

Europe | 2016

Connect-World

www.connect-world.com



Markus Borchert
SVP Europe Market,
Nokia Networks

The Cloud Mobile Synergy



Taking content further

Making great content is tough
Distributing it shouldn't be



CONTENTS

All articles are available for download at www.connect-world.com



Connections

From the Editor-in-Chief's desk 4
by Fred Morris

Imprint 4

Advertorials

EMC 2-3
Swisscom 6
Gazprom Space Systems 11

Advertisements

Globecast IFC
Expo Comm Russia 14
GSMA Asia 19
Expo Comm Indonesia 28
Intelsat IBC
AT&T OBC

DDoS Attacks

DDoS impact on mobile networks – Radio congestion 5
by Bipin Mistry, VP, Product Management, Corero Network Security

Everywhere Enterprise

'Everywhere Enterprise' heightens the need for cloud security 8
by Charles Milton, Director, EMEA Channels, Zscaler

Mobile Cloud and Data

Head in the Clouds? Regaining innovation leadership in telecoms is critical for Europe 10
by Markus Borchert, SVP Europe Market, Nokia Networks

"Go Digital or Die"

by William Morrish, Director of Cloud Services, Interoute 13

Riding the smartphone surge for a superior cloud-enabled user experience 16

by Chris Halbard, EVP and President, International, Synchronoss

The dawn of 'Cloud Brokers'

by Tony Limby, Director, Cloud and Datacenter, BT Business 18

Why operators need to act now to take advantage of the huge opportunities the cloud and mobile synergy is creating 21

by Stefano Pileri, CEO, Italtel

Focus on the data to have any chance of controlling it 23

by James LaPalme, VP of Business Development and Cloud Solutions, WinMagic

Network Function Virtualisation (NFV)

Virtualisation is only the first step for a successful NFV network 25
by Robin Kent, Director of European Operations, Adax

Unified Communications (UC)

Cloud: Liberating today's mobile enterprise 27
by Vik Verma, CEO, 8x8, Inc

The Connected Home

How to create growth from the connected home 30
by Jon Carter, UK Head of Business Development - Connected Home, Deutsche Telekom

EMC and NFV: Modernize then Transform with Evolvable Infrastructure

by David V. Hudson, General Manager, Telecom Transformation Group, EMC Corporation



Since announcing the creation in 2015 of a Network Functions Virtualization Technology Group to supply NFV solutions to the Communication Service Provider (CSP) market, EMC has made a great deal of progress, introducing two highly differentiated platform offerings – one focused on NFVi and one on Telecom Analytics – and is embarking upon an ambitious go-to-market with the Federation of companies that includes EMC, Pivotal, RSA, VCE, VMware and Virtustream.

The EMC Telecom Transformation team, has spent 2015 talking to CSPs of all sizes around the world and has learned a number of important lessons. And the lesson that has had the greatest impact on helping us to formulate EMC's NFV strategy is that there is value in taking a gradual approach to NFV implementation, initially virtualizing one or two VNFs as a first step on the journey to NFV. While CSPs can choose to dedicate enormous resources to embark on broad, multiyear transformation projects, CSPs can also approach the transformation more pragmatically and step by step.

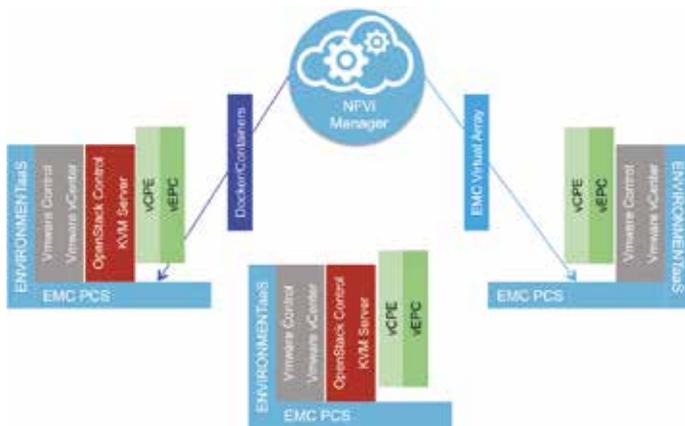
By EMC's definition, a pragmatist is an operator that seeks to test the waters with "VNF-in-a-box" architectures that feature a number

of distinguishing characteristics. The first characteristic is an NFVi architecture that must be customizable yet simple. Operators want to be able to size and configure NFVi platforms to suit specific workload requirements. Whether virtualizing customer-premises equipment or the evolved packet core, operators are intimate with the requirements of their network and subscriber base and want to be able to customize their solutions with the right amount of compute, networking and storage. At the same time, these operators want the deployment and management simplicity typically associated with a turnkey converged infrastructure system.

EMC's approach to NFVi offers the best of both worlds, by providing a set of common building blocks that can be composed to support custom workloads at the factory before being shipped to the customer, while also providing the capability for the customer to auto-deploy their environment, going from bare metal to workload-ready in a simple, repeatable manner. And EMC simplifies management of the running environment with automated collection, correlation and analysis of system telemetry at every layer of the NFVi stack.

Another characteristic that is important to pragmatists is carrier-grade availability and disaster recover. In the mobile and telecom marketplace, customer satisfaction is tied to availability of the network and the voice and data services it delivers. CSPs are under particular pressure to keep their services “always on” in distributed operational environments that can often be harsh and unpredictable. In the traditional world of telecom, systems and system components were engineered from the ground up to meet or exceed “five nines” availability and reliability, resulting in highly engineered and expensive proprietary systems. In the new world of virtualized, commodity components, carrier-grade has to be redesigned – this time, not at the component level, but throughout the distributed environment, with resiliency built across multiple systems and across multiple sites. This is the approach taken by EMC, which has adapted its industry-leading enterprise technology to the telecom world so as to distribute functionality across the network and eliminate single-points-of-failure, providing active-active failover, continuous availability, and workload consistency across sites.

EMC’s NFVi delivers this customizability, simplicity, carrier-grade availability, and distributed operational capabilities, in a platform that is built on three pillars: an abstracted commodity hardware layer, virtual infrastructure capable of hosting multiple services, and advanced management and orchestration with real-time and predictive analytics.



But meeting pragmatists’ requirements is only part of the EMC value proposition to CSPs. Filling out EMC’s vision for transformational NFVi is the belief that infrastructure should be future-proof. This means that instead of choosing a single operating environment and becoming beholden to its unique set of tools and capabilities over time, an operator should be able to adapt to rapidly changing innovations without having to do a rip and replace of its initial investment. In the four years since ETSI began defining the standards for NFV, the industry has seen the technology landscape expand to include proprietary technologies from vendors like VMware, open source innovations from the OpenStack community, and a growing variety of virtual machine technologies that include hypervisors, containers and unikernels. In order to take advantage of this rapidly evolving technology landscape, an operator’s infrastructure should be able to evolve along with it.

An evolvable infrastructure stack should allow for dynamic stack composition and re-composition, and allow for any combination

of NFV operating environments and any combination of VNFs, services and applications to be collocated on a common, scalable, cloud architecture. EMC makes the evolvable NFVi stack possible with EMC NFVi Manager management and orchestration technology designed to allow the automated creation, monitoring and management of service environments on a standard underlying infrastructure stack called the EMC Provider Cloud System (PCS). The combination of EMC NFVi Manager and EMC PCS enables operators to run NFVi as an “environment-as-a-service”, using blueprints and templates to dynamically define, deploy and manage custom multi-personality NFVi environments.



EMC has come a long way in one year and is excited by the opportunity ahead. If you will be in Barcelona between February 22nd and 24th for Mobile World Congress 2016, EMC will be joining VMware to showcase our NFVi capabilities and our Big and Fast Data Analytics capabilities. We invite you to join us at Hall 3, Stand 3K10 in the Fira Gran Via in Barcelona. And if you won’t be there, we invite you to stay up-to-date throughout the year and reach out to EMC for more information at <http://www.emc.com/emctelco/>

CONNECTIONS



The ties between mobile devices and the cloud grow stronger by the minute. The combination of these technologies is accelerating the growth of 'liquid computing' - the software driven ability to seamlessly move from one type of device to another to access, use, process, and change data.

With its head in the cloud, mobile can access - and process - data and applications that until recently were confined to the largest computers. Smartphones and tablets will offer individuals and corporations alike easy, on the spot access not only to emails, social media and the Web, but to high-powered mobile computing, extraordinary virtual and augmented reality, big data and immediate access to analytics such as cognitive computing and machine learning.

Marshalling the resources to offer virtually unlimited access to storage and on demand processing will significantly reduce the infrastructure costs and time to market for untold numbers of applications. Cloud models, on the other hand will become increasingly more complex, powerful and subject to cyber-crime attempts.

The advantages of scale and cost - available in a wide variety of devices - will almost certainly drive the market for mobile / cloud well into the trillion-dollar range within the decade. The mobile market is currently bigger than that for the cloud, but corporate usage and the growth of applications - the Internet of Things, for example - might soon balance the scales between the cloud/mobile and consumer/corporate markets.

Fred Morris,
Editor-in-Chief,
Connect-World
editor@connect-world.com



**Connect-World is published under licence
by INFOCOMMS MEDIA LTD**

email: info@connect-world.com
URL: www.connect-world.com

Editor-in-Chief: Fredric J. Morris fredric.morris@connect-world.com

Publisher: David Nunes david.nunes@connect-world.com

Editorial Department: editorial@connect-world.com

Production Department: production@connect-world.com

Sales Department: sales@connect-world.com

Administration Department: admin@connect-world.com

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise, without prior permission from the publishers. The content of this publication is based on best knowledge and information available at the time of publication. No responsibility for any injury, death, loss, damage or delay, however caused, resulting from the use of the material can be accepted by the publishers or others associated with its preparation. The publishers neither accept responsibility for, nor necessarily agree with, the views expressed by contributors.

ISSN 1468-0211

DDoS impact on mobile networks – Radio congestion

by Bipin Mistry, VP, Product Management, Corero Network Security

To ensure customer reliability, experience and security, CSP's and mobile carriers will need to protect their most valuable asset from congestion and downtime as a result of multi-vector, short duration DDoS attacks.



Bipin Mistry, Vice President, Product Management, Corero Network Security

Mistry brings more than 26 years of industry experience in the enterprise and telecommunications industries to his role with Corero. Most recently, Mistry served as the Chief Architect Mobility for Juniper Networks. In this role, he worked with the CSN's globally to help define their service and security needs in a rapidly evolving mobile environment. Previously, Mistry drove the Service Provider architecture and strategy for Cisco Systems, and ran then Voice over IP (VoIP) line for 3Com. He holds a number of patents, including one in API structure and interfaces specifically tie to mobile monetization.

The evolution of DDoS defence tactics

DDoS attacks against Corero customers grew by a third in the last quarter, with organizations experiencing an average of 4.5 attacks every day. This may sound like a meteoric rise, but it is hardly surprising given the proliferation of cheap and easy-to-launch attack tools. While most DDoS attacks were once launched by bad actors coding in their bedrooms to carry out protests – now, DDoS-for-hire botnets allow just about anyone to launch a crippling attack for just a few dozen dollars – with no coding skills required.

In many cases these attacks are merely a smokescreen, designed not to deny service but to detract attention from the real motive – usually data theft and network infiltration. According to our mid-year report, in the first half of 2015, the vast majority of DDoS attacks experienced

by Corero customers were less than one Gbps. Additionally, more than 95 percent of these attacks lasted 30 minutes or less. As attackers look for new ways to leverage DDoS attacks, they have realized that short duration sub-saturating attacks are more difficult to defeat, because they evade traditional cloud-based scrubbing centres.

Most Communications Service Providers (CSP's) and Mobile Carriers have deployed some form of DDoS scrubbing complex in their network to clean large, long duration DDoS attacks. A scrubbing centre approach will not effectively mitigate the current DDoS threat because they are too short in duration and too small in volume to be re-directed to a scrubbing centre and simply appear as noise on a typical CSP/Mobile backbone network.

As mobile networks carry on increasing in capacity and performance, CSP's and

Mobile Carriers now offer transport services which utilize the high speed radio network (LTE RAN) as backup to their fixed connection or, as in the case for some European Mobile carriers, as a medium for increased capacity. A simple low level Destination IP (DIP) spray attack against these environments will result in radio congestion, collateral damage and impact to subscriber experience. It can also have the detrimental effect of reducing overall cell phone battery life. Even before these attacks hit the radio network they have the ability to impact the Mobile services complex, impacting hosted critical services such as Deep Packet Inspection (DPI) Firewalls and Carrier Grade Network Address Translation (CGNAT). If any of these services are negatively impacted internet connectivity, resource usage/reporting, customer billing and so on can be quite significantly affected.

G.fast: racing into the future

Swisscom's business is shaped by people. It's the way they communicate and how they collect and share information. This development is gathering pace noticeably right now, prompting telecommunication companies to be innovative time and again. Swisscom has always faced such challenges, modernising its network and providing a wide range of technologies for the benefit of consumers in Switzerland. Swisscom puts its infrastructure, innovative services and know-how at the disposal of people and companies alike. By introducing Fibre to the Street (FTTS) and Fibre to the Building (FTTB), combined with the new G.fast transmission standard, Swisscom is taking the next step into the future of telecommunication.

