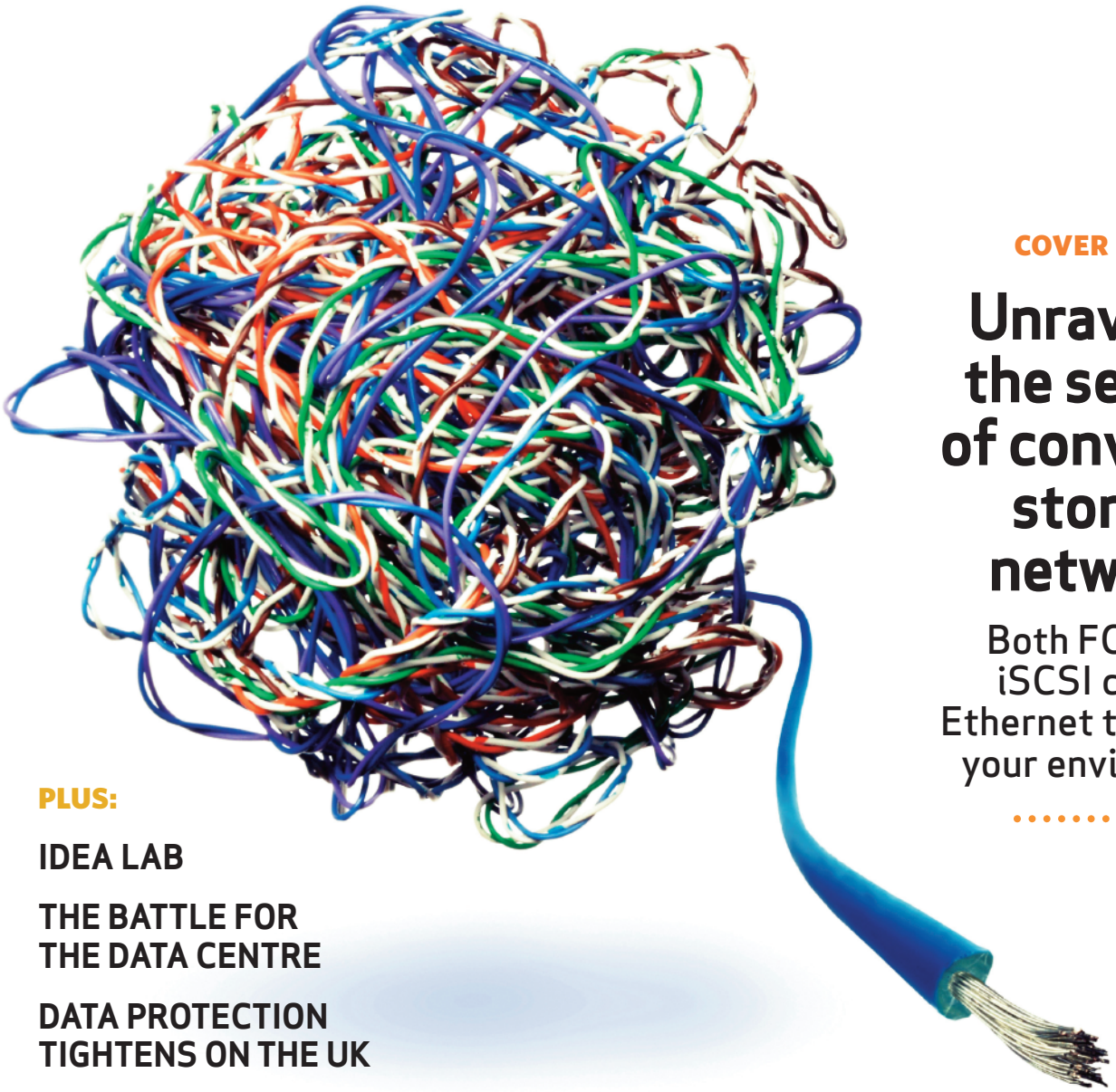
NETWORK evolution

EU EDITION

BUILDING THE INFRASTRUCTURE TO ENABLE THE CHANGING FACE OF IT • MARCH 2011/VOL.1/NO.1

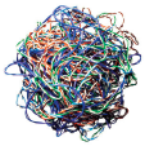


COVER STORY

Unraveling the secrets of converged storage networks

Both FCoE and iSCSI can use Ethernet to simplify your environment

PLUS:



idealab

Where evolving network concepts come together

Network Attached Storage in a Virtualised Environment

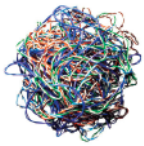
In a virtualised environment, network attached storage appliances can serve as a swap space to move virtual machines between servers, act as a backup medium, or play the role of central repository for all virtual disk images.

