Secure mobile working in public sector – improving productivity and compliance

A Vodafone
White Paper

vodafone

Flexible working for efficiency and effectiveness

Following the May 2010 general election and resulting budget cuts, the UK public sector faces the toughest challenges in decades. Adoption of leaner, more agile work styles, implementation of mobile and flexible working solutions and some strong executive leadership will be called for if the sector is to continue delivering the required levels of public services while producing the many billions of efficiency savings that will be expected of it.

It is not an entirely new agenda item. For the past few years agencies of every type and size have been adopting mobile and flexible working practices, spurred on by the Transformational Government agenda and the cost and operational efficiencies it promises. The new working practices fostered by mobile working not only lead to immediate cost savings from property rationalisation, travel and desk-based IT, but can aid in the management of the workforce, helping optimise productivity and supporting the primary goal of being able to provide better services to the community.

Adoption is accelerating. Mobile working is undoubtedly now commonplace in the public sector, and increasingly fewer employees spend all five days of the working week sat behind a desk in an office. The reason is that mobile working allows more front-line public servants to work out and about in the community, helping put the citizen at the very centre of their services and ensuring they can be delivered in flexible ways, as and when people require, wherever they are. Services are assured even during periods of adverse weather conditions, such as the snowfalls of December 2009 / January 2010, when business continuity is threatened by commuter disruption.

These benefits are driving tangible financial returns. According to one survey commissioned by the UK National Projects Programme Office, mobile working has the potential to generate benefits of up to £336 million across local authorities in England and Wales. Comparable cost efficiencies are prescribed for the National Health and the emergency services sectors.

Balancing productivity and security

The technology of mobile and flexible working has much to offer, providing all that is needed for remote access, effective data sharing and the ability to work in a time efficient way from a variety of 'desktop productivity' endpoint devices.

The pervasiveness of high-speed mobile data networks, and the ever growing popularity and ease of use of smartphones, handheld PDAs, netbooks and laptops, allow people to work wherever they need to. The younger generation in particular value the ability to work flexibly, though flexible workers of all ages generally use their time more productively than their strictly office-based counterparts.

Understandably organisations want to support employees who are able to work in this way, either remotely or while mobile, but they need to do so without compromising security. With sensitive public records and personal information at stake, the issues of identity theft, data exposure, privacy and reputational damage need to be constantly and actively managed to avoid data being accidently lost or maliciously hacked.

Indeed, as of April 2010, any organisation that is found to have fallen foul of a serious data security breach could be hit with a fine of up to £500,000 from the Information Commissioner's Office (ICO). The increased penalties are designed to act both as a deterrent against inadequate security measures or sloppy policies, and to encourage compliance with the Data Protection Act. Factors such as the seriousness of a data breach, the damage and distress it could cause individuals and whether it was due to negligence or a deliberate act will all be taken into account. How proactive an organisation has been to prevent breaches will also influence the privacy watchdog's decision.

The advice issued by the ICO over this matter is that where sensitive personal data has to be transferred in the public sector, the use of formally accredited secure communications channels, such as the GSI (for Government Secure Intranet) or GCSX (Government Connect Secure Extranet) secure managed networks, are strongly recommended. The ICO adds, "Ensuring that your organisation complies with the associated security standards, such as the Code of Connection (CoCo), will minimise the risk of a security breach occurring and demonstrates that security is being taken seriously."

Every public sector body is obliged to meet various recommended CoCo security standards before being able to connect to shared networks such as the GCSX private wide area network that is used by local authorities, central government, police and health authorities to communicate without using the public Internet. Since 30 September 2009, compliance with CoCo 3.2 has been mandatory. As of today, all 357 local authorities in England and Wales are compliant with CoCo 3.2, and the emergency services and organisations across the health sector have followed the lead.

Not only do these moves increase the level of guarantees over secure handling of sensitive public sector information, but they also promise increased compliance with Data Handling Guidelines and the Data Protection Act. However, the threat landscape is dynamic and continually evolving and – as we will see later – CoCo compliance obligations are periodically updated and necessarily refined in step with shifts in the public sector's security posture.

Risk mitigation – reliable checks and regular controls

As different public bodies have discovered, implementing and connecting to the GCSX provides the opportunity to significantly alter the way they interact with each other, with central government departments and with associated government agencies.

Equally, they have found that any form of change brings a degree of risk. For a local authority, for example, being able to communicate securely with the Department of Work and Pensions will also involve additional tasks and bring associated risks such as having to ensure compliance with laws (the Data Protection Act) and national regulations (complying with the handling caveats of restricted data).

