

“Digital Britain” – opportunities and risks for UK businesses

October 2009

Digital Britain is the UK government’s strategic vision for the UK digital economy. While social inclusion and rights protection are major themes, the plans will also have a significant impact on businesses. In stimulating investment in faster and more pervasive broadband access, Digital Britain will encourage the distribution and virtualisation of functions within businesses and further interconnectivity between organisations, their customers, suppliers and employees, wherever they are located. Businesses need to be aware that this will affect security and risk, and they should be taking steps now to minimise any harmful impact.

Rob Bamforth
Quocirca Ltd
Tel : +44 (0) 1264 711101
Email:
rob.bamforth@quocirca.com

Bob Tarzey
Quocirca Ltd
Tel: +44 (0) 1753 855794
Email:
bob.tarzey@quocirca.com

Florian Malecki
SonicWALL
Tel: +44 (0) 7771 982 328
Email:
fmalecki@sonicwall.com



An independent report by Quocirca Ltd.

www.quocirca.com

Commissioned by SonicWALL

©Quocirca 2009



“Digital Britain” – opportunities and risks for UK businesses

The internet has changed the way we all work. Many employees can now access core business applications from anywhere – especially at home or on the move. This revolution has also opened these applications to many external users, leading to much reduced inter-company interaction times and more efficient business processes. The UK government’s Digital Britain strategy will extend the network further, requiring businesses to take positive action to protect their resources:

- **Management, culture and inclusion**

Improved communications allow people to be dispersed, but does not make management processes easier and can lead to the culture of an organisation/business becoming too individualistic and less supportive, with some people feeling isolated, especially when things go wrong. Quocirca recommends that organisations take a management lead to communicate more frequently and more closely with remote workers, use technology that allows the widest possible involvement in different working practices/business processes, so that employees’ presence is felt and noticed in the workplace, even while they are working remotely.

- **Partner collaboration and relationships**

By all means allow partners to access your business’ IT systems, but keep that access segregated, controlled and under a watchful eye. Use separated access where possible, e.g. secured guest access for Wi-Fi, but then extend ‘extranet’ like services through suitably tight authorisation and secured communication links.

- **Threat awareness**

Controlling a connection with a firewall is no longer adequate; the perimeter is no longer impermeable and dispersed employees use many network services, each with threats and vulnerabilities. While large enterprises understand this, they often only have strong protection at central connection points, overlooking other weak areas at the edge of their network or beyond. Small and medium sized businesses are unlikely to be fully aware of the range of security challenges, or have sufficient technical knowledge to deal with them.

- **On grid versus off grid**

While public networks can provide some protection and segregation, there are commercial challenges from coverage to cost reduction that may involve third parties other than a primary carrier in the delivery of connectivity services which are often not visible to the end customer. Each additional relationship introduces more risk, and the potential for things to go wrong. Rather than relying on protection solely from the network, in particular where numerous end points are involved, businesses should apply their own protection to information in transit. This should be in place even over trusted providers, especially as network relationships can be extended to partners, who may in turn use different or unknown carriers.

- **Consumer backdoors**

Employees will often take a consumer approach to the use of technology products that are not available in the workplace, and these can bring increased business risks if used without adequate protection. Denying employees their choice of devices is increasingly difficult, so they should be accommodated - but with controls. Familiarity with technology may lead to contempt or complacency, and so the protection put in place should be kept simple, straightforward and as a default, achieve the minimum security level mandated by the business.

Conclusion

Organisations must remain in control of their distributed digital destiny and extend their networks where they need to in a managed and secure fashion to ensure that the business, the work of its employees and its digital assets are fully protected.

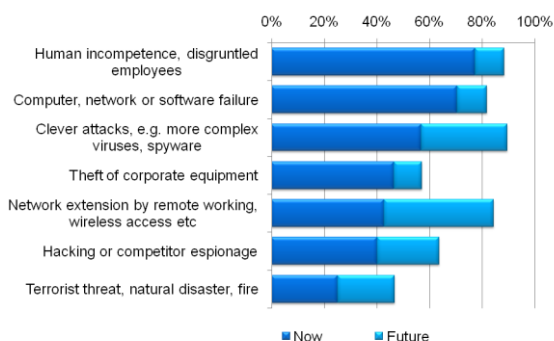
1. Keeping control of risk

The proverb says that “a chain is only as strong as its weakest link”, but first it is necessary to recognise the components of the chain. This is especially true in increasingly sophisticated IT systems, where there are always various security risks associated with information, and organisations need to ensure they take suitable precautions.

In Quocirca research five years ago¹, businesses already recognised many elements of IT security risk, and were concerned about the future impact of more sophisticated attacks, and a more distributed and diverse network (Figure 1).