NAS versus SAN for data center virtualisation storage

There are two major approaches to network storage: network attached storage (NAS) and storage area network (SAN). They vary in both network architecture and how each presents itself to the network client. NAS devices leverage the existing IP network and deliver file-layer access. NAS appliances are optimised for sharing files across the network because they are nearly identical to a file server. SAN technologies, including Fibre Channel (FC) and iSCSI, deliver block-layer access, forgoing the file system abstractions and appearing to the client as essentially an unformatted hard disk. FC operates on a dedicated network, requiring its own FC switch and host bus adapters in each server. An emerging standard, Fibre Channel over Ethernet (FCoE), collapses the storage and IP network onto a single converged switch, but still requires a specialised converged networking adapter in each server. SAN solutions have an advantage over NAS devices in terms of performance, but at a cost of some contention issues. ■

SURVEY SAYS...

A survey of attendees at Gartner's recent Data Centre Summit found that 27% are already converging with NAS and iSCSI, 23% are planning to use NAS and iSCSI and 32% plan to use FCoE in the next three years. No one reported using FCoE today.



Understanding Failover and Failback

BY DEFINITION, failover is the capability to switch over to a redundant or stand-by server, system or network upon the failure or termination of an existing asset. This should occur without any kind of human intervention or warning. This contrasts with switch-over, where you're dynamically making a transition from one environment to another.

Failback is the process of restoring a system or another asset that's in a failover state back to its original state. The assumption is that you're able to bring it back to the state of operation before the disruption.

With a virtualised environment, you can failover to the environment which exists in real time, and it's very easy to failback to the original mode because you can maintain images of your previous environments. What's nice about this is that it speeds up your recovery time and it's possible to do testing on an actual system without adversely affecting your actual production environment. You can then turn it on or off as quickly as you'd like, so virtualisation really helps in the area of testing. ■

NAS IN VIRTUALISATION: NETWORK DESIGN CONSIDERATIONS

→ **ENSURE** that all connections are at least using Gigabit Ethernet.

→ **VERIFY** that the network switches are at adequate subscription levels for the number of ports in use, giving enough bandwidth to the storage appliance.

→ **REASSESS** any Quality of Service (QoS) policies that may impact the links between the servers and storage and adjust if necessary to give additional priority to the increased storage traffic.

→ **SET** network baselines before and after the NAS deployment to get a clear view of the impact of adding a NAS device to the data center network.

→ **TEST** and compare each of the network protocols available on the NAS device, typically NFS and CIFS to determine the best solution for your environment.

The Benefits of Using Virtualisation

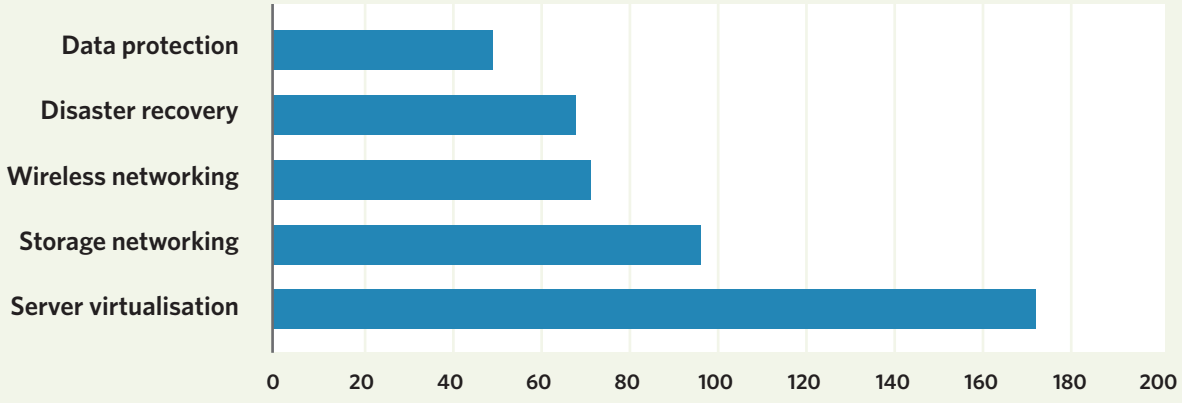
Virtualisation can provide some clear benefits for disaster recovery planning; it can help save money, time and effort, and make the often daunting task of designing and implementing a disaster recovery plan easier.

