For Immediate Release - The Slavin Group appears in internet.com™

This article is reproduced from http://networking.earthweb.com/netsysm/article/0,,12089_1453451,00.html

Should You Offload Messaging Management?

By Jacqueline Emigh

Administering e-mail and other messaging functions can eat up a lot of management resources. As a result, some organizations are now turning instead to service providers, under either traditional outsourcing, hosted management, or remote management scenarios. Aside from cost savings, providers claim to provide guaranteed service levels, as well as expert help with problematic platforms, viruses and spam. Some administrators, though, still oppose working with providers, often citing privacy and security concerns.

Kansas Farm Bureau Services (KFBS) is one example of a relatively early adopter. The bureau hired US Internetworking (USi) for Exchange 2000 migration services and messaging management. Amy Grothaus, KFBS's Web manager, cites four main reasons for the decision: recruitment issues; a requirement for "24/7 availability in a non 24x7 shop"; system uptime; and "a need to focus current staff on other key enterprise initiatives."

In fact, some analysts are predicting a boom in messaging services over the next few years. "Outsourcing can significantly reduce the cost of ownership of a messaging system," maintains Michael Osterman, principal of Osterman Research. Other reasons for teaming with a provider include more predictable costs; guaranteed service levels; better contingency planning; and "a single point of contract for resolving messaging system failures and other issues," according to Osterman.

"Not having to manage the messaging system on a day-to-day basis means that IT can take a more strategic view of key issues," the analyst adds.

"If e-mail outsourcing makes economic sense for your company -- and you want to free your people up from a lot of busywork -- then by all means go ahead," recommends Jon William Toigo, an independent industry analyst specializing in storage and network management.

Still, though, some network managers aren't exactly enthusiastic about managed messaging. "You really need to do a cost-benefit analysis to determine whether outsourcing is right for your company," suggests Zachary A. Slavin of The Slavin Group, a systems and services provider in New York City .The cost-benefit analysis should take into account the cost of hardware, software, and licensing, along with the entire cost of administration.

"You need to look at the cost of salary and benefits for the e-mail administrator, as well as the cost of having a supervisor on call when the administrator is out sick, for instance," Slavin adds.

In traditional outsourcing, the outsourcer comes into your company, and managed outsourced functions on-site. Although managed hosting typically costs less than traditional outsourcing, it offers less customization, too, observes Tom Kucharvy, an analyst at Summit Strategies..

Beyond costs, a number of other factors can tip the scales in one direction or the other. Companies can get be more likely to gain from either managed hosting or traditional outsourcing if they're having trouble attracting and retaining good technical staff, or if they're seeking very specialized skills.

Factors that tend to drive decision-makers away from outsourcing include security concerns and a lack of confidence in outside providers, particularly if the customer has already been burnt in the past.

"If you have confidential matter residing on a server, it's essential to keep the data from prying eyes," according to Slavin.

"Companies are mainly afraid they'll lose granular levels of control," counters Philip Pridmore-Brown, product line manager, enterprise messaging, at Critical Path.

Kucharvy also points to a number of temporary factors that could be holding up some deployments. These include a battered image of hosting providers; shaky financial positions of some of the players; lack of sunsetting announcements by some vendors, "and therefore, a lack of urgency in upgrading;" slow emergence of remote management tools; and many customers' "underestimates" of the costs of running their own messaging systems.

Some vendors, including Critical Path and Syntegra, are now providing their messaging solutions in a choice of two ways: as a product only, or as part of a managed service.

Complexity?
Actually, big enterprises are being quicker to apply traditional outsourcing to the messaging picture than mid-sized corporations, according to Kucharvy.

"The largest corporations have been leading the move to full outsourcing, to get the service levels they need at lower costs, as well as to free up their people from really trivial administrative tasks," says the Summit analyst.

Some companies that are still hanging back "are not comparing apples to apples - they're only counting the cost of the server and the cost of the license, for instance," Kucharvy adds/

For their part, vendors have been carving the messaging outsourcing market into a variety of niches. Syntegra, for instance, sells into both the corporate and service provider markets.

"Most of our corporate customers are very large. If they're not large, their networks have some level of complexity. The typical profile for mid - sized customers is that they've been growing through mergers or acquisitions, and that they now find themselves with a bunch of people who need to be integrated into the corporate networking system," says Judd Frahm, Syntegra's VP of managed services.

Meanwhile, though, some SMBs say that hosted messaging offers just the sort of turnkey solution they want. Grothaus says she was generally satisfied with the USi-assisted Exchange 2000 migration, although it involved some issues around connectivity, as well as the need for user interaction to update profiles.

