowerShell, Group Policy, or WMI. Some specific SKUs of Server 2016 will include the interface. To disable Windows Defender, in order to install the corporate standard AV/AM software or for any other reason, it is necessary to uninstall the application which can be done by using the Remove Roles and Features Wizard.

Microsoft has taken the approach that security is not an add-on. It needs to be built into the operating system from the ground up and should be the default configuration. Rather than IT administrators needing to enable security capabilities, those services need to always be present. Some, like Credential Guard, need to be the standard mode of operation for both client and server, while other capabilities need to be easily accessible and available to IT to implement so the IT department can be assured that these enhanced security features don't make line-of-business applications run slowly or cause problems.

Server administration policies need to present a consistent model that prevents any administrator from being able to infect, crash, or destroy corporate servers or data. By maintaining a very granular level of control across all common server administration activities a combination of the latest technologies and up to date administrative polices can prevent or mitigated the vast majority of security problems that plague the corporate world today.

All of these technologies can be remotely deployed and managed on all of the appropriate servers in your data centers and clients in your enterprise. Properly implementing the technology along with making sure the correct security policies are in place will provide the strongest defense against the huge number of malicious threats against your enterprise. ●

What's new in Windows Server 2016?

The new version includes four technologies designed to stop attackers using compromised credentials to gain access across the enterprise:

Credential Guard

Credential Guard, originally introduced in Windows 10 Enterprise, now uses virtualization-based security to isolate and secure the Local Security Authority. The LSA now uses remote procedure calls to communicate with the small subset of security processes running in the virtualized session, which is not otherwise accessible to the operating system. Most commonly used credential protocols will no longer work as single sign-on, but will prompt for a second credential. With Kerberos, neither delegation nor encryption will be allowed.

http://bit.ly/2ec7kZZ

Remote Credential Guard

Remote Credential Guard, also introduced in the Windows 10 Anniversary Update (build 1607) is designed to provide protection for connections over Remote Desktop. Basically, the user's credentials are never exposed to the host computer.

http://bit.ly/2dSCvpp

Just Enough Administration

Just Enough Administration is a set of Windows PowerShell security controls introduced in the Windows Management Framework 5.0 and the Windows Server 2016 Technical Preview earlier in 2016. Using PowerShell scripting and this technology gives a very granular level of control, giving specific tasks only enough administrative access to perform the required actions and nothing more.

http://bit.ly/2c4E3OG

Just-in-time Administration

Just-in-time Administration is exactly what it sounds like - sufficient access is granted to perform a task just before it is needed and the access approved and permitted for only a limited amount of time. These combine to provide Privilege Access Management (PAM)

http://bit.ly/2e348js

Learn more about Switch SUPERNAP data centers supernap.com/tour

It was estimated, in 2015, that data centers consumed 2% of the power in the United States and that by 2030, data centers may consume as much as 10% of power.

Switch SUPERNAP was founded with sustainability in mind. CEO and Founder, Rob Roy, designed his patented SUPERNAP data centers to be energy conscious and operationally excellent. Today they are the highest-rated colocation data centers on the planet. Back in 2000, Rob Roy knew that data would run the planet, which is why he wanted to ensure it wouldn't ruin the planet.

When companies choose Switch SUPERNAP data centers, they are choosing **the highest rated and the GREENEST data center environments in the world.**

switch

THE TECHNOLOGY SUSTAINABILITY COMPANY

LAS VEGAS TAHOE RENO GRAND RAPIDS MILAN BANGKOK

//dcd**webinars**

Up to an hour of live interaction with senior industry experts on hot data center topics, DCD webinars are available live or on demand, including video, audio and slide presentations. Free to register, the webinars discuss new solutions, case studies and best practices.

Latest webinar:

How to Secure your Critical Assets today and tomorrow

Thursday 1 December

Our panel experts from **Assa Abloy** and **CyrusOne** will discuss and debate digital infrastructure, and provide tips to anyone looking to upgrade and improve on their physical security.