Additional benefits of using virtualisation as part of your disaster recovery strategy include:

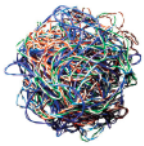
- Fewer physical servers needed at a disaster recovery site reduces one-time and ongoing costs, and results in less idle hardware.
- Lower cost virtual machine (VM)-level replication is storage independent and doesn't require expensive storage arrays.
- Hardware independence allows for more hardware options without compatibility issues.
- Encapsulation turns a VM into a single portable file for easier transport and deployment.
- Snapshots provide an effective method for backup of virtual machines.
- Automated failover and easier testing.
- Easier server deployment; scripting can be used to help automate many configuration and operational tasks.■

WHAT'S EATING YOUR TIME?

In the last year, these technologies/projects have required more time and networking resources than they did in the past.



SOURCE: TECHTARGET NETWORKING PRIORITIES SURVEY - UNITED KINGDOM RESPONDENTS, NOV. 2010



UK Users Lack Off-Site Backup and DR

MORE THAN one-third (36%) of UK businesses have no off-site backup and disaster recovery strategy, and more than two-thirds (71%) do not back up or do not know if they back up their virtual servers as often as their physical servers.

That's according to backup product vendor Acronis, which has launched its Global Disaster Recovery Index to survey 3,000 SME IT managers about the level of confidence they have in their backup and recovery operations.

The survey found that greatest challenge for the majority (67%) of UK IT managers is moving data between physical, virtual and cloud environments. The average UK business currently uses at least two to three separate backup solutions, with one-third (35%) using four or more to manage their different environments and further complicating DR.

Those who have no off-site backup and DR strategy in place cite lack of budget and resources as the primary reasons why it is not more of a priority. But, as a proportion of all IT spend, the UK spends slightly less (10%) on backup and DR than those that came out with the best overall results, Germany (13%) and the Netherlands (14%).

The poor results for UK businesses on backing up virtual servers came despite an expected 25% increase in the deployment of virtual production servers in 2011. More than half (56%) of companies surveyed worldwide use different solutions for both their physical and virtual backups.■

DR PLANNING IN A VIRTUALISED ENVIRONMENT

BECAUSE OF its ease of deployment and integration, server virtualisation can be a highly effective tool for disaster recovery. Here's how:

→ **COST:** It allows companies to reduce the number of physical servers they deploy at production and recovery sites.

→ **PROCUREMENT DELAYS:** It eliminates most hardware dependencies.

→ **RAPID RECOVERY:** Virtualised server images can be rapidly deployed and in some cases, moved across physical systems. ■

FCoE vs iSCSI? How about the one that's ready?

VENDORS CAN push Fibre Channel over Ethernet (FCoE) all they want, but the technology is simply not ready for deployment, argues Stephen Foskett, Gestalt IT community organiser. But iSCSI is another story.

"I am not a big fan of FCoE yet. The data centre bridging (DCB) extensions are coming ... but we don't yet have an end-to-end FCoE solution. We don't have the DCB components standardised yet," Foskett said.

What does Foskett think it will take to make FCoE work?

"It'll take a complete end-to-end network. I understand the incremental approach is probably now what most people are going to do. It's not like they're going to forklift everything and get a new storage array and get a new greenfield system, but right now you can't do that," Foskett said.

iSCSI, on the other hand, works over 10 Gigabit Ethernet today and lends itself to a total solution. So why aren't vendors selling it?

"iSCSI doesn't give vendors a unique point of entry. They can't say we've got iSCSI, so that makes us exceptional. But with FCoE they can say, 'We are the masters of Fibre Channel' or 'We are the masters of Ethernet, so you can trust us.' iSCSI works too well for anybody to have a competitive advantage," Foskett said. ■

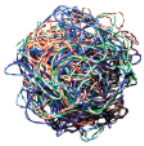
Before embarking on an FCoE implementation, ask:

→ **Will the storage team or the networking team own the infrastructure?** If co-managed, who has the deciding vote?

→ **Which department will pay for it?** How will chargeback be calculated and future growth determined?

→ **Will the teams be integrated?** Typically, the networking team is responsible for IP switches, while the storage team is responsible for Fibre Channel.