Figure 1

What are the major causes of corporate data risk, now and in the future?¹



The following years of experience in many organisations demonstrated their concern appears to have been well founded. Despite increased awareness and use of security tools, 45% of UK companies noted some sort of security incident in the last year²:

Companies suffering in the last year

- Infection by viruses – 14%
- Staff misuse – 16%
- Network attack – 16%
- IT theft or fraud – 4%
- Any ‘serious’ incident – 25%

2. Extended enterprise

The global nature of commerce, combined with the need to stay competitive and have flexible yet strong relationships with suppliers, customers and other third parties, imposes certain demands on businesses to evolve. IT and communications technologies have advanced and merged and now have to more closely support those changing business needs.

The open connectivity of public networks, such as the internet and the fact that the vast majority of private networks are now linked to it, has made many of these changes possible, opening up new opportunities for business. New relationships are not only formed, but enriched as communications constraints – location, proximity, capacity, high investment costs – have been eroded by wireless and fibre technologies, pervasive access and flatter tariffs: transactions over greater distances no longer have the same high cost.

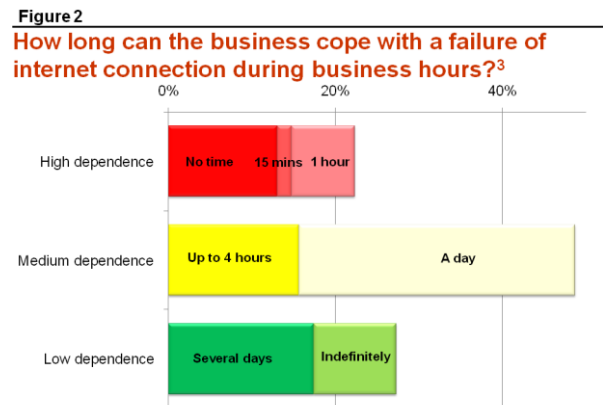
Issues for business and IT:

Yesterday	Tomorrow
On premise	On demand
In-house data centres	in the ‘cloud’
Shrink wrapped	Software as a Service
Upfront investment	‘pay as you go’
Sole, proprietary	open, multiplicity
Simple media	Rich media
Silos	Seamless
Protected perimeter	De-perimeterisation

New applications or IT services can be created, combined and managed from anywhere, and deployed and used anywhere else. Software as a service (SaaS), cloud-based computing, on-demand, hosted and managed services, and other terms used to describe the increasing range of online services, all offer improved flexibility and location mobility.

Economies of scale through shared infrastructure costs and access to specialised skills from using different forms of service providers enables businesses to reduce direct costs, so the connected and extended enterprise has much to recommend it.

In a few short years, the internet has moved from being a useful add-on for advertising a company’s presence and services to being a vital part of the infrastructure. This is true for small and medium sized businesses, most of which could no longer function from day to day without internet connectivity any more than they could without electricity (Figure 2).



This shift has changed the way organisations need to think about risk and control, as the perimeters – often physical, sometimes logical – that have kept them secure in the past, have dissolved. This requires wider consideration of security threats, but while almost all businesses protect themselves against malware, over half have not implemented intrusion detection or prevention solution (IDS/IPS).

3. Workplace 2.0

Employee working patterns have also evolved. While there have always been those whose roles mean they have needed to travel freely within or beyond the boundaries of their organisation, these people now more often need access to IT and communications services to perform their duties.

In addition, those who might previously have always been fixed in their workplace to be counted as ‘working’, now find they can be productive elsewhere. This might be while mobile or travelling between distributed offices or facilities within their own business or its partner and customer ecosystem, or while working from home.

It is here that the UK government investment plans for “Digital Britain” will have further impact on how businesses might look in the future, by raising the bar for minimum levels of network capacity in the core and connectivity and bandwidth at the edges of the internet, and encouraging service providers to offer broadband access to ever more remote communities.

It will require investment, which service providers are unlikely to be willing to commit to if there are poor returns, but the government is sufficiently keen to kick-start this using an additional telecoms tax to part-subsidise the required network investment.

Digital Britain’s impact on businesses:

- Location diversity to where there is sufficient capacity and connectivity, but lower property costs
- Increasing opportunity and demand for flexible and home working
- Emphasis on security in protecting personal digital information and content
- A mix of technologies – DSL, fibre, wireless and satellite - will be required for the Universal Service Commitment.
- Next Generation Final Third project will offer widespread high speed broadband for applications like tele-presence and cloud computing.
- Universal high speed (3G) wireless access, including on trains and the London Underground.

Digital Britain will encourage greater workforce mobility as more employees will be able to work remotely than ever before. This might be just part time to provide employee work/life balance, for flexible working to meet government directives or to extend the working day, especially where there is a need to communicate with those in other time zones.

It will also encourage businesses to set up and employ staff in more diverse locations. This could be beneficial to the business for costs reasons, such as recruiting staff where the cost of living and salary expectations are lower, but could also support social aspects, such as providing employment in areas where jobs have been lost in other industries.