At this point, KFBS is handling new account setup, but relying on USi for other aspects of messaging management, according to Grothaus.

Meanwhile, Mi8 recently added the International Amateur Athlete Federation (IAAF) to its roster. Without the use of hosted management, the organization might have needed to install a messaging server at each of its 400 offices worldwide, maintains Mi8 CEO Dave Castellani.

Mi8 is moving more adding more remote messaging management to its hosted management offering, according to Castellani. Meanwhile, in a non-exclusive deal, traditional outsourcer EDS is now reselling Mi8's services.

Manhattan, Kansas or New York City?
"Being in Manhattan, Kansas, we're two hours away from a major city - which is Kansas City - and it was hard at the time, with the dot coms, to recruit technical talent to this area. So we knew we couldn't manage (Exchange 2000) inhouse," according to the KFBS's Grothaus.

"You might want to outsource if you're unable to recruit and retain competent IT staff, whether because you're small, or because you're in an undesirable geographical location," echoes Slavin.

"If you're a small company, it can be more cost effective to outsource, whether you're located in Kansas or in New York City or San Francisco," agrees Philip Pridmore-Brown, product line manager, enterprise messaging, at Critical Path.

Running in the background?
Advocates argue that outsourcers can manage messaging more efficiently due to economies of scale. Moreover, messaging is seen as especially suitable for outsourcing, since it usually isn't integral to the customer's core business.

"Messaging is strategic, but it's kind of been conquered and solved. It just needs to be running in the background, without problems. If I'm a chemical company, I'm in the business of creating chemicals, not providing networking services. If I'm the CIO, maybe I want the internal staff to be more focused on security, or on managing business applications," Frahm illustrates.

On the other hand, managing e-mail in multi platform environments can be a tough nut to crack.

"I have an environment using a Novell (NetWare) 4.11 server and GroupWise 5.2. Everything is functional. (However), the ultimate decision maker in the office is unhappy with Novell, but loves GroupWise. I have a new server to play with and see if it will be capable of replacing the Novell server. The problem is that it is a Windows 2000 server," writes one administrator, in an Internet newsgroup.

"When I put the checkmark in "workstation only"on the Novell client so that the Win2K server is NOT connecting to the Novell server, Console One can't see anything! No NDS objects, and especially no GroupWise objects. So in that mode I can't adminster anything NetWare/GroupWise-related. Yet GroupWise functions and I can get into mailboxes. I need to be able to log into just the Win2K server and administer the stuff and GroupWise, without logging into a Novell server as a client."

From Windows 2000 to DecNET

Many outsourcers and managed hosting firms specialize in specific platform niches. These can run the gamut from emerging e-mail platforms like Exchange 2000, to mainstream environments such as Exchange 5.5, Lotus Notes and GroupWise; to legacy systems like DecNET and IBM's old PROFS.

"If you're running a legacy system on a mainframe, you might want to outsource management to someone who specializes in that area. Alternatively, you might want to bring in a hosted provider to give you one of the newer solutions," Slavin suggests.

In any case, it's a good idea to find someone with demonstrated experience in managing the platform you choose, whatever it may be. Grothaus found that out the hard way. Before working with USI on Exchange 2000 migration, KFBS hired another outsourcer for Exchange 5.5 migration and management. "We encountered multiple issues of an unstable environment during two-week migration," she recalls. The previous outsourcer also failed to implement the password policy KFBS had requested, in several attempts.

"Each messaging system - whether it's Microsoft Exchange, Lotus Notes, or whatever - has its own unique issues," Slavin concurs. Interliant is one example of an outsourcer that runs a Notes practice.

Many outsourcers specializing in Exchange follow managed hosting and/or remote management models. These include USI and Mi8.

Some outsourcers prefer to use their own proprietary messaging servers, though. "Exchange wasn't designed to scale at the level of the Internet," according to Pridmore-Brown. Critical Path's messaging server runs on Solaris, Linux for S/390, and AIX, as well as on NT.

Syntegra offers customers a choice of either the Syntegra messaging server or Microsoft Exchange. The Syntegra messaging platform operates on Linux, Solaris, AIX, HP-UX, and Tru64.

Syntegra will also manage Lotus Notes, Novell GroupWise, and even the old DEC All-in-One, "but this is more a matter of creating gateways to mainstream Exchange or Syntegra," says Frahm.

Other players converging on the messaging space range from outsourcing giants like IBM, CSC, Hewlett-Packard/Compaq and the "big 5"; to telecom carriers such as Sprint and BT; to smaller specialists such as United Messaging, for instance.