Switzerland enjoys a positive investment climate with regard to communications infrastructure. Swisscom alone invests more than EUR 1.5 billion a year in its IT and network infrastructure. That's about EUR 200 per head of the population and puts Switzerland at the top of the world's investment league table. Aside from classic telecommunication companies, other players are also contributing to the country's high-quality broadband coverage, including 250 cable network operators and about 20 power utility companies. With about 99% coverage at 30 Mbps, Switzerland is already close to achieving the broadband objectives of the EU's Digital Agenda 2020. And all without any state subsidies whatsoever

Lively competition promotes innovation

The good investment climate also encourages market players to be more innovative and drives competition between infrastructure providers. Cable network operators, for example, are upgrading their infrastructure with DOCSIS 3.0, thus providing bandwidths of up to 500 Mbps in selected locations. Swisscom is focusing on a mixture of technologies to provide widespread ultra-fast broadband as soon as possible. In major urban areas, it is currently driving forward the expansion of Fibre to the Home (FTTH), mostly in cooperation with local power utility companies. More than 921,000 homes and businesses – about a third of all households – can already benefit from bandwidths of up to 1 Gbps. At the same time, the universal service obligation mandate obliges Swisscom to ensure that rural and marginal areas aren't left behind.

As mentioned above, Swisscom is using a broad and innovative combination of technologies to meet the growing demand for bandwidth, not only through FTTH. For example, the introduction of VDSL2 vectoring in the existing Fibre to the Curb (FTTC) network architecture will be completed in 2015. In parallel to this, Swisscom is preparing its network architecture for the introduction of G.fast by bringing fibre-optic cabling closer to its customers. Therefore it has been expanding its FTTS and FTTB networks in many communities since 2014. In so doing, Swisscom is shortening the length of copper cabling to its customers' homes and businesses to just 200 metres and creating the conditions necessary to introduce the new G.fast transmission standard.

Huawei and Swisscom: a partnership for the future

G.fast, the successor of VDSL2, uses a wider range of frequencies (up to 106 MHz) on existing copper lines for data transmission. This allows transfer speeds of up to 800 Mbps over short distances under ideal conditions. One novel aspect of this technology is the use of separate time slots for upstream and downstream communication instead of dedicated frequency bands (Time Division Duplexing). The higher frequencies used by G.fast cause strong cross-talk between the individual copper pairs of a cable, requiring improved vectoring algorithms.

This new transmission technology arose out of a European research project that eventually led to standardisation efforts. Swisscom and its technology partner Huawei promoted the standardisation of G.fast from very early on, adding Swisscom's own requirements for G.fast. The International Telecommunication Union (ITU) approved G.9701, the G.fast standard, at the end of 2014. This is a decisive factor for G.fast's success because it defines how network elements and end-user devices must inter-operate to exchange data. Together with Huawei, Swisscom ran through various deployment scenarios which resulted in requirements for the technology and led to the development of initial prototypes of G.fast-capable Micro-CANs. These first-generation prototypes are still being tested and prototype G.fast Micro-CANs are planned to be deployed in field tests by the middle of the year. The aim is to serve several homes in a pilot community with G.fast before the end of 2015. This makes Swisscom a leading telecom provider in the development and use of G.fast.

Come and meet us at the Broadband World Forum

Want to find out more about our experiences with G.fast? Then come and meet our partner Huawei at the Broadband World Forum 2015 in London.



Swisscom (Switzerland) Ltd
3050 Bern

www.swisscom.ch

To ensure customer reliability, experience and security, CSP's and Mobile carriers will need to protect their most valuable asset from congestion and downtime as a result of multi-vector, short duration DDoS attacks.

How CSPs and mobile carriers can do more to eliminate the DDoS challenge

As businesses put more of their assets into the cloud, effectively mitigating DDoS attacks requires real-time protection at the Internet edge. As such, effective DDoS visibility and mitigation is a must have for converged and mobile carriers.

We also believe that a hardened DDoS defence solution is the first step a CSP/ Mobile carrier must consider before rolling out NFV services. Commercial and open-source hypervisor technology is enabling the new NFV economic model to emerge, but this same technology is tremendously susceptible to DDoS – a hardened edge with respect to DDoS will be essential to ensure that this new service model is not compromised by DDoS attacks.

Real-time DDoS mitigation tools which work at the entry point of the network interconnect

In order to keep up with the shifting and progressive range of threats, appropriate solutions need to be always-on and instantly reactive. It's clear they also need to be adaptable and scalable so that defences can be quickly and affordably updated to respond to the future evolution of DDoS threats – whatever that may entail.

The most effective method of fulfilling these aims is to utilise in-line DDoS mitigation, coupled with industry disruptive,

economically viable bandwidth licensing. With this technique, an in-line DDoS mitigation engine is employed but the operator only pays for the bandwidth of attacks actually mitigated. The benefit of this approach is that it delivers full edge protection for locations in the network that are most affected by DDoS, at a fraction of the cost of traditional scrubbing centre solutions. The desirability of these tools is due to the fact that they can be constantly on, with no need for human intervention, and they provide non-stop threat visibility, attack mitigation and DDoS forensics.

Another aspect of effective DDoS mitigation is security event reporting. One of the Achilles heels of traditional DDoS scrubbing centre solutions is that they rely on coarse sampling of flows at the edge of the network in order to determine whether an attack is taking place. DDoS attackers are well aware of the shortcomings of this approach and have modified many of their techniques to ride under the radar, below the detection threshold, in order to evade ever being redirected to a scrubbing centre. Your security posture will only be as good as your ability to visualize the security events in your environment, and a solution that relies on coarse sampling will be unable to even detect, let alone act on, the vast majority of the modern DDoS attack landscape. A robust modern DDoS solution will provide both instantaneous visibility into DDoS events as well as long-term trend analysis to identify adaptations in the DDoS landscape and deliver corresponding proactive detection and mitigation techniques.

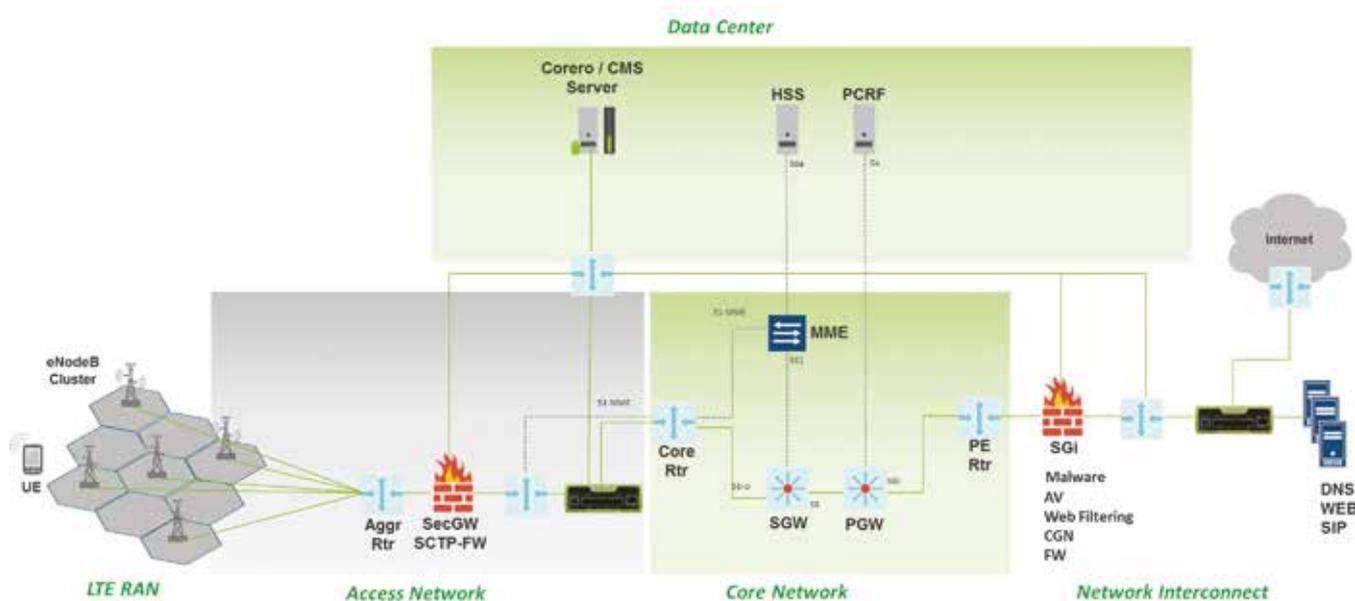
Real-time responses are possible with new, high-performance, in-line DDoS defence solutions. DDoS attacks generally have a bell-

shaped barrage of traffic. This is to throw off sample-based anomaly detectors – however it plays into the hands of DDoS mitigation solutions that utilize modern data analytics platforms that are optimized for detecting that a DDoS attack is underway before the system has reached a critical threshold. This is something that is simply not possible with legacy scrubbing-centre approaches.

A real business opportunity

Effective DDoS defence can be deployed either as an on-site solution or provided as a premium defence-as-a-service offering from an upstream Internet provider. Carriers are in a unique position to effectively eliminate the impact of DDoS attacks against their customers by surgically removing the attack traffic transiting their networks. In a recent survey, we asked enterprise IT teams about the role that ISPs should play in defending against DDoS attacks. Around 75 per cent of respondents indicated that they would like their ISP to provide additional security services to eliminate DDoS traffic from entering their network, and more than half would be prepared to pay for this type of premium service.

It's clear that we are seeing only the tip of the iceberg in terms of size and sophistication of the DDoS attack landscape. So, what's needed is a modern, fully integrated solution that can address the threat today and tomorrow, in real time - a solution that must be matched to the size of the threat. For carriers, this is an enormous opportunity to not only empower themselves to defend their own networks, but to also roll out DDoS protection services to their own customers, thus boosting customer loyalty and gaining new revenue streams. ●



‘Everywhere Enterprise’ heightens the need for cloud security

by Charles Milton, Director, EMEA Channels, Zscaler

As the new age of IT introduces a change in workplace dynamics, Charles Milton, Director EMEA channels at Zscaler, looks at the race against time for Chief Information Security Officers (CISO) to secure a borderless enterprise network.



Charles Milton, Director, EMEA Channels, Zscaler

Charles Milton has been EMEA Service Provider Director for Zscaler Inc. since 2010 and has been instrumental in Zscaler’s rapid growth from market entrant to leading Cloud Security service. Charles manages the strategic Service Provider relationships that form the primary channel for Zscaler’s services. Charles has worked in Information Security for 14 years and previously managed the EMEA service provider team for Blue Coat Systems for 6 years.

Following a whirlwind of employees adopting cloud-based applications and social media platforms in the workplace, it has brought mobility to the top of the agenda for IT. The accessibility of networks means business now happens any time at any given place, establishing an era of the ‘Everywhere Enterprise’.

It is evident that there is no longer a set perimeter as mobile devices can connect to 4G networks (soon to be 5G) rolled out in every major city with ease. To put this into perspective, we can even check our emails at 200 feet below the ground surface on London Underground platforms with public Wi-Fi networks.

While this workplace shift creates the benefits of increased agility and productivity it is creating a number of security concerns and threats if not managed properly.

According to the Ponemon Institute’s “2015 Cost of Cyber Crime Study: UK”, the number of cyber attacks in the UK continues to grow in frequency and severity. The average cost of cyber crime is now £4.1 million per year. That’s a 14 percent increase in the average cost from 2014. Attacks are becoming more sophisticated and pervasive, preying on the weakness of companies that don’t secure the ‘Everywhere Enterprise.’

Mobile workforce security dangers

The mobile ecosystem is very different than the ecosystem of PCs and this is especially true for security. In the workplace, PCs and laptops tend to be company owned/controlled. It’s therefore quite reasonable for the devices to be locked down and pre-loaded with security software that tracks all access and data.

This is not the case with Bring Your Own Device (BYOD) policies. End users are not willing to accept a paradigm whereby they personally cover the cost of a device, but provide the corporation with control over how it can be used. While BYOD may allow enterprises to lessen the cost of devices and service plans, it comes at the cost of losing control over the device.

It’s not surprising then that one of today’s big security challenges involves mobile users moving outside of the traditional security perimeter of organisations. By accessing the Internet with unsecured mobile devices, there is a danger that the device will be infected and import malware back into the corporate network. Or that the employee will fall victim to social engineering attacks when not protected by traditional enterprise security controls.

Outside of the office, security drops dramatically as the employee is no longer behind the network appliances delivering security, and on a smart device, they also likely have no traditional host-based security. In 2014 a staggering 68 per cent of UK businesses suffered a security breach from work mobile phones due to not implementing the right security solutions.

IT struggles to keep up with monitoring such a diverse range of network access points. It is inevitably losing control with the employee now pulling the strings. The worst thing is that attackers are fully aware of this imbalance and are exploiting it. This is why attackers have largely shifted their efforts to targeting end users and are often specifically targeting those that work remotely.

As we’ve seen with recent headlines, mobility has made it even easier to breach corporate security measures. Looking at securing users beyond the company walls means moving away from the traditional focus on perimeter defence.