Reasons to watch:

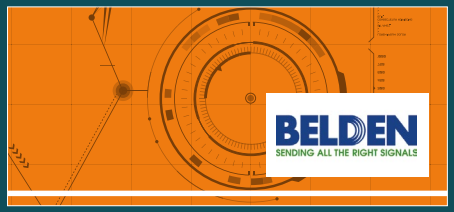
- Covers the risk that businesses face from data loss
- 12 data center security tips
- Case Studies, including insight from CyrusOne
- How to manage compliance with regulatory requirements

Watch now: https://goo.gl/l8w437

WATCH **NOW!**

ON DEMAND

LATEST ON DEMAND DCD **WEBINARS:**



Next Generation Data Centers – Are you ready for Scale?

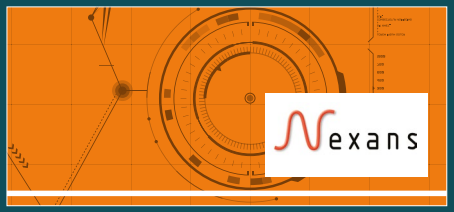
Qing XU, Technology & Applications Manager, Belden
Stephen Worn, CTO, DatacenterDynamics

Watch here: http://bit.ly/2bKEb7a

Powering Big Data with Big Solar

Bill Thomas, Director, First Solar
Stephen Worn, CTO, DatacenterDynamics

Watch here: http://bit.ly/2aUvPUq



Smart choices for your digital infrastructure

Stephen Worn, CTO, DatacenterDynamics
Rob Cardigan, Senior Product Manager, Nexans
Nick Parfitt, Senior Analyst, DCD Intelligence

Watch here: http://bit.ly/1syLUb4

Catch up with our extensive archive of webinars by visiting the link below:
www.datacenterdynamics.com/webinars

Con Air: don't believe the air gap hype

We know mechanical and electrical equipment is vulnerable to attack. It's time to stop denying the danger and improve our security practice, says *Ed Ansett*

Illustration: studionippoldt.de

There is only so long that we can exist within a certain paradigm. Our industry has become aware that cyber-attacks on mechanical and electrical (M&E) control systems can immobilize communication systems and business operations. There are three responses from data center owners and operators:

1 Organizations that know they have a problem and think they are protected through air-gapping.

2 Organizations that have external connections but believe that they have a secure electronic perimeter, and

3 Organizations that think they are exposed to external attack vectors through the Internet and wireless devices, directly or indirectly connected to the control network.

Air-gapping systems as an answer to protecting critical infrastructure from potential cyber-attacks is simply not practical. A new approach is evolving through understanding the issues in more depth.

Whilst the threat of external attack is relatively obvious, what concerns me is the basis upon which data center operators believe they are secure.

Have the operators had the external connectivity status verified, and if so by whom? If it is verified by a control and monitoring systems supplier, that would be one of the organizations who have mysteriously overlooked informing data center operators and owners about their vulnerabilities - even though they know about these vulnerabilities through their ICS experience? When was the last time you heard an M&E control systems supplier telling a data center owner that firewall software is out of date or a device controller needs patching to protect against a known cyber threat?

It seems to me there's an obvious professional and moral duty on the part of the data center control and monitoring systems community to advise data center operators and owners of known vulnerabilities - at the very least those which are published on the vendor website or reported through ICS-CERT.

> *An air gap is not a practical answer to protecting critical systems*

Secure is a relative term within heterogeneous technology environments. As more devices become connected, electronic security perimeters (EPS) become less defined. Virtually every data center uses protocols with little or no security.

The cybersecurity risks associated with physical and remote access, IT architecture, portable and wireless devices, to name a few, must be measured, assessed and remediated.

For example, frequently overlooked security risks include general purpose machines connected to the M&E network and devices, the long lifecycle of M&E components compared to other elements, bad patching policies, and the difficulty of testing configuration or firmware changes.

Firms will have to improve their ability to withstand cyber-attacks under the first EU-wide rules on cybersecurity, approved by MEPs earlier this year. The new *Directive on Security of Network and Information Systems* (NIS Directive) lays down security and reporting obligations for "operators of essential services."

Following a letter issued by the New York State Department of Financial Services (NYDFS) on 9th November 2015 to Federal and State financial regulators, on the 13th September 2016 the NYDFS issued a proposed regulation that would impose rigorous cybersecurity requirements on banks and other financial institutions.

Under the proposed regulation, institutions must have a written cybersecurity policy that outlines every aspect of its cybersecurity program compliant with the proposed regulation's requirements. This is significant as it would be a new first-in-the-nation regulation.

