

Managing Government E-mail

A Technology and Management Challenge



By Michael Esolda
President NJ GMIS (New Jersey Chapter
Government Management Information Sciences)
and Chief Information Officer Woodbridge
Township/Woodbridge Township School District

E-mail. There is too much of it. Today, e-mail is the lubricant of organizational business. And, because it's so easy to use, it presents risks if not properly managed. There are technological, records retention, records disclosure and legal risks that municipalities face, and too few organizations have systems in place to assess or manage these risks. This article looks at those risks and suggests actions local officials can take to mitigate them.

Each of the four risks presents its own challenges and requires the attention of government managers. Fully mitigating them can be challenging, potentially costly, and time consuming. Why? The technology and laws are not in sync with each other and the tools to manage them are trying to catch up with the risks. That's what makes managing e-mail daunting. Let's examine each risk.

Technology E-mail service can be delivered in several ways: using Internet based, online services. These are usually free services such as G-mail*, Yahoo, or MSN (Microsoft) mail. They have the name of the hosting company as the "domain name", i.e., MytownClerk@gmail.com. These services are highly reliable—with thousands of users, vendors have a major stake in keeping the service secure, spam free, searchable and working with minimal downtime. Similarly, private e-mail hosting services, where the domain name is that of the municipality—clerk@mytown.gov are a good alternative, but may pose a little more risk, depending on the size and sophistication of the vendor. Alternatively, the municipality can support and maintain its own e-mail servers and domain name. This is most common in larger municipalities when there are many individuals using e-mail. Here the risk is with the municipality's investment in technology and people to manage it. Is there enough investment in each?

Technology risk is also related to the remaining risks—read on.

Records Retention Is e-mail a public record? Generally, yes. E-mail is just another form of record - like paper. What makes e-mail a specific record is its content! The nature of the content tells what kind of record it is, which then leads to how long the record (e-mail) must be retained.

For example, DARM guidance breaks e-mail into several types of records and retention requirements. First is “Non-Record E-mail,” consisting of personal correspondence, spam, listserv messages, non-governmental publications. These records have no retention value, and can be deleted when they are no longer useful to the recipient.

The next category is “Official Record E-mail;” those meeting the definition of a public record in N.J.S.A. 47:3-16, and three subcategories. “Transient documents,” are those with limited administrative value, such as meeting notices. They can be retained until no longer of administrative value and then destroyed.

“Intermediate documents,” are those with some administrative value, such as non-policy-related general correspondence, internal communications, or meeting notes. These records are generally retained for three years, but, depending on circumstances can be retained longer. See the DARM schedules in the link below for specifics.

Finally, “permanent documents,” can be executive correspondence of agency heads, departmental policies, and board and commission minutes. These are generally permanent in nature.

The DARM website at www.njarchives.org/links/electronic.html has links to a State directive on e-mail retention policies. The page at www.njarchives.org/links/retention.html has information on all retention requirements. Spending some time exploring these DARM resources is time well spent.

Records Disclosure This risk is otherwise known as Open Public Records Act (OPRA) compliance. To respond to an OPRA records request, personnel may have to search e-mail, regardless of how they are stored for relevant messages or documents. If agencies lack e-mail policies and useable search and storage technologies, OPRA compliance can become very time-consuming and expensive, and agencies can run the risk of failing to meet the legal requirements. Having policies and practices for storing e-mail are important, and local officials need to look at how their e-mail system is managed to guide them in meeting retention needs.

Legal Compliance, otherwise known as complying with federal and state “e-discovery” rules lurk below the surface as a risk facing all municipalities. E-discovery is federal and state court rules that describe how and how fast government agencies must respond when they are sued to protect electronically stored material from deletion and to produce it for their adversaries. The rules present legal risks if they are not followed.

Under the rules, municipalities must be prepared to stop deleting e-mails, keep new ones, and find all stored e-mails related to the matter under litigation. E-discovery also presents a technological risk—that of the software tools to assist in meeting the discovery needs. Sophisticated indexing and archiving software applications exist, but they are primarily targeted at larger, more sophisticated computer systems. Lack of software, however, is not an excuse when legal deadlines must be met. Thus, agencies need to consider their e-mail management solutions to address e-discovery.

Managing the Risks As with all matters concerning records, the real challenge is providing users useful tools, so e-mail records (and any electronic record for that matter) can be found when needed. Solutions are needed to identify e-mail that needs to be retained, the retention period, and the ability to find it. Retention risk collides with technology risk because today’s e-mail technology only provides a few good tools to assist users to easily define the category of their e-mails and provide convenient ways to find it.

A good, basic starting point is training users to delete transient e-mail, and copying intermediate records to e-mail and document storage files that replicate an “old fashioned” file folder and file cabinet system is a good starting point. It adds “friction” to the process, as it slows users down and forces them to make decisions about individual e-mails. But, “retaining as you go” can be a useful, practical and low cost approach.

A solution for those who maintain their own e-mail systems can be archiving practices (which can involve copying e-mails to PDF files) to copy everything on a server (less items users may delete) on a regular basis. Alternatively, some agencies simply keep “everything” for years. Both of these last two solutions rely on “search” technology to retrieve documents. They are a range of search products on the market (including some built into internet based e-mail services). Both solutions have their own costs and management challenges.

One commonly made mistake to avoid: using system backups as an archive. Computer backups of e-mail are intended and designed to restore systems when they fail. They are not designed for long-term storage and retrieval of stored information. Relying on backups for e-mail storage usually leads to surprise when users find the backup only covers weeks or days, because it’s intended to restore a system that fails. Using backup technology as an e-mail archive is setting up the system for records retention, disclosure, and e-discovery failure.

Even more challenging however, can be using Internet based public and private services, where the agency does not have access to archiving or recovery software, and relying only upon search technology. These systems provide the greatest risk, unless the system has sufficient storage to save years and gigabytes of information. With some experts estimating that average users can receive as much as 14 megabytes a day or almost 300 megabytes a month, a large amount of storage is required.

A solution for large systems is dedicated and sophisticated archiving and search solutions. These systems have been developing rapidly since the advent of e-discovery and corporate requirements for e-mail retention have increased, and are now being marketed to governments. Designed for large, server based systems, they can be pricey. They can be set to index, secure and retain e-mails and have powerful search and reporting capabilities.

Smaller organizations that rely on third parties for hosting e-mail or managing their servers can also look to their local board of education for e-mail support. Many school systems possess a high level of technological sophistication. In many cases, contracting with a board of education as a shared service may produce cost savings and efficiency improvements. And if not a local board of education, a neighboring municipality, a local authority or county government may be able to help. When it comes to shared services the Department Community Affairs’ SHARE program may be able to support feasibility study or implementation costs.

At the end of the day, each municipality has to make its own decisions to manage its e-mail. That decision will be based on the size of the organization, the e-mail technology it uses, the technical capabilities of the organization or its contractors, and the tools that meet the circumstances. Success will depend on having a good set of tools and sound policies, training users to use them, and ensuring that they do.

One way an organization can help ensure its e-mail management works is providing the technology staff with resources. A valuable resource is the staff of other organizations. New Jersey has a resource that helps bring technology managers together. That resource is NJ-GMIS, the Association of New Jersey Government Technology Managers. By joining NJ-GMIS, municipal technology managers can contact their peers not only in New Jersey, but across the country, as membership in the New Jersey Chapter comes from membership in GMIS International, with members across the country and the world. Information on GMIS International and the New Jersey chapter is available at www.gmis.org and www.njgmis.org.

* G-mail is a free e-mail service provided by Google