15 per cent of large organisations had a security or data breach in the last year involving smartphones and tablets in 2014, up seven per cent from last year, whilst seven per cent experienced this relating to one of their

cloud computing services as the use of cloud continues to rise. This is according to findings from the 2015 Information Security Breaches Survey conducted by PWC.

In this new age of progressive IT, with cyber security threats coming in from all directions, CISOs require a new approach to security; one that provides consistent policy, protection and visibility to all user and devices irrespective of location.

Insider threats

To make the 'Everywhere Enterprise' a reality, employees have access to more appliances, cloud services and mobile apps these days than ever before.

Businesses need to see through the misconception that the danger of cyber attack is only from external hackers. More often than not with the 'Everywhere Enterprise,' it's caused – often innocently – by insider threats. Many employees may not even be aware that they have left the gate wide open for criminals to enter freely.

Cloud services and mobile apps have become so readily available that many of the applications used by employees are no longer securely managed inside the IT 'fortress' of a business. Cyber criminals are fully aware of the open gateway and the opportunity to exploit users. When users download apps or files from an apparently trusted site, malware is seeded inside the corporate network undetected. Once the initial infection is planted, it can easily spread to all corners of the organisation network.

In fact, most of the major enterprise hacks are conducted through internal breaches. Plus, according to figures from the 2015 State of the Endpoint by Ponemon Institute, 78 per cent of IT professionals consider negligent or careless employees who do not follow security policies to be the biggest threat to overall security.

On one hand as cloud applications become mainstream, traditional methods of protection are no longer sufficient to combat web-based crimes.

But as businesses transition to the cloud, there is also an education process that must take place. Employees need to be aware of the hidden risks when sharing and syncing files from multiple devices and accidental data disclosure.

Challenging traditional security

The 1990's idea of using security appliances installed in a data centre to protect employees who are on their laptops sitting in cafés and working via the cloud, no longer makes sense.

Not only are security appliances tied to legacy location concepts, dictating limitations to the business rather than enabling it, they tend to be built for one security function only. This creates an explosion of new appliances in the data centre to keep up with each new threat, all of which must be individually purchased, installed, maintained and updated.

Appliances also lack the pace to counter evolving threats and fail to meet the architectural flexibility to accommodate new enterprise technology. As a result businesses are operating on outdated security models that don't provide enough visibility to enable security executives to maintain control.

As such, the traditional 'block vs. allow' strategy is no longer fit for purpose in today's 'Everywhere Enterprise'. As the working environment evolves, organisations require a shift to a 'manage and monitor' approach. After all, prohibiting access to Internet resources will only encourage users to bypass security controls.

Bridging the cloud gap

Looking at new strategies to tackle the threats of the digital age means searching beyond the tools traditionally deployed in the enterprise, towards the benefits of cloud delivered security.

However, while the return on investment of cloud solutions has been well documented, the trend towards using them for security purposes has been treated with trepidation. That's due to the perceived risks that have been driven by ill-equipped security appliances featuring in the majority of workplace architectures today.

Pointing to this, a Eurostat study showed only 19 per cent of European businesses used cloud computing services last year. The main factor limiting the use of cloud computing is security, found Eurostat, but yet the business benefits of cloud are undeniable – so it is on the rise.

To remain competitive, European businesses must work through security challenges. After all, as cloud applications become more widely accepted and deployed, CISOs are starting to see the competitive advantages of cloud computing in terms of flexibility,

agility and competitive advantage. Why pay for capital investments and the resources to manage them when you could redeploy the money for strategic projects?

New technologies and processes can deliver enormous gains in productivity and efficiency to drive business metrics like revenue generation and customer satisfaction. And that's not the only critical advantage. Cloud solutions are integral to helping businesses realise advanced security capabilities – most importantly, better visibility.

In today's complex IT environments, the ability to see how every user, device and application is accessing the corporate network is no longer a 'nice to have', it's a business imperative. The next generation of enterprise security is about the Direct-to-Cloud Network approach. This is much more than blocking threats. It will support critical security protection by enabling IT to take back control.

Shifting power to the CISO

The proliferation of mobile and cloud technologies has shifted the centre of gravity toward the user.

Moving security to the cloud shifts the balance of power back in favour of the CISO. A cloud security model acts like a check post between the user and the Internet and all Internet bound traffic goes through it, enabling businesses to embrace mobility and cloud while enforcing security policies that follow the user.

It allows companies to embrace innovation securely, while providing the visibility and controls needed to ensure compliance with corporate policies. It also helps executives to regain control of the enterprise's digital assets and user activity, whether located internally or externally on the Internet, so they can spot potential threats before they escalate.

The challenge for today's CISOs is shifting focus from basic infrastructure projects to more strategic initiatives. Moving security to the cloud is an example of this type of transformational process. It provides business agility, reduced costs and more importantly, it enables CISOs to use security capabilities as a business enabler.

Many CISOs are beginning to act on the principle that protection is no longer enough, prevention is now key. Forward thinking European executives will be investing in cloud-based security to facilitate initiatives in light of this new reality. ●

Head in the Clouds? Regaining innovation leadership in telecoms is critical for Europe

by Markus Borchert, SVP Europe Market, Nokia Networks

To apply cloud to mobile broadband networks requires re-inventing telcos for the cloud, which also makes networks more agile and reduces time to market for new services from months to minutes. For end users, this means newer services can be rolled out quickly and customized to their needs. The fast pace of change in the industry means it is simply not possible to predict all requirements future networks will face. There will be many use cases that are not known today. Therefore, flexibility must be a key requirement. In short, the aim is to create an agile, programmable network infrastructure.



Markus Borchert is the Senior Vice President of Europe Market, Nokia Networks. Previously, he was President Greater China Region, Nokia Networks (formerly NSN)

Prior to Nokia Networks, Markus Borchert was SVP Strategy and Marketing, Siemens Mobile Networks, SVP Global Customer Unit Vodafone, Siemens Mobile Networks; and multiple leadership and management roles, Siemens Nixdorf Information Systems and Siemens Business Services.

Markus Borchert holds the following degrees: Master of Science in Electrical Engineering and Information Technology, Technical University, Munich; and Master of Business Administration (Sloan Fellow), Massachusetts Institute of Technology.

Mobile traffic continues to grow dramatically. In the last 3 three years alone, mobile traffic has nearly doubled every year, Europe included. One of the most important mechanisms to maximize resource utilization is cloud technology. Telco networks are evolving to cloud to enhance their flexibility, scalability, configurability and adaptability, and to address the changing needs of services and connectivity.

The Shift towards Telco Cloud

Cloud computing has been transforming the IT industry over the last decade. It has helped to drive down costs, improve business agility and has enabled new business models. The gains are due to the separation of software-based applications from the underlying

hardware via virtualization and a highly automated way to operate the applications on a hardware platform with a cloud management system.

These cloud design principles are being applied to telco networks and telco applications built according to the traditional infrastructure approach. This is creating the foundation for what we call the telco cloud using the main industry programs like Network Function Virtualization (NFV), Software-Defined Networking (SDN) and Mobile-Edge Computing (MEC).

Traditionally, network architecture has been built around a specific use-case. For example, GSM was built primarily for voice and LTE primarily for mobile data.

In the future, this 'one use-case network fits all' approach will be redundant and the design criteria will be to offer personalized networks built around each user because future networks need to go beyond voice and data to serve many diverse uses, services and applications. And each user needs to feel as he is the only one using the network.

To apply cloud to mobile broadband networks requires re-inventing telcos for the cloud, which also makes networks more agile and reduces time to market for new services from months to minutes. For end users, this means newer services can be rolled out quickly and customized to their needs. The fast pace of change in the industry means it is simply not possible to predict all requirements future networks will face. There will be many use

Yamal-300K' Eastern Campaign

by Gazprom Space Systems

Two and a half years ago the Russian satellite operator Gazprom Space Systems replenished its orbital constellation with a new satellite Yamal-300K.

The satellite was launched from Baikonur cosmodrome and put into the 90°E slot on the geostationary orbit. After the successful launch of Yamal-401 satellite into the same orbital slot, and moving all the customers from Yamal-300K to the new satellite, Yamal-300K started planned relocation into the other orbital slot 183°E. This position is located over the Pacific Ocean, and enables coverage of the Russian Far East, Korea, Japan and other South East Asian territories; and as far as Alaska. These regions have good market prospects and, because of this, Gazprom Space Systems made a decision to extend its business eastwards and arranged this “Eastern Campaign”.

The satellite in its new designation is interesting for the Russian as well as international customers. Gazprom Space Systems experienced it already at the stage of preliminary sales. One of the Yamal-300K beams perfectly covers the Russian Far East and attracts the attention of, for example, Russian mobile operators concerned about creation of backhaul infrastructure for their cellular networks in the region.

The steerable beam of the satellite is ready to serve any region of the South East Asia, Australia, New Zealand and the waterlocked states of the Pacific Ocean. However, the most attractive coverage, in our opinion, is provided by the wide shaped beam of Yamal-300K that covers the north of the Pacific Ocean with its intensive aeronautic and maritime traffic and big transport hubs on the coast.

Recently, Gazprom Space Systems essentially renewed and extended its satellite assets. Launch of the three high power satellites resulted in the 3.5 time growth of the satellite capacity amount in 2015 in comparison with 2012. Nowadays satellite flit of the company is rather young (the average satellite age is less than three years).

The company markets 30% of Yamal satellites capacity outside Russia. In particular, one of the new satellites Yamal-402 55°E has achieved prominence on the markets of Africa and the Middle East, and Yamal-202 49°E has already been successfully working for Asian markets for more than ten years.

In Russia, Gazprom Space Systems is not only a satellite operator but also a service provider and system integrator. The key element of the

company's ground infrastructure is the Telecommunication Center in Stchelkovo near Moscow, from where the satellite constellation is controlled, and where the main ground assets to provide services are concentrated (hubs, up-links, NOC and so on). From this place the company also controls wide scale satellite communication earth stations network placed in the Russian regions.

Concerning further business development, along with the plans to create new own satellites, Gazprom Space Systems also searches for new business models. The company relies on cooperation with the other satellite operators to build and use orbital assets. Joint efforts with other operators helps to resolve increasingly frequent collisions connected with overcrowding of the GEO.

Cooperation allows us to share the risks of financing capital-intensive satellite projects. The idea to create joint satellites, or hosted payloads, has become ever more popular. During those periods when our large investments are impeded, similar solutions provide operators with the opportunity to gain business traction.

While similar business ideas are waiting for their implementation, the business project “Yamal-300K' Eastern Campaign” has already started. ●

cases that are not known today. Therefore, flexibility must be a key requirement. In short, the aim is to create an agile, programmable network infrastructure.

To transition towards user-oriented networks, current telco network architecture needs to undergo a fundamental transformation from a vertical to a cognitive and cloud optimized architecture. The shift towards cloud based networks implies that equipment makers will need to comply with IT standards and open source. It also means that they need to collaborate more with IT players and vice versa. The architecture itself will transform from static & vertical to dynamic & cloud optimized.

Laying the foundation for the future

While the benefits of the telco cloud are clear, the transition for operators is complex and cannot be completed in a single step. One of the key technology shifts towards the cloud and cognitive network architecture includes the evolution to 5G and its programmable multi-service architecture. This is essential to enable use cases which today's networks have not been built for.

To provide the required data rates, latencies, robustness and connectivity, novel technologies are required for 5G. Most of these technologies are characterized by their flexibility and ability to adapt to different scenarios and use cases. In both radio and core network telco cloud, virtualization and Software Defined Networking will enable network-wide programmability, elasticity and scalability. Network orchestration enables automation across network components through centralized management of network resources.

5G will allow for massive growth in traffic, peak data rates much higher than 10 Gbit/s (compared to 300 Mbit/s for LTE), virtually zero latency and it will integrate pre-existing technologies while lowering energy consumption. 5G will also be prepared to support applications and industries of the future such as innovative health care services and self-driving cars.

Europe has traditionally been driving the technology development in the telecommunications space. But when it comes to 4G/LTE roll-out, the center of activity has shifted in the recent years and we have seen a stronger momentum in other parts of the world. In fact, it's now Europe who has some catching up to do.

Now, with 5G approaching, Europe has an opportunity to seize the chance and regain the technological and innovation leadership. Actually, Europe is at the forefront of 5G development – and is risking to fall behind again if implementation would lag behind due to insufficient infrastructure.

Boosting investments in telecommunications infrastructure is vital for European competitiveness beyond just the ICT industry. For most industries, connectivity and mobility are becoming critical in order to stay competitive and change the way they are doing business. An important example of this transformation effort is the so called 4th Industrial Revolution which will lead to a fully automated and flexible production process. This is the reason why we need a strong and successful telecom industry in Europe: to reinforce the competitiveness of Europe overall – all sectors – not just ICT. In other words: Europe needs a modern digital infrastructure that can be the backbone for success across industries.

On July 1, a number of research projects began within 5G Infrastructure Public-Private Partnership (5G-PPP) that is part of the largest global research and innovation program Horizon 2020. 5G-PPP is a joint initiative of the ICT industry and the European Commission to define future 5G communication systems. The research projects will facilitate the upcoming standardization of 5G by consensus building and contributing to the 5G technology portfolio.

