



Where is **mobility** taking you?

Time to **redefine mobility**?

The surge in **education**

Unravelling the Grid

Healthy options for **NHS data security**

Do we care enough about **information security**?





Ian Jackson, Managing Director



Welcome to Business Download, the regular IT bulletin from Imerja Limited

If like me you are reading this on your iPad, or other tablet device, then you are one of the growing number of people that have embraced true mobile working. The exploding market in mobile devices has seen a step change in how businesses need to approach the challenges of delivering information and applications securely to multiple devices that can connect in a variety of ways.

In this edition we consider how mobility is changing the business landscape, and how the specific challenges it presents can be addressed. I am delighted to welcome guest writers Zeus Kerravala, Senior VP at Yankee Group, and Andrew Peters, VP at Extreme Networks, who provide insight and opinion on the new era of mobility; Alwyn Nash from Check Point looks at the information security challenges faced by healthcare organisations; and Gary Clawson, former CEO at the North West Learning Grid, considers the future of broadband services in the education sector following changes to funding in IT.

We comment on the biggest challenges facing information security, and question the commitment some people demonstrate towards their responsibilities.

Recent recognition in the Deloitte Fast 500 and being placed runner up in the national Network Computing awards help demonstrate Imerja's strength and success through what continues to be a challenging time for many. With our strong compliance status, now including N3 approval, and new services relevant to today's IT demands, we are looking forward to our continued growth.

I hope you enjoy the read, as always your comments and views are welcome.

Ian Jackson
ian.jackson@imerja.com

imerjing NEWS

Imerja on the fast track

Imerja has once again been included in the Deloitte Technology Fast 500 for EMEA based on revenue growth over the last five years.



High customer retention and an increase in multi-year contracts has helped sustained growth, underpinned by the strong relationships that the team has fostered since Imerja started in 2004.

Looking ahead, Imerja has planned for future growth by introducing new services, such as managed mobile, managed security service for schools, and by expanding its existing 24 hour managed services package, able to offer more flexibility to customers and remain leaders in our industry.

David Halstead, Deloitte United Kingdom, partner in charge of the Deloitte Technology Fast 500 EMEA programme, commented:

"Making the Deloitte Technology Fast 500 EMEA ranking is a testament to a company's commitment to technology. With its 479 per cent growth rate over five years, Imerja has proven that its leadership has the vision and determination to grow in difficult conditions."

Further industry recognition

Following our nomination in the national Network Computing Awards, Imerja was placed as



runner up for Reseller of the Year, narrowly missing out on the top prize. One of Imerja's key vendor partners, Check Point, picked up two awards in the categories of UTM Product of the Year and Hardware Product of the Year, so there was enough to celebrate on the evening.

This national award recognises excellence in the delivery of solutions, service and support, taking into consideration the ability to deliver real benefits and meet customer objectives in terms of improved efficiency, ROI and investment protection, and cost reduction.

Being associated with the award as a finalist is a great accolade for Imerja, and we would like to thank everyone who voted for us and took the time to support our nomination.



Is it a thumbs up for mobility?



Mark Evans
Marketing & Communications
Director, takes a look at the
impact of changes
in our mobile
environment

If you give a laptop to a toddler they will instinctively poke at the screen - they are used to touch-screen technology and are growing up with mobility.

People of a certain age (myself included) will often use a forefinger to type on a touch screen device, whereas those of a younger generation will automatically use their thumbs. Whilst being 'all fingers and thumbs' was once a sign of clumsiness, the boom in mobile phones and handheld technology means the human hand has undergone a physical mutation - research even tells us that the thumbs of teenagers and young adults have overtaken their fingers as the hand's most muscled and dexterous digit.

Whilst this is a light hearted view of how technology is changing the world around us, there is a more serious issue to consider in how we utilise mobile solutions safely and responsibly in our personal and work activities.

Businesses are constantly under pressure to provide more flexibility and realise greater productivity across their operations. Mobility is exploding - with that comes greater risk.