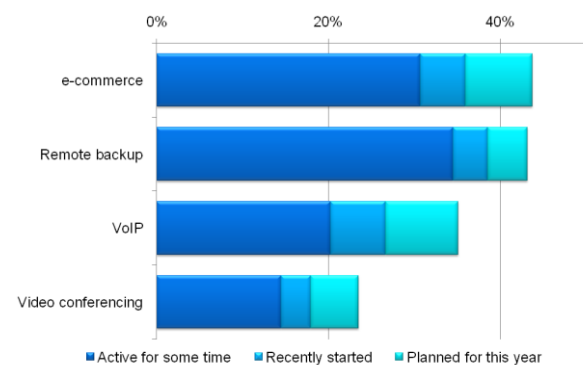
There are many considerations to weighing up the benefits and costs of working from home to the business. Reducing travel can boost productivity and have a positive impact on the environment, but there are other aspects, such as ensuring the organisation can retain control of its culture and costs, while securing its now remote assets. Also, the social needs of the worker should not be overlooked - a sense of working in isolation can easily happen for those working from home for extended periods of time.

4. New services, new threats

The use of the internet has evolved and is now increasingly an integral and critical component for the business community. This criticality and the ongoing need to support new applications have to be considered when extending the reach of the organisation to employees in remote locations.

With suppliers, partners and customers also likely to be ‘always online’, this creates opportunities for widespread use of advanced internet applications that include rich media, such as audio or video (Figure 3).

Figure 3
How many are adopting new internet applications?³



Businesses need to recognise that services like Voice over IP (VoIP) and remote backup will need protecting just as email and remote login always have. Each has different frailties and will be affected differently in the event of exploitation or attack, so suitable solutions need to be considered to mitigate the specific risks.

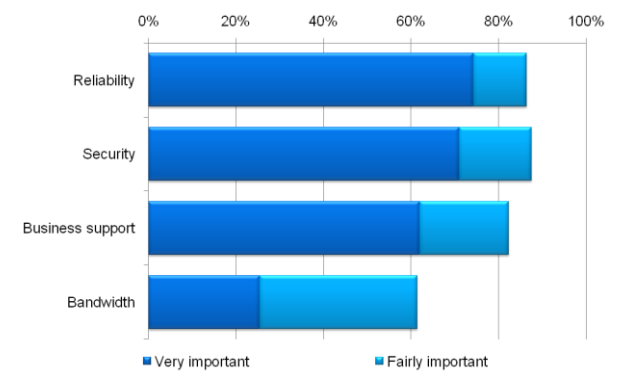
The need to secure access to services and their content is not new – seals and ciphers have been around for centuries – but the number of applications and the diversity of content has grown exponentially. Each new service adds new demands on performance and reliability, and exposes new areas of vulnerability and risk. For example many companies allow employees to use Instant Messaging at work, but half of those that do apply no controls over its use².

There is also an increased dependence on the timeliness as well as authenticity of delivery, and many services can be impaired or denied by unscrupulous or inappropriate activity. The more widely distributed the network, with employees at home or remote locations, the greater the need to ensure that protection and security measures are also spread right out to all points of access and use.

5. Conclusion

As Internet connectivity has become vital and businesses now rely on an ever-growing set of networked applications, there is a need to ensure high levels of service and connectivity (Figure 4).

Figure 4
What are important attributes of internet service?³



While most are aware of the need for reliability and security, this is often focused on the primary connection, and not the links to those working from home or in remote locations. Although some remote access protection measures are put in place, most often this is by restricting which staff have remote access, and to what. Still, 16% of businesses apply no additional controls for remote access security².

Initiatives such as Digital Britain will encourage even greater use of public infrastructure to distribute businesses and extend flexible working practices. Companies need to be aware of the impact of this, and of the new online services and applications that will need protecting, and plan accordingly. The corporate IT network may no longer have a perimeter, but it will still need to be protected.

References:

- 1 – Quocirca “IT security, bridging the gap”, Summer 2004
- 2 – Department for Business Enterprise & Regulatory Reform “2008 Information Security Breaches Survey”
- 3 – Quocirca “Soaring not surfing”, May 2008

About SonicWALL

Founded in 1991, SonicWALL, Inc. designs, develops, and manufactures network security, secure remote access, Web and e-mail security, continuous data protection, and policy and management solutions. Its appliances are engineered to reduce risk, cost and complexity by integrating state-of-the-art firewall, UTM, wireless and VPN technologies to deliver comprehensive protection and maximum performance. SonicWALL solutions are successfully deployed across small, medium and distributed enterprise environments around the world, including government, healthcare and retail point-of-sale installations.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with firsthand experience of ITC delivery who continuously research and track the industry and its real usage in the market.