Currently there is a lack of non-IT, M&E specific, cyber engineering knowledge. IT security teams have to bring their critical facilities up to the same level of security. Will legislation eventually drive the integration of both software and the M&E physical infrastructure within critical infrastructures in order to identify risks and implement mitigation procedures? ●

DatacenterDynamics

AWARDS

EMEA 2016

CELEBRATING 10 YEARS

FINALISTS 2016

We had hundreds of entries for our 10th EMEA Awards. These are the finalists chosen by our independent panel of judges

01 ENTERPRISE DATA CENTER

CATEGORY SPONSOR

DigiPlex

- **Ericsson Iberia Cloud Data Center**
  Ericsson, Spain
- **Government of Navarra Tier III Data Center in collaboration with Aquads**
  Government of Navarra, Spain
- **Management & Technology Team Delivers Application and Infrastructure Services**
  Surrey County Council, UK
- **University of Dammam Data Center Project in Collaboration with Emerson Network Power**
  University of Dammam, Saudi Arabia

02 INTERNET DATA CENTER

CATEGORY SPONSOR

Future-tech

- **Ericsson Iberia Cloud Data Center**
  Ericsson, Spain
- **West Africa's Largest Purpose Built Tier III Data Center**
  MainOne, Nigeria
- **MEEZA Datacentre M-VAULT 2**
  MEEZA QSTP, Qatar
- **The Virtus London4 Data Centre**
  VIRTUS Data Centres, UK

03 SERVICE PROVIDER DATA CENTER

itconic Madrid 4 Campus Upgrade
Itconic, Spain

LuxConnect, The Unique Multi-Tier Data Centre
LuxConnect, Luxembourg

MEEZA Datacentre M-VAULT 2
MEEZA QSTP, Qatar

Virtus Intelligent Portal (VIP)
VIRTUS Data Centres, UK

"To us it is a recognition of our efforts to try and become more and more energy efficient. Even in ways that aren't very obvious at first glance, but when you take a closer look are very clear."

Paul Driessen, KPN

04 SUSTAINABLE DATA CENTER

Fetsund Data Centre (Sweden)
DigiPlex, Norway

Equinix AM6 - A Flagship for Sustainability
Equinix, Netherlands

Datacenter U.S.E. Program
KPN N.V., Netherlands

Athens-2 Data Center
LAMDA HELLIX, Greece

05 PUBLIC SERVICES DIGITAL DELIVERY

Aberdeen City Council Cloud Computing Project in Collaboration with Brightsolid
Aberdeen City Council, UK

Government of Navarra Tier III Data Center in collaboration with Aquads
Government of Navarra, Spain

The MET Police Data Centre Transformation Project in Collaboration with Keysource
Metropolitan Police Service, UK

Stockport MBC Data Centre Project in Collaboration with Sudlows
Stockport MBC, UK

06 MODULAR DEPLOYMENT

Flexenclosure in Collaboration with Angola Comunicações e Sistemas Modular Data Centre
Flexenclosure, Angola

Lamda Helix River-Powered Containerised Data Center
LAMDA HELLIX, Greece

Rack Centre Phase 1A and 1B in Collaboration with Bladeroom
Rack Centre, Nigeria

ALJUF Data Center Project in Collaboration with Huawei
Saudi Arabia ALJUF,
Saudi Arabia

07 DATA CENTER CRITICAL ENVIRONMENT TEAM OF THE YEAR

CATEGORY SPONSOR

Life Is On Schneider Electric

CBRE Multi-Disciplinary Team Cloud Services Deployment
CBRE, Irleand

CenturyLink M&O Certification for EMEA Data Centres
CenturyLink, UK

Ericsson Iberia IT & Cloud DC Migration
Ericsson, Spain

Garanti Bank New Data Centre Design Development in collaboration with HPE
HPE/Garanti Bank, Turkey

08 CRITICAL ENVIRONMENT FUTURE THINKING AWARD

CATEGORY SPONSOR

CBRE

Next-Generation Subsea Fibre Optic Cable System
Aqua Comms, Ireland

Concert Control Project (Sweden)
DigiPlex, UK

Datacenter U.S.E. Program
KPN N.V., Netherlands

ArCTIC (Adsorption Chiller Technology for IT Cooling)
Leibniz Supercomputing Centre, Germany

