

How Does Email Serve Your Association?

By Jeanne L. Allert

Reprinted from *Executive Update, Special Technology Section Feature*

September 2003 ~ All rights reserved

During 17 years of working with nonprofits and technology, I have yet to encounter an organization that hesitated to implement e-mail, waiting until it had a clear business strategy before putting this powerful tool to use. In most cases, the "switch was flipped" without much preparation or training, and it's almost an anomaly to find an organization not using e-mail. Overall, the massive and nearly immediate access to e-mail hasn't been a bad thing. On economic merits, e-mail is a powerful tool. Add to that the ability to reach millions of persons around the globe — almost instantaneously — and you see why many call e-mail "the killer app."

But using e-mail means accepting the upside along with the downside. In some ways associations are still in the wave of the upside, not wholly affected by the undercurrent of this tool's potential negative consequences. There have certainly been incidences that give us some insight into the risks. Most organizations probably have a story like the CFO who inadvertently sent payroll numbers to "all staff" in an e-mail blunder. Or the employee who was terminated for running a football pool online. Or the manager who criticizes the association's policy and somehow that e-mail gets routed outside of the organization — and maybe even into the hands of the media. Even the innocuous but nonetheless annoying employee who thinks we all want to see pictures of his dog.

The misuse of e-mail can produce significant risk. According to Gartner Inc., "As e-mail moves from personal correspondence to valuable business information, analysts ... predict that e-mail overload will hurt productivity, more lawsuits will include subpoenaed e-mails, and the market for products to fight unwanted e-mail will begin to consolidate."

Some organizations are questioning whether unbridled access to e-mail is a good thing. More than likely, you already run some kind of e-mail virus checker. You've

probably received e-mail from an attorney that has a 12-line disclaimer as the signature. Maybe your organization requires staff to sign a letter of understanding that e-mail is to be used for business purposes only and is the property of the organization. "The major danger [with e-mail] comes from viruses, but in addition, there are the less obvious problems of wasted bandwidth consumption, spam, and legal liability," says Steve Bachman, U.S. president for Marshal Software. Little light bulbs of concern are beginning to illuminate the landscape of risk and exposure.

The Need for E-mail Strategy

What's called for — before the panic pendulum swings too far — is a thoughtful and reasonable e-mail strategy. Over the past three years, many organizations have begun to articulate a strategic definition and direction for their Web efforts. It's interesting that you can find fully staffed Web departments or interdepartmental steering committees for the Web (a tool that usually only a select group of staff can affect), but it is rare to find an organization that has an e-mail management department (for a tool that virtually everyone can manipulate).

Formulating an e-mail strategy should be on the task list for every leadership team. But although most senior executives have a sense that unbridled e-mail could lead to certain exposure, loss, or risk for their organizations, reining in their current culture, user patterns, and management systems seems too daunting. But the tangled mess you perceive now will only get worse unless you raise the importance of this dialogue within your organization.

We can begin to untangle the situation by looking at the fundamental flow of e-mail within an organization. Most simply put, e-mail comes in (incoming communications); e-mail goes out (outgoing communications); and e-mail circulates within your organization (internal communications). That flow is supported by the platform, tools, and internal practices of the organization itself (infrastructure issues).

These four "issue buckets" can help you think through the considerations unique to your organization and also develop a reasonable sense of what you can actually control. Apply the following set of questions to each of these aspects of e-mail activity:

- What are the risks? What could possibly happen?
- What is your exposure? What would be the negative consequence to the organization?
- What assets do you need to protect?
- What controls will support your desired practice?

Let's take a look at each phase of e-mail in light of these guiding questions.

Incoming Communications

These are the e-mails sent by someone outside your organization to someone within your organization. Once you have opened up your organization to e-mail, there is only so much control you can exert on the actions of others who are outside of your organization.

As we look purely at the flow of e-mail traffic that comes into the organization, the risks fall generally under the category of "compromise to staff or infrastructure." That is, your strategy should be to protect your staff from e-mail that is undesirable, inappropriate, or solicitous. This is where you have to carefully think through various content-filtering options. This also means protecting your infrastructure from e-mail that contains elements such as viruses that could be harmful to your IT infrastructure. Some organizations also need to protect their infrastructure from elements that they cannot support, such as media files or attachments exceeding a particular size. You may incur unnecessary expense or hardship as a result of letting unwanted e-mail in.

It's important to think through all the implications of restricting incoming e-mail. You may inadvertently be shutting out mail that is actually desirable. In a recent personal example, my correspondence with an association manager was filtered out as spam (undesirable, often solicitous, e-mail) because, buried in the text of my message, I had the word "free." This is where some organizations are now putting exceptions over exceptions by implementing "white lists" to exempt desirable mail from filters.

Your e-mail strategy should not be solely based on preventing hazards or misconduct, though. It also should include provisions for encouraging the proper use of e-mail as a business tool. For incoming e-mail, that means establishing clear paths for how e-mail is processed once received and ensuring that member inquiries are routed properly and that reasonable service levels are established and maintained. This is where you will debate how to use such tools as auto-responders, how

you will track the nature of the e-mails for business intelligence, and how you will ensure high responsiveness.

