

## WHITE PAPER

---

# Secure Remote Access: Empowering the Mobile Worker

---

Sponsored by: Vodafone

---

Mark Kitchell

July 2009

### Key Message

Secure remote access solutions provide a reliable means for employees to work outside of the office. It is a major contributing factor to a growing willingness among managers to allow office-based employees to work remotely either part of the time or all of the time. It is also a key tool for the 'road warrior' type of employee who rarely (if ever) returns to the office.

In order for the mobile worker to be truly effective outside of the office, he or she must have access to the same tools as their office-based colleagues. However, the worker's mobility provides a number of challenges to the IT department. The mobile worker must be identified and authenticated from remote log-in locations and security policies must be maintained, even on potentially non-secure access networks. Software updates need to be downloaded and installed in an environment of sometimes brief log-ins. And compliance with regulations must be maintained in the more vulnerable mobile environment.

This white paper argues that secure remote access solutions are a viable option for Dutch organizations from a productivity, cost, management and security perspective. Organizations looking to empower their remote workforce in a secure and controlled environment should consider access software that provides the appropriate tools.

In addition, a case study of an organization that has recently decided to equip its mobile laptops with secure remote access software demonstrates how organizations can benefit.

---

### **A mobile workforce is the rule, not the exception**

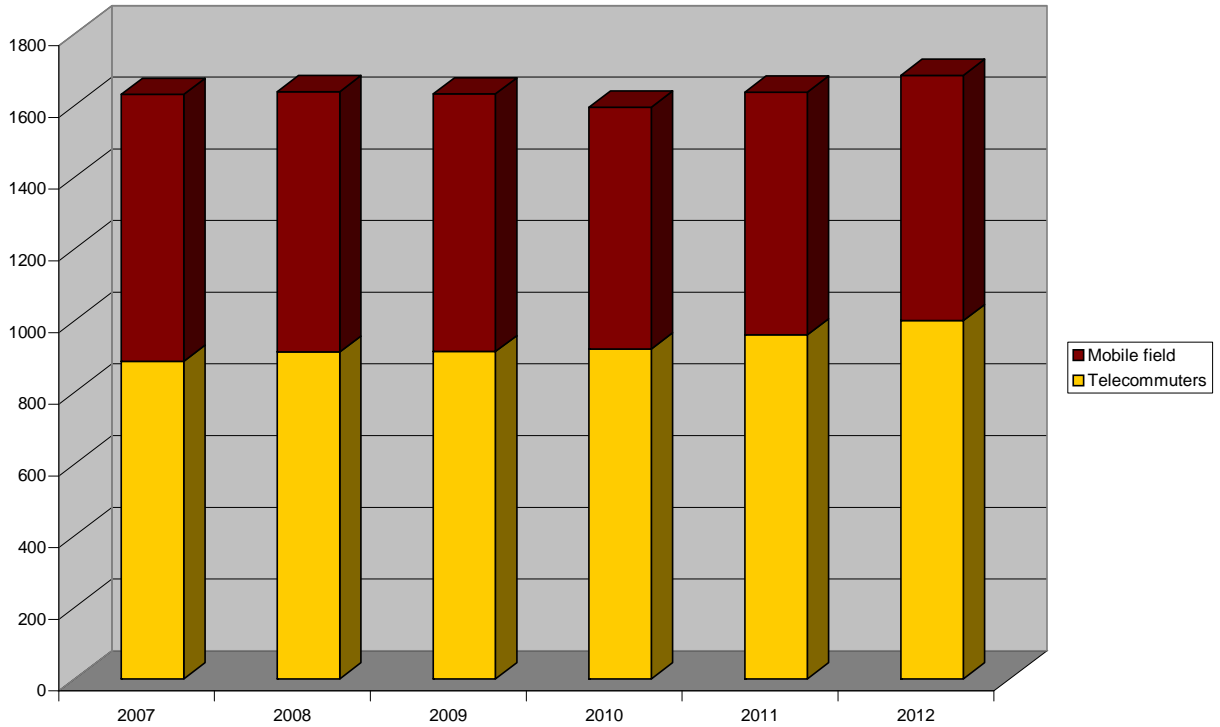
Despite recessionary pressures, the number of mobile workers in the Netherlands continues to slowly grow both in absolute numbers and as a percentage of the work force. Figure 1 shows that in 2009, telecommuters totaled approximately 910,000 workers in the Netherlands, or about 12%-13% of the total workforce. Mobile field workers totaled an additional 720,000 workers, or 10% of the total workforce. This data indicates that on any given day in the Netherlands, up to 22% of the workforce may be working outside of the 'protected' office environment.