→ **Who will own day-to-day operational issues?** If a decision needs to be made regarding whether more bandwidth is given to local area network (LAN) or storage area network (SAN) traffic, who makes the call? Will companies have to create a single, integrated connectivity group? ■



FCOE OR ISCSI? DOESN'T MATTER! IT'S ABOUT THE ETHERNET

THE HYPE SURROUNDING data center network convergence and the battle between FCoE vs. iSCSI can obscure the core issue: At the end of the day all storage will traverse the production Ethernet network and engineers must be prepared for this transition.

Listening to vendor stories can be mind-numbing since each is choosing its own corner. Cisco Systems and Brocade lead the FCoE charge. Meanwhile, Dell tells its customers that iSCSI over Ethernet is the path to convergence. Chip vendors like Intel and network adapter vendors like QLogic and Emulex are backing all horses, ready to support whatever technology an enterprise chooses.

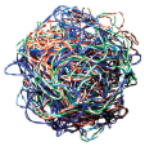
Enterprises must overlook the vendor hype and instead consider their existing infrastructure investments to determine which technology to choose. They also must understand that network convergence may occur in small increments, not necessarily going beyond the rack level in the short term.

"Typically [customers] have one type of convergence in mind when they come to us, and we have to open their minds a bit to the fact that there are many different options and they aren't mutually exclusive," said Joe Onisick, technical solutions architect with the data centre practice of a large system integrator.

WHY MOVE FORWARD WITH DATA CENTER NETWORK CONVERGENCE?

With the proliferation of 10 Gigabit Ethernet (GbE), server virtualisation and other technologies, enterprises must look seriously at network convergence to control capital and operational expenses and reduce complexity.

"If you have a rack with a lot of servers, especially a VMware rack,



you might have 10 copper Gigabit Ethernet connections and two Fibre Channel connections to each server," said Darren Ramsey, director of technology for Wellmont Health System, a Tennessee-based hospital chain. "If you have 10 servers in that rack, that's 120 cables. That's a lot to try to work around, a lot of inflexible copper, lots of heat. Switch ports aren't cheap."

In his data centre, Ramsey recently introduced network convergence to eight racks of virtualised Dell servers using Cisco's Nexus line. He consolidated 10 NICSs and two host bus adapters (HBAs) on each server to two QLogic converged network adapters (CNAs) that provide dual 10 GbE FCoE links to redundant top-of-rack Nexus 2232 Fabric Extenders. All eight pairs of Nexus 2232 Fabric Extenders connect upstream to two redundant Nexus 5020 switches. Storage and data traffic is converged via FCoE up to the Nexus 5020s. From there, storage traffic returns to native Fibre Channel and connects to a pair of Cisco MDS 9506 Director switches on the storage area network (SAN). The production data traffic continues upstream to Catalyst 6509 switches.

"The FCoE streamlined and downsized the number of Fibre Channel ports we needed since all hosts now run directly into the Nexus," Ramsey said. "We no longer need to tie directly into the MDS [from the server]. And it cut down on the complexity that was in each rack. And when we went to two 10 Gigabit links on each server, that allowed us to have more virtual machines on that box."

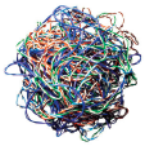
CHOOSING A CONVERGENCE TECHNOLOGY: ISCSI OR FCOE?

FCoE gets all the data centre network convergence hype, but many industry veterans say iSCSI is another viable option. As an IP-based storage networking protocol, iSCSI can run natively over an Ethernet network. Most enterprises that use iSCSI today run the storage protocol over their own separate networks because convergence wasn't an option on Gigabit Ethernet. But with 10 GbE switches becoming more affordable, iSCSI-based convergence is becoming more of a reality.

"Certainly iSCSI is the easier transition [compared to FCoE]," said storage blogger and IT consultant Stephen Foskett. "With iSCSI you don't have to have data center bridging, new NICs, new cables or new switches."

Ultimately the existing infrastructure and the storage demands of an enterprise will govern the choice of a network convergence path.

"There are very few times where I will steer a customer down an FCoE route if they don't all ready have a Fibre Channel investment," said



Onisick. "If they have a need for very high performance and very low throughput block data, FCoE is a great way to do it. If they can sustain a little more latency, iSCSI is fantastic. And if they have no need for block data, then NAS [network-attached storage] and NFS [network file system] is a fantastic option."

