E-mail has replaced the phone as the most critical internal business communications system for most companies. Yet many organizations do not apply the same operational rigor to e-mail that they apply to other mission-critical business systems. We believe companies must apply traditional data center discipline to e-mail infrastructures to maximize system stability and efficiency.

E-mail is going through an evolution that is somewhat circular in nature. The first e-mail systems were host-based, and although limited in functionality, they were extremely stable and centralized in data centers. Shared-file LAN e-mail systems appeared next, which were more functional but far less stable, and multifunction LAN administrators typically performed management locally. LAN mail systems evolved into a client/server model, which was highly functional and provided more stability than LAN architectures, but the systems still delivered less uptime and were more costly to operate than the original host systems. Currently, client/server mail systems are typically managed by a combination of both local and centralized human resources. We expect that architecturally e-mail systems will remain largely in client/server mode through 2007, albeit with an increasing trend toward larger, more centralized servers (followed by a thin-client model). We believe it is desirable to return e-mail to the discipline of data center management.

In many ways, the e-mail market is already moving in this direction. As part of the upgrade to Exchange 2000/2003 or Domino 6.x, most organizations are consolidating servers and removing small-office e-mail servers in favor of remote WAN access to centralized e-mail servers, often as part of larger server-consolidation efforts. At the same time, e-mail management duties are quickly migrating from local control to centralized control, with the help of remote monitoring and administration of decentralized servers. We view these as positive developments, but we believe companies must adopt the additional data center disciplines typically applied to other mission-critical applications (e.g., inventory management, order processing/billing systems). There are six critical disciplines required for optimal e-mail operations: change management, configuration management, asset management, systems monitoring, capacity management, disaster recovery. To these categories we add requirements that are more e-mail-specific: network and storage management, as well as hygiene requirements (see Figure 1). Ultimately, the goal is to maximize e-mail system uptime while limiting impact on other enterprise application and infrastructure components. We believe that during the next several years, 99.9% uptime will become mandatory and 99.99% uptime will become desirable (see Figure 2).

All of these disciplines are deeply dependent on each other and require a holistic approach from IT organizations:

- **Change management**: Change management for e-mail entails consideration of the impact that any code, configuration, upgrade, or deployment changes have on both end-user operations and e-mail-dependent applications. Organizations must establish a rigorous impact-assessment and testing program for new versions of e-mail software and operating systems, including patches, hot fixes, and service packs. Rollback procedures must be in place before any migration occurs, in case the new version proves to be unstable.

- **Configuration management**: Appropriate change management is predicated on thorough configuration management, including complete documentation of what the system looks like before and after any change (i.e., recording

**META Trend**: As ad hoc electronic communication grows in importance (e.g., e-mail, instant messaging, Web conferencing), organizations will be challenged to create a hygienic and low-cost infrastructure, with special attention through 2005 focused on spam blocking, policy enforcement (e.g., archiving, regulatory compliance), and relevancy (e.g., knowledge management). Through 2007, rising electronic communication volumes will frustrate users coping with information overload. IT groups, struggling to manage resource consumption, will accelerate server consolidation and use of centralized topologies to reduce e-mail and instant messaging costs and risk.
the “last known good environment”). All system changes must be tracked and maintained; this is essential for proper change management procedures (e.g., rollback), asset management, and disaster recovery.

- **Asset management:** Economic conditions since 2001 have led many organizations to scrutinize the cost of e-mail systems. Most organizations have focused on a snapshot in time for system economics. Asset management suggests a longer-term, structured approach to e-mail economics, encompassing maintenance agreements, license management, depreciation cycles, personnel levels, and utility tracking. An ongoing and thorough approach to e-mail asset management enables accurate change modeling exercises to determine, for example, when it is economically attractive to eliminate a local e-mail server in favor of remote user access to e-mail.

- **Systems monitoring:** Many organizations are still in reactive mode when e-mail systems go down, due to reliance on only the native monitoring services of the overall e-mail infrastructure. These tools typically examine only vendor-specific functions and not the end-to-end performance (e.g., response-time measurement) and health of the e-mail system. We recommend investment in specialized life-cycle operational management tools that do a significantly better job of proactive and reactive management (e.g., establishing thresholds, reporting, alerting, exception handling, overall component monitoring). The total systems monitoring solution should include tools that address all system components (e.g., client performance, SMTP servers, mailbox servers). Optimally, we believe tools should be integrated into an enterprise console; at the least, they should pass events to the console via SNMP.

