



# Technology Brief...

June 5, 2006

J.Gold Associates, 6 Valentine Road, Northborough, MA 01532  
www.jgoldassociates.com jack.gold@jgoldassociates.com 508-393-5294

*Research, Analysis, Strategic Consulting*

## INSIDE THIS ISSUE

- 1 NOC-NOC: Who's There?
- 2 The Mobile Data Loss Epidemic
- 3 Abstracts of Current Research Reports  
Published for our Clients

## NOC-NOC: Who's There?

The war of words continues over which is better: email delivered wirelessly through a Network Operations Center (NOC), or pushed directly from server to device without an intermediary step. Those companies that deploy NOCs to deliver push email (e.g., RIM, Good) argue that because of cellular's switched circuit network and the roaming from cell to cell of data enabled devices, there is no way for an individual device to maintain its network address continuously, as would be the case within an IP based network, and therefore a NOC tied directly into various carriers can act as a buffer: with the NOC looking to the server behind the corporate firewall as a constant IP address which the server can then use to push out information. The NOC receives that information, and acts as a switch to then route the information to the device based on the address it has obtained from the specific carrier.

Detractors of the NOC system argue that since the data must be routed through a server in the NOC, it is subject to possible security breaches. Further, since the NOC routes the information to the devices, should the address translation table be defective, it could send a data stream to the wrong device and allow the user of that device to read a message intended for the private use of another party (this has happened in the past but is a very rare event). However, since any adequately secure system that transmits data through a NOC would encrypt the data from the originating server straight through to the receiving device, the loss of any data within a NOC is a minimal risk and security breaches on that data are highly unlikely.

---

*"..There is currently room for both NOC and no-NOC based mobile solutions.... in the future (in 3-5 years), the debate will become irrelevant, as NOCs will no longer be needed."*

---

Those companies utilizing non-NOC based systems (e.g., MSFT, Nokia) argue their system is superior as it eliminates the middleman. However, mobile devices change addresses frequently due to network induced changes. In order for these systems to work, the device must regularly "ping" the server, essentially saying to the server "here I am and this is my address, send me any data you may have for me". One effect of this schema is that the device has to regularly transmit "pings" in order to initiate receiving traffic, thus shortening battery life. Further, should the device stop the "pinging", the server will not know where to deliver its data (though arguably if the pings stop, it is because the device is off

line or powered off, both of which would cause the data not to be delivered in any event).

The NOC vs no-NOC debate has recently moved beyond email and into the mobile applications arena. Antenna Software has made a business of running a NOC in its NJ location specifically for mobile field force applications. The application runs on its server, and queries the SAP, Siebel, Oracle, etc. data behind the corporate firewall, formats it for the device and sends it out (or receives it back from the device and reverses the process). Though most companies still prefer to run middleware servers for such tasks from behind their own firewalls, Antenna is seeing a ready market among many companies with relatively small deployments (tens to hundreds of seats) who don't want to manage the complexity of a middleware application (e.g., iAnywhere, Intellisync).

**Bottom Line:** There is currently room for both NOC and no-NOC based mobile solutions. Both have proven to be reliable and secure. The argument over "push vs ping" is a moot point for most companies and users. Companies should choose based on cost, reliability, security and overall performance/capability. As we move to fully IP enabled wireless networks in the future (in 3-5 years), the debate will become irrelevant, as NOCs will no longer be needed. Devices will be assigned a true IP address, so no address translation will be required, nor will the regular pinging back to the server (though because of legacy switched network infrastructure, NOCs may not go away for some time).

## The Mobile Data Loss Epidemic

Near daily reports of loss of sensitive information compiled by organizations and stored within their computers is making the public acutely aware of the risks associated with companies obtaining and keeping sensitive information. Indeed, what this is teaching most consumers is that many companies can not be trusted to maintain enough security to keep that sensitive information repository from being exposed and the data contained therein lost (in the best case), or stolen and used for identity theft and fraud (in the worst case). Recent notebook data losses, e.g., US Veterans Administration exposing 2.6M records, Fidelity Investments exposing 200K records, and many others, cause real and substantial damage to companies, and will ultimately provide fuel for public sanctions to be imposed on offending organizations (several regulations are already in place and many more are being proposed).