For Ramsey, iSCSI was never a viable option because of Wellmont's high-performance requirements.

"We played around with iSCSI, but that was still going to run over TCP, and you're still going to contend with buffering, flow control, windowing or packet drops and queuing, so we stayed away from it. What FCoE brings to the table—It doesn't run over Layer 3. It's an encapsulation of your Fibre Channel packet inside a native Layer 2 frame, and all we're doing is transporting that between the server and up to the Nexus 2232 and the Nexus 5020."

NETWORK CONVERGENCE: NEW STRATEGIES AND CULTURAL CLASHES

With storage and data convergence, networking pros will have to think about networking in a new way.

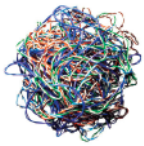
"You have to realise you're going to have a lot more traffic and it's going to be a lot more sensitive to latency and it's going to be incredibly sensitive to availability," Foskett said. "You've got to make sure the network doesn't go down. If you lose your data center, people cry about it. If you lose your storage network, then servers fall over and that's a really big difference."

With storage and data convergence, networking pros will have to think about networking in a new way.

What's more, networking professionals will need to familiarise them-selves with the management concerns of storage professionals if they are going to have storage traffic on their production networks, according to Stuart Miniman, principal research contributor to Wikibon, an online technology research community.

"A storage person is really concerned about data availability and making sure there is never a data loss, as opposed to a networking administrator who is really concerned about making sure there is connectivity, bandwidth and resiliency," Miniman said.

These different mindsets have traditionally led to culture clashes when storage and networking professionals work together. Now they



must find common ground.

"We heard that there were a lot of folks who never do [convergence] because their network folks and their SAN folks don't talk to each other," said Bob Cloud, executive director of IT infrastructure services at the University of Alabama at Birmingham. "We're unique because our network guys work for me and our SAN guys work for me."

Cloud has brought his storage and networking teams together while piloting FCoE-based network convergence in his data centre. As a Brocade customer on both the Ethernet and Fibre Channel side of things, Cloud elected to pilot FCoE with Brocade's technology beginning last September.

In one server rack he has introduced two redundant Brocade 8000 top- of -rack switches. The servers in the rack connect to each switch via FCoE. The 8000 switches then use Fibre Channel connections to send storage traffic to a Brocade DCX storage director switch and Ethernet uplinks to send production data traffic to upstream Brocade FastIron SuperX switches. At first the storage and networking teams were confused about who would own the Brocade 8000 FCoE switches.

"I think there was some natural confusion over who was going to own the switch and who was going to name the switch," Cloud said. "But we got past that pretty quickly because in our data center both the networking group and the SAN group report to me. I told them to work it out because it's a trial. The purpose of the trial is to uncover the organisational issues."

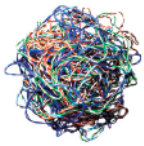
DEFINING MANAGEMENT DUTIES

A common management platform will be essential to working out those organisational issues, Cloud said. Brocade has announced a new unified management product, Brocade Network Advisor, which supports management of Fibre Channel, FCoE, MPLS and IP switching and routing. Cloud is still waiting for the product.

"We may always have a route access level person in the networking group and I think the SAN folks are fine with that. The networking group will have a little more authority over management of the switch than the SAN folks, but the SAN folks will have everything they need to troubleshoot and monitor Fibre Channel," he said.

Wellmont's Ramsey also manages both the storage and networking teams in his data center, so he's been able to keep his eye on the big picture. "I'm not going to have anyone fight over a sandbox," he said.

He doesn't see convergence as being that big a change organisationally. The Fibre Channel demar-



cation line has been pushed back from the server to his Nexus 5020 switches, putting that into the networking team's domain, but the storage guys do everything else in managing their SAN.

"It's just that, instead of managing ports that correspond directly to a server, now they go to the connections on the 5020 and it's all kind of virtualised. Our SAN guys are more than welcome to jump in there and learn [Ethernet], but they are busy doing what they do—provisioning storage and making sure that SRDF [EMC Symmetrix Remote Data Facility] is working properly. And I think that they embraced the idea of getting that extra network burden off of them," Ramsey said.

NETWORK CONVERGENCE BEYOND THE RACK

Although Cisco and other vendors will begin delivery of end-to-end FCoE switching capabilities this year, with technologies like Shortest Path Bridging and Transparent Interconnection of Lots of Links (TRILL), Ramsey doesn't see moving beyond rack-level network convergence within the next five years.