09 ENERGY EFFICIENCY IMPROVER'S AWARD

CATEGORY SPONSOR

STARLINE

Mistral Reliability and Failure-Free Operations Project in Collaboration with Emerson Network Power
DKRZ - German Climate Computing Centre, Germany

CBRE-CWS delivers PUE Improvement Program
European Data Hub, Luxembourg

Datacenter U.S.E. Program
KPN N.V., Netherlands

ArCTIC (Adsorption Chiller Technology for IT Cooling)
Leibniz Supercomputing Centre, Germany

10 DATA CENTER TRANSFORMATION PROJECT OF THE YEAR

CATEGORY SPONSOR

AIRSYS
Expert In ICT Cooling

Positioning Aberdeen as a Global Tech Hub in collaboration with Brightsolid
Aberdeen City Council, UK

Ericsson Iberia Cloud Data Center Migration
Ericsson, Spain

itconic Madrid 4 Campus Upgrade
Itconic, Spain

Repsol Data Center Consolidation Project
REPSOL, Spain

"We are excited that the global data center industry continues to recognize our innovation and leadership in the EMEA region. It is also more fulfilling because we are the only data center in Africa to be recognized in this category."

Funke Opeke, CEO MainOne

EMEA Awards Finalist Internet Data Centers

11 "OPEN" DATA CENTER PROJECT

Public procurement of OCP at CERN
CERN, Switzerland

Equinix Joins OCP; Collaborates with Facebook
Equinix, Netherlands

Schneider Electric Produce Comprehensive Research Analysis, Trade-Off Tools and Open Rack Solution to Support The Open Compute Project
Schneider Electric, UK

"Being a finalist of the DCD awards, the industry leader in data centers, is a source of pride and satisfaction. It is also the recognition of work done with great effort and at a high quality."

Felipe Martinez-Sagarra, Ericsson

12 CLOUD JOURNEY OF THE YEAR

CATEGORY SPONSOR

HUAWEI

ATEIS Middle East Moves to "The Paperless Office"
Oryx Technologies, United Arab Emirates

SDL's Machine Translation to the Cloud
SDL, Netherlands

FASTdesk by UKFast
UKFast, UK

Worldwide Use Collaboration with Vissensa Hybrid Clouds
Vissensa Limited, UK

13 YOUNG MISSION CRITICAL ENGINEER OF THE YEAR

ARUP — Andrew Higgins, Arup, UK

CBRE — Viktor Arnetz, CBRE Data Center Solutions, Sweden

future facilities — Paul Harrison, Future Facilities, UK

keysource — Tom Blundy, Keysource, UK

14 BUSINESS LEADER OF THE YEAR

CATEGORY SPONSOR

MERCURY

?

15 OUTSTANDING CONTRIBUTION TO THE DATA CENTER INDUSTRY

CATEGORY SPONSOR

RITTAL

?

FIND OUT THE WINNERS OF THESE TWO CATEGORIES ON WEDNESDAY DECEMBER 7 - THE NIGHT OF THE AWARDS

CATEGORY SPONSORS

AIRSYS Expert In ICT Cooling | CBRE | DigiPlex | Future-tech | HUAWEI | MERCURY | RITTAL | Life Is On Schneider Electric | STARLINE

CHARITY PARTNER

Sparks 25

PATRON SPONSORS

foster ENVIRONMENTAL LIMITED | RED | WHITE & CASE

For more sponsorships and table booking information, please contact:
Paul Mangles at **paul.mangles@datacenterdynamics.com** or **+44 (0) 207 426 7838**

www.datacenterdynamics.com/awards

DCD Com

Highlights from DCD Zettastructure London, November 1-2

Schneider Electric golden ticket balloon drop prize giveaway

Dennis O'Sullivan
Eaton

"DCD seems to pull together everyone in the industry who wants to showcase their latest products, trends and it's the best place to come see it."

Main Stage presentation

Solution Stage

Training

November Course Dates

- **Data Center Design Awareness**
  November 28-30, Dublin
- **Data Center Technician**
  December 1-2, Dublin
- **Data Center Design Awareness**
  December 5-7, Paris
- **Data Center Design Awareness**
  December 5-7, London
- **Energy Efficiency Best Practice**
  December 8-9, London

Visit **www.dc-professional.com** to view our full course schedule

DCD Turkey | December 6, 2016

DatacenterDynamics (DCD) Converged Turkey is celebrating its 7th year in 2016, providing once again a platform for the local and international IT infrastructure communities to come together in Istanbul.

