Inadequate Approaches to Contact Optimization

Many organizations in both the government and private sectors have approached the challenge of managing contact information, and reaching employees, through a variety of methods. Nearly all these approaches are incomplete and have drawbacks in normal circumstances that are magnified in an urgent situation.

Contact Management Strategy	Shortcomings
The IT department updates contact data in the global address list (GAL).	• The GAL may lack some contact information that resides in other databases and files in the company. • Usually, the GAL has many records that are sparsely populated, with a number of fields empty. • IT personnel are highly paid, relative to the repetitive work of obtaining updated information. They are needed for other IT priorities. The updating process is rarely automated. • Obsolete contacts are rarely deleted. • Access to a large GAL on a high latency (slow) connection is inefficient compared to accessing a local copy on the handheld device.
An Excel file is maintained and distributed by e-mail periodically.	• Maintaining the master list is labor intensive and will be less accurate than self-service updates • Unsecure. Document can easily fall into the wrong hands. • Multiple departments, multiple cross functional teams might create and maintain lists with redundant and sometimes conflicting information. • The list is rarely available in user contact folders where it is most needed. Even less frequently, it is loaded correctly into their smart phones. • When it is needed urgently, the list might be unavailable outside the office. • This method does not scale well.
Laminated wallet cards with key contact data are distributed intermittently.	• Monthly labor and printing costs add up. • Cards can be out of date within a few days. • This solution does not scale well. • A lost wallet card can violate employee privacy policies. • Obsolete cards must be collected and destroyed to insure privacy.
Individuals inform their co-workers each time their e-mail or phone(s) change.	• Each user must prepare and address their notification to potentially large groups of people. • Manual intervention and time required of each recipient. • Recipients can be inadvertently omitted or inappropriately included. • This method does not scale well.

Rev. February 2011

HR dept. distributes hard copies of employee contact information.	▸ This is unsecure; booklets easily lost or stolen. ▸ Despite warnings, these booklets frequently end up in the hands of recruiters raiding your staff. ▸ Hard copy becomes outdated quickly. ▸ Users with PIMs must manually add data, but data changes are not marked in the hard copy to ease that task.
IT managers implement intranet web applications to make contact information available via browser.	▸ Users with PIMs are not informed when data that is pertinent to them has changed. ▸ Users with PIMs must manually add new data to their handhelds. ▸ No Caller ID Reverse lookup benefits
Internally developed system, with data updated at intervals by a group or department.	▸ The update process is usually not automated, and therefore is labor-intensive and more error-prone. ▸ Internally built systems usually have only ¼ to ½ the functionality of an independently built system like itrezzoAgent. ▸ The developer who built and maintained the system leaves the company, or IT has other mission critical priorities. ▸ Any particular group that handles updates may not include all new phones used by employees. The most reliable method to obtain all information is to have each employee supply it.
Internally developed contact data system which updates from payroll system.	▸ Payroll systems rarely include or update the data which changes most frequently: cell phone and home phone numbers.
Employees update their contact data at an external, Web-based portal. Some mass notification systems use this approach.	▸ Instructing employees to click on an email link to the external website, and then enter PII (Personally Identifiable Information) conflicts with a security best practice: employees should not follow links from email and divulge sensitive information.

About   i·trezzo

Since 2001, itrezzo has developed enterprise-grade infrastructure and applications that solve the problems of enterprise contact optimization (ECO) and sustain communications during emergency situations. One of the first third-party developers for BlackBerry, **itrezzo** is trusted with servers deployed behind the firewall of over 1000 companies and government agencies, including the Department of Justice, Department of Veteran Affairs, Department of the Treasury, The Federal Communications Commission, US Army Corp of Engineers, Miami Dade Schools, The Carlyle Group, HBO, Lockheed Martin, Shell Oil, and The Blackstone Group.

Rev. February 2011