There's no cutting corners

Driving 5G development is essential, but 5G development is not enough. 4G is needed because 5G communications will involve a combination of existing and evolving systems, like LTE-Advanced and Wi-Fi, coupled with new, revolutionary technologies designed to meet the new requirements. There is no way to leapfrog 4G and directly go to 5G.

Areas without 4G coverage will be the 5G white spots of the future. Therefore, Europe should strive to catch up with 4G roll-out, where we are clearly behind other regions: In 2014, 13% of total connections have been LTE (4G) connections in (geographical) Europe, compared to 47% in Japan, 51% in Northern America and 84% in South Korea. Additionally, Europe reached 70% 4G network coverage (by population), whereas Northern America

reached 98%, Japan 99% and South Korea 100%. This is a serious threat – not only for the European telecoms industry, but for the European economy altogether.

Korea and Japan have announced that they will launch 5G in the next few years, Korea in the Winter Olympic Games in 2018 (pre-commercial) and Japan in the Summer Olympic Games in 2020. If it takes Europe until then to roll-out LTE, Europe will fall behind again.

With the right steps to speed-up 4G roll out and continuous investment in the development of 5G, Europe can reclaim the pole position – once again.

Building bridges between industries

Europe has a very strong position in vertical industries, such as automotive, advanced healthcare, medical, engineering, utilities, and many more. These industries are in a transition period at the moment. Digital technologies are changing the way we communicate, manufacture goods, and drive cars, how we do sports and how we get medical treatments. Telecoms is enabling this transformation, building bridges between our physical, virtual and social worlds.

If these aforementioned industries and the strong European telecoms sector joined forces, we could create a strong momentum in Europe. The key will be collaborative innovation projects displaying what 5G can do for various industries, and the new possibilities it provides for the consumer. With this approach, there could be early traction for 5G in the European market.

Europe's targets must therefore be ambitious. We should aim for having the first commercial full spec 5G roll-out in 2020 – in time for the European football championship. But first, we need substantial investments in Europe to close the 4G gap. And in order to encourage investments, the conditions for investing need to improve. This should be a common goal: governments and regulators should attend to creating conditions for a more innovation-friendly environment and the ICT industry needs to drive innovation leadership together with customers to bring Europe back to lead in the telecom sector. Europe needs to be ambitious – and invest on its future. ●

“Go Digital or Die”

by William Morrish, Director of Cloud Services, Interoute

Being told to go ‘all digital or die’ is more than a daunting prospect, and it’s often one which is faced with a feeling of apathy due to this legacy. Going digital is not about moving to the cloud or any other technology, its really about a sociological change of how technology sits within the business. When done right, IT changes from being a financial burden, to a team that can affect, create and drive real business change via these new digital technologies and provide ideas that will have both top and bottom line effects.



William Morrish, Sales and Marketing Director for Interoute Virtual Data Centre

William Morrish is an avid technologist and works as a Global Sales and Marketing Director with over 20 years of business experience, covering high-level technical detail, customer service and sales.

William is responsible for the strategy and execution of the global sales activities for Interoute’s global Cloud services division, as well as accountable for the multimillion dollar marketing budget to ensure our messaging reaches the correct target audience.

Our goal is to automate the delivery and integration of connectivity, communications and computing services by creating a massively scalable platform for IaaS globally.

Prior to Interoute Will has worked at a number of cloud and network operators fulfilling a mix of both on-site technical and sales roles.

We are increasingly seeing that success in today’s world of IT comes from ‘going digital’. Just ten years ago we didn’t have access to smartphone apps, social media and even email was much more limited. Alongside the new generation of tech-savvy consumers in the market and the proliferation of digital channels, every piece in the puzzle of communications has been impacted and for the better.

Whether this involves changing businesses from the ground up and building fresh approaches to old problems, the use of DevOps, cloud or other technology, the stark reality is that most IT departments now have

a range of applications and an established (although sometimes partially unknown) estate in place. The time has come to think differently about the IT organisation but also about how to integrate processes properly to build from the past and into what’s called a ‘bimodal’ digital future – where both old and new can seamlessly operate.

The DNA of digital

Being told to go ‘all digital or die’ is more than a daunting prospect, and it’s often one which is faced with a feeling of apathy due to this legacy. Going digital is not about moving to the cloud or any other technology,

its really about a sociological change of how technology sits within the business. When done right, IT changes from being a financial burden, to a team that can affect, create and drive real business change via these new digital technologies and provide ideas that will have both top and bottom line effects.

It’s important to really understand the DNA of today’s digital sphere and how this can transform business processes. There are five key elements to making this move:

- Social: Does this mean having a Twitter or Facebook account for your business? The answer is no, going social from

EXPO COMMTM RUSSIA

See the Future of Communications

Russia's International Exhibition + Forum
of Advanced Information Communication
Technologies and Solutions

April 19 - 21, 2016

Moscow, EC VDNH, Pavilion 75



The unique exhibition and conference platform will include Network Integration, Unified Communications, Information Management, IOT/Cloud Computing and Mobile ICT

For more information please contact:

China
E.J. Krause & Associates, Inc.
Xiaohua Chen
xiaohua@expocomm.cn

EUROPE
E.J. Krause & Associates, Inc.
Gudrun Tegge
tegge@ejkgermany.de

USA
E.J. Krause & Associates, Inc.
Ron Akins
akins@ejkrause.com

Organizer:



E. J. KRAUSE &
ASSOCIATES, INC.

Co-organizer:



www.expocomm.ru

a business perspective means really thinking about the interaction you have with your customers - whether they are internal or external - through to how you as a business can think about changing these terms of interaction and making them more effective.

- Mobile: Importantly this does not necessarily mean having a mobile app or something in the Google or Apple store. This requires thinking about how you interact with both your internal and external customers, the mobilisation of IT using things such as 'bring your own device'/'choose your own device' and others. This again requires thinking about the business services in place and how to leverage better interactions.
- Big data & analytics: These are changing the way we think about customer behaviour, and how we can react to their requirements. They provide a crucial extra layer for understanding user patterns, which enable businesses to look internally at customer behaviour to build profiles and use pattern changes to help determine what they can do to work more relevantly with customers. It's also about enabling real-time business operations, giving insight into the 'right now' of your business making you more nimble and effective in the marketplace.
- Consumerisation of IT: With an evermore technically advanced workforce not all of the technology change will come from IT. This is creating exciting opportunities for the development of ideas. For example, where the use of services such as Box and Dropbox may have previously been avoided for corporate practice, this shadow IT has now become mainstream – where if your users need it, they're able to get it. It raises best practice concerns and it's one that IT needs to stay one step ahead of. After all the next big idea in IT could well bubble up from somewhere unexpected in the business.
- The Cloud: Going digital is not about putting everything in the cloud. The cloud is an enabler, a toolset that can complement or replace current practices and make it more efficient. This is why going digital is more about a sociological change rather than a technical one, it's a change in process and approach. This is also where the transformation must be put into context. For example, large platforms cannot simply be ripped out and replaced

by the cloud and therefore a pragmatic approach must be taken to properly see the benefits.

Gartner classifies this transformation or revolution from an old to a new model of IT as 'Mode 1' (old/ITIL) and 'Mode 2' (new/Digital). The reality is that going digital is not optional - businesses need to change to retain their relevance. It is now crucial to build new ways of delivering services that will enhance business change and promote a bimodal digital future. Those who are not heading in this direction will almost certainly struggle under the challenge of keeping up with competitors to harness market share.

React and adapt

However, it's too simplistic to think in terms of old (legacy and existing systems) and new (appetite to change). It should be considered against what can be changed to deliver the most benefit to the business. Cloud adoption should not be seen as the essential panacea and indeed some cloud services already under your control may be themselves classed as old and part of the established estate. Cloud should be seen as an enabler of tools and services when and where it is appropriate to use them.

Using Uber as an example, many taxi companies across the world could have seemingly created this hugely successful model which has seen an incredible amount of growth in a short space of time. The differentiator here, however, is that Uber also took on a large amount of risk to get there. Imagine the reaction from employees to the head of the local taxi firm saying "I have had a thought, how about we ditch all of the cars and turn this into an app!" Many businesses wouldn't be able to start again entirely from the ground up as this is often perhaps a little more risk than most shareholders would be willing to bear. Therefore businesses must begin thinking in this way and asking: is there an Uber to your business and how you can change it? Businesses need to build a plan that will enable new services and models to exist and build in this new mode, while also updating and integrating with existing estates.

The key piece to any technical transformation of business is integration and control. Businesses must establish a bimodal model of IT, an all-encompassing base strategy of consolidation, renewal and integration of old and new. This focus is critical to allow businesses to consolidate, migrate and build for the future by

integrating what they have got, with what they want, and what they do not yet know, on one globally integrated IT structure. ●



**Connect-World now on
Facebook & Twitter**

Connect-World, the world's foremost discussion forum for leaders in the ICT industry, is now available on Facebook and Twitter.

The world's top ICT decision makers express their opinions in *Connect-World*. They use clear, non-technical, English to discuss how ICT helps shape regional and global development. The articles essentially examine the influence that ICT products and services have on the way people live and do business. With separate editions for each of the world's regions, the reports highlight the most important ICT trends and issues influencing socio-economic growth.

Connect-World is now available to follow on Twitter (<http://twitter.com/#!/ConnectWorldICT>) and Facebook (<http://www.facebook.com/connectworld.ict>)

Also, it is still possible, for FREE, to directly access all past and present *Connect-World* articles, ICT Industry press releases, eLetters, ICT News and more at www.connect-world.com.

Riding the smartphone surge for a superior cloud-enabled user experience

by Chris Halbard, EVP and President, International, Synchronoss

In Europe, smartphones are more popular than ever. So too is mobile data. How can communication service providers deliver more value to their subscribers in today's smartphone-focused, data-first world? The answer is in the evolution of personal cloud services.



Chris Halbard serves as EVP and President, International at Synchronoss.

In his role, Chris will lead the direction and execution of the company's international business development initiatives and operations. Specifically, he will be responsible for driving global growth and international sales initiatives.

Prior to joining Synchronoss, Chris was a Senior Advisor to The Boston Consulting Group serving clients within the technology, media and telecommunications industries. Previously, he was the COO and CFO of the Global Services division of British Telecom plc (BT). Prior to British Telecom, Chris held a number of senior positions at Lucent Technologies, AT&T and Arthur Andersen & Co.

Based in London, Chris is a qualified Chartered Accountant and received his BA HONS in Economics and Business Studies from The University of Sheffield.

The smartphone surge

The smartphone juggernaut shows no sign of slowing down in Europe. In the second quarter of 2015, Apple iOS returned to growth across Europe's five largest countries, recording its first year-on-year gain in France since February 2015. According to media reports, Apple has asked suppliers to manufacture between 85 and 90 million units of two new forthcoming iPhone models by the end of the year.

Meanwhile, in its latest smartphone report (August 2015), research firm IDC reports over 341.5 million smartphone shipments worldwide in the second quarter of 2015, up nearly 13% from 2Q14. According to CCS Insight, sales in Western Europe are close to saturation and are poised to peak in 2017; however research firm Gartner highlights Eastern Europe as one of the fastest-growing regions in Q2 2015. The iPhone 6 and 6 Plus are proving a popular choice in mature Western European markets for consumers replacing older devices. The increasingly affordable iPhone 5c is also bringing in new

customers, with the rumoured release of the 6c likely to generate similar interest.

More mobile data

As more people worldwide upgrade to smartphones, the volume of mobile data they use is increasing: according to Gartner, this year global mobile data traffic will reach 52 million terabytes (TB) – a rise of 59 percent from 2014. This rapid growth is set to continue through 2018, when Gartner estimates mobile data will reach 173 million TB.

The many functions and features that handset makers cram into our devices – hi-res cameras, video playback, bigger HD screens, WiFi connectivity – make them ideal for, firstly, creating our own user-generated content, and also for consuming a vast range of additional content from third parties.

More users are taking more photos, sending more messages, shooting more video and consuming more media on their phones. And when the time comes to replace their trusty handset, they don't want to lose all this data:

they want it safe and secure on their new phone, accessible there and then.

Personal Cloud services were originally created by operators as a means of helping their customers store and secure content, and enable them to sync it from device to device to ensure content is continually accessible. These capabilities have subsequently led to operators offering a certain amount of cloud storage capacity for free with every new connected device activated. The reality today is that most major tier one operators in developed markets offer these personal cloud services to their customers and the amount of free storage capacity offered will gradually increase.

The OTT threat

But while the growth of user content has proved to be an effective way for operators to 'seed the cloud' and retain subscribers, the ability for operators to offer one dimensional storage services to customers is quickly becoming a commodity. In fact, some see greater smartphone uptake as the latest development to push operators further down

the telecoms value chain and further away from their customers.

In particular, consumer tech brands and OTT service providers like Apple, Whatsapp, Google and Dropbox have been attempting to seize mindshare and brand awareness, with the aim of eroding operators' relationships with subscribers – and their bottom lines. There is an assumption now that users immediately think of Google Drive, iCloud or Dropbox as the preferred location when considering where to back up and store the content on their phone.

But let's remember that mobile operators have built their businesses over the last 25 years by providing trusted and highly secure transport networks – firstly for voice, but latterly for data. The above assumption overlooks two crucial technical advantages that mobile operators have over their rivals – the ability to firstly, connect to and support multiple device types, screens, and Operating Systems securely and at scale: and secondly, the means to connect users to their content and data wherever they are, wirelessly, on whatever device they're using.