Out with spam, in with IM?
Syntegra also specializes in anti-spam, anti-virus, instant messaging, and wireless messaging management, according to Frahm. On the anti-spam side, Syntegra is partnering with Brightmail.

Just about every outsourcer in existence, though, is now claiming to pay special attention to spam and viruses. "We're very focused on eliminating spam and viruses before they ever hit. If customers don't have this, the repercussions to their business can be enormous," maintains Pridmore-Brown.

According to a survey conducted by Brightmail, the total volume of spam skyrocketed by 46% between November, 2001 and January, 2002. Over the same period, though, the total volume of e-mail rose just 14 percent.

"You're already beginning to see more of a tilt toward instant messaging (IM), and away from e-mail, on a regular basis. You might see that going forward this will accelerate, particularly with the continuing growth of spam," predicts David Strassel, an analyst for the Intermarket Group.

Others, though, think that spam and viruses can be easily dealt with inhouse, assuming a company has the resources. "There are hardware and software products readily available for both problems, depending on what you want to do. You can insert antivirus and antispam controls in your firewall, for instance," Slavin says.

Regulations a driver, too
In the current regulatory climate, companies in fields like finance and health care are having a hard time figuring out which e-mails need to be archived, and for how long, Toigo notes.

NAC requirements, for example, dictate that messages dealing with broker- dealer solicitation need to be archived for seven years, sources say.

"I think this is a driver for outsourcing, too. Different clients have different interpretations. We get quite involved with customers' legal people," according to Frahm.

Loss of control?
Despite these advantages some organizations are seeing, others continue to resist managed messaging.

"In some instances, the loss of control can be frustrating for clients. So we try to stay in line with them, rather than being just an extension on the other side of a wall," Frahm acknowledges.

While conceding that other factors can be barriers, vendors tend to argue that security and privacy shouldn't be one of them. For one thing, organizations can encrypt their e-mail, according to Mi8's Castellani.

Moreover, organizations outsource other functions, without worrying that the outsourcer will commit abuse. "Most companies outsource their payroll, for instance. And actually, e-mail is far more interesting for people that work inside a company, anyway," Castellani contends.

Organizations should, however, check out the viability of the outsourcing firm, and to make sure the SLAs being offered are realistic.

"Companies should look for an outsourcer that has financial wherewithal, and for one that is also willing and able to live up to its SLAs," cautions Frahm.

Jacqueline Emigh *(pronounced "Amy") is a 12-year veteran of computer journalism. She is currently freelancing for several leading technology and business publications. She was previously a senior editor for Sm@rt Partner Magazine, and before that, a bureau chief for Newsbytes News Network.*

August 28, 2002

For Immediate Release - The Slavin Group appears in internet.com™

This article is reproduced from http://networking.earthweb.com/netsecur/article/0,,12084_963021_2,00.html

Dealing with Network Security Scofflaws

By Jacqueline Emigh

When it comes to security, some end users just don't get it, according to many network managers. Intentionally or not, these troublesome users keep jeopardizing security by downloading forbidden attachments or visiting off limits Web sites. When technical interventions alone don't ward off these problems, some administrators are resorting to social sanctions, either informally or through company policies.

Parrish S. Knight is one network manager who's faced down pesky users. "In our particular case, we were infected (with a virus) by someone who refused to follow safe computing practices. Everyone had been warned not to open e-mail attachments from a particular proxy server, but she did so, anyway -- not just once, but twice," says Knight, an Internet and LAN administrator at Market Access International.

Knight's also found himself up against people who eat up bandwidth during peak network periods by spending too much time on Napster.

At other companies, users have left corporate networks wide open to viruses by circulating spam mail, according to Paris Trudeau, product marketing manager for SurfControl.

Knight has dealt with some problems at his company by speaking directly to either the abusers or the abusers' bosses. Also, to "help protect users against themselves," he's using anti-virus software on both a proxy server and users' desktops. The WinProxy server updates its signatures every three hours. The Symanetic desktop software is also configured for automatic updates.

Although individual companies' strategies vary, other frequently used technical interventions include firewalls; asset management and monitoring tools; content filtering software such as SurfControl's products; and subscriptions to signature database lists.

Though not in the same category as antivirus software, SurfControl's tools can be configured to screen out e-mails with.spamlike subject lines and .vbs and double file extensions, for example, Trudeau says.

Often, however, technology interventions themselves aren't enough. For one thing, anti-virus software can't do much of anything to protect against a brand new virus, until the first incidences of that virus have been detected and reported.

"What's most important, really, is a company-wide security policy, in which employees are fully informed and aware of prohibited conduct and proper usage," maintains Zachary A. Slavin of The Slavin Group, a systems and services provider in New York City.