Telecommuters are corporate employees who work at home during normal business hours. The threshold for telecommuters is three days a month or more, although some telecommuters may spend no time in traditional offices (in effect, they are telecommuting full time). Mobile field workers are typically field service employees

from various vertical industries who collect data. Increasingly, these employees are delivering enhanced services beyond data collection (such as sales functions) to better serve clients' needs and provide an up-sell opportunity for the company.

**FIGURE 1**

Mobile Workers (000) in the Netherlands, 2007-2012



Source: IDC, 2009

---

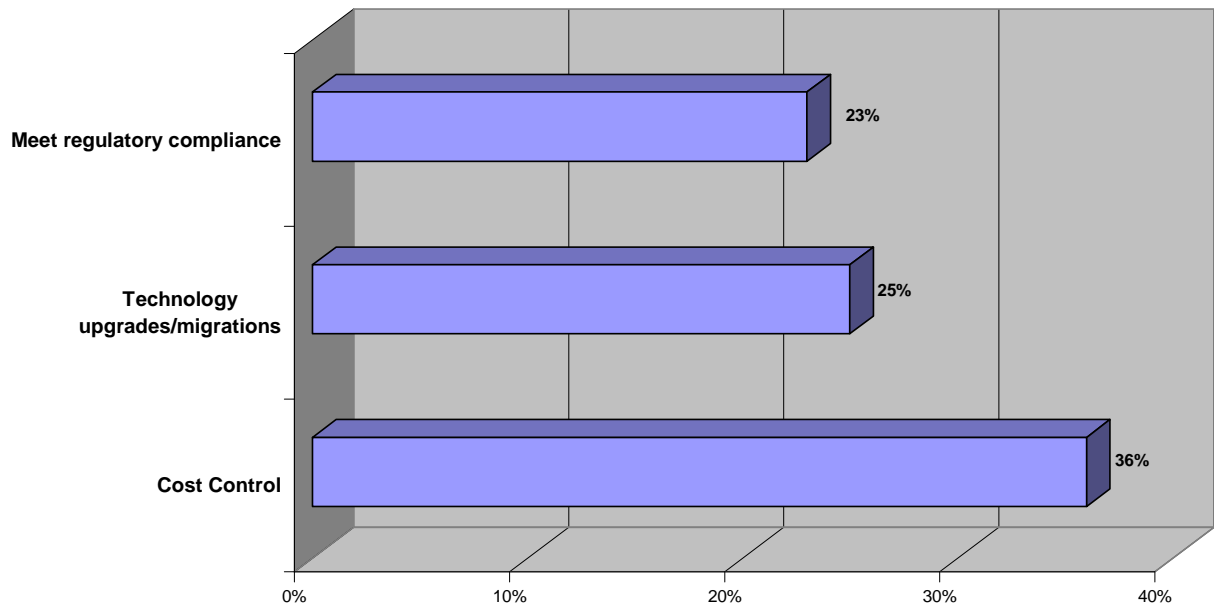
## Challenges of managing the mobile workforce

In managing the mobile workforce, organizations have to deal with a number of challenges that are specific to mobility, but also have to take into account the general challenges and direction of the IT department. Figure 2 shows the top 3 challenges facing the IT department in the Netherlands. Each of these challenges can apply to the mobile worker as well as the 'in-office worker'.

- ☒ **Cost control:** The primary non-hardware cost for the mobile worker is remote access for their laptop or Converged Mobile Device (CMD).
- ☒ **Technology upgrades/migrations:** Ensuring that required updates are installed on the devices of mobile workers can be difficult. The user can reject the update or cancel it in mid-download.
- ☒ **Compliance:** Compliance with national and international laws and regulation becomes even more critical in the mobile environment as data is taken out of the office.

**FIGURE 2**

What are the top challenges facing the IT department in the Netherlands?



Source: IDC, 2009

On top of these general challenges to the IT department, mobile organizations need to take into account the specific difficulties in managing the mobile worker. Issues of security, costs, management and compliance are even more challenging when the worker is outside of the office.