However the competition posed by OTTs means it is time for operators to take their personal cloud capabilities to the next level. Particularly if you consider how much personal cloud services can teach an operator about its customers' behaviour and preferences, a failure to evolve further could look very short sighted. It is this continual secure access to content, irrespective of device type, that is the key in the evolutions of operator cloud services.

Multiple devices, multiple connections

In its last Mobility Report (June 2015), Ericsson predicts that in developed, mature markets like Western Europe in particular, growth between now and 2020 will come from individual users owning an increasing number of devices. Not just a smartphone, but also a tablet, home PC – perhaps even a connected car.

What if a user, having downloaded a video on their Android tablet or Smart TV at home, then wants to watch it on their iPhone during their morning commute? Will they need to configure their various devices themselves in order to access their content? Or is it more straightforward to let their operator deal with these complex cross-device, cross-connectivity issues instead? After all, operators are already

trusted by their subscribers to provide a reliable and secure service.

Viewed in these terms, the global smartphone surge plus subscribers' data appetite actually represents a significant opportunity for operators to take back some of the ground lost to rival providers and reassert themselves in the telecoms value chain. In particular, it is an opportunity for operators to show their deep customer understanding, and begin to offer subscribers even more relevant ways of accessing their content, and provide context to that content and their interaction with it.

Cloud as catalyst

By using personal cloud services to firstly, simplify and speed up the handset upgrade process for their customers, operators can again add value in a new way and play that meaningful role in their customers' mobile lives. For operators, this meaningful role isn't just about data, files and storage. It's not even just about smartphones and other connected devices. It's about screens and sharing: that is, giving users the means to access their data and content across multiple screens – their phone, their tablet, their PC, their smart TV at home, their connected car.

Operators are beginning to realise that in order to drive consumer engagement for personal cloud services they need to increase levels of convenience and accessibility in relation to their customers' content. In the first instance, this has led operators to provide access to centrally held content across any device, anytime, anywhere. This has been a critical component in helping consumers benefit from a truly connected life by syncing content across smartphones, tablets, wearable technology, connected cars and the connected home.

Be the enabler

The ultimate goal for operators is the ability to take all the information that an operator knows about its customer to create an individual "digital profile".

Operators can go further in reclaiming the user experience from their OTT rivals by assuming the pivotal "enabling" role for providing all cloud content to their users. The operator can use the cloud as a secure hub to gather, store and analyse subscriber data – user contacts, content, calendar, location, transaction history. This hub will establish and securely curate a unique digital profile for each of their subscribers that gathers together their personal information to act as their identity in

the cloud, and which then follows them from device to device and from screen to screen. This operator-enabled digital profile allows the consumer to securely access the content that is most relevant in a way that is most convenient to them at that particular moment, and also allows the operator to provide context via analytics to that content.

With this digital profile in place, the operator can then add extra context and relevance to whatever cloud-based service or content that their subscriber wishes to access - according to what device they're using, their account settings and preferences, their location and so on. This digital profile provides an opportunity for operators to revolutionise the customer experience by giving subscribers even more choice, while also leveraging personal cloud services to generate extra revenue. Here are two anecdotal examples:

- You're driving in your car and it's nearly lunchtime. The operator uses your location to identify restaurants either immediately nearby, or close to your final destination: it references your credit card payment history to see what your preferences are (e.g.: Mexican, Thai, modern European) and chooses a shortlist of suitable restaurants for you to choose from. It then provides directions on how to reach each one from your current location.
- You're out of the house when you receive a notification on your smartphone that your children at home want to purchase and watch a film on the connected TV. The notification gives you information on the film in question, plus the choice to disable the parental lock. It then automatically charges the cost of the film to your service account or credit card.

In this way, the cloud becomes the foundation for operators to not only deliver an enhanced user experience and a deeper customer understanding, but to expand their own ecosystem of features and services, through revenue-share partnerships with content and media companies, other service providers and merchants. This can be constantly updated and leveraged to create contextually relevant and valued offers and services to each individual.

The emergence of this operator-led personal cloud technology places operators at the heart of a potentially lucrative value chain and draw upon their key assets: strong existing customer trust, the ability to deliver services at scale, business longevity and security best practice. This will all be critical in preventing the ceding of further competitive advantage to OTT providers. ●

The dawn of 'Cloud Brokers'

by Tony Limby, Director, Cloud and Datacenter, BT Business

As an ever-increasing number of organisations start to consider the wider use of the cloud within their businesses, and start to move more critical applications away from on-premise infrastructure, they expect improvements in related areas of technology provision. That belief is particularly strong in the areas of resilience and functionality, where IT managers are aware that the security of online processes is crucial



Tony Limby is Director, Cloud and Datacentre, at BT Business, where he is responsible for defining and delivering the IT Services Cloud and platforms roadmap for its IT Services division.

He has formerly held senior roles at Lynx Technology, Siemens, Sema Group and ComputerLand, and currently sits on the Interim Advisory Council for Cloud 28.

The cloud market has matured to such an extent during the past few years that a tipping point has been reached. On-demand technology started the decade as an alternative means of service provision, but has quickly become one of the key routes for procuring IT services.

Such is the crucial role played by the cloud that as many as 57 per cent of IT executives believe on-demand technology is now critically important to the business, according to ZDNet and TechRepublic research .

On-demand applications and services, in short, have been adopted and accepted by businesses, and that rate of implementation

is set to grow exponentially during the rest of the decade. So, why has there been a rush by organisations to move IT on-demand?

One crucial explanation is that the cloud has transitioned from a theoretical and over-hyped concept to a practical business tool. IT directors and their senior business peers understand how external service provision can help transform the use of technology across the functions of an organisation.

More to the point, such managers are beginning to see real business benefits. The cloud provides a great fit with the modern objectives of many organisations, helping executives to both cut costs and increase

agility. Most on-demand arrangements, after all, allow businesses to increase their use of IT resources as business demands dictate.

But the benefits are not just related to short-term objectives. The cloud can provide long-term plus-points, too. Closer integration with service suppliers means IT and business managers can benefit from the latest applications, without the capital outlay for hardware and software, and on-going maintenance.

Many organisations are only just beginning to see the first raft of benefits. Use of on-demand IT is often centred on commodity areas, including email hosting, and non-core



The GSMA Asia Mobile Awards are back for 2016!

The GSMA Asia Mobile Awards (AMO Awards) are making a return. The AMO Awards recognise everything from game-changing mobile devices and technologies, to applications and services developed or available in Asian markets, showcasing the ever growing value that mobility brings to users, industries, businesses, communities and economies across the region.

AWARD CATEGORIES 2016



Mobile Apps Category

- ▶ Best Mobile Music App
- ▶ Best Mobile Game App
- ▶ Best Mobile Sports App
- ▶ Best Mobile App for Media, Film, TV, or Video
- ▶ Best Mobile App or Service for Enterprise



Connected Lifestyle Category

- ▶ Best Mobile Innovation for Connected Lifestyle
- ▶ Best Mobile Innovation for the Internet of Things
- ▶ Best Mobile Innovation for Emerging Markets



Mobile Devices Category

- ▶ Best Smartphone or Tablet Device
- ▶ Best Affordable Smartphone



Outstanding Achievements Category

- ▶ Best Mobile Technology Breakthrough – Asia
- ▶ Outstanding Contribution to the Asian Mobile Industry

Note: The "Mobile Apps" and "Connected Lifestyle" categories are open for submissions; the "Mobile Devices" and "Outstanding Achievements" categories are not open for entry, as nominations for these are put forward and judged by a panel of independent experts.

KEY DATES FOR THE 2016 AWARDS

Deadline for Entries: Friday, 15 April, 2016

Shortlist Announced: Early June 2016

Awards Announcement and Presentation at MWC Shanghai: Wednesday, 29 June, 2016



Submit your entries now @ www.asiamobileawards.com

areas of technology provision, such as testing and development.

Yet as business leaders begin to see the payback from a move to the cloud, they start to consider its relevance to other organisational processes. Our research suggests IT managers are also using the cloud for packaged enterprise apps and non-core areas of hardware, including storage back-up, virtual desktop infrastructure and disaster recovery.

As an ever-increasing number of organisations start to consider the wider use of the cloud within their businesses, and start to move more critical applications away from on-premise infrastructure, they expect improvements in related areas of technology provision. That belief is particularly strong in the areas of resilience and functionality, where IT managers are aware that the security of online processes is crucial.

A rise in the number of online interfaces can also produce a management challenge. IT leaders will increasingly have to draw on an ecosystem of providers, as the breadth of applications and services that are available through trusted partners via the cloud continues to rise.

Suppliers will need to help senior executives to overcome this challenge. Strong external service partners will alter the types of service they provide and the means through which they offer such technologies.

Rather than the constraints of a traditional licensing arrangement, smart suppliers will use flexibility as a watchword for quality, offering businesses exactly the kinds of services they need in the forms they choose to consume.

This new arrangement will definitely include flexibility in pricing, but will also draw upon an increased range of applications and services that customers can buy from their preferred supplier. A proper and effective cloud system represents a platform from which users in the enterprise can pick their tools on-demand.

For vendors, this change towards service flexibility could be seen as a threat. The standard means of procuring IT, which might rely on the purchase of an enterprise stack from a single supplier, is no longer workable in the age of the cloud.

We believe that, in the future, the key role of a trusted supplier will be as a 'broker' for cloud services. This specialist orchestrator will give customers the opportunities to source the breadth of services they require on-demand, but through the convenience of a single, expert supplier.

Modern executives, particularly those in charge of IT, are time poor and pressure heavy. They are expected to keep key systems up and running, while also sourcing innovations that can help transform the way a business operates and the means through which it serves its valued customers.

That's where we believe suppliers can step in and help. A trusted, one-stop shop for cloud provision will take the weight off business and IT leaders. A great provider will manage the ecosystem of relationships, and provide the first line of support and management.

Smart provision in the age of the cloud doesn't only extend to vendor management. We believe suppliers should help businesses to overcome contract complexity and to deliver cloud services integration. Such assimilation should ensure all vendor offerings, no matter how niche, are brought together under collective or single Service Level Agreements (SLA).

Our Global Services division recently announced a new generation of cloud services that allow larger organisations around the world to connect easily and securely to the applications and the data they need, independently of where they are hosted.

Badged as the 'Cloud of Clouds' strategy, this is exactly the kind of approach that we believe will allow businesses to take advantage of the move on-demand. The strategy will allow customers to bring together IT resources hosted in their own private clouds, as well as on our own cloud platforms and on the platforms of other leading cloud providers.

We work closely with our Global Services division, but have developed our own new platform to help our customers make the most of cloud-based applications. Flexibility really is the watchword for this platform, giving us the elasticity to bring new services online. Proof comes in the fact that we have launched ten new cloud-based products through the platform during the past year.

For us, the development for the cloud goes further still. We have created an 'App Direct'

platform that allows us to provide a richer range of services to our customers. Key differentiators include the ability to back up a company's entire system to the cloud. In the event of a worst-case scenario, we can use this back-up to get the customer up and running within 24 hours.

We believe a final, key element for successful brokers of cloud services is an awareness of the subtle nuances involved in service orchestration. It's something we practice a daily basis. We have a single view of technology plans and investment across our organisation. Such orchestration means we can set priorities and source developments and innovations that will help boost the quality of our own technology, and the services we provide to our customers.

Take our 'hunt teams' programme, which use experts to monitor technology developments in key centres of excellence around the globe, such as Silicon Valley, Israel and Brussels. When our experts discover a potential innovation that will be useful to customers, we work with the vendors in these centres of excellence to ensure any product is of the highest possible quality and resilience. Once our exacting standards are satisfied, we bring the product online rapidly.

In the end, going on-demand should not be feared. Successful use of technology in the era of the cloud still involves the key tenet of technology management – IT managers must understand the requirements of business stakeholders and should then work with a trusted partner to ensure high quality services are delivered. Any partner must be reliable but they should hold the expertise to overcome complexity and to provide a full range of cloud-based services under a single contract, with a single SLA.

The days of going to a supplier and only being able to purchase a specialist application or service are drawing to a close. In the future, the success of vendors – and the businesses they serve – will be closely related to their ability to draw on and manage a wide range of cloud services from many different sources. For this reason, the 'broker' of cloud services will hold the key to the successful adoption of on-demand technologies. ●

Why operators need to act now to take advantage of the huge opportunities the cloud and mobile synergy is creating

by Stefano Pileri, CEO, Italtel

So far, the telco environment has remained fairly traditional but as more and more data, both professional and personal, is moved into the cloud, the risk of cyber-attacks is continuing to grow. In order for the cloud and mobility synergy to reach its ultimate level, operators need to accelerate their approach and competences and react to the situation.

The need for action from operators becomes even more pressing when we consider that in the not-too-distant future it will not just be smartphones and tablets accessing the cloud but also things like connected cars and smart meters. In this scenario, where all applications have devices that access the cloud, a cloud that just stores data is no longer good enough. Instead, we need to have a more powerful and more distributed cloud which can manage a much larger amount of data and greater number of applications.