It is always necessary to balance against any perceived benefit, the two key factors of managing risk and maintaining control. Compliance with CoCo standards plays an important part in both of these.

CoCo provides a list of security controls with which authorities must be compliant before their GCSX circuit can be fully activated. This requirement applies to all public sector agencies that need a direct connection, or who are connecting via an aggregated gateway, and also extends to their outsourcing and managed service providers, and any other third-party supplier with which they share sensitive data.

The requirements are adapted from ISO 27001, a framework for assessing risk published by the International Organisation for Standardisation (ISO) which considers parameters for risk in the four broad categories of technical, procedural, physical and human. The central communications infrastructure of the GCSX is accredited and is continually reviewed by The Pan Government Accreditor and CESG, the Government's National Technical Authority for Information Assurance. However, because many risks are introduced by the connections from the member networks, the onus is on every participating organisation to reliably identify and appropriately manage all risks associated with the network it intends to connect to the central infrastructure.

It is a not just a case of maintaining security within the internal network, but also extending checks and controls out to network boundaries, to offsite remote and mobile end-user devices – be they smartphones, mobile laptops or PDAs – and portable data storage devices. Of particular relevance, any mobile or home working solution has to be operated in accordance with CESG Good Practice Guidance. In short, this recommends that:

- Data at rest on a remote device, or in transit, has always to be encrypted
- Any use of portable electronic devices has to be authorised, managed and configured and operated in accordance with latest CESG guidance
- Remote connections must be from authorised official and/or managed devices, which means indiscriminate access from home PCs or desktops in an internet cafe is not allowed
- Records of activity have to maintained
- Personal firewalls must be installed, enabled and subject to configuration management for all remote working devices
- Two-factor authentication must be used for remote access from remote working devices.

Organisations also have to be able to demonstrate that their risk management activities reduce these identified vulnerabilities to an acceptable level.

Working with CoCo compliance

After some initial uncertainty and anxiety about their CoCo obligations, public sector agencies are now cognisant that compliance has to be built into the fabric of their business processes. In the context of remote working, rigorous measures are required to secure mobile handheld or remote PC devices, and watertight solutions need be put in place to manage and enforce security policies, manage connectivity and monitor ongoing compliance.

There are also cultural changes to consider with mobile working. Staff need to be trained on what is – and what is not – expected of them. With the greater freedom and flexibility to structure their working day to better suit their own needs and those of their customers and employer, comes the responsibility of maintaining security protocols when working with applications and data outside the office environment.

Coco compliance is not a tick-the-boxes, one-time event. The security of business processes has to be constantly monitored, managed and re-adjusted. Drift from compliance can introduce significant remedial costs from a re-authorisation standpoint to ensure continued connectivity.

Indeed, local authorities are duty bound to submit for re-authorisation a new set of CoCo documents a year after their last Code of Connection approval. Formally, re-submission is also necessary where an agency has connected to a new network or service, has introduced new or additional facilities for remote working (including mobile email devices), has any devolvement or amalgamation affecting the authority, or made any change to any outsourcing partnership, any facilities management procedure, or has had any sort of system redesign. Equally, re-submission is needed if the body has identified a major breach of security. In addition, the authorities will from time to time undertake random spot-check reassessments.

Public services when required

Police agency

Lancashire Constabulary wanted to give senior police officers and neighbourhood policing teams remote access to intelligence systems. Historically, the risks of using intelligence systems across open networks were too great and previous approaches lacked the security, cost effectiveness and flexibility to make this a reality. As a result, employees travelled to headquarters to access data, reducing time spent in the community and affecting the speed and quality of decision-making processes. Broadband-based VPN access overcame some security issues, but was not flexible enough to meet the needs of the end users. Working with Vodafone, the constabulary implemented a solution based on Vodafone Secure Remote Access (VSRA). The outcome is that staff can securely access intelligence at temporary incident rooms, in meetings and while travelling, resulting in improved service delivery. VSRA preinstalled on netbooks gives the force reliable, secure connectivity through a choice of networks. Crucially, VSRA will enable the constabulary to provide this access in compliance with National Policing Improvement Agency (NPIA) standards. The solution has dramatically changed the way that senior officers and neighbourhood teams work, while complying with NPIA standards.

The outcome:

- Faster and better informed decision making
- Increased local presence
- Lower costs
- Increased responsiveness
- Fewer security concerns

Managed service skills for secure mobile working

Managing CoCo compliance can be onerous for agencies both big and small, especially where the relevant expertise may not be available in-house. Typically, practitioners say it can take at least 10 man days to complete the documentation, but only if all the supporting information and data is available and up to date.