- ☒ In the mobile environment, security threats are increased while the user's ability to bypass corporate policy is also increased.
- ☒ The potential for cost over-runs (particularly in regards to remote access) is much higher.
- ☒ Management and monitoring of the remote user is made much more difficult, and monitoring of compliance is also challenging since the IT department has lost day-to-day control of the mobile worker and his/her laptop or other mobile device.

### ***A (bad) day in the life of one mobile worker***

As Anneke reflects over the past three months, she cannot get over how far she has come in her new position. As the sales director for a major airport security firm based in the Netherlands, she is responsible for managing a sales force of 20 account managers who are tasked with selling and promoting security services to over 75% of the international airports in Western Europe. She spends more than 90% of her time on the road, with at least 5 hours per day in front of potential customers.

As she opens her laptop to check on a customer order, Anneke realizes how important her connection to the home office network is. She can prospect customers, develop proposals, create sales presentations, all from her home, the train, or a hotel room. As a manager she can connect to her company's sales database to develop sales forecasts, analyze the pipeline, and even access diagrams of their x-ray machines and bomb-detection devices.

Unfortunately, some of the actions taken by Anneke have opened her company up to major security, liability and cost challenges. Lets review some of the actions taken by Anneke the past few days. On Monday she boarded a TGV from Brussels to Paris. Using her credit card, she logged onto the train WiFi network. After arriving in her hotel, she pays at the front desk to log onto their hotel's Wifi network. Later at a café nearby, she pays to log onto yet another public Wifi network. In one day, Anneke has spent over 60 euros on basic Internet access!

That evening, Anneke notices her computer is running slow and that there is a new program (an anti-spyware application) in her systems tray. She finds that by disabling this program her computer runs much faster. Minutes later a key-logging program is installed on her computer by an automated hacking program.

Later that evening she received a message from her IT department that software updates are ready for her laptop (updates to both the anti-virus software and her company's sales tracking database). Not wanting to be slowed down by a large download, she rejects the updates.

The next day Anneke logs onto her laptop in order to send new pricing specs to her sales representatives. Everything she types is recorded and sent to a group of hackers. Additionally, the pricing specs she sends her team are wrong, since she failed to download the software update the night before.

Although Anneke is a hard worker and effective manager, she took a number of actions over the past 24 hours that a) exposed her laptop to viruses and hacking, and b) wasted company funds on

excessive access charges. Additionally, her failure to update her sales tracking software put sales force at a disadvantage.

---

## **Access: The lifeline of the mobile worker**

Today's mobile worker may leave the office but they cannot leave behind access to their email, calendar, documents, presentations, etc. Ten, even five years ago, it may have been acceptable for someone like Anneke to be out of touch from the office for hours, even days. This is no longer the case. Today, the mobile worker must be able to log in with the laptop from various locations throughout the day. The mobile worker has a number of access options, all with various levels of cost and security:

- ☒ **Public WiFi:** Certainly the most ubiquitous but least secure. Public WiFi is available in hotels, cafes, airports, train stations, etc. Cost ranges from free access to 20+ euros per day. Public WiFi networks are often targets for hackers.
- ☒ **Private WiFi:** Some companies offer WiFi access for visitors. Although the service is sometimes offered at no charge, security can be very lax.
- ☒ **Access via mobile data card (UMTS/GRPS):** Laptops with embedded data cards can access the Internet from almost anywhere. These connections are very secure. Cost for mobile data access via a wireless provider's network is often included in the company's mobile data and mobile voice plan. However, costs can escalate when roaming on another provider's network.
- ☒ **Home broadband:** While it is critical for the mobile worker to access the corporate network via their home broadband connection, this is still a potential problem area for the IT department. While the cost is usually negligible, the IT department is often not able to monitor or enforce any type of security or firewall settings.
- ☒ **Hotel wired broadband:** Although increasingly rare, some hotels (especially older or non-chain types) still offer access via in-room Ethernet connections. Security may be better compared to a public WiFi network and costs are often 15-20+ euros per day.
- ☒ **Train or 'in-flight' WiFi:** Although access onboard a moving high-speed train or on an airplane remains somewhat rare, it will be ubiquitous in the next 2-3 years. Security levels will be similar to public WiFi but costs will be significantly higher.