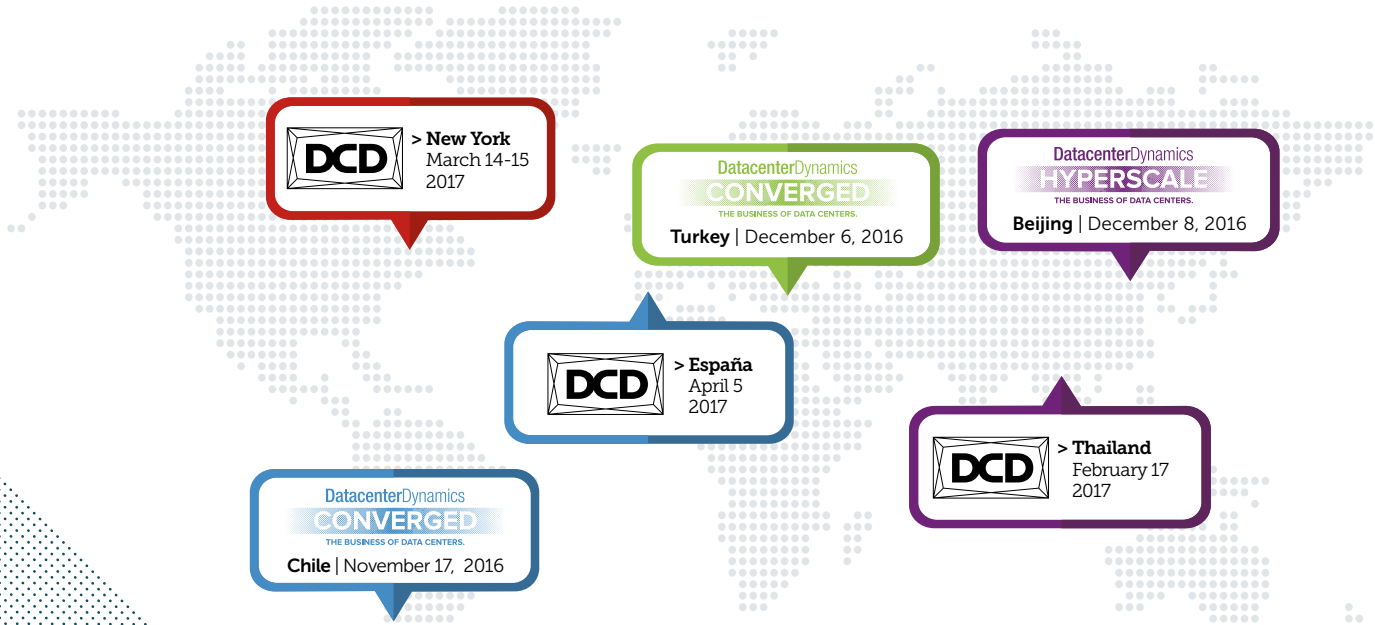
Reflecting Turkey's growing prominence as a transcontinental hub between the East and the West, this year DCD Converged will be opening up a wider debate on the future of cloud and data center infrastructure across the region. With the proliferation of cloud and IoT and Smart Cities, there is a growing demand for data center services capable of supporting enterprise-class IT infrastructure requirements in Turkey.

For more information regarding this event please go to:
www.dcdconverged.com/conferences/turkey2016

DON'T **MISS OUT!**

munity

Upcoming Events: DCD Converged



Book your place now and celebrate with key players from across the industry.
www.datacenterdynamics.com/awards

EMEA
December 7, 2016
Hilton on Park Lane,
London

Brazil
November 2017
Centro de Eventos Pro Magno
São Paulo

US & Canada
March 2017
San Francisco

Asia Pacific
November 2017
Hong Kong Convention
& Exhibition Center

Insecurity

Some data centers are built like fortresses, with thick concrete walls, pneumatically driven bollards and armed guards - we've heard of several facilities surrounded by actual moats. Some look like spaceships, with glass tubes instead of doors, laser-based intrusion detection systems and biometric security. There are data centers built to withstand electro-magnetic pulses (EMPs) and data centers built inside nuclear bunkers. There are fences out there that are impossible to cut, and cabinets that are impervious to explosion damage. All of this exists for one simple reason: physical security is easy to demonstrate, and we live in paranoid times.