Echoes another administrator: "The potential value of published security policies is reached when something occurs, and you attempt to discipline the employee who has flagrantly breached its conditions."

It isn't necessarily easy, however, to arrive at workable policies around controversial areas such as employee monitoring, personal Web surfing, and personal use of corporate e-mail addresses.

"I think a certain amount of personal e-mail usage is okay -- if users occasionally get in touch with their folks, for instance. But how much is too much? Where do you draw the line?" asks Knight.

"If someone is surfing the Web between noon and 1:00 pm each day, maybe that's not an issue," Slavin says. "If someone is doing nothing but downloading files from 9:00 am to noon, that's probably an issue. But you can't overdo things either, or you can run into problems with productivity and employee retention. You can monitor employee usage, but you don't want to get into a 'keystroke Big Brother' situation. It's a balancing act. If the policies are making people miserable, the company might end up losing money due to high employee turnover."

Moreover, just because a policy has been put in place, employees won't necessarily abide by it. Patrick Hinojosa, general manager at Panda Software, points to the need for specific language.

"The policy needs to be clear and unambiguous. It can't say just, 'Don't do bad things.' It has to say something like, 'You aren't allowed to use Web-based e-mail ever, under any circumstances," Hinojosa says.

Some recommend getting written signatures to be able to prove -- in court, if necessary -- that employees are aware of the company's security policies. Slavin, though, sees HR-sponsored security training sessions as a better way. "HR can just go to the employee training file for documentation," he observes.

Enforcement is essential, experts agree. As punishment for breaking security policies, employees can be reported to their bosses, banned from the Internet at work, suspended, or in some cases, even terminated from their jobs.

Increasingly, IT departments are starting to team with HR on both security training and policy enforcement. "For enforcement to be effective, though, HR must act right away, the first time someone violates policy. Otherwise, employees will tend to ignore policies. Sanctions should then be applied uniformly, to all perpetrators. It isn't a good idea to just 'put on a head on a pike,' or in other words, to 'make an example' out of someone," says Hinojosa, who was a VP of HR at another company before joining Panda.

Slavin says that one of his customers is already practicing IT/HR teamwork. "Mainly, though, it isn't that prevalent yet," he adds. Meanwhile, administrators at some companies are trying less formal enforcement methods.

In organizations without clear cut security policies, some network managers are reporting troublesome users directly to top management.

"Unless there's already a high level of interest among executives, though, this will only work if you emphasize the potential consequences of user actions. You can't just say, 'I don't like users to download these particular kinds of files.' Then the execs will be thinking, 'Why is he bothering us with this?' You have to tell them, for example, that viruses can cause a loss of critical data."

Generally speaking, many administrators are finding formal policies the best way to go. "I have learned that unless (a policy) is on paper, it doesn't hold up," says one administrator. "Implied security policies don't cut it. What I consider 'wrong' may not be considered 'wrong' by the next guy."

All too often, though, companies don't even implement security policies until an incident actually takes place. Notes Hinojosa: "Then the executives will be saying, 'Oh my God, our accounting reports are gone! How could this have ever happened?'"

Jacqueline Emigh *(pronounced "Amy") is a 12-year veteran of computer journalism. She is currently freelancing for several leading technology and business publications. She was previously a senior editor for Sm@rt Partner Magazine, and before that, a bureau chief for Newsbytes News Network.*

January 28, 2002

For Immediate Release - The Slavin Group appears in Enterprise Storage Forum.com

This article is reproduced from http://www.enterprisestorageforum.com/industrynews/article.php/3066211

Businesses Report Systems Glitches from "Big Blackout"

August 20, 2003 By Jacqueline Emigh

As last week's Big Blackout of '03 begins to fade into history, businesses are starting to report the first crop of resulting problems with storage and other computer systems. IBM Global Services (IGS) and other consultancies began hearing from customers from last Thursday through early this week, with problems blamed on the outage ranging from lost data to damaged hard drives and "fried" computer monitors. Meanwhile, systems at larger companies like Computer Associates (CA) appear to have emerged from the blackout unscathed.

At IBM's business recovery center in Sterling Forest, NY, the focus was on fast data recovery. "There were some customers who 'declared disaster,'" acknowledges Pat Corcoran, chief of global marketing and business development for IGS's Business and Recovery Services Unit.

Financial firms of various sizes — "all sizes except for the very largest" — arrived at Sterling Forest on Thursday and Friday, often with backup tapes in hand, according to Corcoran. "They needed to recover their businesses, and they couldn't get into their own facilities." The cafeteria at IBM's Sterling Forest plant, ordinarily closed after lunch, stayed open for dinner to feed hungry victims of the power outage.