"What you're talking about is multi-hop FCoE, and Cisco is still working on fleshing that out. The most bang for the buck right now is to simplify the rack environment. If you want to go all FCoE, all your EMC stuff is going to have to be retrofitted with FCoE 10 Gigabit. And at that point you could probably get rid of your Fibre Channel.

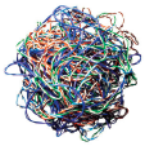
The most bang for the buck right now is to simplify the rack environment.

Maybe in five years we'll look at that, but that's not really going to buy us anything right now. We're just not pushing into the type of bandwidth where we would need dedicated 10 Gigabit to the storage. We don't need that much data. Where FCoE helps us is simplification inside the rack, making it faster, cheaper and smaller."

Cloud is also not ready to look past the rack until he gets a better handle on management of converged networks.

"[Brocade] just announced a lot of this stuff, and we want to test out the management system. Once we prove that out, we'll be looking to go further [with convergence]. We are trying to figure out the total cost of ownership." ■

SHAMUS MCGILLICUDDY, news director, TechTarget Networking Media



THE BATTLE FOR THE DATA CENTRE

DATA CENTRE networks are more important than ever, but in the battle for control over data centre management, network managers have lost their voice. Now they must regain a stronger decision-making role by showing how their technology can enhance the enterprise's overall business strategy.

Currently, facilities management (FM) teams and other IT organisation factions (namely storage and server teams) each believe they should have the upper hand in data centre decision making—and they have different perspectives.

POWER STRUGGLE

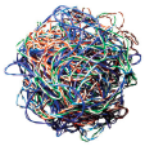
"Facilities tend to look only at the building, power and cooling, and don't really give a rat's bottom about the IT equipment inside. The network manager or IT director has the opposite problem—the kit is everything and the building is just the shell it all goes in," said Clive Longbottom, principal analyst at Quocirca.

"If [facilities managers] say that no more power can be delivered or that there is not enough cooling, then who can argue? The pure IT players believe that the world revolves around them—after all, the servers and storage hardware is what is keeping the business alive these days, isn't it?" Meanwhile, the modern network has the reputation for being commoditised.

"Everyone tends to see the network as 'plumbing.' The fact that without the network everything else collapses is neither here nor there," Longbottom said.

THE NETWORK IS KEY

The first thing networking teams and overall IT organisations must do



is prove what a central role they have in delivering energy efficiency and other savings to the enterprise.

All the main areas of responsibility, such as regulation compliance, cost management, resource optimisation and energy efficiency can fall within the remit of the network manager.

All of those factors boil down to performance while reducing power, argues Damian Milkins, CEO of ControlCircle, a data centre networks solution provider. Cloud computing will alter these factors dramatically, and the network manager will have his work cut out in staying on top of this entity as the complexity multiplies.

Network managers specifically have lots of influence on sustainability policies, as these policies largely involve software or network automation, said Joe Polastre, co-founder and CTO of Sentilla, an enterprise energy management solution provider.

As a result, network managers "can be both commercially aware and technically savvy, a great asset for any business which is growing," Polastre said.

COMPROMISING WITH SHARED SYSTEMS

In the meantime, IT and FM must reach a compromise to better serve the overall business strategy. They can do this best by using shared information systems, such as nlyte, Romonet or Aperture.

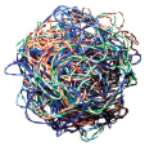
Of course, even within these systems there is disagreement. FM executives lean toward using nlyte and Aperture, while network managers believe in tools like Tivoli, BMC or CA that give them pure systems management.

Either way, using combined systems and workload and data centre management tools enables network managers to understand the impact of any changes on the facility while the FM team can use these "what if?" scenarios to plan more effectively.

These tools force FM and IT to make joint technology and facilities decisions that serve the organisation's business strategy.

"The business states what the desired end goal is, and IT and FM work together to come up with a range of different possibilities that meet the various aspects of the business' own risk profile, whether that means cost reduction, risk reduction or increased business value," Longbottom said. ■

NICK BOOTH is an independent industry analyst. He started working in IT, networking and telecoms in the days when even the visionaries couldn't see the Year 2000 coming.



DATA PROTECTION TIGHTENS ON THE UK

UK DATA protection regulations and data privacy laws are getting more stringent. In this interview, **PAUL GERSHLICK**, partner at law firm Matthew Arnold & Baldwin LLP, explains what organisations need to know to meet data protection and privacy regulations in the UK.