Worldwide sales of tablet computers are forecast to hit over 50 million in 2011 and double that figure in 2012. At some point this year analysts predict we will pass the point of inflection where shipments of smartphones and tablets outstrip those of PCs and laptops, a clear illustration of our changing environment.

In the past companies typically developed their corporate IT infrastructures first and then layered security on top, often deploying between 12 and 15 different products including firewalls, antivirus software, malware and spyware protection, intrusion detection and so on. But those were the days when people had permanent desks at the office and mobile working meant a

laptop at the kitchen table using your home network; now, companies are facing user demands for untethered mobility, with smartphones and tablets operating outside the business infrastructure, and connecting wherever there is a mobile signal or internet coverage.

The threat landscape is also increasingly complex; malicious attacks are ever more sophisticated and businesses must meet rigorous compliance standards. They cannot, perhaps should not, force employees to work from a single desk, but when sensitive information is both stored on and accessed through mobile devices, they need to consider how the security environment is changing and presenting different challenges.

Companies are increasingly realising that security policies shouldn't simply be added to IT systems, but rather implemented from the outset. We are seeing a shift to outsourced managed services that deliver business IT solutions with a solid security foundation, and require compliance built in from the start.

Increasingly, individuals want to work on personal mobile devices, and arguably businesses have an interest to encourage this since it provides greater flexibility and productivity - but they need to understand the security implications.

It is not simply a case that businesses need to implement appropriate security measures, individuals must also take ownership of information, whether it be their own personal

data, customer details or corporate secrets. We want, demand even, the convenience and flexibility that true mobility can provide us, but with that comes responsibility. Ask yourself:

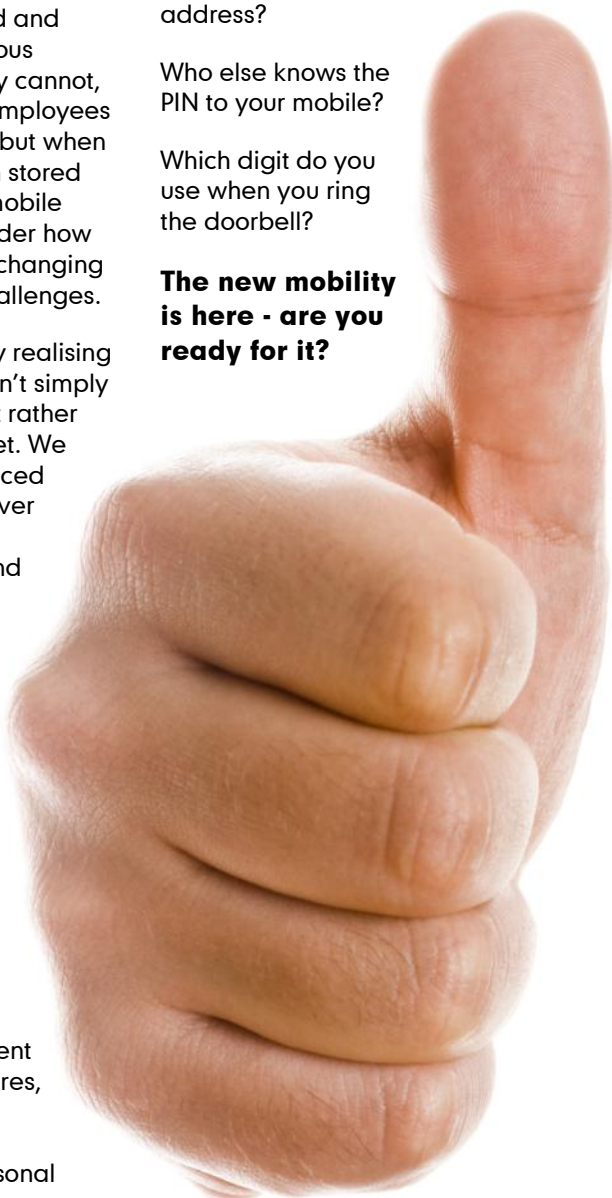
Do you access business email or documents on a mobile device?