Stefano Pileri is the CEO of Italtel

Since September 2010 he is Italtel Chief Executive Officer with the task of leading the company in financial restructuring following a new industrial strategy based on the development of the Network and System Integration In Europe and Latin America with a strong component of Engineering, Research and Development in the Telecommunications Market, Enterprise and Public Administration Market.

Before becoming CEO of Italtel, he has spent his entire career in Telecom Italia where, until the end of 2009, he was the Chief Technology Officer and Director of Technology & Operations. Reported to him the divisions Open Access Network, Information Technology and Real Estate, with the aim of increasing the transparency and quality of the network, develop innovation in services offered to the enterprises, public administration and families and then continue along the path of efficiency and cost reduction.

He has received several international awards. Among these, the Tele Management Forum Award, the International Engineering Consortium Award in the USA and EUCIP Champion.

Stefano Pileri graduated in Electronic Engineering in 1980 and holds a Masters in Applied Electromagnetics. His thesis, in Microwave Technology, was published in the IEEE Proceedings on Communication.

As technology continues to transform our lives and the way we communicate, there are two stand-out trends which promise to keep on growing – cloud and mobility.

The increase of mobile devices in the enterprise, combined with their integration with business processes, has increased IT support demands. Gartner projects that 40 per cent of service desk calls will be driven by mobility by 2018. The same is true for cloud adoption which is also growing at a phenomenal rate. IT spending on public cloud Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service

(SaaS) and Business Process as a service (BPaaS) is growing at a five-year compound annual growth rate of 18% through 2018 – more than six times the growth rate of IT spending generally (2.7%) over the same time period. According to Gartner, 75% of organizations use public cloud services today and 78% plan to increase their investment in cloud services in the next three years.

Traditionally associated with enterprises and the workplace, cloud has irrevocably altered companies' IT Systems, taking core activities, information and applications out of physical, often incumbent, hardware

and into a virtualized space, kick-starting the 'as a service' era. Meanwhile, mobility has also seen huge growth, particularly in the consumer sphere, where the rapid rise of smartphones and tablets means people have become accustomed to accessing the day-to-day content that makes up their lives anywhere, anytime – whether it be friends, photos, calendars or correspondence.

But, of course, these two trends are not happening in silo. In enterprises, certain roles have always required mobility and are increasingly taking advantage of the cloud which enables this. Sales teams, for example,

spend more time at customers' premises than in the office, while field technicians, by definition, work in the field where they often require access to their company's core information and applications. Smartphones, and to some extent tablets, provide the interfaces required to access these through the cloud. This same crossover can also be seen in the consumer market, where personal data is increasingly being stored in the cloud and accessed on the move from various devices.

With the crossover set to grow in the future, are mobile devices and the cloud ready to handle the new and different applications that will utilize them – or are there improvements which need to be made before we can take full advantage of the potential the cloud and mobility synergy promises?

The future outlook

In order to answer this question, we must first look at how the convergence of cloud and mobility is likely to develop in the future. With the ties between mobile devices and cloud growing stronger by the minute, the synergy between the two will accelerate further as the Internet of Things (IoT) concept begins to be realized.

In the healthcare market, for example, we are beginning to see wearable sensors which measure people's parameters, such as blood pressure and heart rate, in order to communicate this information to doctors and nurses so appropriate action can be taken if required. Here, the mobility is provided by the wearable sensors, while the cloud plays its part by hosting and storing patient data and statistics.

In other words, IoT – whether in healthcare, agriculture, home automation, energy efficiency or manufacturing – will be a big driver which will further promote cloud and mobility synergy, as well as take full advantage of the smartphone trend. Gartner expects global sales of mobile phones to end-users to grow from 1.9 billion units in 2015 to 2.1 billion units by 2019. By 2020, Internet-connected things will outnumber humans with a ratio of four-to-one, creating new dynamics for marketing, sales and customer service. Consequently, our industries will have a completely new way of operating.

Let's get virtual

In terms of how this trend affects our work, we have already seen a huge shift. As a company which has traditionally helped

operators and enterprises optimize their communications platforms – namely voice and video – we have been a key enabler of the growing synergy between cloud and mobility. We were one of the first players in market to evolve products for operators, like our Session Border Controllers, for the cloud through Network Functions Virtualization (NFV), replacing embedded hardware and software with real-time software that runs on cloud platforms.

Vodafone Germany is just one operator which was taken advantage of this approach. Vodafone's NFV and SDN strategy, called Telco over Cloud, and its implementation in Vodafone Germany, which we supported via a partnership with worldwide IT leader Cisco, was a large and ambitious network evolution program. The initiative saw the migration of the German operator's fixed legacy networks and the deployment of innovative services onto a common virtualized infrastructure empowered by VCE technology. This included the migration of six classless proprietary-based soft-switches serving more than two million SIP subscribers onto three Vodafone Data Centers spread in the country.

We have done the same thing in the enterprise world, where traditional telephony equipment has been sidelined in favor of Unified Communications and Collaboration (UC&C) platforms. Many large enterprises now utilize this technology in both private clouds – provided 'as a service' by telcos – and public clouds from OTT players, like Amazon and Apple.

To give an example, we have delivered UC&C solutions for very large Enterprises in Energy and Banking, as well as for smaller dynamic companies. For instance, Pasta Rummo – which was founded in Benevento in 1846 and now supplies its products to more than 45 countries – chose our Collaboration At Work 2.0 solution. At the core of the solution, based on Italtel NetMatch SBC, is Italtel Embrace, a platform for WebRTC (Web Real Time Communications) with enhanced functionality which delivers unified communications services, audio and video conferencing, instant messaging and desktop sharing, with the only requirement being the most common web browser. The solution also incorporates Voice over IP, allowing reliable and integrated communication between fixed and mobile devices, such as PCs, smartphones and tablets.

The main benefit of this approach is economical, with the total cost of ownership

reduced by between 35 and 40 per cent. Customer proximity and productivity is also increased, while time to market for new services is reduced.

The next steps

To prepare for the era which will come as a direct result of the growth of IoT, we have also spent time researching and developing a full cloud-oriented IoT platform which collects data from sensors. From this point of view, the initial steps to realize the future outlook has already begun, so what is left to do to join the dots between where we are now and reaching it?

While there is nothing particularly missing from the picture, improvements are needed. The first and perhaps biggest issue still to be addressed is the matter of security and network capabilities. It is here, in the core network and cloud architecture, that operators can play a very important role in completing the coming together of cloud and mobility. So far, the telco environment has remained fairly traditional but as more and more data, both professional and personal, is moved into the cloud, the risk of cyber-attacks is continuing to grow. In order for the cloud and mobility synergy to reach its ultimate level, operators need to accelerate their approach and competences and react to the situation.

The need for action from operators becomes even more pressing when we consider that in the not-too-distant future it will not just be smartphones and tablets accessing the cloud but also things like connected cars and smart meters. In this scenario, where all applications have devices that access the cloud, a cloud that just stores data is no longer good enough. Instead, we need to have a more powerful and more distributed cloud which can manage a much larger amount of data and greater number of applications.

Conclusion

The benefits of cloud and mobility synergy are numerous and when applied to industries like agriculture, energy and health could be even more far reaching. While we are not far off this vision, there needs to be an evolution of the network architecture which moves the cloud from being a centralized system into an edge cloud which encompasses every aspect of both the business and consumer spheres. Only then can we take full advantage of the virtually unlimited access to storage and on demand processing the cloud and mobility synergy promises. ●

Focus on the data to have any chance of controlling it

by James LaPalme, VP of Business Development and Cloud Solutions, WinMagic

Organisations are under enormous pressure to control sensitive corporate data. Most have to comply with overlapping laws concerning data breach notification, meaning in general terms that they must disclose the loss or theft of data that can identify people. Other organisations are governed by laws, data sovereignty stipulations, or industry-dictated rules regarding controls placed on data about individuals. The language, tone and jurisdiction of these schemes varies widely, but the overall message is the same: keep track of data on your corporate networks.



James LaPalme is the Vice President of Business Development at WinMagic with expertise in channels (VAR, VAD, OEM, Embedded, IPR, SI), alliances, eco-system and business development, mergers and acquisitions. His focus includes developing mutually, commercially successful global software alliances and channel partnerships. He is currently applying these skills to his role as the Vice President of Business Development at WinMagic. He held similar roles previously at Irdeto, CloudLink (acquired By EMC) and Counterpath (acquired by FirstHand).

DropBox takes the prize. IT departments block it more than any other mobile app, according to a customer survey by mobile device management vendor MobileIron. DropBox's faux "honour" demonstrates how mobility is driving cloud computing and how cloud computing is crucial to the future of mobile work. The cloud where DropBox lives and stores data allows for easy mobile access to that data; and without Internet-facing mobile devices, workers would not have overly convenient reasons for wanting DropBox.

The rise of DropBox's enterprise file sync and share service (EFSS), cloud computing and mobility scares many IT pros and security managers, hence the reason so many blacklist the app. Those security managers recognise

that cloud computing and mobility are here to stay. First off, the productivity gains are too great to ignore. Thanks to mobile connectivity to cloud computing, employees can access corporate data anywhere and therefore can be productive anywhere. As a second related point, those productivity gains will drive employees to work around IT blockades. If DropBox is blacklisted on their corporate phones, they will install it on their personal phones. An example of "shadow IT," the consequences of such DIY tendencies are as insidious as "shadow" would imply.

Cloud computing means far more than just DropBox, and the enormous popularity of EFSS (today there are more than 140 DropBox competitors) is mirrored via other cloud-enabled corporate applications, all of

which can be accessed via mobile devices. Just about every significant enterprise IT solution can be delivered as a service (via models called software as a service, or SaaS and IaaS, or infrastructure as a service). This means that mobile devices can access those applications and resources, and the sensitive data they contain, from the cloud.

This predominance of SaaS and IaaS, like EFSS, further shows the synergistic relationship between mobile computing and cloud computing. And their unchallenged effects on business mean IT pros and security managers need to face the facts. With cloud computing here to stay, they need to address the risks posed by cloud computing. Fortunately the security industry is poised to help.

Evaluating risk of the Mobile Cloud

With mobile devices, for the first time in the history of enterprise IT, workers are using machines that IT doesn't necessarily control or own—or even know about. More employees use their work devices, be them phone or tablets, to manage personal data. Or they use their personal devices for work, logging into mobile applications to view sensitive data. This clash of the personal and enterprise workspace creates a new and unique series of security risks.

Organisations are under enormous pressure to control sensitive corporate data. Most have to comply with overlapping laws concerning data breach notification, meaning in general terms that they must disclose the loss or theft of data that can identify people. Other organisations are governed by laws, data sovereignty stipulations, or industry-dictated rules regarding controls placed on data about individuals. The language, tone and jurisdiction of these schemes varies widely, but the overall message is the same: keep track of data on your corporate networks.

A data breach is expensive, costing by one estimate an average of US \$3.8M, according to IBM-commissioned research released in mid-2015 by Ponemon Institute. Breaches severely damage a company's reputation, and they mean significant investments to identify and remove a source of compromise, and then to make sure it doesn't happen again.

Unfortunately, the intense desire to control data stored in the cloud, and accessed via mobile devices, runs contradictory to the needs of end users to access that data. As noted previously, IT is unable to stop many methods for their employees to access data in the cloud.

Users oblivious to cloud risks, or they just don't care

Perhaps because of the convenience of cloud-based data accessed on mobile devices, most end users do not notice the security concerns inherent to data mobility. According to an early-2015 Harris Interactive survey commissioned by WinMagic in the U.S., 76 percent of adult EFSS users believe the data stored in the service is protected. That means they won't hesitate to use the service on their own devices to store company data.

A WinMagic commissioned survey by CensusWide in September 2015 of 1000 office workers at companies with at least 50

employees amplifies risks related to cloud usage. A StorageReview.com story notes that "the survey found widespread employee use of cloud storage services that were at times either not sanctioned by employers or the employee had no knowledge of their companies [sic] policy of the use of cloud storage services."

Given that a cloud storage services are top of the list of blacklisted mobile applications, IT pros are aware of the profound truth: Their employees use cloud services and think that data stored there is safe, in all likelihood with no regard for any sort of company policy regarding Cloud usage.

What are companies to do?

Mobile device management solutions are widespread, and they manage personal and corporate phones, tablets and other gadgets that access corporate data. These solutions set access control policies; e.g. they manage which devices can access corporate data and apply rules based on the user's role or access privileges. IT pros use them to block usage of certain applications—such as EFSS—that might pose a security risk. From its origin as a method for preventing physical data "leakage" via USB storage devices, mobile device management must remain a mainstay of any corporate IT security strategy.

The conventional wisdom within corporate security circles recommends (appropriately) deploying a "solution tapestry" to protect sensitive data and critical infrastructure. Network-based offerings sniff for suspicious traffic. Firewalls, message gateways, and other perimeter solutions block the obvious and ward off denial-of-service attacks. Authentication and network access offerings check nefarious user behavior that might indicate insider attacks or bot-based attacks via privilege escalation.

And while the variety of company-deployed software solutions do their work, eye-in-the-sky type services apply what's happening in the big-bad world to the corporate footprint. Threat intelligence vendors watch the bad guys and apply the learnings to corporate defenses, given the rise in company-specific attacks.