Internal Communications

It may seem like you have no risk with — and no control over — e-mail that is circulated by and among staff. Not so. Proportionately, more e-mail is generated within the enterprise, and this poses some risk to your organization.

For collegial e-mail, your e-mail strategy should address (at least) these two aspects: using e-mail to facilitate the business of the organization; and preventing compromise to the organization, staff, or IT infrastructure.

It should not be a foregone conclusion that staff members know how to use e-mail to facilitate their work. Training in specific skills to increase efficiency (such as setting up e-mail groups or linking with calendars) should be a part of your e-mail strategy. Likewise, pay attention to how e-mail affects the culture of your organization. More organizations are offering instruction in e-mail protocol and etiquette. This education should also inform staff of various legal implications, such as privacy of e-mail communications or the right of the organization to perform "search and seizure" on an employee's e-mail account or the penalties for using business e-mail for nonbusiness purposes.

Perhaps one of the greater underestimated risks of internal mail is the sheer amount of IT resources it consumes. If staff don't delete old or unnecessary e-mail, you may soon be putting servers where you once housed filing cabinets. Your e-mail strategy should include operational policies for archiving and disposing of e-mail.

Outgoing Communications

Outgoing communications are those e-mails generated from within your organization to some external audience. Some of the considerations noted for internal e-mail also apply to your practices for outgoing mail, particularly in protocol and etiquette. The most significant risks in outgoing communications fall under the heading of "protecting the recipients and protecting the organization."

Here you grapple with the challenging task of list management. This includes your tactics for acquiring e-mail addresses for your various markets, keeping those

lists current and accurate, providing for opt-in and opt-out policies, determining who has access to those lists and for what purpose, and other considerations. If you are in a more complex environment, this also may include setting up user profiles so recipients can select the mode or format of the information they receive. This aspect also includes the controls you set on what e-mail is sent out from your organization, to whom, and at what interval. More organizations are centralizing outgoing e-mail to members for fear that they may be "stuffing the inboxes" of their members, thereby compromising the impact of messages. You can implement software solutions to control e-mail distribution or can govern the activity through internal policies and approvals.

Protecting the organization means being a careful steward of your brand and your message. One of the significant risks to organizations in an open e-mail environment is that your carefully crafted position or message can now be readily manipulated, propagated, misdirected, and misused. An inflammatory, critical, or contrary message disseminated internally can easily find its way outside and into the wrong hands. Less potent, but nonetheless troublesome, can be the risk that staff may give less attention to composing e-mail, and your outgoing, public correspondence is fraught with errors, slang, and colloquialisms. Quality consistency also is a reflection on your brand and should be key in your internal staff education program. At present, there aren't technology solutions that can ensure that your outgoing correspondence is well crafted, articulate, and consistent with your positions. You are going to have to rely on human systems for that.

Infrastructure Issues

Perhaps the area where you have the greatest control is on the tools you use, such as the platform used and how e-mail is managed, stored, archived, and deleted, for example. Your e-mail strategy should assess what your e-mail usage patterns and trends have been and also contain your projections for growth in usage over the next two or more years. The choices you make about IT upgrades should be supported by what you understand about your e-mail use. Likewise, related IT initiatives, such as rolling out a content management system (CMS) or customer relationship management (CRM) system should link back to your e-mail strategy. Will your systems upgrade give staff the ability to access your member e-mail lists? What policies and controls need to be put into place?

The protections to your internal infrastructure deal mostly with ensuring that your hardware and software resources are being used efficiently and that you have the tools needed to support the work of your organization.

This aspect of your strategy spells out the technical structure of your e-mail flow. It includes your automated and manual systems for monitoring and reporting on e-mail activity, as well as your thresholds for e-mail storage and consumption. It includes your plan for disaster recovery and technical support.

Your internal capabilities also may include creating standards for your most frequent communications. A communications audit should be performed within your organization at least every two years. You should know what's being created and sent from all departments; you may choose to build into your strategy the development of hard-coded templates for these communications products. Even a simple gesture such as standardizing the e-mail signature line for your staff can go a long way to presenting your communications as polished.

Getting Started

To get started in the development of your own e-mail strategy, first understand your communications landscape: What are your current communications products — both those which are formalized within your organization and also those that have evolved since e-mail became an option? You need to have a grasp of the e-mail patterns within your organization and among the market segments with which you interact. Make sure you can isolate your assets and your potential risks. Start with where you are, then begin to look outward to the kind of e-mail user you want your organization to be. It's important to set goals for how this tool will be used in your organization: to facilitate its work, serve members, mobilize your audience, persuade, educate, sell, and inform, for example. Use the model of the four e-mail "buckets" and the guiding questions to isolate the concerns unique to your organization. These should help you focus your energy and resources, respecting what you can and cannot control.

Much of this examination of an e-mail strategy has to do with implementing prudent controls and practices to ensure that your organization does not suffer a negative consequence from the "downside" of e-mail. Those safeguards are important. So too are the elements of your strategy that set forth preferred practice, optimal use of resources, and guidelines for being a "good" user of e-mail. The incredible power, expanse, and economy of e-mail should be met with a similarly significant attention to harnessing this tool to your organization's best advantage.