Have you ever sent a work document to your personal email address?

Who else knows the PIN to your mobile?

Which digit do you use when you ring the doorbell?

The new mobility is here - are you ready for it?



Time to redefine mobility



Zeus Kerravala
Senior Vice President
Global Enterprise and
Consumer Research
Yankee Group

The coming together of cloud computing, wireless networking and device evolution have created a "perfect storm" in IT which is redefining the very nature of mobility.

Prior to the intersection of these forces, the term mobility was used interchangeably with wireless. I would argue that we've never really had the building blocks of true mobility; instead we had devices that allowed us to be portable.

Legacy mobility involved IT handing a corporate worker a device that had all of the content and applications the user would want preloaded onto it. The user would then carry the device everywhere, attach to the network and be able to work from anywhere. Seems like mobility, but it's really not.

What would happen if the user were to lose the device? All of the data stored on the device would be lost. What if the user wants to carry a second device such as a tablet or notebook? Then the onus would be on the user to continually find a way to synchronise the information between the devices.

This isn't ideal but is manageable when the user has just a couple of devices, but today workers carry anywhere from 3 to as many as 7 devices. Managing the manual movement of data between many devices will be unreliable at best.

The redefinition of mobility involves mobilising not only the device and the user but the content as well. For example, shifting from a premise based e-mail system to a cloud based solution means that a worker could have the same

experience on a mobile phone, tablet, notebook or desktop. Any change made on one device would instantly show up on the other devices. Any content over any network on the device of the users choice. This is made possible by the fusion of device evolution, cloud computing and pervasive wireless. Mobility redefined.

To achieve this level of true mobility, the network needs to evolve, adapt and change in order to provide a high quality, secure experience.

To enable this 'redefined mobility' the network must provide the following:

- Security integrated into the network. Since the IT department has little no direct control of the end point, security must be pushed into the network.
- Personalised experience for the user. Network policies will dictate when users can access information depending on role and location. Additionally, the network should be able to tune itself to optimise multimedia applications such as VoIP and video.
- Consistent policies across the wired, wireless LAN and cellular networks.
- Open and standards based architecture that will allow for the fast integration of compute and application resources.

Mobility is being redefined and users are demanding a high-quality experience along with the ability to access what they want, when they want from wherever they are.

These trends have changed the way users work, and the network now needs to enable the new definition of mobility – mobilising the user, device, content and applications.



The mobility surge in university education



Andrew Peters
Director of Enterprise
Solutions Marketing
Extreme Networks

The high saturation of mobile devices in the hands of students has caused many institutions of higher learning to rethink their network strategy. The smart phone, tablet, and iPad have transformed from social and entertainment 'toys' to true learning tools so students can access real information, collaborate, share, and better participate in learning.

This is the advent of mobile learning, where the walls of the classroom are no longer brick and mortar and interactive learning will occur whenever and wherever it needs to without barriers of space and time.

Mobile learning at the university level is an incubator for the evolving mobile workplace. Since it can help propel each graduate to be prime contributors and leaders in their professional careers, the IT department holds an increasing responsibility for the success of their institution and its students. So universities, with their budget and human resource constraints, need to make clever choices that enable a leading mobile learning environment.

This mobile learning environment is far more extensive than a wireless access network, which was fine in the PC era which comprised static workstations or portable laptops with thick clients and on-board storage that was fairly tolerant of low-speed and inconsistent networks.

Mobile learning requires a resilient mobility ecosystem comprised of users, a plethora of devices, operating systems, clients and apps, a network of wireless and wired access, a switched network, firewalls, directories, storage and SAN networking, servers, or "the cloud", the Internet, firewalls, management, remote access, and much more.

This mobility ecosystem must be identity-aware of each user/device combination and each application that are in constant motion, and ensure consistent, high-performance and secure services. In other words, it's automated, fast, and always-on.

