Enabling
Secure
Mobility

While applications like e-mail, CRM, Sales Force Automation etc. are increasingly being accessed from the mobile, organisations need a definitive security strategy around the mobile platform. **By Varun Aggarwal**

IMAGING BY SUNEESH K

YEAR 2011 is not just an eventful year because of the disaster in Japan or the coup in Egypt and Libya or the increasing oil prices. For the first time in history, we've seen the greatest number of virus releases on the mobile platform that are a serious threat to both an individual as well as organisations. While a series of viruses have hit the mobile platform this year, there are at least a few that require serious attention.

More than 50 malicious apps were found this month on the Android Market. All of the offending apps contained a trojan horse with the potential to infect unsuspecting users' phones and steal their data. These are apart from the large number of malicious apps that already exist on third party web sites.

In another big development this month, the highly infamous Zeus malware that is known to steal banking data from PCs has moved to the Blackberry platform.

Therefore, it is no more casual threats on consumer devices that enterprise chose to ignore. Even enterprise mobile devices like the Blackberry are becoming a target of attacks.

A survey conducted by Symantec reveals that 53 percent of adults in India have fallen victim to mobile phone loss or theft, but despite that, only two in five Indians currently have a password protecting their devices. Moreover, Indians have some of the highest confidence levels in the region with regard to the use of software services on their mobile phones. Six out of ten Indians are comfortable allowing software on their phones to identify their location, and a similar number are comfortable with online banking. With mobile phones becoming such a central device in the lives of consumers, it is important to protect these devices, especially the data that is stored on such devices.

Smartphone threat a reality

Mobile threats aren't really new, but what's new is the increasing use of confidential data on the mobile and enterprise applications including financial applications, bank-

"IT Act 2008 doesn't differentiate between a computer and a smartphone. Mobile phones are now considered computers as per the law."

—**Adv. Prashant Mali**
President - Cyber Law Consulting

ing applications, CRM, SFA, or even the ubiquitous e-mail that make our very own mobile phone (or rather the smartphone) highly vulnerable.

More importantly, before you even realise, sensitive customer information might be leaked through the mobile platform and your organisation would be liable for huge penalties. "IT Act 2008 doesn't differentiate between a computer and a smartphone. Mobile phones are now considered computers as per law also in India, so security management framework of computers can be applied directly with some downward scaling," opines Adv. Prashant Mali, President - Cyber Law Consulting.

Heavy penalties can be imposed to an organisation if its employees accidently or knowingly leak out sensitive customer data. Even then, sadly, most organisations do not take mobile phone security seriously. There are also various challenges that enterprises face when trying to secure the mobile platform.

For starters, mobile platform is highly heterogeneous unlike the computer where you'll have perhaps only a couple of platforms. On the mobile side, you have the Blackberry, the Android OS, the Apple iOS, Nokia's Symbian platform, Windows Mobile and many others. Consumerisation of IT has become a reality. Businesses would demand the use of various platforms and it may be extremely counterproductive if you try to restrict them from using these devices.

Building the right security policy

Smartphone security should be treated in a similar way that laptop security is handled. The security challenges with smartphones is quite similar to what we have with laptops. Considering the growing computing power on the smartphone, there is very less difference left between a laptop and a smartphone in terms of what kind of applications can run on them and what kind of data can reside on them. Laptop security however has come a long way, and mobile phone security also needs to adopt a similar maturity curve.

Antivirus Policy: With the increasingly number of malware attacks, it is important that all the smartphones in the enterprise
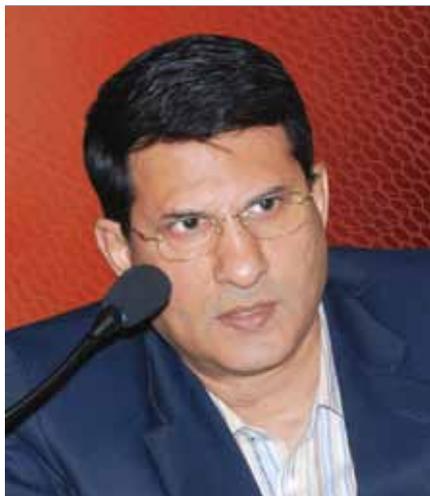
"DRM solutions can be considered to ensure the document expires after a specified time on the mobile."

—**Felix Mohan**
Chief Information Security Officer,
Bharti

are secured with an antivirus software. The challenge however, remains that there only a couple of antivirus software that run on all the platforms. One way of handling this situation is to make it a mandate for the employees to install an 'approved' antivirus' solution on their device and then take a refund from the company for the same. However, considering a drop in performance due to such solutions, users often disable them even if they are installed on the mobile. The key is to create awareness among the employees to activate and use the anti-malware solution on their mobile phones.

Access Rights Management: Just like any other device, access rights to mobile phones should need to be role based. An employee should get access to only those applications that he needs on the go depending on his role in the organisation. While an employee may have access to certain applications on the desktop, extending the same rights to

the mobile may not be prudent, considering not all employees need to access their applications outside the organisation.

Mobile Data Leakage Prevention: "Extending Data Leakage Prevention solution to the mobile is extremely important in order to prevent any security breach on the mobile. Loss of mobile is a common phenomenon and solutions such a DLP would prevent any confidential information from falling into the wrong hands," opines Felix Mohan, CISO, Bharti.

"As an extension to the DLP, DRM solutions can be considered to ensure a document expires after a specified time on the mobile. This would prevent any misuse of the document without worrying about how to secure it," Mohan added.

Mobile asset management policy: "You also need to clearly draw a line between personal and company assets. A company asset would typically include Blackberry, Android phones or iPad/iPhone. However, a personal asset could be pretty much any device," suggests Rishi Mehta, Chief Information Security Officer, Religare. Therefore, it is best to allow access to confidential data only on company assets and restrict any downloading of company data on personal devices.

Mobile camera policy: While many organisations do not allow you to carry cameras inside their office, cell phones are usually given a permit even though cell phones with cameras are for all practical purpose work exactly like the stand alone camera. When copying documents becomes difficult, employees with malicious intent can use the camera phone to capture sensitive data. To prevent this from happening organisations should look at tools that can remotely block the camera of the employee's cell phone once he's inside the office.

Training: More than anything else, it is the awareness campaign that can truly plug the security gaps on the mobile. Trainings could be through poster campaigns, SMS campaigns, classroom sessions etc.

Just like any other end point in the organisation, mobile platform deserves to be an important part of the organisation's security policy. As they say, we are only as safe as the weakest point in the organisation. And, mobile certainly is an extremely weak point for most organisations. ▣