The wide variety of access methods is a boon for the mobile worker. He or she can now access the Internet almost anywhere. However, with widely available access come major cost pressures. As Anneke demonstrated above, a mobile worker can easily saddle their company with multiple charges for access *each day*. The mobile worker has one thing in mind when looking for access: convenience. However, the IT department must think beyond convenience, and needs to consider cost and security. Therefore, it is vital that the access solution provided to the mobile workers not only gives them convenient and widely available access (through a single, integrated software platform), but must also direct them to use the most secure and cost-effective access available.

---

## Managing the mobile worker

While an increasingly mobile workforce may be good for business, it creates new challenges for the IT department. The increase in access locations and access technologies results in potentially higher costs for the IT department (in both payment for access services and increased time to manage multiple vendors). The growth of access technologies and types of devices used by the mobile workforce will put even more strain on the IT department.

Therefore, it is important that access software can do more than just connect the mobile worker to the corporate network. The software also needs to provide tools that will allow cost-effective management of the mobile worker and his or her device, and enforces compliance. An effective remote access solution will usually include the following management tools:

- ☒ **Management of software updates:** Software updates (security, business applications and otherwise) cannot be left to the end-user. Updates must be *pushed* onto the device. Interrupted downloads need to be monitored and re-started at the next log-in.
- ☒ **Enforcement of corporate web-surfing policy:** End-users are generally aware of corporate web surfing policy when in the office. These same standards must be enforced for the mobile worker who tends to be less sensitive to this, as he or she perceives the laptop as almost private property.
- ☒ **Application control:** Management must be able to control and monitor the types of applications installed on the mobile laptop. This will ensure worker productivity, compliance and can help reduce the security threats. A remote access solution needs to allow for application black lists, and for blocking of non-approved instant messaging software.
- ☒ **Management of access vendors:** Allowing the mobile worker to choose the access vendor can be both expensive and a threat to security. An efficient remote access solution will manage and maintain supplier relationships with access providers worldwide. The software will connect the mobile worker with a preferred supplier first (if their network is available). Only if a preferred supplier is not present should the software connect using an alternative (and more expensive) supplier.
- ☒ **Reporting:** A strong reporting tool will allow management to measure online activity and choose the most cost-effective access plan for each mobile worker.

Anneke could have benefited from some management tools attached to the remote access software on her laptop. She would have received the required updates to her sales software, and been directed to her company's preferred access vendors.

---

## Security and the mobile worker

Within an enterprise, the growth of the mobile work force leads to a growth of threats to both the remote PC (laptop) and to the corporate network. No longer is the PC

contained within the corporate network, under the watchful eye of the IT department. Rather, the mobile laptop is exposed to non-secure networks, downloaded viruses, rogue access points, etc.

To make matters worse, the mobile user may have the ability to (often unnoticed) violate company security policies by:

- ☒ **Disabling of security software.** If the mobile laptop is running slow, the user may disable any programs which he or she does not recognize (through Windows task manager).
- ☒ **Installation of unapproved applications.** Users often try to install their own personal software, irrespective of company policy and whether the software was purchased legally or not.
- ☒ **Connecting USB (mass) storage devices.** Connecting to USB storage devices leads to additional risks of data exposure and exposes the mobile laptop to virus attacks and other security threats.
- ☒ **Connecting to the Internet without use of the corporate VPN.** This may allow the user to surf unauthorized or virus-prone websites.

It is critical that each mobile worker be required to follow his or her company's corporate security policy. However, the use of remote access software alone will not provide security protection to the mobile worker. Rather, an effective remote access software package will leverage the existing corporate security infrastructure to protect both the mobile device and the corporate network through the following procedures:

1. **Identity and access management (IAM):** The remote access software must identify and control users' access to the corporate network via a unified authentication platform.
2. **Security Enforcement (procedures and updates):** The remote access software should enforce company security policies and push security software updates onto the mobile laptop. The software also needs to be capable of removing unauthorized applications and tearing down connectivity if a threat is detected.
3. **Compliance solutions:** The software needs to integrate with leading encryption software in order to meet both internal policies and external regulations such as Sarbanes-Oxley or Basel II.

## CASE STUDY

With over 15,000 employees, the Bolton Council is one the largest employers in the Greater Manchester (UK) region. The Bolton Council comprises 60 elected Councilors and provides governmental services to 262,000 residents, including administration, education, police and fire services, benefits, public transport, business promotion and environmental services.

