Meeting the challenge of security in a mobile environment

White Paper

power to you
The bottom line:
With the needs of the global business in mind, this white paper explores one of the key findings of a major independent European survey undertaken on behalf of Vodafone Global Enterprise, examining the current opportunities and challenges to the broader implementation of secure mobile communications solutions.

Key concepts:
The issue of network and data security remains a major concern to enterprise businesses, despite the availability of a wealth of management tools to reduce areas of vulnerability. The survey looks at the problems facing enterprise businesses today and the solutions available to improve security, to the benefit of both the business and its employees.

Who should read:
This white paper is of particular relevance to CIO, CTO, IT and Telecoms Heads, Communication Consultants and Global and Regional Procurement Directors.

The white paper should be read in conjunction with the Vodafone Global Enterprise White Paper, Securing your business mobility with confidence – power to you
This is the first in a series of white papers looking at the major pain points facing today's CIOs.
A recent survey of European multi-national enterprise businesses found that one of the biggest challenges facing today’s CIO is the need to address the problem of maintaining data and network security in an environment of growing workforce mobility.

Executive Overview

The survey, undertaken by Circle Research on behalf of Vodafone Global Enterprise this year, was designed to examine the major issues facing today’s senior executives, as they look to manage their telecommunications activity in a way which is both cost efficient and effectively supports the broader business.

The findings identified a number of critical ‘pain points’ facing enterprise businesses, including flexible working, the need to control communications expenditure and data/network security. The following white paper will look in more detail at key pressures on the CIO in considering the security challenges facing the business and how well-prepared they are to deal with them.

It is generally recognised that communications represents one of the largest areas of any organisation’s expenditure, yet for many it is the least transparent or controlled. The Vodafone Global Enterprise survey highlights those areas where this causes the greatest corporate pain.

Today’s best practice communications solutions can address these issues, giving back essential control to the business in a safe environment, whilst providing proactive support to the strategic direction of the enterprise.

Increasing pressures

Whichever way you look today, businesses are coming under growing regulatory, environmental and social pressures to implement more flexible methods of working for their staff.

At the same time, recent events such as the swine flu pandemic and the volcanic ash cloud have demonstrated how business continuity benefits significantly from the creation of a ‘work anywhere, with anyone’ environment for those staff stranded in a remote location away from the office.

Yet increased mobility and remote working brings with it new security challenges safeguarding access to the corporate network. As a result, the issue of security remains a major pain point, and for many businesses is a continuing barrier to its effective implementation. Just as mobility has become mission-critical, so the related area of security as a key enabler must also be tackled as a strategic issue - supporting true flexibility for employees, not just a series of one-off tactical implementations of individual flexible working initiatives.

For it is only by taking an enterprise-wide approach that the social, economic, regulatory and environmental benefits to be had can be fully secured across the business.
Survey methodology: A European perspective

In seeking to establish a comprehensive picture of what issues are putting the most strain on businesses today, Circle Research undertook a detailed series of telephone and online interviews of multi-national enterprise businesses, each employing more than 1,000 staff, in the following countries:

<table>
<thead>
<tr>
<th>Country</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>150</td>
</tr>
<tr>
<td>Italy</td>
<td>90</td>
</tr>
<tr>
<td>Netherlands</td>
<td>40</td>
</tr>
<tr>
<td>Spain</td>
<td>70</td>
</tr>
<tr>
<td>UK</td>
<td>150</td>
</tr>
<tr>
<td>Total</td>
<td>500</td>
</tr>
</tbody>
</table>

In 72% of cases, the business was operating in five or more countries, with the remaining 28% in three or four countries. The survey included a broad spread of industry sectors, from manufacturing, utilities, wholesale/retail and transport/distribution to financial services, IT/communications, utilities and government/public sector.

All respondents were involved in the selection of suppliers of telecommunications services. Of these, 63% were ‘decision-makers’ and the rest defined as ‘decision influencers’.

