

Disaster recovery for mobile fleets

Disaster recovery for communications first hit the headlines back in 2001 with the 9/11 attacks. Since then, mobile devices have increased exponentially in importance for the business sector and are now taking the place of landline-based systems, being the device of choice for most users in and outside the office. So what are companies able to put in place to protect their mobile communications, both from network failure, viruses, theft and acts of God? Heather McLean takes a look...

Once the domain of senior executives, mobile smartphones are becoming prevalent further down in organisations. This means that there is a greater strain on systems, and any downtime will affect more people, leading to greater demand for disaster recovery products.

In essence, the mobile fleet disaster recovery market could be said to be as big as the number of GPRS, 3G connected, WiFi or Bluetooth handsets currently in use in a business environment, states James Browning, managing director at 20:20. "Given the growing number of malicious mobile viruses in circulation, it is perfectly feasible that one email circulated to the entire company could inadvertently infect the entire mobile fleet."



▲ James Browning, managing director at 20:20

There are many things to consider when looking at the impact of disaster on the mobile market, states Andrew Barnes. Barnes is senior vice president for corporate development at Neverfail, a software company focused on providing continuous availability and disaster recovery for Windows-based applications in physical, virtual or mixed environments. He comments: "Today, mobiles are portals into many corporate information systems ranging from email to SQL and Sharepoint systems. This means that estimating the size of the market means looking at these systems as well."

The ROI for smartphone users on disaster recovery is very compelling, explains Barnes. "Downtime of BlackBerry's is not tolerated, particularly in light of statistics such as those from RIM themselves, that BlackBerry delivers an extra hour of productivity per user per day," he states. "Clearly if there is any downtime that value decreases and could even disappear. Focusing on eliminating BlackBerry downtime is well received by both customers and resellers."

Mobile disaster recovery has exciting potential for those in the mobile channel willing to learn. Mobile devices are portals into corporate information systems, which means disaster recovery extends beyond the mobile fleet to become an essential requirement for Exchange, SQL, SharePoint and many others, so there are numerous follow on opportunities for sales, says Barnes.

The potential for resellers in this area is massive, Barnes continues. "The opportunity for disaster recovery for mobile devices is immense. One example of this is RIM BlackBerry. The BlackBerry handset depends

on interfacing with the BlackBerry Enterprise Server (BES) software installed in the corporate server room. Estimates of the installed base of BES vary, but there are at least 100,000, which means that there is a very addressable market just for this software."

Growth in demand

Barnes states that protecting BES availability for planned maintenance and unexpected outages is a rapidly growing area. He says in the UK, both O2 and Vodafone deliver options for high availability and disaster recovery managed services built on Neverfail continuous availability software. This approach by service providers means that users do not suffer and interruption of data services even when there is a data centre outage.

Curt Hopkins, head of enterprise mobility solutions at Vodafone UK, comments on why Vodafone partnered with Neverfail this year: "Earlier this year we responded [to the growing demand for disaster recovery for mobile devices] by forming a partnership with the software company Neverfail to provide continuous availability and disaster recovery solutions. As a result we now offer business customers a high availability and disaster recovery service for BlackBerry mobile email using the Neverfail software."

The service provided by Vodafone monitors the health of the entire email environment, including the server hardware, the network infrastructure, the application and the operating system. If any anomalies are identified, Neverfail will immediately take action to prevent loss of service. It will either automatically attempt to restart applications before they fail, switch over to a secondary server, or alert the IT staff so that no downtime or loss of service is experienced. Once the issue is resolved, they are automatically switched back to the main servers and neither users nor administrators are required to restart their applications.

Hopkins adds: "It's important for us to be able to offer this service because we can now offer enormous service expertise to protect critical parts of our customers' IT infrastructure. It's a significant part of our strategy to offer strategic managed services and indicative of the way the general telecommunications market is heading."

Barnes states that dealers are focusing on lost ROI as an important approach, in selling disaster recovery, as well as the disruption to senior managers and executives who rely on their BlackBerry access. Any disruption to



▲ Anthony Keyworth, director of product marketing, Orange UK

email flow and usability of BlackBerry's tends to quickly attract the attention of decision makers in the organisation, and these are the ones with the purchasing power for such technology, he says.

Commenting on how to sell disaster recovery for mobile fleets, Barnes explains: "The consultative approach is definitely required to help customers understand the impact of downtime, through to the ecosystem that supports information availability to the mobile devices itself. It also means that customers can better understand the importance of their organisation to be able to deal with unexpected failures, bearing in mind the whole point of a BlackBerry is to be available 24/7."

Solutions for SMEs

While there is a market for companies selling high end continuity and disaster recovery plans to large corporates, which can run into the thousands or even millions of pounds, there is also a market for more affordable solutions, states Anthony Keyworth, director of product marketing at Orange UK.

Orange Device Management falls into the latter category. It allows SMEs to change settings, enforce security policies and even wipe data from lost devices in case of a disaster situation. The solution also includes a 'scream' function so that if a device is lost or stolen it can emit a high pitched yell to draw attention to unauthorised people using the device, explains Keyworth.

Browning agrees that demand in the SME market is strong: "Selling disaster recovery



▲ Andrew Barnes, Neverfail, SVP Corporate Development

for mobile fleets demands a consultative approach and can often open the door for a dealer to sell additional software to a SME customer, such as sat-nav, push email, a credit card transaction application, or just a simple application that provides the end user with information like the weather forecast."

Prevention is better than cure, states Browning. He says 20:20 always recommends the installation of an anti-malware client when deploying mobile fleets to corporate sector clients, and his company has seen increased demand for SMEs. "There has also been a substantial increase in demand recently, no doubt fuelled by the increasing numbers of those users infected by a mobile virus, from all sectors of the market but especially from B2B dealers for their SME customers."

If disaster strikes, 20:20 has a range of products and services for dealers to implement. This includes remote handset OTA support as part of a Mobile Device Management package to a customer's Mobile Fleet Management Programme. This will provide a like for like device swap (pre-loaded with any applications that were initially installed) on the next working day in the UK or two working days across EMEA, to ensure normal service is resumed as soon as possible.

Horror stories

Yet at the moment, mobile disaster recovery and device management is being sold as a nice to have when really it is a must have, says Keyworth. Recent horror stories of



▲ Curt Hopkins, Head of Enterprise Mobility Solutions, Vodafone UK

laptops being left in pubs and on tubes have served as a good wake up call to business that basic human error can be one of the biggest risks to an organisation.

Keyworth says: "As a result of the heightened awareness of the role human error can play in causing a security breach, we expect products like Orange Device Management to move higher up the security requirements list in 2009. Application encrypted will also gain traction as the UK Plc's appetite for the delivery of more and more information on the move continues to grow."

He adds that disaster recovery packages such as that available from Orange provide a good additional sell for dealers: "Something like Orange Device Management is a good revenue driver for resellers. The fact it is web based, requires no additional software, and is very easy to use makes it an appealing proposition to SMEs, whose in-house IT skills might not be as developed as those of a larger organisation.

"When you consider how much potentially sensitive information is carried round on mobile devices, the ability to lock and even wipe a lost or stolen device from as little as £50 a year is becomes a very appealing proposition," continues Keyworth.

Dealers can expect to see more activity in this market in 2009, says Browning: "This is a market that can only grow substantially. As mobile devices become more complex with multiple access points, the scope for malicious intrusions will mirror the PC environment and what we have all seen happen across the internet." ■