- **Capacity management:** The dynamic nature of e-mail systems mandates careful consideration regarding system capacity management (e.g., planning, demand/capacity forecasting). Currently, all components of the mail infrastructure are suffering from increased loads. To maximize performance, administrators must have a good understanding of usage patterns and peak-load metrics to determine the appropriate time for resource upgrades or configuration changes. Spam, for example, now accounts for more than 50% of inbound traffic at most organizations and stresses existing relay infrastructures. In organizations where user storage is left unrestricted, mailbox sizes are routinely creeping up to the 1GB level. Overtaxed system components are more likely to fail.

- **Disaster recovery:** Many organizations are ill-prepared for large-scale e-mail system outages, and lack even appropriate backup/recovery scenarios for systemwide failures. Even fewer enterprises have off-site resources to protect system availability in the event of catastrophic failure. Organizations must perform the appropriate economic modeling to determine the warranted level of investment in disaster recovery services. Given the increased business reliance on e-mail, we believe it is increasingly likely that enterprises will determine that significant disaster recovery investments are in order.

Data center management of e-mail operations is often more difficult compared to other applications, given the battery of complex moving parts. These include multiple clients (e.g., rich clients, browser access, mobile clients), message stores, message transfer agents, mobile servers, application servers, directories, Internet gateways, and hygiene/policy servers. Unfortunately, e-mail management vendors often take a parochial view of managing e-mail. Most vendors offer fixed-function services (e.g., monitoring, spam blocking, content blocking) and have not yet addressed data center needs. Conversely, startup suppliers for the data center market such as Relicore, Troux, and Collation do not offer services for e-mail systems.

Monitoring console vendors sometimes offer acceptable e-mail monitoring plug-ins (from BMC, HP, IBM, and CA), but these vendors have not branched out into other e-mail system data center disciplines. As an exception, the e-mail system disaster recovery market is a source of innovation, with new suppliers such as Evergreen Assurance and MessageOne entering the market. We believe this dearth of appropriate tools will create new opportunities for new and established vendors. In the meantime, however, enterprises must make do with existing tools, craft custom services, or handle some duties manually to bring data center rigor to e-mail operations. Organizations should also treat the newer collaboration technology (e.g., instant messaging, Web conferencing), which will surely become mission-critical, with data center disciplines upon the first introduction of the technology.

**Bottom Line**

**Organizations must apply data center discipline to e-mail systems to maximize uptime and efficiency. Yet a dearth of appropriate tools means enterprises must adapt existing automation tools and create manual processes to execute certain duties.**

**Business Impact:** E-mail has proven to be the most critical communications infrastructure operated by organizations. Utmost measures must be taken to ensure continued uptime and maximize system efficiency.
Figure 1 — Other Crucial E-Mail Disciplines

**Network Management**
As e-mail systems become increasingly centralized, dependency on WAN infrastructure is growing. Companies must add appropriate bandwidth, monitoring, and redundancy to WAN infrastructures to ensure adequate e-mail performance and reliability.

**Storage Management**
E-mail is a tremendous consumer of storage resources, with increasing need for fast restores and archival services. User demand and consumption of storage must be monitored closely, and compliance and records management personnel must be consulted to plan for archival needs. Appropriate tape rotation and purging cycles must align with legal guidance for e-mail retention schedules.

**Hygiene and Security**
E-mail brings with it unique hygiene and security needs, including spam and viruses, denial-of-service attacks, and unencrypted sensitive messages sent over the Internet. Every e-mail management strategy must focus resources on perimeter management to deliver adequate protection against these threats.

Source: META Group

---

Figure 2 — E-Mail Availability/Downtime Calculations

Calculations of e-mail availability are as follows:

<table>
<thead>
<tr>
<th>Availability</th>
<th>Total Accumulated Outage per Year</th>
<th>Class (# of 9s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>90%</td>
<td>More than a month</td>
<td>1</td>
</tr>
<tr>
<td>99%</td>
<td>Just under 4 days</td>
<td>2</td>
</tr>
<tr>
<td>99.9%</td>
<td>Just under 9 hours</td>
<td>3</td>
</tr>
<tr>
<td>99.99%</td>
<td>About an hour</td>
<td>4</td>
</tr>
<tr>
<td>99.999%</td>
<td>A little over 5 minutes</td>
<td>5</td>
</tr>
<tr>
<td>99.9999%</td>
<td>About half a minute</td>
<td>6</td>
</tr>
<tr>
<td>99.99999%</td>
<td>About 3 seconds</td>
<td>7</td>
</tr>
</tbody>
</table>

Source: META Group