Overall, the survey found a broadly consistent approach to cost across the geographies surveyed. However, a number of significant national and sector differences also emerged, which are highlighted in the following individual findings.
Key findings

1. A high-profile issue
Companies are increasingly coming under pressure to introduce new, more flexible working practices in which employees are enabled – and in many cases encouraged – to work remotely, without any loss of productivity. In order for this to happen, businesses have to address a new and greater range of security issues, if staff working away from the office are to easily access the corporate network and share data in a way which reflects ‘business as usual’.

Security has always sat at or near the top of the corporate agenda. It is not surprising therefore that in this fast-evolving environment, the issue of network and data security continues to loom large as one of senior management’s recurring nightmares.

For more than one half of respondents overall, the issue of addressing telecommunications security threats remains a high priority for their organisation. It is currently a low priority for only 10% of businesses.

Somewhat more surprisingly perhaps, there is a significant divergence of view at an individual country level, with 66% of enterprise businesses in Italy viewing security as a high priority issue, compared to only 35% of their counterparts in the Netherlands. Similarly, the Netherlands also had the highest ratio of businesses for whom security was of low priority (20%), whereas in Spain, only 3% shared this view.

A sector analysis also reveals a wide range of reactions to where security sits on the corporate priority list. Given the inherent nature of their day-to-day business, it is not surprising that this is an area of greatest concern to financial services businesses, of whom 58% see this as of high priority. By contrast, only 33% of wholesale/retail companies put security on their list of high priority concerns.

2. The problem of mobility
Reflecting the growing emergence of mobility, respondents identified a number of specific security threats in the use of mobile communications tools.

In total, more than one third (34%) registered the potential security threats associated with lost or stolen mobile devices as of significant concern. In Spain, this was especially worrying to management, with 46% reflecting this level of concern. Conversely, only 7% of Spanish companies had little concern in this area, in stark contrast to 40% of companies in the Netherlands.

Unlike the earlier sector comparison of security threats overall, financial services organisations showed the lowest level of concern in the area of mobile devices (26% registering significant concern). This perhaps reflects lower usage of mobile devices across these businesses than in the manufacturing (39%) and other business services sectors (36%).

Reflecting another aspect of communications security worrying senior managers, a similar 34% of respondents in total admitted to significant concerns over the use of mobile devices on insecure networks, a reaction reflected consistently across all geographies. At a sector level, transport/distribution companies were most worried here (47% registered significant concern and 11% little concern) compared to wholesale/retail businesses (17% and 31% respectively).

This reflects the inherently more mobile transport and distribution sector, in which a much higher proportion of devices are used away from the office or depot base as a mission-critical part of the business’s day-to-day operation. As a result, managers working in such an environment will be more acutely aware of the risks associated with any shortfall in network security.

However, the situation may be starting to improve here, as advances in technology appear to be allaying people’s fears to some degree. In the case of smartphones, for example, far fewer businesses are significantly concerned about the threat of smartphone viruses. This was most strongly reflected in the Netherlands, where only 15% registered significant concern and 50% little concern.

IT/Communications firms in particular were well ahead of other sectors in seeing smartphones as of little risk – reflecting perhaps their greater understanding of the varying levels of security inherent in different devices.
3. A question of control
As with other aspects of communications management, a lack of visibility and control typically sits at the centre of such security concerns.

When asked how well they were able to monitor the status of mobile devices in issue across their organisation’s global footprint, nearly one half (44%) agreed that they knew how many had been issued but were unsure how many were now dormant. Of even greater concern, 4% were unsure exactly how many had been issued in the first place and were in use. More positively, 65% of businesses in the Netherlands confirmed that they were certain how many devices had been issued and whether or not they were active and in use, compared to 52% overall.

From the standpoint of operational support, this variable picture was reinforced by the fact that only one in three businesses (35%) were confident that they provided a consistent level of handset repair and replacement across their global footprint. For a further 59%, they felt that, though this was generally the case, ‘in some markets this simply is not possible’.