The Bolton Council has over 1,000 purely mobile workers providing 'in the field services' throughout Bolton. Additional staff may work from home from time to time or may travel within the UK and internationally with their laptops.

Like all IT departments, the Bolton Council is facing serious challenges as a result of the financial crisis. Some of these challenges are unique to governmental organization and some can apply to any major IT department, including:

- ☒ **Budget Cuts:** The Bolton Council IT department is facing budget cuts of 3%-10%. Some programs have been frozen or scraped altogether. Budget cuts have also been implemented with other sectors relating to IT. For example, travel authority has been significantly curtailed and those traveling must reduce expenses, including costs for mobile laptop network access.
  
- ☒ **Compliance:** For the Bolton Council, the biggest challenge in supporting its mobile workforce was to give them the ability to connect anywhere at anytime. Prior to 2009 (due to security regulations), mobile workers could never connect from public locations (public wireless hotspots, hotels, etc.) and could only connect from home via a dedicated DSL line installed and maintained by the Bolton Council. These regulations meant working from home for the general staff was quite difficult, and made it almost impossible to field a mobile workforce using laptops and smartphones.

While facing these budget and compliance challenges, Bolton also faced increasing demands for a flexible and secure mobile workforce. Between 2005-2009 the number of mobile workers increased from less than 200 to over 1,000. At the same time, the demands of the mobile workforce increased, with access required throughout the UK and Europe and demands from the workforce to connect to any network (wired or wire line) available.

Bolton Council addressed both these challenges with the VSRA product from Vodafone (Vodafone Secure Remote Access). As an early adopter of VSRA, Bolton was able to customize the product to meet their own requirements. "We could not find a robust remote product off the shelf from any vendor, so we told Vodafone exactly what our requirements were" said Vinod Vora, Senior ICT Development Manager for the Bolton Council.

In terms of cost efficiency, VSRA had two main benefits to the Bolton Council. One, it provided a single, uniform remote access client that could be installed on all mobile laptops. VSRA replaced multiple remote access clients, which had varying monthly costs and support fees. Second, VSRA cut down on network access cost for the mobile workforce. Now, mobile workers are automatically connected to pre-approved access providers (including wireless, Wi-Fi, hotspot, hotel access, etc). The cost for remote access are now manageable and predictable, regardless of whether the user is traveling in the UK or internationally.

VSRA made the biggest impact for Bolton in terms of compliance with government regulation on security and the mobile workforce. The VSRA security overlay, which requires all mobile workers to fully comply with Bolton security directives, has added an important layer of compliance to the Council's mobile workforce. No longer can

workers bypass mobile security by turning off certain programs, surfing restricted websites or installing unauthorized software. Security updates and key software patches are pushed directly to the mobile laptop without the participation of the end-users. Encryption procedures must be adhered to.

These security enhancements have allowed Bolton's staff to work from almost anywhere and to log-on from home or any public hotspot while still maintaining compliance with UK regulations such as GovConnect. "We have been able to maintain our guiding principle of security, VSRA has only provided us with an effective tool to manage these principles and to ensure they are maintained outside of the office. The (remote access) client has become a key tool for us to serve the mobile workforce" Vinod concluded.

---

### **Bottom Line**

IDC believes that the use of secure remote access solutions provides vital benefits to the both the IT department and to the mobile worker. By implementing a secure remote access solution, the enterprise can realize key security and management objectives while providing the remote worker with a seamless connection to important network resources.

Anneke's employer has no option but to provide her with the IT tools she needs to do her job effectively. She holds a key position in the company and needs to have the best possible conditions in which to work. In order to remain productive, Anneke must have consistent and secure connectivity to both her corporate network and the Internet. Just as important as this need for connectivity is the need for security. As seen in a number real-life incidents, insecure remote access can lead to problems for the enterprise. Such problems can result in more than just downtime and cost overruns and can influence reputation, legal exposure, and loss of business. Secure remote access solutions provide important tools to mitigate these risks.

---

### **Methodology**

Market data and forecasts are based on existing published IDC documents. The case studies are based on IDC analyst interviews with Bolton Council, a Vodafone customer. The interview was conducted during April 2009.

---

## **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2009 IDC. Reproduction without written permission is completely forbidden.