A well-executed security strategy relies on all these approaches, in concert, to provide protection, while security teams sit watching them work, hopefully in harmony, less the tapestry turn into a tangled mess of overlapping software deployments

overwhelming response processes with false alarms.

But what of the data itself? Many security software solutions—while absolutely necessary to overall security—operate in their own silos with respect to the data that's being protected. MDM solutions only affect data when it temporarily resides on a mobile device; companies must trust the security of the data as it traverses from PC, to mobile device, to Cloud service, to other areas where data needs protection (Internet of Things devices, etc.). While no one is blind to the fact data can reside everywhere today, the focus is heavily on securing the endpoint where data might reside rather than on securing the data itself.

Given the importance of the cloud and mobility to each other, companies must concentrate on a security strategy that considers both concepts, while focusing on the data. On the horizon are IT security solutions that encrypt the data and apply granular policy rules to manage how that data is decrypted. The policy rules can consider a variety of parameters potentially governed by other security or IT solutions, such as role, user, location, device, etc.

Certainly companies must evaluate risk ahead of considering data-centric security approaches. At WinMagic, we've authored an ebook that simplifies the risk calculation for EFSS. Inevitably, however, as more and more companies investigate cloud, mobility, and other paradigms transforming IT, they will discover that these paradigms create complexity that weakens security. From within that evaluation, the fundamental element of IT is data, and focusing on data security cuts through the complexity.

While it's a cliché to say that the cloud and mobile devices are changing the world, it is true to say that imagination is the only limitation on the possible applications of the two concepts. This reality necessitates a renewed focus on security solutions, below the security software tapestry, that protect data wherever it resides. ●

Virtualisation is only the first step for a successful NFV network

by Robin Kent, Director of European Operations, Adax

Operators must now assess how they approach virtualisation. It's an attractive prospect for smaller operators, but hardware must be included to support virtualised software. There isn't a one size fits all solution with NFV – it's about getting it right for the specific application or individual network function. Operators must know the best way to deploy a particular function to give the end-user the best experience. The prospect of virtualising everything may be a draw if operators are suffering from concurrent network issues, but it is essential for operators to consider the security and packet inspection implications of not using hardware to assist the virtualisation process.



Robin Kent is Director of European Operations at Adax Europe. For many years, Robin held senior positions within established equipment manufacturers, software houses and integrators in the telecom, wide area network, and office automation markets. He joined Adax in 1994 to establish the Adax business unit in Europe. He has overseen the company's successful transition from an OEM technology supplier to a customer focused provider of high quality, high performance telecommunications products to network equipment providers and VAS companies throughout EMEA and India.

Network Function Virtualisation (NFV) has continued to grow and prove popular across many industries in today's connected world. Telecommunications is one such industry that is reaping the benefits and promises it offers. Lee Doyle, principal analyst at Doyle Research, states, "NFV technologies are synergistic, and offer improved programmability, faster service enablement and lower CAPEX/OPEX for CSPs"¹. With industry views such as Doyle's, the attraction for operators is clear to see. According to a whitepaper from

Linux Foundation, the main goal of NFV is to increase service agility while enabling better asset utilization"². However, this goal often gets lost in the search for 'software only', NFV/SDN solution without really understanding the needs of individual networks and applications. The question operators need to ask themselves when it comes to virtualisation is 'does the solution fit the problem'?

A common misconception is that all is virtualised in a 'virtualised network' and

that hardware is not needed to support the applications that are running. However, contrary to this view, in order to prove successful, NFV can only occur when there is architecture in place for both hardware and software. Considering software in isolation doesn't work. Individual networks will vary according to local demands and operator preferences, and an appreciation of the roles of both hardware and software is essential for the NFV architecture. This is especially true when considering applications that require a simplified hardware assist solution.

¹ <http://searchtelecom.techtarget.com/opinion/NFV-and-SDN-technology-benefits-drive-telecom-changes>

² <https://www.opnfv.org/news-faq/blog/2014/09/enabling-transition-introducing-opnfv-integral-step-towards-nfv-adoption>

“The performance demands of certain applications and network functions such as security gateway, Deep Packet Inspection (DPI) and the 4G/LTE core network require hardware acceleration on the data plane because of the high data throughput of these applications which need to be analysed thoroughly.”

Hardware is also vitally important when it comes to virtualised mobile networks as there are potentially severe security pitfalls that operators can fall into if they don't have the necessary hardware in place. Telecom publication *Virtualization World* makes an acute observation of virtualisation, identifying it as: "...the process of combining hardware and software network resources and network functionality into a single, software-based administrative entity, a virtual network." This certainly rings true in the telecoms industry, and operators should certainly consider when searching for the much-hailed 'software' only solution.

The performance demands of certain applications and network functions such as security gateway, Deep Packet Inspection (DPI) and the 4G/LTE core network require hardware acceleration on the data plane because of the high data throughput of these applications which need to be analysed thoroughly. Separating the control and data planes improves the control of the network and paves the way for a more effective and reliable NFV implementation. But it's not enough to stop there.

This separation will centralise the control plane so that third party applications can run autonomously which turns the control plane into a Virtual Network Function (VNF), leading to a more flexible and dynamic network. Yes, agility and flexibility are improved but also the OPEX cost to the operator is reduced by simplifying the control and programming of the network.

The best practice for operators should be to move the control plane to a virtual machine, offering a simplified solution for network management whilst adding to the quality and value of the overall solution with hardware acceleration for the data plane. Operators need to ensure they have virtualisation and distribution management system resources in place. The role of a Virtual Network Function Manager (VNFM) is a necessity to establish close communications between the NFV manager, and therefore the software and hardware in the field.

Operators should not focus their resources on searching for a virtualised network solution that is on generic COTS

(commercial off-the-shelf) hardware, without understanding the actual network or user requirements. In fact, hardware and software can and should work in tandem but it's essential to recognise how and where that hardware runs in the network. For now, applications that require hardware assisted virtualisation require dedicated and specialised COTS hardware. It's also important to make sure the control and data planes are decoupled for NFV. Separating the control and data planes simplifies network control and operators need to have the hardware solution in place to accelerate and deliver cost-effective, reliable application performance.

With a control plane that's both centralised and virtualised, the next question is how to ensure the applications can meet the demands of performance, reliability, flexibility and scalability when faced with high throughput. As a result, the performance demands of certain applications, network functions and nodes such as a Security Gateway, DPI and the 4G LTE core network points towards the need for hardware acceleration at the data plane.

Operators must now assess how they approach virtualisation. It's an attractive prospect for smaller operators, but hardware must be included to support virtualised software. There isn't a one size fits all solution with NFV – it's about getting it right for the specific application or individual network function. Operators must know the best way to deploy a particular function to give the end-user the best experience. The prospect of virtualising everything may be a draw if operators are suffering from concurrent network issues, but it is essential for operators to consider the security and packet inspection implications of not using hardware to assist the virtualisation process.



Connect-World now on Facebook & Twitter

Connect-World, the world's foremost discussion forum for leaders in the ICT industry, is now available on Facebook and Twitter.

The world's top ICT decision makers express their opinions in *Connect-World*. They use clear, non-technical, English to discuss how ICT helps shape regional and global development. The articles essentially examine the influence that ICT products and services have on the way people live and do business. With separate editions for each of the world's regions, the reports highlight the most important ICT trends and issues influencing socio-economic growth.

Connect-World is now available to follow on Twitter (<http://twitter.com/#!/ConnectWorldICT>) and Facebook (<http://www.facebook.com/connectworld.ict>)

Also, it is still possible, for FREE, to directly access all past and present *Connect-World* articles, ICT Industry press releases, eLetters, ICT News and more at www.connect-world.com.

Cloud: Liberating today's mobile enterprise

by Vik Verma, CEO, 8x8, Inc

This past decade has seen the rise of unified communications (UC) that promised to bring all the piece-part, siloed elements of communications together into a more manageable experience for the mobile worker. In many ways, unified communications has improved the speed and flow of information across an organization, one user at a time. However, the major vendors serving the market handcuffed both themselves and their clients by building architectures dependent on a complicated mix of on-premises systems, with equally daunting licensing schemes, offered by vendors that are often coming from diametrically opposed positions on what the end result should look and feel like.



Vik Verma, CEO at 8x8, Inc.

Vik Verma loves to take complex technologies and transform them into unique customer value. As part of his early work at Savi Technology on RFID and the Internet of Things, the World Economic Forum in Davos named Verma one of 2003's Top 40 "Technology Pioneers" in the world. At 8x8, Verma focuses on revolutionizing enterprise cloud communications with ground-breaking unified communications and contact center technology.

Previously, he served as Savi's Engineering VP before becoming COO, and later President and CEO. Prior to 8x8, he became President of Strategic Venture Development at Lockheed Martin, focusing on its military technologies and programs for global commercial ventures. Vik Verma earned engineering degrees from Florida Institute of Technology, University of Michigan, and Stanford University.

Communications is the life blood of business. That is precisely why, in this world of high transport, full of broadly mobile, distributed workforces, so many businesses are accelerating their move to the cloud, for a broad spectrum of enterprise class cloud services— but specifically communications services.

With an endless array of choices in front of the modern business leader, the necessity of moving in a precise direction and adhering to core objectives remain the fundamental measures by which a business can tell if they

are still on course, or wavering in pursuit of their mission. With an increasingly mobile workforce, it's easier than ever for businesses to fall out of synch, especially when everyone from the CEO down to the first-time new hire moves in different directions.

The failure of unified communications 1.0

My own communications experience, before the cloud, required what seemed like an endless and delicate balancing act of managing communications across a mix of applications and devices that is best described

as communications interrupted. An email invites a response, so you send another email, which very soon leads to the need for a phone call or meeting. The old world required the individual to act as the traffic cop, starting and stopping a discussion in one medium, to move to another.

This model of inefficiency adds a significant real, but largely undocumented cost of doing business. It involves a cumbersome process that uses many separate, isolated tools of business communication running on a private corporate network. And the



IN SUPPORT OF THE GOVERNMENT'S USD \$20 BILLION ICT SPEND OVER THE NEXT 5 YEARS

EXPO COMM™ INDONESIA 2016

THE 4TH ANNUAL TELECOMMUNICATIONS, MEDIA & INFORMATION TECHNOLOGY EXHIBITION
9-11 NOVEMBER 2016 | JAKARTA CONVENTION CENTER

SECURE CONNECTIVITY FOR INDONESIA'S CRITICAL INFRASTRUCTURE

BROADBAND - CYBER SECURITY - IT -  SMART CITIES

**Contact us today to find out
how your brand can access this lucrative market!**

ASIA
PT Infrastructure Asia
Alex Hawkes
alex@infrastructureasia.com

EUROPE
E.J. Krause & Associates, Inc.
Gudrun Tegge
tegge@ejkgermany.de

Co-Organized by



**E.J. KRAUSE &
ASSOCIATES, INC.**

Part of

 **Indonesia Infrastructure Week**

WWW.CONNECTINDONESIA.NET

problem is compounded for the mobile business person, who lacks the same access to communications services that are readily available in their office setting.

This past decade has seen the rise of unified communications (UC) that promised to bring all the piece-part, siloed elements of communications together into a more manageable experience for the mobile worker. In many ways, unified communications has improved the speed and flow of information across an organization, one user at a time. However, the major vendors serving the market handcuffed both themselves and their clients by building architectures dependent on a complicated mix of on-premises systems, with equally daunting licensing schemes, offered by vendors that are often coming from diametrically opposed positions on what the end result should look and feel like.

This UC 1.0 model involves paying, and repaying a hefty premium every year, yet we're all still waiting for delivery on the promise of a much simpler communications archetype. As a consequence, many business leaders who invested in these leading UC vendors are left wondering whether the vision they bought into will ever see the light of day. Presently, we have started to see a marked shift away from these vendors, as they continue to move their strategies away from their once "safe" on-premises roots.

The problem with the old model is more than just a disagreement between competitors. The source of the problem goes back to the structure of the solution delivery itself. You don't need to be an industry expert to recognize that any technology solution whose success is dependent on two or more gorilla competitors from very different markets cooperating in depth is going to struggle over time, and often, that solution is going to fail. And when the market that solution was built to serve is the massive, high-growth mobile user market, then the smart money is to approach the problem from a completely different angle.

The Cloud transformation of UC

Enter the cloud, as a communications service delivery vehicle that is equally suited to serving both the mobile and office-based worker. Reality now looks quite different, when you talk about unified communications. So different in fact, it requires a completely new term to define its enhanced delivery model: continuous communications.

The reason the cloud changes everything comes down to a few key factors. First, the cloud is able to leverage new technology from multiple sources, regardless of vendor, to deliver the kind of $1+1=3$ value equation that was always expected from UC. That's because the cloud, by design, is open and accessible to the markets it serves.

As a result, cloud CRM services, for example, can easily be integrated into cloud UC services, so that the CRM user can conduct and track call activity without leaving their CRM application. The business gains the value of faster, more informed processing of calls and their customers get superior, more complete service.

What's even better is that the IT staff didn't have to find the time, budget and expertise required to design, plan and deliver the solution. It's already done by the cloud vendors themselves, through their use of application platforms that were designed to naturally co-exist.