Compromising data security
The bottom line of all this is that security is not as watertight as it could, or should, be. And this was reinforced by the survey’s findings concerning both built-in security and the ability to respond effectively in the event of a potential breach, with a broadly common picture emerging across all geographies and business sectors.

For example, when asked how confident they were that data stored on the device or the network would not be compromised in the case of a lost or stolen device, though many were positive about their ability to cope with this effectively, nearly twice as many expressed varying degrees of doubt.

Overall, 34% of respondents expressed confidence, on the basis that ‘robust measures and systems were in place’. However, 57% had some doubts, concerned there might be vulnerabilities for which they were unprepared. Further, 9% had serious doubts, on the basis that their organisation was ‘likely to have gaps in their security measures’.

Yet there is a greater concern here. If a device is lost or stolen, more than half of respondents overall (53%) were unable to remotely erase data stored on that device, a finding once again broadly consistent across each country and sector surveyed.
The survey provides a major opportunity for businesses to take advantage of the best practice mobile working solutions provided by Vodafone Global Enterprise. As a result, the CIO and his team will be able to implement more flexible mobile working practices and secure greater control of telecommunications expenditure in a fully secure environment.

However centralised or distributed the enterprise, both the organisation and its staff expect nothing less than continuous availability, which in turn requires the communications infrastructure to be stable and reliable at all times. In order for an organisation to safely mobilise its business applications, security controls need to address a number of key components within an enterprise-wide Security Policy Framework:

**Security strategy**
In mobilising business applications safely, a best practice security strategy framework should identify new threats and incorporate the following three components:

- **Device security**: protecting each mobile device against attacks and threats, e.g. from loss or theft, malware or local wireless networks
- **Service security**: offering secure service involving the device and the network, e.g. mobile email and secure access to corporate applications
- **Network security**: operating a mobile network with high availability and enforcing access control. Also running secure protocols over a wireless network and between networks

Two examples show how this works in practice. **Vodafone Secure Remote Access** seamlessly integrates connectivity and security - it gives your people a single way of connecting securely to enterprise networks, whether it is via wireless broadband or fixed line access. It offers a long term connectivity and security platform that works alongside your existing security infrastructure to control the cost of supporting your remote workers.

Ensuring complete remote control of your mobile fleet, **Device Manager** is a sophisticated online tool for global businesses who need to fully understand the mobile devices they have, ensure that they are secure and conform to corporate policies. In addition to being able to audit devices remotely and keep them up to date, if a mobile device containing confidential information is misplaced, it can be remotely locked anywhere in the world at any time of the day. If the device is lost, the contents can be completely erased.

And this approach has an unrivalled heritage of success, as Vodafone brings more than two decades’ experience to wireless security management in helping businesses protect their corporate information in a wireless environment.
Conclusion

Today’s commercial environment is more competitive and more global than ever before. As a result, businesses need to improve productivity and responsiveness if they are not to fall behind in meeting customer demands and expectations.

As companies respond by driving up workforce mobility, so this in turn demands a new approach to security. For it is generally recognised that traditional ‘behind the firewall’ security measures are neither practical nor sufficient as businesses look to protect corporate information in today’s increasingly wireless environment.

It is no surprise therefore that security remains one of the biggest hurdles to overcome in enabling a more diversified and flexible workforce. Multiple security policy policies are now essential that are capable of covering network security, mobile devices, supporting IT systems and infrastructure, personnel and processes enterprise-wide.

Security is not a static environment and Vodafone is committed to staying fully up-to-date and ensuring that its multi-national corporate customers benefit from the latest solutions and emerging technologies. Vodafone will continue to offer the most secure service, giving businesses the confidence to implement secure wireless mobility solutions in driving competitive differentiation in their chosen markets.

For as the survey makes clear, those best practice solutions which can combine effective security with enhanced cost control and mobility will enable communications to become an enabler, rather than an inhibitor, to the successful growth of the broader business.