The network is the critical infrastructure that enables these services that makes it easy for students and others to get access without disruption. But the university network needs to be more than theoretical; it needs to deliver this corporate network of the future today so students get personalised service for any device or application so teachers can teach and students can learn, unencumbered; services are automated and customisable so IT can focus on extending applications and services such as a mobile web framework, open learning portals, multiuser virtual environments (MUV), and other collaborative multimedia learning adjuncts.



In our work with universities on their networks we've observed several rules that have led to happy students and IT departments.

- Give the students what they want: a hassle-free network that just works with any device and is personalised to their learning needs. And if they have a problem it gets fixed really fast from an IT operation that listens and responds.
- Use network technologies built for mobility with identity awareness, flexibility, and automation to provide consistent security and quality services to users in motion on the edge, and applications in motion in the data centre cloud, and open systems that are easy to change and customisation.
- Maintain control by automated policy enforcement from an identity-enabled infrastructure.
- Maintain flexibility with open systems that allow best of breed technologies and seamless migration to cloud services.

Mobility is expanding its place in learning, and the intelligent choices IT departments make to build their mobile ecosystem will have a strong impact on the success of the students and the reputation of the university.

Unravelling the Grid



Gary Clawson
Former CEO
North West Learning Grid



In the beginning...someone had the bright but obvious idea that if IT was to be an important development in our schools then we should have strong broadband connectivity not just within schools but between them.

With nearly £1 billion of grant funding spanning 10 years the construction of a National Education Network began in 1997. Built on a JANET(UK) backbone and developed by Regional Broadband Consortia (RBCs) and Local Authorities (LAs) it has been a consistent 'utility' in all of our schools.

Two things changed last year.

- First, the funding was deemed to be no longer affordable. If enablers of school connectivity (RBCs and LAs) had better embedded the annual costs with schools this would not have been a serious issue, but few of them had.
- The second major change is that we got a new government whose ideology is focused on reducing the role of Local Authorities and in enabling schools to act and develop independently as Academies. In effect deregulation.

There is absolutely no doubt that the Secretary of State for Education, Michael Gove, is determined to coerce every school into becoming an Academy, so much so that he is withdrawing LA funding for schools and returning it only to those that become Academies.

This creates a situation where Local Authorities and their regional partnerships will quite simply, not be able to maintain existing service provision and will make them extremely vulnerable to schools switching providers.

Within 12 months the subsidies that the JANET network has will also disappear. With the availability of RBC and LA services uncertain, this will further accelerate a breakup of the National Education Network.

The current situation provides clear evidence of the very limited ability of central government policy makers who seem unable to consider the preservation of existing and effective provision when implementing new policy. We simply have to make the best out of this enforced situation.

Rather than schools randomly moving to different suppliers of ISP services there is a more sensible model for them and service providers to offer.

Suppliers, should be encouraging the creation of federations of schools, with shared connectivity and shared services. These are best formed around Secondary schools who can bring in their feeder Primary schools, reducing the risk them being prey to poor connectivity sold to them by 'shallow' service providers. It also enables suppliers to offer significant, long term service developments centered around connectivity.

Responsible suppliers will offer solutions that will be best for families of schools, smart schools will work together not as individual Academies.

For details on Imerja's **Managed Security Service** for schools, and other complimentary services, contact your account manager or email us at info@imerja.com.

Managed security service for schools

Information and communication technologies (ICT) are strategically important to education and the teaching process – not just for the subjects where it is core, like computer studies, business studies and media studies, but across the whole curriculum.

The ability to deliver specialist teaching resources and multi-media material safely and securely to students at all stages of their formal education is core to the way subjects are taught. Secure and reliable access to the internet is now an essential part of learning.

Cuts in public sector funding, specifically in respect to education budgets such as Harnessing Technology Grants, have brought uncertainty over the longer term affordability of secure and reliable internet services into schools and colleges. Coupled with pressure on spending and the planned changes to the Learning Grid Networks, this has led to concern over the impact on delivery of materials to support learning and development.