---

*"...Companies should add security to mobile devices immediately, before a major breach occurs and causes the company substantial monetary damage...."*

---

We believe all companies must take immediate steps to safeguard sensitive data, especially that data which is contained on mobile devices (primarily notebook computers currently, but increasingly other portable devices, e.g., smart phones, PDAs). We have highlighted a number of

steps companies should follow to secure data and assure regulatory compliance in our recent White Paper, *Compliance in the Mobile Enterprise* (copies available upon request). Further, we believe that while certain industries are more prone to the threat of loss due to the type of records they keep (e.g., banking, health care, insurance), nearly all industries have sensitive data which they collect and must defend from exposure. Immediate and forceful measures are part of the cost of doing business. Such measures taken by organizations must be more than cosmetic, as any data loss can cause major financial damage to a company.

We estimate companies will spend approximately \$35 in notification costs for each exposed customer. So, in the case of Fidelity, it would have cost \$7M just to notify all its customers that their data had been exposed. However, the cost does not stop there. Remediation costs, such as a credit monitoring service which Fidelity offered each customer to allow them to monitor that no fraud is taking place, can add up to several million more dollars. And the loss of some percentage of its angry customers, perhaps as much as 20% of its clients, will add even more to the total cost of the data breach. It is also likely that Fidelity will ultimately be assessed fines/penalties from government agencies, resulting in total monetary loss to Fidelity from this one data breach in excess of \$10M.

We strongly urge all companies to immediately add security and management suites to all mobile devices carrying any type of sensitive data (i.e., virtually all devices). At \$100-\$150 per device, the cost is relatively low compared to the potential exposure caused by even one device being involved in data loss. Many vendors of security management products focused on the mobile user exist (e.g., iAnywhere, Credant, Pointsec, Trust Digital, Good Technologies, and others), as do secure connectivity solutions (e.g., Ecutel, iPass, Padcom, Columbitech, etc.). We do not believe that current Microsoft OSes offer adequate protection for possible mobile device exposures, although newer OSes (e.g., XP) at least provide some level of disk encryption, though it is rarely enabled. This is a good first step, but not sufficient. The upcoming Vista Ultimate with BitLocker encryption for enterprise users will offer more security, but even it will have to be supplemented with third party products to achieve adequate protection of sensitive data, and lesser levels of Vista will offer minimal protection.

**Bottom Line:** Companies should add security to mobile devices immediately, before a major breach occurs and causes the company substantial monetary damage, as well as loss of good will which will be hard to repair. The relatively small cost of these products offers a substantial ROI if they prevent even one data loss episode. In any event, they provide an insurance policy that should be required for any company which provides their users with mobile devices.

## Abstracts from Current Research Reports Published for our Clients

---

*These reports are  
delivered to our  
subscribing clients.  
Contact us for  
information on how to  
obtain these reports.*

---

### **RIM's Next battle: No, Not MSFT, Nokia.....**

RIM has been a leader in the enterprise wireless space for years, starting with the play for wireless email, but increasingly branching out into enterprise mission critical apps (e.g., CRM, SFA, logistics, field service). It is now facing an upsurge in competition from device manufacturers (e.g., Palm, Motorola, Nokia, HTC), and SW middleware players (e.g., Good, Visto, Nokia/Intellisync, MSFT). Indeed, many industry watchers have assumed that MSFT and its Windows Mobile platform powered phones, with an affinity to MSFT based apps, and its large installed base of Exchange servers, would overpower RIM and make RIM a minor player within the next 3-4 years. We do not believe that this will be the case, as MSFT and its partners in phone manufacturing, continue to stumble (e.g., as we reported, the latest Windows Mobile powered device, the Motorola Q, just released in May 2006, does not even have the most recent version of Windows Mobile, so it can not work with Exchange Direct Push email). In fact, in the next 2-3 years, we see RIM's primary competition coming not from Redmond, but from a different location; Espoo, Finland. But will Nokia succeed in eclipsing the current market leader?

### **The Cost of Deploying Microsoft Exchange Push Email (Introduction)**

Microsoft has recently released its latest version of Exchange Push email service for wireless devices. It claims that it will allow users of Exchange to eliminate third party middleware solutions (e.g., RIM Blackberry Enterprise Server, Good Technologies GoodLink) and thus provide a cost advantage to those users who deploy it. Indeed, with this product Microsoft believes it can overpower the current market leader (RIM) and capture the majority of Exchange-based wireless email enterprise (and even SMB) deployments. However, after examining the solution, we have come to several conclusions on the true cost to organizations deploying this solution, and the prospects of Microsoft becoming dominant in this market segment.



#### **J. Gold Associates**

6 Valentine Road  
Northborough, MA 01532

**Phone:**  
508-393-5294

**Web:**  
[www.jgoldassociates.com](http://www.jgoldassociates.com)

**E-mail:**  
[Jack.gold@jgoldassociates.com](mailto:Jack.gold@jgoldassociates.com)

***Research, Analysis,  
Strategic Consulting***