Sometimes on their own, and sometimes with IBM's help, customers mounted backup tapes and recreated their business environments, relying on data from their last backups. "Some people do backup several times a day, but others do backup only at midnight, for example," notes Corcoran. Other IGS customers use data vaulting.

The Sterling Forest site itself had lost electricity Thursday afternoon, but IBM kept operations running with a diesel-powered generator.

IBM: 'Declared disasters' might have been higher before 9/11

Corcoran speculates, though, that the number of declared disasters from a massive power failure likely would have been much higher a few years ago. Many organizations have taken the lessons of 9/11 to heart, he contends. "Instead of waiting every three years, businesses are updating their business recovery plans a lot more often."

Corcoran also detects a rise in the number of customers with colocated mirrored sites. "These are the people, though, who are the most proactive. Their on-site facilities tend to be fairly sophisticated, too."

'Databases don't like to be shut down'

"I've heard that some companies might have experienced data loss or corruption because of the electrical blackout," says Zachary Slavin, president of The Slavin Group, a business systems consultancy headquartered in New York City. While Slavin didn't mention specific company names, he did say that none of his own customers had been impacted.

Most of The Slavin Group's clients are mid-sized financial firms. Some customers are hosting mirrored sites at the consultancy's data center on Long Island.

"Databases don't like to be shut down when data is being moved. You need to keep the computers online until they can be shut down properly. 'Smart UPS' is best practice. You want the UPS to be able to signal the computer to start shutting down," Slavin advises.

When dealing with critical data, it often makes sense to combine UPS with both electrical generators and mirrored backup sites, according to Slavin. A battery-operated UPS typically runs for an hour or less, while most generators, on the other hand, can operate for up to two days, even without refueling.

Meanwhile, ActionFront Data Recovery Labs received about 260 phone calls on Monday, twice the typical daily average of 130 calls. ActionFront's offices are located in Buffalo, Atlanta, Chicago, Santa Clara, and Toronto. Almost all the calls represented "new business," reports Nick Majors, company president.

"A lot of businesses were still closed on Friday. Even if a business was open, people were still trying to reconfigure systems by themselves last week. By Monday, though, our phones started ringing all day along."

Most callers reported damaged hard disk drives, but others pointed to compromised RAID systems or glitches in "advanced operating systems."

Majors suspects, though, that some reported computer troubles are not really blackout-related at all. "It's possible that some people are blaming problems on the power failure, just to cover up for their own failures," he theorizes.

CitySoft, Inc. also received twice the usual number of calls at the start of this week. David Rosenthal, president of the New York City-based IT consultancy firm, says he expected to get calls about hard drive problems stemming from abrupt shutdowns. A number of callers, though, got in touch with CitySoft about "fried" computer peripherals.

"At one company, all monitors from one particular manufacturer got fried. At another, all printers from a different manufacturer got fried. I can't really blame the vendors, though. I think there must have been some sort of a big power surge about a microsecond before blackout. This type of thing would be outside the vendors' usual design parameters."

Computer Associates has a mirrored data center — but didn't need it

Big systems vendor Computer Associates has a pre-established backup site in the Midwest that mirrors its main data center at company headquarters in Islandia, NY.

"We are headquartered on Long Island. If we'd gone 50 miles west (of Islandia), the mirrored site would have been located in New York City. So the company made a decision that if we had to go farther west anyway, we might as well put the site in the Midwest," says Walt Thomas, CA's CIO.

The Midwest site is colocated at another CA facility. Above and beyond their usual job duties, staff at the Midwest facility are trained to take over emergency backup data center operations.

As things turned out, CA didn't need to resort to the mirrored data center at all last week. The lights came on in Islandia at 4 AM on Friday morning.

Until then, CA temporarily depended upon on-site electrical generators. "If we'd run out of fuel before the power came back on, we could have then refueled the generator — although whether we could have gotten the supplies from the fuel companies is another question," says Thomas. "On the other hand, it's more costly to implement a mirrored data center than to use a generator. These are the kinds of tradeoffs you have to weigh."

An Ounce of Prevention...

All in all, disaster prevention measures and recovery systems appear to have held up remarkably well in their most widespread test in recent memory. With damage to critical corporate data apparently nominal for most companies, the tried and true adage of "an ounce of prevention is worth a pound of cure" appears to have proven its point once again.

Jacqueline Emigh ***(pronounced "Amy") is a 12-year veteran of computer journalism. She is currently freelancing for several leading technology and business publications. She was previously a senior editor for Sm@rt Partner Magazine, and before that, a bureau chief for Newsbytes News Network.***