In response to this challenge Imerja has developed a cost effective service especially for schools and colleges, so they can benefit from the growth in low cost internet provision while maintaining high levels of security and integrity expected from a Learning Grid service.

Using the latest Unified Threat Management technology the service can be delivered as an enhancement to standard managed internet access, regardless of the internet service provider (ISP).

As the delivery of educational content across the internet grows and the use of bandwidth hungry multi-media applications increases, the service from Imerja is flexible to accommodate changes in how it is managed, and where required increase or decrease bandwidth into the school or college (subject to contract with your ISP).

Imerja's Managed Security Service (MSS) offers schools and colleges all the benefits of secure, managed internet provision through simple, cost effective service packages suitable for any size of school.

Using an onsite UTM appliance, installed by our qualified engineers and located between the school's curriculum network and its internet service, the service provides all the benefits commonly associated with a Learning Grid connection, meeting content filtering standards set by Becta for schools and higher education.



The fully managed service is delivered from Imerja's dedicated ISO27001 certified operations centres, ensuring security and service integrity is maintained at all times. Optional back up connectivity can be provided to ensure minimal downtime and continuity in the event there is a break in connectivity, whatever the reason.

Whilst the service is centrally monitored and managed, each implementation is made on a separate basis for each school, thereby avoiding the compromises associated with a shared infrastructure.

This service is independent of ISP, meaning individual schools or groups working collaboratively can select the most cost effective provider that will meet bandwidth requirements, with the reassurance that the service will be continually monitored to ensure users are safe and secure at all times.

Imerja is a technology partner and reseller of third party internet services, able to provide managed internet services in conjunction with a range of broadband products from BT, Virgin Media and other ISPs as required to ensure you get the most cost effective and reliable service possible.

Imerja's MSS provides:

- **Perimeter Security**
- **URL Filtering**
- **Web AntiVirus**
- **Web Proxy**
- **Email AntiVirus**
- **Email AntiSpam**
- **Remote Access**
- **Reporting**

Healthier options for NHS data security



Alwyn Nash
Strategic Partner
Alliance Manager
Check Point Software
Technologies Ltd

How do healthcare organisations apply security so that it protects systems and data without interfering with users' everyday work?

Primum non nocere - first, do no harm

This is the fundamental principle in healthcare. The same principle should also apply with IT security solutions. No organisation wants to risk data losses, but the security solution should also let users go about their everyday computing tasks freely, without the user noticing or being able to tamper with the protection.

If you make security transparent, then it's much more likely that systems and data will stay protected. Data losses and leaks are often blamed on individuals failing to protect data on a laptop or USB memory stick. But this simply diverts attention away from the real problem.

While an individual's actions may have breached security policies, it's unlikely that there was malicious intent involved. The users were probably just trying to do their job a little quicker, or work a little smarter. Can they really be blamed for that?

Avoiding the blame game

An effective security solution enforces policies using products, to remove from users the responsibility of deciding what data needs protecting.

If data needs securing as part of a process – such as copying data to a laptop or storage device – it's done automatically, without the individual having to worry about it.

Sounds simple, but how does an organisation go about deploying this kind of data security solution to all its employees?

Broadly, there are three things the organisation needs to do:

- encrypt all data stored on laptops, tablets, and USB devices automatically
- control data transfer to removable media, such as USB sticks or CDs
- centrally manage the security policy running on all computers in the organisation

Centralising security management

The starting point is to audit the organisation's entire computer fleet, to find out what security is already deployed, and what needs updating. As the NHS central procurement contract with McAfee has ended, now is a good time to look at rationalising the number of security agents used on laptops and desktop PCs – which will save costs and simplify management.

Then each computing device needs to be equipped with an integrated, centrally-managed endpoint security suite. Check Point's approach to endpoint security integrates all of the agents needed for protection, enabling policies to be created, automatically enforced and monitored using the same tools that manage network and gateway security solutions. Personal tablets, laptops and smartphones can be managed and secured with Check Point's Mobile Access Blade, and its Secure Workspace extends flexible working to home PC and laptops in a secure way.

