Managing E-mail Overload

Grego Kosinski shows how to turn a menace into an opportunity

E-mail is now the dominant force for information exchange in most organizations. It has supplanted the telephone, fax machine, copier, and even the once-critical overnight express delivery. Even the most sensitive information and records are commonly moving through organizations via e-mail. Why? It's easy to send from a multitude of devices and clients; it's fast; it provides an auditable communication trail; and it's inexpensive. E-mail transcends international and organization boundaries. Thus, e-mail is now a mission-critical application, vital to almost every business' operations.

As good as e-mail is, its proliferation has created a number of problems. If it's down, productivity is halted. And the sheer number of e-mails and the size of e-mail attachments, which continue to grow exponentially, have their own impact. End users face mailbox overload. Information Technology (IT) teams struggle to maintain availability and application performance while containing costs. And, compliance and legal departments are often overwhelmed with concerns of meeting internal and external regulations, as well as the legal ramifications of eDiscovery requests. Although the information overload generated by e-mail means something different to each group of stakeholders, all need an effective and comprehensive e-mail management strategy to achieve their business objectives.

Impact on end-users

End users view e-mail as the key to communication, planning, collaboration, decision making, and knowledge sharing—and thus productivity. End users live in their inboxes. A recent AIIM study (Industry Watch: "Email Management: The Good, The Bad and The Ugly"*) found that the average information worker spends 1.5 hours per day processing e-mails—and 1 of 5 spend more than 3 hours. With such a considerable part of the workday dedicated to e-mail, end users simply have no time to waste.

End users demand a lot from their e-mail applications. They want to use familiar, easy-to-use interfaces that don't hinder their ability to manage and classify information in their inboxes. The increasingly distributed workforce also requires immediate access to e-mail from a multitude of devices (laptops, Blackberries, iPhones, etc.) and locations. Even if they're offsite or offline, their demands don't change.

End users don't want to be bothered with the mechanics of how messages are being archived. They want to be able to retain and reuse content such as contracts, invoices, and Microsoft Office docu-

© AIIM 2009, www.aiim.org/research

ments for future purposes. But, they also want to easily search and retrieve their messages with transparent access to the archive—and they want to do it all without wasting time.

And when end users are provided with a less-than-ideal solution, they manage to come up with ways to circumvent any limitations placed on their e-mail use. When faced with an intervention measure such as mailbox quotas, end users might simply delete messages "en masse" to gain space, or even create personal archives (PST/NSF) on their own hard drives. Unfortunately, these tactics can lead to greater storage costs, the inadvertent deletion of critical business records or the inaccessibility of information needed by the entire organization.

Impact on IT

IT is responsible for managing e-mail throughout the enterprise—across multiple geographies, languages, and platforms – while ensuring that end user expectations are met. With the mission-critical nature of e-mail, IT is expected to ensure uninterrupted application performance and recover quickly from outages—an extremely difficult challenge.

From the IT perspective, e-mail's greatest impact is on storage and data protection. Runaway e-mail volume can quickly overtake expensive primary storage—IT must find ways to keep e-mail storage costs under control. Simply purchasing more and more storage ad infinitum is not a viable option.

Storage is a primary concern, but IT must also ensure the security of the information it manages, and protect the privacy of employees, customers, and others. IT is also expected to back up massive amounts of data and deliver the shortest possible recovery windows. At the same time, IT must keep the growth of the e-mail archive from negatively affecting business operations or further stressing budgets.

Although it is a less expensive option, retaining e-mail on backup tapes for archiving purposes is a losing strategy, particularly when the team is called upon to respond to discovery requests. Tapes are susceptible to physical damage over time and messages on tape are difficult to index, lengthening search time. Legal actions may look back many years. Yet, an IT team with little legal expertise is expected to produce a complete set of e-mail records without delay. Reliance on tape backup to fill the need for an archive is not the best way to maximize efficiency.

Impact on legal and compliance

Like IT, compliance and legal departments face many critical responsibilities that are impacted by e-mail overload, though the challenges are different. To avoid fines and unfavorable legal outcomes, these teams must be able to determine the business value of each message, and know that e-mails will be deleted or retained based on their value. They demand that e-mail be properly classified so it can be found in the future for regulatory compliance, corporate policy mandates, or eDiscovery. A disparate scattering of e-mail is therefore unacceptable.

To minimize the risk of noncompliance with internal and external policies, regulations, and laws, compliance and legal must maintain a unique perspective of e-mail. Beyond being able to find messages, they must be able to prove message authenticity and chain of custody. They need the flexibility to apply both time- and event-based retention policies—consistently.

Of course, the costs of not preserving control over e-mail can be much higher for these departments, especially for the legal team. Many organizations find it necessary to turn to outsourcing each time a legal matter occurs. Thus, time wasted on searching through irrelevant e-mail can quickly add up to exorbitant costs (especially over time). A decision made by IT to store older messages on backup tapes can come back to haunt the organization that must spend even more to find e-mail needed for the case at hand.

Turning challenges into opportunities

E-mail overload impacts numerous stakeholders (end users, IT, and compliance/legal representatives) that need to save time, reduce capital expenses, and minimize risk. And these are the same groups that need to come together to create an e-mail policy that not only meets their individual needs, but ultimately drives significant benefits for the entire company.

Using these challenges to bring stakeholders together is the first step. The second step is the creation of an information governance plan—a proactive, policy-driven information management strategy. This strategy should ensure that information, particularly e-mail, is managed according to business value and policy. The third step is to find a technology solution that addresses your organization's pain points today, while being flexible enough to address future requirements.

The right unified information governance strategy, coupled with the right technology solutions, enables organizations to be better prepared for tomorrow, while addressing individual needs today:

- End users can use the interfaces they're comfortable with (whether online or off) to maintain control over their mailboxes and access the information they need to be efficient and productive, eliminating the need to create renegade PST or NSF archives.
- IT can improve performance and lower costs for production systems, backup and disaster recovery. They can reduce the size of the production storage environment by proactively deleting non-business critical information or moving e-mail that meets certain business rules to lower-cost tiers.
- Compliance and legal can ensure that a legally sound and repeatable process is in place to protect the company's reputation, avoid fines and penalties, and ensure that eDiscovery is not a recurring expense.

By bringing these three different viewpoints together under an information governance strategy, organizations can improve business operations, gain a greater return on investment, and assume a competitive advantage. ■

Grego Kosinski, Director, EMC

For more information about how EMC products, solutions and services can help your organization address e-mail and information overload, visit www.EMC.com/SourceOne.