What are the most important regulations affecting networks and communications in the UK now?

The Data Protection Act (DPA) is a big one. RIPA (Regulation of Investigatory Powers Act) is also important. The DPA and RIPA actually regulate how data is treated on networks. There is also the Directive on Privacy and Electronic Communications 2002, known as the E-Privacy Directive.

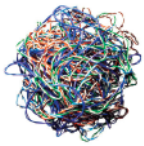
How have enterprises secured their networks to meet UK data protection regulations?

If you look at the stories that come out almost on a daily basis, there are so many cases of people not taking appropriate measures. The Independent Parliamentary Standards Authority data leak [that occurred]

> The IPSA is meant to enhance standards and it has been guilty of poor standards.

during IT maintenance because of failure to implement sophisticated access rights is a classic case. [The IPSA] is meant to enhance standards in public life and [it has] been guilty of poor standards.

The Data Protection Act says that



data controllers have to take appropriate technological and organisational measures against unauthorised or unlawful processing or against accidental loss or damage to personal data. What are appropriate technological and organisational measures? There are always more measures you can take. You have to weigh up what is the level of security appropriate to the harm that could be caused and the data that is being protected.

Recently the penalties for serious breaches of the Data Protection Act changed. Instead of the ICO (Information Commissioner's Office) having to issue a warning notice first and then issue fines, now it can issue fines up to £500,000.

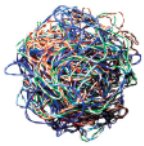
The European Commission (EC) is taking the UK to the European Court of Justice for failure to properly implement European Union rules for data protection and privacy. What has the UK done wrong? How is the EU's action likely to change English law regarding the interception of communications?

The Commission alleges the UK is failing to meet its obligations under the EU Data Protection Directive and the E-Privacy Directive. Communications can be intercepted in the UK where an interceptor has reasonable grounds to believe that consent has been given. At EU level you can only do it if you know you have got consent. Anyone who is to be sanctioned under the law regarding interceptions in the UK can only be sanctioned if an interception is committed intentionally; whereas at EU level it applies to anyone whether it was an intentional interception or not. The UK is going to have to tighten its position. I suspect there will be a new law in the next few months to bring the UK into line with the rest of the EU.

The penalties for serious breaches of the Data Protection Act changed and instead of the ICO having to issue a warning notice first and then issue fines, now it can issue fines up to £500,000.

Are enterprises vulnerable to prosecution for losing data via wireless networks, particularly resulting from employee remote access?

This is a massive and growing area that has not yet been fully tested.



Theoretically any organisation is in charge of what is done on their network, but you have to say "what is the network?" When you start looking at wireless networks, when people are logging on to corporate systems remotely, are corporates responsible for that? I am not aware of any case that says that they are. It is an area to watch.

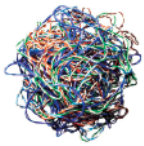
The European Commission has published a proposal for a new directive on attacks against information systems. Might this cut down on the number of attacks on networks?

There is the Computer Misuse Act in the UK addressing unauthorised access and modification of systems that was also changed in the past few years to specifically deal with DDOS attacks, so UK law is very much up to date on that. If you are caught under the Computer Misuse Act you can end up going to jail for years so if that is not doing much good, what would? The attack may not come from the UK though; it may come from outside of the EU. Anything like this has to be worldwide-led, not just European.

How might UK communications services providers be affected by plans to implement the EU E-Privacy Directive by May 2011?

The main impact on communications providers is they will have to let consumers know if there has been a personal data breach. At the moment there is no requirement for them to tell anyone if data has been compromised. ■

TRACEY CALDWELL is a professional freelance business technology writer.



UK HEADS FOR A MOBILE DUOPOLY

THE NUMBER OF UK mobile network operators is dwindling rapidly due to mergers and operator agreements that stifle competition. The question for businesses is what effect this network consolidation might have on both the mobile services available to them and the prices they will have to pay. And if the implications are negative, how can they be avoided or mitigated?

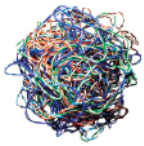
First, the background: Until quite recently, the UK had nine physical mobile phone networks, four 2G and five 3G. It will soon have only two access networks left, following a series of mergers and network-sharing deals.