But when was the last time you actually heard of a data center heist? Nobody really breaks into a data center to steal data. Nobody will blow a hole in the wall of your facility, load a truck full of servers and disappear in the direction of the nearest airfield, where a small airplane will take them across the border. A data center located outside the 100 year floodplain? That's fair enough. But I remember receiving a press release, highlighting the fact that a particular facility was located out of the flight paths and removed from major airports, something that was supposed to minimize the threat of hijacked planes crashing into a colocation cage. There's no kill like overkill. Even EMP weapons – while certainly posing a real threat to data centers – haven't been used nearly enough to justify this level of concern.

Earlier this month at the Zettastructure conference in London, Rich Johanning, vice president of Critical Infrastructure Protection at Aecom, explained how he would gain access to a server: "The first thing I do when we get hired to do pen testing on a data center is buy rack space in that data center. I walk in with a laptop and I now have access to everybody's networks. They might be segmented out, but there's no provisions in place to say 'hey, why has Rich been sitting over there for hours, and all he has done is play on his laptop?' I have been able to do that for four hours at a time. I have been able to pivot to a bunch of places."

Laser-resistant fences won't help if your enemy is an army of security cameras

For the most part, physical security has one simple purpose: to show customers just how much the service provider cares about the security of their data. There's no way to easily demonstrate your firewall, or display your encryption tools, and the best cyber security experts on the planet will not impress an executive nearly as much as a few ex-military types.

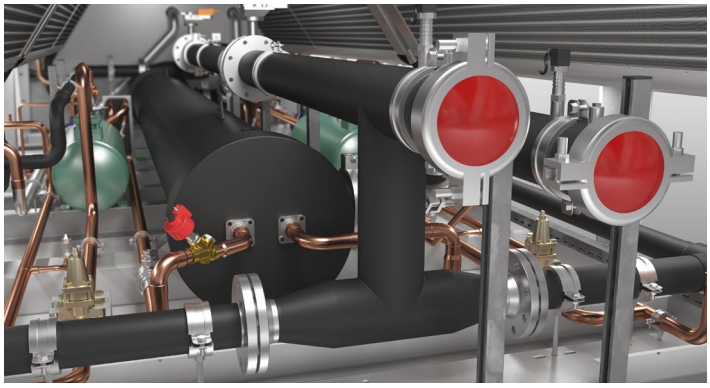
But let's not lose sight of what's important in our industry. Cyber security, not physical security, should be at the top of your agenda. Laser-resistant fences won't help if your enemy is an army of enslaved security cameras, attacking remotely from around the globe.