Vodafone can help public sector bodies meet obligations in this area, having extensive experience designing and deploying remote access solutions on laptops, smart phones and PDAs. Indeed, it is the first and only mobile operator to obtain accreditation under the CESG Claims Tested Mark (CCTM) for the Vodafone Secure Remote Access (VSRA) v2.8 laptop security and connectivity management suite of services for protecting remote and mobile workers.

VSRA is a security service which ensures staff remain in compliance with an organisation's policies at all times, even when working out in the field and away from the fixed office network. The award made under the CCTM scheme is synonymous with a stamp of approval and provides a government quality mark based on accredited independent testing. The certification attests to the overall effectiveness and performance of a product and is a highly regarded and recommended among local authorities, NHS, education, criminal justice, police and central government.

In November 2009, public sector managers will have received notice of the new version 4.1 of CoCo. In short, some of the 'recommended' controls from CoCo 3.2 have become a 'must-do' in the new CoCo 4.1. In particular, new requirements for mobile working (which formalise the CESG Good Practice Guidance given above) have been formally introduced, as well as specifics around firewall specifications, execution of unauthorised software and the labelling of emails with protective markings.

The updates to CoCo are a necessary step towards improved information assurance, but public sector executives will want to be mindful that any required changes introduced are both manageable and relevant to the evolving view of risk.

Of significance here is the ability of VSRA to manage connectivity controls on laptops, to ensure that any mobile or remote user can only select an approved connection method. It will also monitor applications and restart a required application, terminate a blacklisted application, or warn a logged-in user before disconnecting a non-compliant connection to the network or VPN. The system is flexible and highly configurable so that security for each user can be enforced by a centrally configured policy, whether or not access to the policy servers is currently available.

Done well, the procedures needed for CoCo compliance can become embedded in a reliable 24 x 7 public service, where all aspects of security across all devices are actively monitored, where clear and comprehensive reports are produced routinely, and where issues and exceptions are flagged automatically for fast resolution.

In this light, the appeal of managed service alternatives like VSRA becomes clear. With all the different applications involved in security, monitoring them all for compliance can become extremely challenging. VSRA can act as a central monitoring service for all deployed security components. Not only does it provide the reassurance that communications are secure, but removes the not inconsiderable burden of monitoring and reporting on compliance from the hard-pressed internal IT team.

Fit for purpose: Vodafone Secure Remote Access in profile

Different organisations will have different remote access requirements. Some organisations will have measures in place to meet many of their remote access security needs and others will need to take significant steps to ensure compliance. Depending on the current environment, Vodafone can supply a solution covering any or all of the following requirements.

- VSRA can enforce the launching and establishment of a VPN connection back to the office whenever the PC connects to the Internet. This prevents the user from obtaining unrestricted and unfiltered access to the Internet.
- VSRA can include full disk encryption to protect all information at rest on the laptop. Vodafone can provide a Media Encryption and Port Control component that allows removable media to be either disabled or usable only with strong encryption to protect the stored data, as suits the business needs of the individual user.
- If access to the Internet is required when the VPN is not up then Vodafone can supply software to enforce filtering of Internet access
- VSRA can be configured with a list of prohibited applications. If VSRA detects a prohibited application, it can be terminated. If software cannot be terminated, then access to the Internet or corporate network can be denied if desired.
- VSRA can monitor installed anti-virus software to confirm it is present and running. If the software should stop, it can restart the application, or prevent access to the Internet or corporate network.
- VSRA deployments can include a personal firewall or monitor an existing firewall to confirm it is running and to restart it if it is stopped. Access to the Internet can be denied or restricted to a PC which does not have a required security component running.
- Vodafone provides a full suite of security solutions from network to endpoint protection, to ensure and to demonstrate that compliance is met, accompanied by managed and professional services providing easy deployment and peace of mind.

Conclusion: Proven productivity gains

Organisations that have forged ahead with their remote and mobile working programmes are found to report improved responsiveness and greater job satisfaction among employees, because their staff can take fuller control of the job in hand, prioritise workflows, and manage their working time effectively. Customer service levels tend to improve, and there can be an overall boost in operational efficiency.

The business case is strong, with public sector organisations of all kinds reporting tangible cost-benefits. Ultimately, decisions about flexible, mobile working should be treated no differently from any other decision.

There is a need to balance productivity gains from technology investment against an assessment of risk and the prevailing regulatory requirements.

Why not find out more?

Talk to your Vodafone account manager, call us on 0845 084 0157
or visit vodafone.co.uk/securitybuiltaroundyou

Registered address: Vodafone House,
The Connection, Newbury,
Berkshire RG14 2FN.

Registered in England No. 147587

vodafone.co.uk/resources

TT 0210

vodafone