Two of the UK's five mobile network operators, Orange and T-Mobile, are in the process of merging. The new combined company, called Everything Everywhere, has inherited T-Mobile's 3G network-sharing agreement with 3UK. Meanwhile, O2 and Vodafone agreed upon a pan-European network-sharing deal in 2009; in the UK this includes the two sharing their sites, masts and antennae via management company Cornerstone.

FROM NINE TO TWO

So, despite persistent rumours that 3UK is a takeover target, we will most likely have two access networks by later this year, each providing both 2G and 3G service. We are unlikely to see mobile phone brands affected until 2012, when Everywhere Everything is expected to introduce a single new brand.

The Orange/T-Mobile merger was quickly approved by the European Commission, with a couple of provisos. One proviso was issued because the new company would



have 60MHz of overlapping spectrum in the 1800MHz GSM band. This could make it the only UK player able to offer next-generation 4G LTE (Long Term Evolution) mobile data services in the medium term, so in order to get EC approval Everything Everywhere will sell off a quarter of this spectrum.

The other proviso was to revise its agreement with 3UK to prevent the new company from terminating the network share early in order to eliminate a competitor. The 3UK/T-Mobile joint venture, which is called Mobile Broadband Network Ltd, manages the front-end access network (i.e., the masts and associated infrastructure), but the two companies retain their own separate core networks.

DRAWBACKS TO MOBILE NETWORK OPERATOR CONSOLIDATION

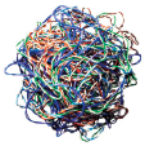
In theory, all this consolidation should mean better coverage for users, because each of the four remaining network operators immediately has the use of more base station sites. The danger is that, by weakening competition, it could also push prices up.

Indeed, economic researchers writing at VoxEU.org suggest that when you roll in the European Commission's determination to reduce mobile termination rates (MTRs), which are the fees that networks charge each other for accepting incoming calls to their subscribers, the only benefit will be higher profits for the mobile networks. They say customers could see fewer cheap calls. Jobs will also be at risk, with 1200 employees of Everything Everywhere told last year that their positions were in jeopardy.

For buyers of mobile telecoms services—whether they are end-user businesses, or even the MVNOs (mobile virtual network operators) that resell phone services, such as Virgin Mobile, Tesco Mobile and BT Mobile—the implication is a less competitive market. Less competition means less incentive for the networks to offer business-grade services and invest in improving their networks, especially on the mobile data side.

That, in turn, means more work for the telecoms regulator, said Andy Buss, service director at market research company Freeform Dynamics.

"Regulation has to ensure that they don't cut investment," he said. "If we look at what's happened with consolidation in the rest of Europe, regulation has become more important." He suggests that a long-term option might be ADSL-style unbundling, where the regulator insists that the access networks be opened up to competition, with other suppliers able to install their own core equipment and sell mobile services.



Of course, with two access networks shared by four network operators, and an existing tier of MVNOs already reselling capacity on those networks, the arguments in favour of unbundling are not as strong as they were for ADSL, where BT largely monopolised the last mile.

WHAT CAN YOU DO?

So what can network and comms managers do in the short to medium term to protect their organisations from consolidation among the mobile networks? One important thing is to shop around. Most large businesses already do this, sometimes playing two or three of the networks' business divisions against each other.

Small and mid-sized businesses can do this too, but should also consider striking deals with smaller, more responsive suppliers such as business-grade MVNOs and mobile service providers, suggested Andy Buss. That can help them get the level of service and visibility they need and also take advantage of better network coverage, while hopefully avoiding lock-in and profiteering. ■

BRYAN BETTS is a UK-based freelance journalist specialising in business and technology. Read about him at http://www.bryanbetts.com/.

TechTarget
Where Serious Technology Buyers Decide

Network Evolution Ezine is produced by TechTarget Networking Media.

Rivka Gewirtz Little
Senior Site Editor
rlittle@techtarget.com

Shamus McGillicuddy
Director of News and Features
smcgillicuddy@techtarget.com

Michael Brandenburg
Technical Editor
mbrandenburg@techtarget.com

Kara Gattine
Senior Managing Editor
kgattine@techtarget.com

Linda Koury
Director of Online Design
lkoury@techtarget.com

Susan Fogarty
Editorial Director
sfogarty@techtarget.com

FOR SALES INQUIRIES, PLEASE CONTACT:

Brent Boswell
Director of Sales, EMEA
bboswell@techtarget.com
+44 (0) 7584 311 889

Cover photograph by Stephen Webster/plainpicture