This type of granular control and application of policies ensures that data flows in a traceable and secure manner, while enabling users to work efficiently. It ensures that the security solution truly does no harm.



Do we care enough about information security?

Data loss and security breaches happen every day, but these days the loss of a mere million or so personal records will probably make the news for a day at best. Back in 2007 when the HMRC lost a couple of CDs it was in the news for weeks and resulted in very public, high level resignations.

So what has changed?

Compliance has tightened; financial penalties increased and enforced; household names and global businesses have been publically embarrassed. Cybercrime is now worth more on a global scale than the illegal drugs trade, and the activities of politically motivated 'hactivists' now compete with their financially motivated counterparts in terms of the number and sophistication of attacks. And then there are the general internet anarchists who simply enjoy the challenge of taking down websites of well known organisations!

Many people still view information security as someone else's issue, as long as they are not directly affected, and act in a reactive way rather than proactive.

If we go back a couple of years, interest in end point security grew dramatically following a period when lost USB memory sticks and unencrypted laptops were frequently at the centre of reported data breaches. However, security measures were often implemented after the event to demonstrate compliance and win back customer confidence. It would have been more effective, cheaper and less damaging to put something in place before data was compromised, as once it is out who knows where the data will end up?

Recently, a member of the Information Security Community group on LinkedIn started a discussion, asking people to use one word to describe the biggest challenge facing information security today. The results were revealing in what they showed. Just taking a snapshot of comments posted over a month*, the consistent themes of people, awareness and attitude accounted for half the challenges identified. The discussion continues to attract posts daily, so if you are a LinkedIn user you can see the trend for yourself, but the underlying message is clear.

Disinterest and complacency in respect to the handling and management of sensitive data has to be challenged if this practice is to change. Rather than see it as a problem that needs to be addressed by a series of technologies and point solutions in order to satisfy the compliance auditor, information security should be incorporated into your overall strategy and be seen as a business process in its own right.

As we become less tied to desks through greater mobility, and rely more on hosted services to help run our business and personal lives, it is important to understand the risks our changing environment presents. Unfortunately, there is no quick fix to the challenge of educating people and raising awareness about information security.

Tighter compliance and financial penalties have not, unfortunately, stemmed the number of incidents reported.

I wonder what will?

People / Users	23%
Education / Awareness	14%
Attitude / Complacency	11%
Ownership / Responsibility	8%
Trust / Ethics	8%
Convergence / Integration	7%
Cybercrime / Hackers	7%
Zero Day attacks	4%
Cloud / Social	4%
Financial	4%
Others	10%

* Based on 207 comments posted between 22-May to 21-Jun 2011

Due to the variety of postings made the categories are consolidated from actual comments posted, based on the author's interpretation of the intended meaning. For example, the category Financial includes actual postings of cost, budget, money, expense, ROI.

Imerja secures N3 approval

Imerja has been approved by the NHS Connecting for Health for a direct connection to the national NHS N3 network.

N3 is one of the largest Virtual Private Networks in Europe. The high speed, secure broadband infrastructure has become the enabler for many innova-

tive IT solutions in healthcare, and underpins the NHS National Programme for IT.

Imerja already works with a number of high profile healthcare organisations such as Chelsea & Westminster NHS Trust, Lancashire Healthcare, Alder Hey and Liverpool Women's Hospitals. With

approval for N3 connectivity it is now able to provide services over N3.

Operating within the secure NHS environment builds on the company's existing compliance status, which already includes certification to ISO27001 as well as meeting the government Code of Connection and PCI standards.

Imerja plays host to Alder Hey

Imerja has been selected to deliver a data centre hosting project to Alder Hey Children's Hospital, one of Europe's biggest children's hospitals and one of the UK's top performing NHS Trusts.