This model extends to a whole host of other cloud services and web application integrations, each one of which would have involved a colossal effort on the part of vendors and IT teams in the old world, but are now very simple, or even out-of-the-box, pre-packaged user-installable accelerators to time-sensitive business processes, such as sales and customer support.

The second key factor of the new cloud reality is the ubiquitous availability model of the cloud. The cloud model enables users to go online from anywhere, without any specialized equipment, applications or devices, and just log in to a browser and gain full access to your services.

That was never going to be possible with the old world UC vendors because they were always more interested in selling you their next new client or device, than they were on solving your business problem with a highly personalized user experience.

With the cloud, you can have one-number access that you take with you anywhere you go and assign that number to whatever device you prefer, today, tomorrow, and every day of your business lives.

Mobile liberation through continuous communications

This is where we get to the choice of new terminology "continuous communications." In this cloud-enabled world of

communications, the user can be anywhere, engaged in a business activity that requires input from another party. If they're in email, they click to call directly from the phone number in that email. If they're in CRM, click-to-call is right there. If they're on the go, they might start with an IM to a colleague on their smart phone, and then escalate that to a call, or conference, or even an HD videoconference, all from the smart phone in their hand.

The beauty of continuous communications gives users the ability to seamlessly switch from chat, messaging and voice while roaming across multiple networks, such as 3G/4G LTE and Wi-Fi. This continuous communications experience offers users added flexibility to suit their personalized business needs, taking their communications service with them wherever they are in the world. You can use the tools of your choice, and can lead the transaction, from start to finish, across all the devices and applications you require—seamlessly, without ever having to stop and start, until your task is done. Users can share documents from Dropbox, or Google docs. Annotate, collaborate and move the business forward. Resolve customer issues as they emerge by bringing in the experts you need to answer the question, and move on, without wasting time on call backs and re-scheduling contact. Pure business agility at your fingertips. This has become the new normal and new "Day in the life" for most business users.

The pace of business only continues to increase daily, and mobility is right at the core of this increased pace that drives our connections, interactions and productivity. Fortunately, with the cloud innovation engine revved up and ready, the continued liberation of the mobile enterprise is on a sure course. ●

How to create growth from the connected home

by Jon Carter, UK Head of Business Development - Connected Home, Deutsche Telekom

Many firms still need to grasp the impact that the connected home will have on them. Over the next five years, the connected home will affect multiple industries that provide products or services to consumers in their home. For many firms, the implications will be dramatic. There will be further commoditisation for many players, disintermediation of others, and dramatic changes in the relationship between brands, and routes to market.



Jon Carter is the UK Head of Business Development – Connected Home, Deutsche Telekom AG

Jon leads UK Business Development for Deutsche Telekom's white label and open connected home platform.

Successfully launched in Germany in late 2013, Deutsche Telekom's open platform is now available internationally, with an initial focus on Europe, and particularly the UK. Deutsche Telekom's platform has been designed to move the industry beyond simple control of connected devices, to create a foundation for new revenue generating services.

Jon's focus is on establishing partnerships with telcos, utilities, insurers and retailers, as well as third party platform providers and OEMs to enable the realization of innovative new models and revenue generating services.

Jon has worked in and around the connected home space since the early 2000s, and has a deep knowledge of the European market, and in particular what will finally drive growth in this market.

In a new market analysis report, 'How to create growth from the connected home', Deutsche Telekom sets out the impact that connected home technologies will have across multiple different industries.

The report details a number of different areas from energy management, to security and home automation, which could be exploited by a range of players – telcos, utilities, retailers, insurers, warranty providers, home assistance providers, and appliance and consumer hardware manufacturers. In total, the report highlights research by Strategy Analytics that the Western European connected home market will be worth up to €12 billion annually by 2019, with almost 50 million homes benefiting from such services.

A great deal of this revenue will be due to new growth, but much of the change in the coming Internet of Things (IoT) revolution

will be about value shifting from one sector to another. One of the many insights in the report is that companies will need to move from selling mainly consumer hardware to a services-based approach, which will impact existing business and operating models, margins and routes to market.

The report also makes much of the very real threat that much of the value that will be created in this new market might be taken by players from outside Europe, if the industry here does not 'step up to the plate' and take a proactive stance. It claims that global giants have their sights firmly set on European markets, from connectivity and energy, to insurance and warranty. They will not wait for European players to finalise their strategies and product development plans.

It asserts that many firms still need to grasp the impact that the connected home will

have on them. Over the next five years, the connected home will affect multiple industries that provide products or services to consumers in their home. For many firms, the implications will be dramatic. There will be further commoditisation for many players, disintermediation of others, and dramatic changes in the relationship between brands, and routes to market.

The report sets out how IoT reaches into the connected home and how it will transform the way we live both in and out of our homes: from micro-ordering of consumables, to providing greater peace of mind through safety, security and insurance solutions, to saving energy and managing home appliances.

Industry-wide platforms and standards are currently lacking, and Deutsche Telekom believes that many companies will not survive without partnering. Proprietary and

closed approaches, or ‘gated communities’, won’t do: we need to open up a high level of collaboration. In the long run, no company can establish the connected home alone – those who think that they can will not succeed.

Let’s look at three of the key industries with a compelling interest in the connected home.

Strategies for utilities

Home energy management services (HEMS) enable utilities to create a positive interaction with their customers through the energy visualisation, monitoring and control of energy use. Smart thermostats and data from other connected home appliances, such as smart meters and smart home systems, represent a compelling opportunity for utilities to help consumers better manage their energy costs and improve tenure, whilst exploiting new and innovative models.

The report examines how utilities can increase adoption of smart thermostats and related smart devices through innovative pricing and retention strategies with existing customers, and also develop new channels to market, such as by setting up affinity partnerships with insurers and retailers to drive growth.

With closer integration between energy demand in the home and energy generation, it is clear that consumers can save money, be more energy efficient and so combat climate change. Home owners can benefit from new, flexible tariff structures that enable them to pay less for energy when there is excess supply and only run energy hungry appliances, such as washing machines or tumble dryers, when the cost is low.

The report also recommends that utilities consider emulating telcos by offering such appliances on a subsidised basis, employing demand disaggregation smart meters and demand side management to provide new energy tariffs. This will provide greater differentiation for utilities, as well as new revenues and much improved customer loyalty. The risk for utilities if they do not adopt such an approach is further commoditisation, especially with the introduction of legislation in some countries that will mandate same-day switching to other providers.

Telco options

The report advises telcos to consider establishing ecosystems of third party

manufacturers and service providers to create greater differentiation and so boost customer loyalty – leveraging their ownership of the broadband router. It also outlines opportunities for telcos to enter new markets, such as home security.

The connected home is a natural extension of the telcos’ quad play offerings. For integrated operators that provide customers with a broadband router or TV set-top box, it is an obvious next step. In the near future, operators won’t just be providing Wi-Fi connectivity, so customers can connect their PCs, tablets, smart TVs and smart phones, but will also be connecting the majority of their home devices and domestic appliances to the internet.

Insurer incentives

Deutsche Telekom argues that there is a particular urgency for insurers to act, as it claims that there is evidence that a number of players in adjacent markets are looking to disintermediate them, deploying more agile business models and innovative solutions that turn existing actuarial models on their head.

The most frequent claims are the same across much of the world – escape of water, smoke or fire damage, and burglary. When technologies allow a home to be monitored, some of these traumatic events can either be prevented, or alerts can be issued to ensure the relevant individuals are made aware before there is any serious issue. By far the biggest risk for insurers are water leaks and the related damage, and innovations in water flow meters coupled with analytics software ‘in the cloud’ offer a potential to lessen the risk, or ensure no issue ever occurs.

The connected home will also be able to provide insurers with more reliable data for risk management, and more real-time data.

Success factors

Key to any firm’s success in this market is understanding the needs of the customer. What are their day to day issues and pain points, and how can these be met by new forms of connectivity? To date, this market has been too focused on technology for technology’s sake. Flexible business models and payment structures will be critical for the broadest appeal, with the aim of providing consumers with comfort, convenience and peace of mind.

There also needs to be greater willingness to work with partners to grow and shape the

future of this market. The biggest winners will be those that are prepared to innovate, take risks, and become leaders in a new community of open, connected home ecosystems.

Open for business: Deutsche Telekom’s Connected Home Platform

One of the greatest challenges facing firms seeking to enter the connected home market is the lack of common standards and architectures for connectivity itself, as well as a lack of openness in terms of the APIs between platforms. Today, many proprietary and incompatible wireless protocols exist, which is a major obstacle to mass market adoption of connected home services. To get past this, Deutsche Telekom has built an open platform so that end-users and partners can rapidly integrate connected devices and create new services.

Beyond creating a truly open and interoperable connected home platform that can be utilized by a wide range of industry players will bring faster time-to-market, Deutsche Telekom is also leveraging the Eclipse SmartHome/openHAB initiative open source developer community to further maintain this openness. This open source software is a core component of the platform architecture.

With an open ecosystem, partners can play to their core strengths, benefit from multiple synergies, discover new routes to market, deepen consumers’ loyalty to their brand, and create new growth for their business.

Deutsche Telekom now has more than 35 partners integrated into the platform, including Philips, Osram, Miele, eQ-3, Sonos, Samsung, Huawei, Netamo, Bosch Junkers, DÖM, Provedo, Urmet, Kärcher and Assa Abloy. In Germany and Austria, Deutsche Telekom has also partnered with utilities such as EnBW, Vattenfall, Rheinenergie, Entega and eww Gruppe to provide a range of home energy management services designed to meet the needs of consumers and the regulatory environment.

Now is the time to join forces

Now is the time to join forces, combine industry-specific knowhow and drive the connected home forward to realize new growth for everyone. The key to success for the future is to maintain an open, agile and flexible course. Only then will we – as a broad and eclectic range of businesses – be able to drive the connected home market forward and realize that long desired growth.





Send me the following *Connect-World* issues

- | | |
|--|---|
| <input checked="" type="checkbox"/> Africa & the Middle East issue | <input checked="" type="checkbox"/> ICT Global Challenges issue |
| <input checked="" type="checkbox"/> Latin America issue | <input checked="" type="checkbox"/> Asia-Pacific issue I, II & III (3 issues) |
| <input checked="" type="checkbox"/> North America issue | <input checked="" type="checkbox"/> Europe issue I & II (2 issues) |
| <input checked="" type="checkbox"/> EMEA issue | <input checked="" type="checkbox"/> India issue |

A total of 11 issues for the publishing year of 2015, at a special discounted rate of £100. Online subscription also available.

Subscribe to receive your copy now!

Subscription Form

Title (Mr/Mrs/Miss): _____	Name*: _____
Company*: _____	Job Title*: _____
Address*: _____	City*: _____
State/Province: _____	Postcode/Zip*: _____
Country*: _____	Telephone*: _____
Fax: _____	Email*: _____

(Fill all fields marked *)

Check preferred subscription medium

- Online** - Digital Magazine £15 (11 issues, Online download PDF)
- UK** - Printed Magazine for UK subscribers £95 (11 issues hard copy by post)
- Europe** - Printed Magazine for Europe subscribers £100 (11 issues hard copy by post)
- Foreign** - Printed Magazine for Rest of the World subscribers £115 (11 issues hard copy by post)
- Corporate** - Printed Magazine for Corporate subscribers (11 issues hard copy by post)
 - sign my company up for a two-years subscription to *Connect-World* series of magazines with an additional 15% discount. Please charge my credit card once a year until I notify you otherwise. I'll get the same low subscription rate I've chosen above for as long as I am a subscriber. Please note: all corporate subscriptions must be pre-paid. Please provide your credit card information when placing your order.

Note: Please allow up to 4 weeks for mailing of first issue.

Please charge my:

- Visa MasterCard American Express

Card Number: _____ Expiry Date: ____/____(MM/YYYY)

Signature: _____

Bill me later

- Tick here if you want us to bill you later. Available only to domestic UK addresses.

Please sign _____ and send back by:-

Email: info@Connect-World.com or

Post: InfoComms Media Ltd., 1 & 2 Riverside Offices, 17 Towcester Road, London E3 3ND, UK.



Epic Flexibility, Endless Connectivity

Reliable, five-bar connectivity for service providers in emerging markets

With Epic^{NG}, Intelsat's next-generation, high-throughput, backhaul solution, delivering future connectivity in the Americas just got easier. Intelsat Epic^{NG} is engineered for mobile operators that need to serve remote customers, across any terrain, regardless of conditions. Best of all, Epic^{NG} works with your existing infrastructure, making it the most cost-effective and reliable solution for your network.

Only Intelsat, a company with 50 years of technical and operational expertise, a global fleet of 50+ satellites, and the next generation satellite platform can promise you epic flexibility and endless connectivity.



INTELSAT

Envision. Connect. Transform.

www.intelsat.com/LatAm_Connect



Empower more end users

AT&T Wholesale brings you the reliability, security and reach of the AT&T global network. So, you can offer economical solutions almost anywhere you and your customers do business.

You'll gain access to a full range of communications services – including voice and data, cloud, Ethernet, mobility and much more.

Are you ready to go as far as your drive and determination take you? You've got the solutions end users want to help manage their business and expenses.

Get the details at att.com/gowholesale.

AT&T Wholesale

© 2013 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.