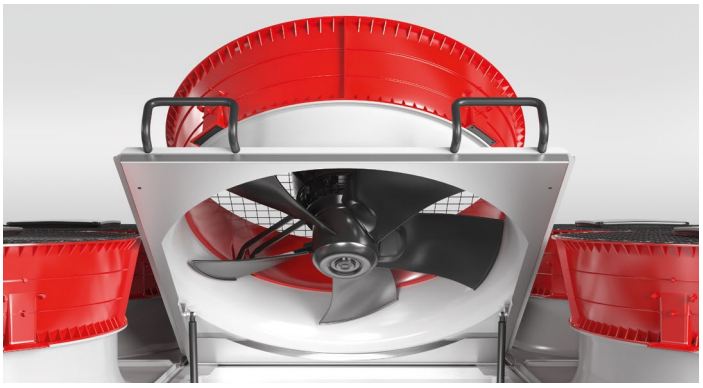
•

Max Smolaks – *News Editor*
@MaxSmolax

STULZ

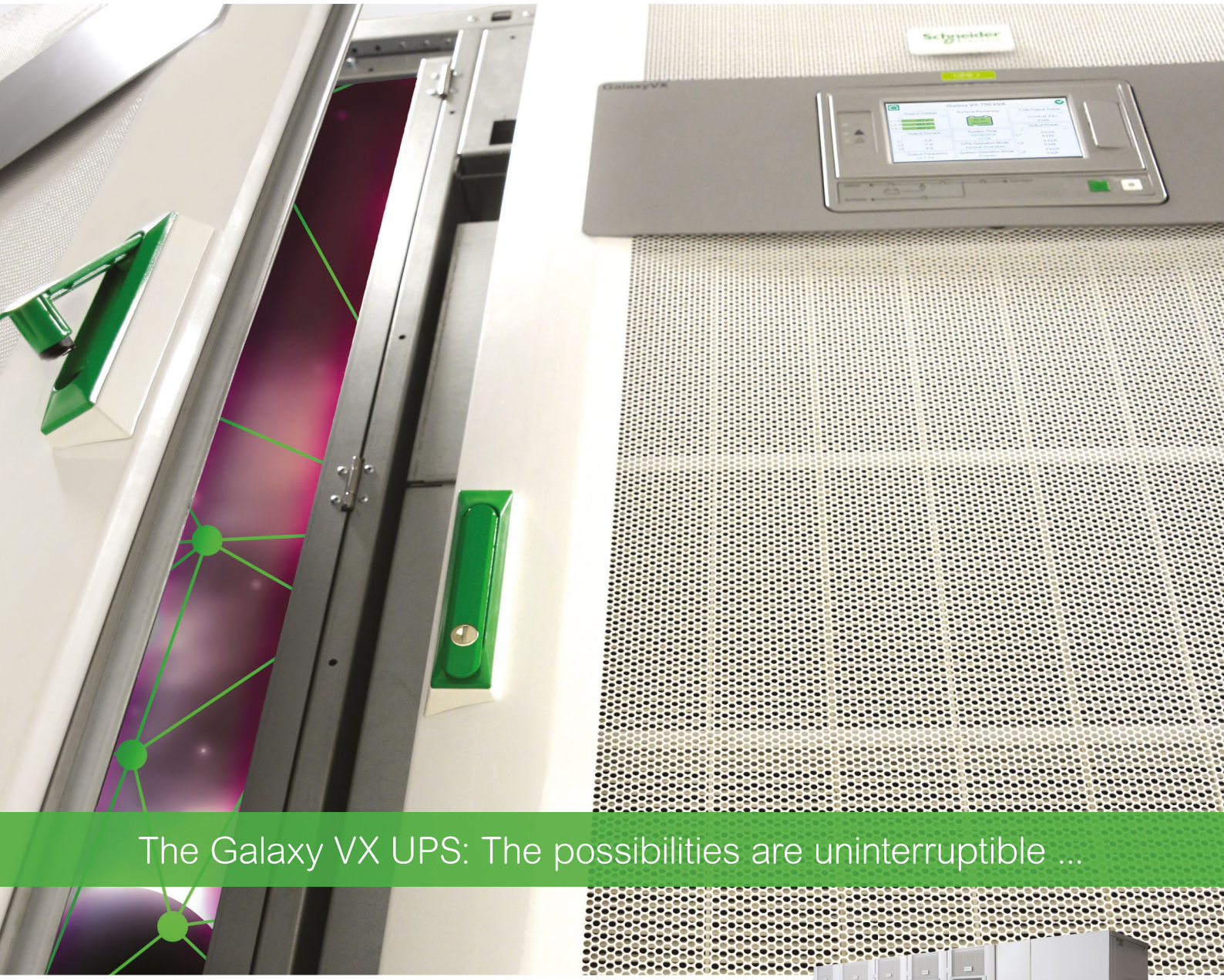
CLIMATE. CUSTOMIZED.





CyberCool 2
High-end cooling made in Germany

Our CyberCool 2 chillers are optimized for continuous 24/7 operation. They cool industrial facilities and data centers to the optimum operating temperature, extremely reliable and with maximum efficiency. Flexibility included: With a cooling capacity from 110 to 1,400 kW and eight different sizes, the CyberCool 2 is capable of satisfying most industry-specific requirements and individual customer requests. **www.stulz.com**



The Galaxy VX UPS: The possibilities are uninterruptible ...

Explore a galaxy of innovation.

The Galaxy™ VX UPS provides unyielding power-security for high-demand colocation facilities. Its future-proof, pay-as-you-grow architecture grants exceptional cost of ownership, and with a kVA of 500+ and the ultra-high efficiency ECOnversion™ Mode, you'll run your enterprise with uninterrupted peace of mind.

schneider-electric.com/galaxyvx

Life Is On | Schneider Electric