The solution will securely host the hospital's data, including patient information, within a new data infrastructure located at Imerja's purpose built facility in Bolton. Ensuring such information is securely stored and readily available, despite any external disruptions to the hospital such as power cuts or building damage, is vitally important in helping Alder Hey's patients receive the best possible experience and care.

Imerja's private cloud solution will provide the hospital with access to a world-class data centre, saving the hospital both the space and cost of an on-site data centre and provide Alder Hey with the distance required for secure disaster recovery solutions.

The hospital will use this cloud to provide infrastructure-as-a-service, delivering to Liverpool Women's Hospital and other Trusts, effectively functioning as a service provider,

saving smaller Trusts substantial capital investments. Virgin Media Business will operate as a partner in the hosting project, providing the link between Imerja and the hospitals.

Alder Hey is recognised for delivering world-class international standards based IT. By owning the hardware and renting the hosting service, it has the ability to scale as required whilst reducing the need for capital investment. This innovative and forward thinking solution will match the new buildings the Trust is set to move to in the near future.

Dr **Zafar Chaudry**, CIO at Alder Hey and Liverpool Women's NHS Foundation Trusts, added:

"We wanted a cost-effective solution that would allow us to concentrate on our most important job of caring for our patients, while saving space and money. In order to hold our information in a secure fashion we wanted experts in the field, who we could trust with our critical systems, and we are delighted to be working with Imerja."

Imerja provides secure hosting services compliant to ISO27001 and N3 approved

Healthy list of new customers

In addition to those case studies presented, Imerja is delighted to welcome a number of new customers in recent months including several healthcare organisations: **Bradford District Care Trust** with a network refresh based on Extreme technology; **North East London Foundation Trust**, providing LifeSize video-conferencing solution in partnership with Virgin Media Business; provision of consultancy and support services to **South London &**

Maudsley Hospital NHS Trust, Gathesed Hospital NHS Trust, and Highland NHS Trust.

Other recent additions include the **Aircraft Research Association Ltd, Transactis** (in partnership with Virgin Media Business), and a growing number of **secondary schools** selecting Imerja MSS as part of their replacement service for the traditional Learning Grid solution.

Schools take Grid alternative

With the changes to educational funding already impacting schools' IT plans, and the growth in lower cost internet services, institutions such as **Watford Grammar for Boys**, **Windsor High** and **West Bridgeford** are amongst a growing number that have signed up to Imerja's Managed Security Service (MSS) as part of their own migration strategy from traditional Learning Grid services.

In each case, deployment of the MSS provides greater flexibility and visibility on the use of their internet connection whilst maintaining the security and integrity required for an education environment.

For details on Imerja's **Managed Security Service** for schools, and other complimentary services, contact your account manager or email us at info@imerja.com

SELFRIDGES & CO

Key network upgrade for retail giant

Imerja has completed a significant overhaul of the LAN network at leading luxury retailer, Selfridges.

The project required the installation of a new monitoring and maintenance system to support Selfridges' complex network, which runs across the company's four stores in London, Birmingham, Manchester Trafford Centre and Manchester Exchange square.

The monitoring system helps to ensure Selfridges' service availability and IT security throughout its stores, underpinned by the latest hardware and software technology to accommodate changes to the infrastructure and consumer requirements. The new system helps to protect Selfridges against security threats and isolated faults in the network, which can cause disruption to business. Ongoing maintenance and reviews of the system are also in place to ensure the Selfridges stores are regularly updated with the latest technology.

To service this, a team of engineers is on hand 24 hours a day to provide rapid response to identify and address issues before problems can develop. The Selfridges network is protected by Imerja's ServiceAlert proactive monitoring system, and supported by the 24x7 Imerja Network Operations Centre.

In today's fast-paced retailing environment even the smallest outage can be an expensive problem to experience and resolve, both in terms of financial impact and customer satisfaction. A network such as Selfridges' therefore requires careful monitoring to prevent faults occurring and interrupting trading.

As one of the UK's best-known retailers with a global reputation, its customers expect an exceptional level of service. It was essential that Imerja provided a bespoke system that offered maximum efficiency and the highest levels of protection against external threats and technical problems.

Selfridges has a complex network that requires specialist technical knowledge and dedicated ongoing support. Imerja has supplied Selfridges with a bespoke infrastructure that will work to improve functionality and provide the flexibility to develop the system on an ongoing basis.

Imerja's **m|four** services suite is a complete portfolio of service elements that can be applied to any part, or all, of your business

Partner Update

As part of our ongoing commitment to providing customers with the true best of breed solutions we continue to invest in both existing and new partnerships.

We are delighted to confirm Imerja has been promoted to Select Partner status by **Juniper Networks**, with recognised specialisation in its enterprise switching portfolio as well as its security solutions.



Other new vendor partnerships include **Aruba, Cryptzone, Fortinet** and **RandomStorm**, each of which brings specific value to help strengthen Imerja's overall technical solution capability.

Appointments

Growth in Imerja's **m|four** services business, and internal promotions from within our own operations and services team, has resulted in the appointment of three new Support Engineers with **Zahan Al-Rashid** and **Sam Kingdom** joining the ISOC team in the south and **Daniel Goodall** in the north.

Further expansion in the sales team as we focus on continued growth across the business has seen the appointment of two new Account Managers, with **Graham Green** and **Michael Sharwin** joining the team in recent months.

Penyem Village Update

In February Mark Evans and his family visited Penyem, the Gambian village where Imerja has been supporting the development of a health centre through the Northampton Trustee Fund (NTF). Imerja's involvement includes sponsoring a full time doctor to work at the centre, Dr. Musa Colley (below) is now in his second year of employment.



Prior to the trip Imerja ran an appeal to collect medical supplies - the response was overwhelming filling 15 suitcases, each carefully packed to utilise all the double baggage allowance provided by Thomas Cook. Mark and his family made the trip with students from Kingswood School in Corby, transporting over half a ton of supplies across the group.

A new ceiling and tiled floor has improved the fabric of the building, and the installation of solar panels and electric lighting enables it to stay open after sunset as well as operate basic equipment.

The formal opening of the health centre was filmed and reported by Gambian national TV. The day was rounded off by



a village versus visitors football match – 40 degree heat and a sand pitch made for challenging playing conditions – after a gruelling 20 minutes of play the home team won 3-2.

Since Mark's visit the charity has financed the construction of a further building for the school providing additional classrooms, and in the process freeing up space for the health centre including the addition of a private examination area and isolation ward.

The work of the NTF continues all year round, and there is still much more that can be achieved to build on the successful projects to date. For more details on the work of the NTF please visit <http://www.northamptontf.blogspot.com/>.



Imerja is a specialist provider of business IT solutions and managed services. With dedicated 24x7 operations centres located in the north and south, N3 approved and certified to ISO27001 and ISO9001 across all services, Imerja provides confidence that your organisation is protected around the clock to the highest standards.

Included in the Deloitte Fast 500 EMEA listing for two consecutive years, Imerja is recognised as one of the fastest growing technology companies in EMEA. We pride ourselves on being a trusted partner to our customers and business associates, and have received wider industry recognition including the MicroScope ACES Public Sector Reseller of the Year, IoD Ackroyd Award for Corporate Social Responsibility, Crains Best Places to Work, and Check Point EMEA Endpoint Partner of the Year.

To find out more about how Imerja can work with you to help add value to your organisation please contact your account manager or call the number opposite.

Head Office:

Hallmark House
Paragon Business Park
Chorley New Road, Horwich
Bolton, BL6 6HG

Midlands :

Bennetts Place, 30-31 High Street
Market Harborough
Leicestershire LE16 7NL

South:

Regent House, Allum Gate
Theobald Street, Elstree
Hertfordshire WD6 4RS

T: 0844 225 2888 | F: 0870 861 1489
E: info@imerja.com | Twitter: @Imerja
www.imerja.com